Secret Sharing Schemes Based on Error-Correcting Codes

Dissertation

der Mathematisch-Naturwissenschaftlichen Fakultät
der Eberhard Karls Universität Tübingen
zur Erlangung des Grades eines
Doktors der Naturwissenschaften
(Dr. rer. nat.)

vorgelegt von
Claudia Kässer
aus Hildesheim

Tübingen
2016

Gedruckt mit Genehmigung der Mathematisch-Naturwissenschaftlichen Fakultät der Eberhard Karls Universität Tübingen

Tag der mündlichen Qualifikation:	03.06.2016
Dekan:	Prof. Dr. Wolfgang Rosenstiel
1. Berichterstatter:	Prof. Dr. Peter Hauck
2. Berichterstatter:	Jun. Doz. Dr. Britta Dorn

Für Bernhard und Niklas

Abstract

In this thesis we present a new secret sharing scheme based on binary error-correcting codes, which can realize arbitrary (monotone or non-monotone) access structures.

In this secret sharing scheme the secret is a codeword in a binary error-correcting code and the shares are binary words of the same length. When a group of participants wants to reconstruct the secret, the participants calculate the sum of their shares and apply Hamming decoding to that sum. The shares have the property that, when the group is authorized, the secret is the codeword which is closest to the sum of the shares. Otherwise, the sum differs strongly enough from the secret such that Hamming decoding yields another codeword.

The shares can be described by the solutions of a system of linear equations which is closely related to first order Reed-Muller codes. We consider the case that there are only two different Hamming distances from the sums of the shares to the secret: one small distance k for the authorized sets and one large distance g for unauthorized sets. For this case a method of how to find suitable shares for arbitrary access structures is presented.

In the resulting secret sharing scheme large code lengths are needed and the security distance g is rather small. In order to find classes of access structures which have more efficient and secure realizations, we classify the access structures such that all access structures of one class allow the same parameters g and k. Furthermore we study several changes in the access structure and their impact on the possible realizations.

This gives rise to special classes of access structures defined by veto sets and necessary sets, which are particularly suitable for our approach.

Zusammenfassung

In dieser Arbeit stellen wir ein neues Secret Sharing Scheme basierend auf fehlerkorrigierenden Codes vor, mit dem beliebige (also auch nicht monotone) Zugriffsstrukturen realisiert werden können.

Das Geheimnis ist ein Codewort in einem binären fehlerkorrigierenden Code und die Teilgeheimnisse sind binäre Wörter derselben Länge. Wenn Teilnehmer das Geheimnis rekonstruieren wollen, bilden sie die Summe ihrer Teilgeheimnisse und wenden Hamming-Decodierung auf das Ergebnis an. Die Teilgeheimnisse sind derart beschaffen, dass für alle zulässigen Konstellationen das Geheimnis das nächstgelegene Codewort ist. Andernfalls ist der Abstand der Summe zum Geheimnis so groß, dass Hamming-Decodierung ein anderes Codewort liefert.

Die Teilgeheimnisse können durch Lösungen eines linearen Gleichungssystems beschrieben werden, welches in engem Zusammenhang zu Reed-Muller Codes erster Ordnung steht. Wir betrachten den Fall, dass es nur zwei verschiedene Hamming-Abstände von den Summen der Teilgeheimnisse zum Geheimnis gibt: ein kleiner Abstand k für die zulässigen Konstellationen und ein großer Abstand g für die unzulässigen. Für diesen Fall stellen wir eine Methode zur Erstellung passender Teilgeheimnisse vor.

Die Codelängen im resultierenden Secret Sharing Scheme sind jedoch sehr groß und die Sicherheitsabstände g sind eher klein. Um Klassen von Zugriffsstrukturen zu finden, die effizientere und sicherere Realisierungen zulassen, klassifizieren wir alle Zugriffsstrukturen, so dass alle Zugriffsstrukturen in einer Klasse dieselben Parameter g und k erlauben. Außerdem untersuchen wir die Auswirkung einiger Änderungen an der Zugriffsstruktur auf die möglichen Parameter.

Spezielle Klassen von Zugriffsstrukturen, die über Vetomengen und notwendige Mengen definiert sind, erweisen sich als besonders geeignet für unseren Ansatz.

Danksagung

An erster Stelle danke ich meinem Doktorvater Herr Prof. Dr. Peter Hauck sehr herzlich für die Überlassung dieses interessanten Themas und für die hervorragende Betreuung meiner Arbeit. Er war mir stets ein verlässlicher und kompetenter Ansprechpartner.

Frau Jun. Doz. Dr. Britta Dorn danke ich herzlich für die Erstellung des Zweitgutachtens und die hilfreichen Tipps.

Desweiteren bedanke ich mich bei meinen Kollegen für die angenehme Arbeitsatmosphäre und die freundschaftliche Zusammenarbeit. Vor allem bei Dr. Michael Beiter bedanke ich mich für die erhellenden fachlichen Diskussionen zu Beginn meiner Arbeit.

Ganz besonders danke ich meiner Familie, vor allem meinem Partner Jan Loderhose, für die Geduld und die Unterstützung, die diese Arbeit erst ermöglicht haben.

Contents

Chapter 1

Introduction

1.1 Sharing Secrets

The security of many protocols for digital transactions is based on the secrecy of some sensitive data. These "secrets" can be, for example, passwords or private keys in a public-key cryptosystem, which are used for digital signatures.

There are situations, where a secret has to be provided to a group of users, which are, viewed individually, not entirely trustworthy. Only certain groups of participants, which are considered as trustworthy, should have access to the secret. Furthermore, when storing highly sensitive data it might be advisable to split it up into pieces and store these pieces in different locations. The single pieces should provide as little as possible information about the data and only if a minimum number of pieces is combined, the original data should be recovered. This increases the required effort for an attacker significantly.

In both cases the use of a secret sharing scheme can be helpful. As the name suggests, a secret sharing scheme is a method of sharing a secret among a set of participants. For a given secret the so-called *dealer* calculates suitable shares and distributes them to the participants. The shares shall have the property that only certain predefined subsets of participants are able to reconstruct the secret from their shares. These subsets are called *authorized* and the set of all authorized subsets is called *access structure*. The remaining subsets are called *unauthorized*. They should learn as little as possible about the secret from their shares.

Secret Sharing Schemes were introduced independently by Shamir [35] and Blakely [7] in 1979. Both schemes are designed to realize so-called *threshold access structures*, where all sets of participants are authorized if and only if their cardinalities reach a predefined threshold. In 1991 Simmons et al. proposed a secret sharing scheme which can be used to realize all *monotone* access structures ([27]). In these access structures all supersets of authorized sets are also authorized. For further reading on monotone secret sharing we recommend the surveys [36] and [3].

It depends strongly on the access structure if there exists a suitable secret sharing scheme to realize it. Almost all secret sharing schemes are limited to special types of access structures, especially to monotone access structures.

However, there are many scenarios that require more general access structures and it is worth developing secret sharing schemes to realize them. Suppose, for example, that the participant set consists of two disjoint sets $\mathcal{A}$ and $\mathcal{B}$ and that the reconstruction of the secret should be possible if and only if at least as many participants from $\mathcal{A}$ as from $\mathcal{B}$ are involved. This access structure is non-monotone: Consider an authorized set $A \cup B$, $A \in \mathcal{A}$, $B \in \mathcal{B}$. That means $|A| \geq |B|$. When we add more than $|A| - |B|$ participants from group $\mathcal{B}$, the resulting set is unauthorized since it contains more participants from $\mathcal{B}$ than from $\mathcal{A}$.

Another example of non-monotone access structures are those, where certain participants have veto power. That means there is a set V of participants, such that all sets B with $B \cap V \neq \varnothing$ are unauthorized. This access structure is non-monotone since for all authorized sets A and all participants $v \in V$ the superset $A \cup \{v\}$ is unauthorized.

By now very little is yet known about secret sharing schemes realizing *arbitrary* access structures. The only exception is a secret sharing scheme presented by Schulze [34]. He proposed a linear geometric construction to realize arbitrary access structures. However, depending on the access structure, linear spaces of very large dimensions are needed.

In this work we present a new secret sharing scheme based on error-correcting codes that realizes all kinds of access structures.

1.2 Our Approach towards Secret Sharing

Consider the following secret sharing scheme on the participant set $\mathcal{T} = \{T_1, \ldots, T_t\}$. The secret as well as the shares are binary words of the same length n and the recovery of the secret is done by adding the shares in the vector space $\mathbb{Z}_2^n$. Then, for example, the access structure $\Gamma = \{A \subseteq \mathcal{T} : T_j \in A\}$ for a fixed j can be realized easily by assigning the secret s as share to the participant T_j and the zero word of length n to each of the other participants. When a group of participants tries to reconstruct the secret they add their words and receive s if T_j takes part in the reconstruction. Otherwise they receive the zero word and learn nothing about the secret. The security and efficiency of this secret sharing scheme can hardly be topped, but the example is unrealistic as actually no secret sharing scheme is needed. Furthermore, most access structures have no realizations like that. For example $\Gamma = \{A \subseteq \mathcal{T} : |A| = 1\}$ cannot be realized with this method if there are three or more participants: Each participant needs to receive the secret as a share and therefore each set with an odd number of participants gains the secret.

We improve this concept by sharing *codewords* of an error-correcting code $\mathcal{C} \subseteq \mathbb{Z}_2^n$. Thus we can allow the sums of shares of the authorized sets to differ a little bit from the secret. Using a decoding algorithm this error can be corrected if it does not exceed the error-correction capability of the code $\mathcal{C}$ and the authorized sets receive the secret codeword s. That means, when a group of participants is authorized, we want the secret to be the codeword which is closest to the sum such that Hamming decoding yields the secret. Otherwise, when the participants are unauthorized, we want the sum of their shares to differ strongly enough from the secret such that Hamming decoding outputs another codeword.

1.3 Outline of this Thesis

This work is organized as follows.

In Chapter 2 we give an overview of the fundamentals of secret sharing schemes. We start with the formal definition of secret sharing schemes and introduce the terms perfectness and rate. Then we present two well known secret sharing schemes which realize threshold structures and general monotone access structures. Furthermore, we describe Schulze's secret sharing scheme which realizes arbitrary access structures. Finally, we have a look at management models of secret sharing schemes which include another trusted entity, the combiner.

Chapter 3 summarizes the fundamentals of error-correcting codes. This includes terms like the error-correction and detection capability, the minimum distance and the covering radius of a code. Furthermore we deal with the weight distribution of a code and its dual code and their connection given by the MacWilliams identity. Finally, we present four important families of codes where we focus on Reed-Muller codes, which play an important role in this work.

In Chapter 4 we present our new approach towards secret sharing based on error-correcting codes. We start with an overview of the current state of research. Then we turn to our approach and develop a method of how to find suitable shares for all kinds of access structures. For this purpose the structure of the shares is extensively studied. We restrict ourselves to the case that the share sums of all authorized sets have the same distance k to the secret and that all sums of the unauthorized sets have the distance g. It turns out that large code lengths are required and that the distance g is rather small.

The rest of this work deals with the search for access structures which allow more favorable parameters.

Chapter 5 is about the classification of access structures such that all access structures in the same class allow the same parameters b_1, g, k, where b_1 is the weight of the secret. Provided that there is one access structure with favorable parameters, this gives us the possibility to identify a whole class of access structures with these parameters. We also present a refinement of this classification such that all access structures in the same refined class also have the same suitable codes.

In Chapter 6 we present several techniques of how to construct new access structures from already given access structure and study their impact on the possible parameters b_1, g, k and the suitable codes. These techniques are the transition from an access structure to its dual access structure (which consists of the unauthorized sets), the embedding of access structures into larger participant sets, the symmetric difference of an access structure with an unauthorized set, the intersection of access structures and the removal of one authorized set.

In Chapter 7 we use the results of Chapter 5 and 6 to identify special classes of access structures which allow very good parameters. On the one hand these are access structures related to Reed-Muller codes. On the other hand certain access structures defined by veto sets and necessary sets have favorable parameters.

Chapter 8 summarizes the results of the previous chapters and gives a brief outlook on possible further work.

Chapter 2

Basic Concepts of Secret Sharing

In this chapter we give an overview of the basic concepts of secret sharing. We introduce the basic definitions and methods and describe the most commonly known secret sharing schemes. Furthermore, we describe Schulze's scheme which realizes arbitrary access structures. We start with the formal definition of secret sharing schemes in terms of distribution functions as Stinson proposed in [37].

2.1 Basic Definitions

Definition 2.1. Let $\mathcal{T} = \{T_1, \ldots, T_t\}$ be a set of participants. The subsets of $\mathcal{T}$ which should be able to recreate the secret from their shares are called *authorized*. The other subsets are called *unauthorized*. The set Γ of all authorized subsets is called *access structure*.

According to our definition *any* subset of $\mathcal{P}(\mathcal{T})$ is an access structure. However, there are types of access structures which appear to be more natural than others and have been widely studied. The most prominent types are the following.

Definition 2.2. (a) An access structure of the form $\Gamma = \{A \subseteq \mathcal{T} : |A| \geq \alpha\}$ is called $(|\mathcal{T}|, \alpha)$-*threshold structure* with *threshold* α.

(b) An access structure with the property that for all $A \in \Gamma$ any superset $B \supseteq A$ is also authorized is called *monotone*. Otherwise we call the access structure *non-monotone*.

It is easy to see that threshold structures are monotone. For a monotone access structure Γ let

$$\Gamma_{\min} = \{U \subseteq \mathcal{T} : U \in \Gamma \text{ and } V \notin \Gamma \text{ for all } V \subset U\}$$

be the set of all *minimal authorized sets* and

$$\overline{\Gamma}_{\max} = \{U \subseteq \mathcal{T} : U \notin \Gamma \text{ and } U \not\subset V \text{ for all } V \subseteq \mathcal{T}, V \notin \Gamma\}$$

be the set of all *maximal unauthorized sets* with respect to Γ. $\Gamma_{\min}$ and $\overline{\Gamma}_{\max}$ uniquely characterize the monotone access structure Γ.

Definition 2.3. A *secret sharing scheme* on a participant set $\mathcal{T}$ which realizes the access structure Γ is a 6-tupel $(\mathcal{T}, \Gamma, \mathcal{S}, \mathcal{K}, \mathcal{F}, r)$ with the following components:

(a) $\mathcal{T} = \{T_1, \ldots, T_t\}$ is a non-empty participant set.

(b) Γ is an access structure on the participant set $\mathcal{T}$.

(c) $\mathcal{S}$ is the set of all possible secrets that can be shared with the scheme.

(d) $\mathcal{K}$ denotes the set of all possible shares.

(e) $\mathcal{F} = \bigcup_{s \in \mathcal{S}} \mathcal{F}_s$ is the set of the *distribution functions.* For each secret $s \in \mathcal{S}$ each distribution function $f_s \in \mathcal{F}_s$ assigns appropriate shares k_j to the participants T_j.

$$\begin{aligned} f_s : \mathcal{T} &\rightarrow \mathcal{K} \\ T_j &\mapsto k_j \qquad \text{for all } j = 1, \ldots, t \end{aligned}$$

(f) r is the *recovery function.* For each set of shares r outputs the secret s if the shares come from a distribution function for s and if the related group of participants is authorized. Otherwise r outputs a definitely different value $s' \in \mathcal{S}$, $s' \neq s$, or a random element of $\mathcal{S}$. This depends on the concrete realization of the secret sharing scheme.

$$\begin{aligned} r : \mathcal{P}(\mathcal{K}) &\rightarrow \mathcal{S} \\ \{k_{j_1}, \ldots, k_{j_\ell}\} &\mapsto \begin{cases} s \text{ if } \{k_{j_1}, \ldots, k_{j_\ell}\} = f_s\left(\{T_{j_1}, \ldots, T_{j_\ell}\}\right) \\ \quad \text{with } \{T_{j_1}, \ldots, T_{j_\ell}\} \in \Gamma, \\ \\ s' \text{ otherwise.} \end{cases} \end{aligned}$$

We use the term “function” in a general sense as random choices are involved.

The computation of the shares and their distribution to the participants are performed by a trusted entity, the so-called *dealer.*

All components of a secret sharing scheme are public. The security of the scheme depends on the structure of the shares. They have to be constructed in a way that the shares of each unauthorized subset provide little to no information about the secret. So-called *perfect* secret sharing schemes provide maximum security.

Definition 2.4. A secret sharing scheme $(\mathcal{T}, \Gamma, \mathcal{S}, \mathcal{K}, \mathcal{F}, r)$ is called *perfect* if for all secrets $s \in \mathcal{S}$ and all distribution functions $f_s \in \mathcal{F}_s$ the following equation holds:

$$p\left(s \middle| \{k_{j_1}, \ldots, k_{j_\ell}\}\right) = p(s)$$

for all $\{k_{j_1},\dots,k_{j_\ell}\} = f_s\left(\{T_{j_1},\dots,T_{j_\ell}\}\right)$ with $\{T_{j_1},\dots,T_{j_\ell}\} \notin \Gamma$,
where $p(s)$ is the probability of guessing the secret s and $p\left(s|\,\{k_{j_1},\dots,k_{j_\ell}\}\right)$ is the conditional probability of guessing the secret s when the shares $k_{j_1},\dots,k_{j_\ell}$ are known.

That means, in a perfect secret sharing scheme the shares of each unauthorized set of participants yield no further information about the secret. For this reason only monotone access structures can be realized by perfect secret sharing schemes: If there is an unauthorized set B containing an authorized set A, the participants from B get to know the secret from the shares of A.

Next we consider the *information rate*, which is a measure for the efficiency of a secret sharing scheme.

Definition 2.5. For each participant T_j, $j = 1,\dots,t$, let $\mathcal{K}_j = \{f(T_j) : f \in \mathcal{F}\} = \bigcup\limits_{s\in\mathcal{S}} \{f_s(T_j) : f_s \in \mathcal{F}_s\}$ be the set of all possible shares for all possible secrets that he might receive from a distribution function. Define

$$q_j = \frac{\log_2(|\mathcal{S}|)}{\log_2(|\mathcal{K}_j|)}.$$

Then

$$q = \min\{q_j : 1 \leq q \leq t\}$$

is called *information rate* of the scheme.

Since there are $|\mathcal{S}|$ secrets, each secret can be represented by a binary word with length $\log_2(|\mathcal{S}|)$ and one can say that each secret contains $\log_2(|\mathcal{S}|)$ bits of information. In the same way each share of the participant T_j contains $\log_2(|\mathcal{K}_j|)$ bits of information. That means q_j is the ratio of the information contents of an arbitrary secret and an arbitrary share of participant T_j.

A high information rate is desirable as it means an efficient distribution of the information of each secret on the corresponding shares. In [37] Stinson shows that each perfect secret sharing scheme realizing a monotone access structure has an information rate $q \leq 1$. This motivates the following definition.

Definition 2.6. A perfect secret sharing scheme with information rate $q = 1$ is called *ideal.*

If, for example, a secret sharing scheme is perfect and each element of $\mathbb{Z}_p$ can be chosen as a secret and as a share, we have

$$q = q_j = \frac{\log_2(p)}{\log_2(p)} = 1$$

and the secret sharing scheme is ideal. In the non-perfect case larger information rates are possible. For example, consider the following t-threshold scheme on the participant set $\{T_1,\dots,T_t\}$. Let $\mathcal{S} = \mathbb{Z}_p^t$ be the secret set. Suppose that each participant

T_j receives the jth component of the secret. Then $\mathcal{K} = \mathbb{Z}_p$. The scheme is not perfect, since the knowledge of each component restricts the search for the secret. The information rate is $q = \frac{\log_2(p^t)}{\log_2(p)} = t \geq 1$.

2.2 Secret Sharing Schemes Realizing Special Access Structures

In this section we present two very well-known secret sharing schemes realizing threshold structures and (general) monotone access structures. An overview of secret sharing schemes using error-correcting codes is given in Chapter 4.

2.2.1 Shamir's Threshold Scheme

In [35] Shamir presents a perfect secret sharing scheme which can realize all threshold structures. It is based on the fact that one needs at least α data points to interpolate a polynomial of degree $\alpha - 1$. Shamir's scheme has the following components.

(a) $\mathcal{T} = \{T_1, \ldots, T_t\}$

(b) $\Gamma = \Gamma_\alpha$ is a $(|\mathcal{T}|, \alpha)$-threshold structure with an arbitrary threshold $1 \leq \alpha \leq t$.

(c) $\mathcal{S} = \mathbb{Z}_p$, p prime, is the set of all possible secrets. p is a security parameter. When p increases it becomes more and more unlikely to guess the right secret.

(d) The share set is $\mathcal{K} = \mathbb{Z}_p \setminus \{0\} \times \mathbb{Z}_p$.

(e) In order to distribute a secret $s \in \mathbb{Z}_p$ according to the access structure Γ_α the dealer chooses randomly a polynomial $f \in \mathbb{Z}_p[x]$ of degree $\alpha - 1$ with $f(0) = s$ and pairwise disjoint values $x_1, \ldots, x_t \in \mathbb{Z}_p \setminus \{0\}$. Then he assigns the shares $k_j = (x_j, f(x_j))$ via the distribution function

$$\begin{array}{rcl} f_s : \mathcal{T} & \rightarrow & \mathcal{K} \\ T_j & \mapsto & (x_j, f(x_j)) \end{array}$$

to the participants.

(f) When some participants $T_{j_1}, \ldots, T_{j_\ell}$ want to recover the secret they apply an interpolation algorithm on their data points, for example Lagrange interpolation. They determine a polynomial g of degree at most $\ell - 1$. If $\ell \geq \alpha$ the participants receive $g = f$ and are able to determine $s = f(0)$. Otherwise $g \neq f$ and no information about $f(0)$ is provided. The recovery function is given by

$$\begin{array}{rcl} r : \mathcal{P}(\mathcal{K}) & \rightarrow & \mathcal{S} \\ \{k_{j_1}, \ldots, k_{j_\ell}\} & \mapsto & g(0), \end{array}$$

where $g \in \mathbb{Z}_p[x]$ is the result of an polynomial interpolation algorithm with input $(x_{j_1}, f(x_{j_1})), \ldots, (x_{j_\ell}, f(x_{j_\ell}))$.

Since the shares of any unauthorized set provide no information about s, Shamir's scheme is perfect. Additionally, when we always use the same x-values $x_1, \ldots, x_t$, for example $x_j = j$ for all $j = 1, \ldots, t$, we have $\mathcal{K} = \mathbb{Z}_p = \mathcal{S}$ and the scheme is ideal.

2.2.2 Simmons' Linear Secret Sharing Scheme

In [27] Simmons et al. propose a linear algebraic secret sharing scheme which can realize all monotone access structures. The shares as well as the secret s are points in a projective space. s is the intersection point of a publicly known line L and a secret subspace U. The participants receive elements of U such that only the authorized sets are able to generate U and to determine s.

(a) $\mathcal{T} = \{T_1, \ldots, T_t\}$

(b) Γ is an arbitrary monotone access structure on $\mathcal{T}$ with $\left|\overline{\Gamma}_{\max}\right| = n$.

(c) The secret set $\mathcal{S}$ is a 1-dimensional subspace L of a projective space $\mathbb{P}$ of dimension n.

(d) The set $\mathcal{K}$ of all possible shares is given by $\mathcal{P}(\mathbb{P})$. Each share consists of a set of points in the projective space $\mathbb{P}$. The empty set can also be a share.

(e) Let $\overline{\Gamma}_{\max} = \{U_1, \ldots, U_n\}$. In order to distribute a secret $s \in L$ according to Γ the dealer chooses randomly a $(n-1)$-dimensional projective subspace U of $\mathbb{P}$ such that the secret is the intersection point of U and the secret set L. He determines a basis $\mathcal{B} = \{b_1, \ldots, b_n\}$ of U such that $b_1, \ldots, b_n$ and s are in general position. Now the dealer distributes the shares using the distribution function

$$\begin{aligned} f_s : \mathcal{T} &\to \mathcal{K} \\ T_j &\mapsto \{b_i \in \mathcal{B} : T_j \notin U_i\}\,. \end{aligned}$$

(f) When a set T of participants wants to recover the secret they join their points $b_{i_1}, \ldots, b_{i_\ell}$ and determine the projective subspace $A := \langle b_{i_1}, \ldots, b_{i_\ell} \rangle$. Since Γ is monotone we know that T is unauthorized iff $T \subseteq U_i$ for an $1 \leq i \leq n$. In this case the basis element b_i is missing in the shares of all participants of T. $\dim(A) \leq n-1$ and $A \cap L = \varnothing$ since $b_1, \ldots, b_n$ and s are in general position. When T is authorized, then $T \nsubseteq U_i$ for all $i = 1, \ldots, n$ and each b_i must be distributed to one or more participants of T. Hence $A = U$ and $A \cap L$ gives the secret. The recovery "function" is given by

$$\begin{array}{rcl} r : \mathcal{P}(\mathcal{K}) & \to & \mathcal{S} \\ \{k_{j_1}, \ldots, k_{j_\ell}\} & \mapsto & \begin{cases} \text{the unique element of } \langle \bigcup\limits_{m=1}^{\ell} k_{j_m} \rangle \cap L & \text{if } \langle \bigcup\limits_{m=1}^{\ell} k_{j_m} \rangle \cap L \neq \varnothing \\ \text{a random element of } L & \text{else.} \end{cases} \end{array}$$

Simmon's scheme is perfect, since the shares of the unauthorized sets provide no further information about the secret. But it is not ideal because the shares may consist of more than one element of $\mathbb{P}$.

2.3 Schulze's Scheme Realizing Arbitrary Access Structures

Schulze's scheme described in [34] is inspired by Simmon's scheme. It is based on the following idea. Let Γ be an access structure with the authorized sets $A_1, \ldots, A_n$. For each authorized set $A_i = \left\{T_{k_{1,i}}, \ldots, T_{k_{\ell_i,i}}\right\}$ the set $\{A_i\}$ can be considered as a monotone access structure on the participant set $\left\{T_{k_{1,i}}, \ldots, T_{k_{\ell_i,i}}\right\}$ with the only authorized set A_i and with $\overline{\{A_i\}}_{\max} = \{A \subseteq A_i : |A| = \ell_i - 1\}$ and $|\overline{\{A_i\}}_{\max}| = \ell_i$. Hence it can be realized with Simmon's scheme using a ℓ_i-dimensional projective space $\mathbb{P}_i$. These realizations of the single $\{A_i\}$ are merged into one realization of Γ by choosing the $\mathbb{P}_i$ to be independent subspaces of a larger projective space $\mathbb{P}$. For this purpose, each secret needs to have a representative in each of the $\mathbb{P}_i$.

Schulze's scheme is perfect. But unfortunately, the dimension of $\mathbb{P}$ increases with the number of the authorized sets and the number of participants within these sets. Schulze's scheme has the following components.

(a) $\mathcal{T} = \{T_1, \ldots, T_t\}$ is the participant set.

(b) $\Gamma = \{A_1, \ldots, A_n\}$ is an arbitrary access structure on $\mathcal{T}$ containing the authorized sets $A_1, \ldots, A_n \in \mathcal{P}(\mathcal{T})$. For $i = 1, \ldots, n$ let $\ell_i = |A_i|$.

(c) In a projective space $\mathbb{P}$ of dimension $d = n - 1 + \sum\limits_{i=1}^{n} \ell_i$ the dealer chooses n linearly independent subspaces $\mathbb{P}_1, \ldots, \mathbb{P}_n$ and in each subspace $\mathbb{P}_i$ he chooses a one-dimensional subspace L_i. Each secret is represented by a certain element of each L_i, where all L_i represent the same set of secrets. That means each secret s has n representatives $s_1, \ldots, s_n$ with $s_i \in L_i$ for all $i = 1, \ldots, n$. W.l.o.g one can say that the secret set is $\mathcal{S} = L_1$ since all L_i have the same cardinalities.

(d) The set $\mathcal{K}$ of all possible shares is given by $\mathcal{P}(\mathbb{P}) \setminus \{\varnothing\}$. Each share consists of a non-empty set of points in the projective space $\mathbb{P}$.

(e) Let s be the secret to be shared. Then s has a representative s_i in each L_i. In each $\mathbb{P}_i$ the dealer chooses randomly a $(\ell_i - 1)$-dimensional projective subspace U_i such that the representative s_i is the intersection point of U_i and L_i. For each authorized set $A_i = \left\{T_{k_{1,i}}, \dots, T_{k_{\ell_i,i}}\right\}$ he chooses ℓ_i elements $u_{k_{1,i}}, \dots, u_{k_{\ell_i,i}}$ of U_i which generate U_i, such that these elements and s_i are in general position within U_i. Finally, he determines a basis $\mathcal{B}_i$ of $\mathbb{P}_i$ for all $i = 1, \dots, n$. Now the dealer distributes the shares using the distribution function

$$\begin{aligned} f_s : \mathcal{T} &\rightarrow \mathcal{K} \\ T_j &\mapsto \bigcup_{i:T_j \in A_i} \{u_{j,i}\} \cup \bigcup_{i:T_j \notin A_i} \mathcal{B}_i. \end{aligned}$$

(f) When a set T of participants wants to recover the secret they determine the subspace B which is generated by all their elements. Then all sections $B \cap L_i$ are considered Since the $\mathbb{P}_i$ are linearly independent, these sections can be studied separately. We have

$$B \cap L_i = \begin{cases} U_i \cap L_i = \{s_i\} & \text{if } T = A_i \\ \varnothing & \text{if } T \subsetneq A_i \\ \mathbb{P}_i \cap L_i = L_i & \text{if } T \neq A_i, T \not\subset A_i \end{cases}.$$

When T is authorized, there is exactly one section $B \cap \Gamma_i$ which consists of one element s_i. This element represents the secret s. Otherwise, when T is unauthorized, the participants do not learn anything about the secret from their shares and can only guess a representative for the secret. Hence Schulze's scheme is perfect.

The recovery "function" is given by

$$\begin{aligned} r : \mathcal{P}(\mathcal{K}) &\rightarrow \mathcal{S} \\ \{k_{j_1}, \dots, k_{j_\ell}\} &\mapsto \begin{cases} \text{the element of } \mathcal{S} \text{ represented by the unique element of} \\ \langle \bigcup_{m=1}^{\ell} k_{j_m} \rangle \cap L_i \text{ if } \langle \bigcup_{m=1}^{\ell} k_{j_m} \rangle \cap L_i \notin \{\varnothing, L_i\} \\ \text{the element of } \mathcal{S} \text{ represented by a random element of } L_i \\ \text{ if } \langle \bigcup_{m=1}^{\ell} k_{j_m} \rangle \cap L_i \in \{\varnothing, L_i\} \text{ for all } i = 1, \dots, n \end{cases}. \end{aligned}$$

2.4 Management Models

In this section we have a closer look at the parties involved in a secret sharing scheme and their connections to each other. In the classical management model the lifetime of a secret sharing scheme consists of two phases:

1. Initially, the dealer chooses a secret $s \in \mathcal{S}$ that he wants to share according to Γ. Then he distributes suitable shares $k_1, \ldots, k_t$ among the participants $T_1, \ldots, T_t$ using a distribution function $f_s \in \mathcal{F}_s$. This phase is called *sharing phase.*

2. In the so called *recovery phase* a group $\{T_{j_1}, \ldots, T_{j_\ell}\}$ of participants pool their shares $k_{j_1}, \ldots, k_{j_\ell}$ together and calculate $r\left(\{k_{j_1}, \ldots, k_{j_\ell}\}\right)$.

In this model the recovery is public in the sense that all involved shares and, if the participants are authorized, also the secret become public to all attending participants. Therefore the scheme can be used only for one time. But there is an even more serious problem.

Consider a non-monotone access structure Γ and an authorized set $A \in \Gamma$ such that there is an unauthorized superset $B \supset A$. When the participants of B try to recover the secret using all their shares, they fail. But since all members of B want to know the secret and the risk of being caught is very low, it is very likely that they will agree on the following. Only the participants from A reconstruct the secret and the remaining members of B watch that process and learn the secret, too. This can be avoided by introducing another trusted party: the *combiner*. A combiner driven management model works as follows.

1. In the sharing phase the dealer chooses a secret $s \in \mathcal{S}$. Then he calculates suitable shares $k_1, \ldots, k_t$ as in the classical model, but keeps them secret. For each $j = 1, \ldots, t$ the participant T_j receives a *concealed* share k'_j instead of k_j, such that the original share k_j can be recovered from k'_j when some additional information c is known (for example c is a set of keys of a symmetric encryption system and k'_j is the encryption of k_j using one of these keys). The dealer sends the additional information c to the combiner. All transmissions are performed via secure channels.

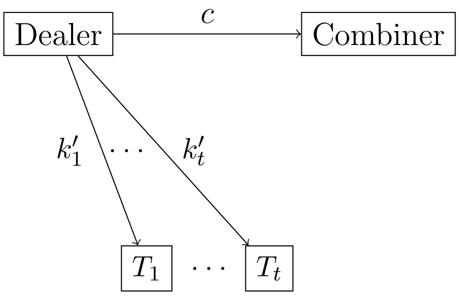


Figure 2.1: Sharing phase in a combiner driven model

2. In the recovery phase a group $\{T_{j_1}, \ldots, T_{j_\ell}\}$ of participants send their concealed shares $k'_{j_1}, \ldots, k'_{j_\ell}$ via a secure channel to the combiner. Using his additional information c he recovers the original shares $k_{j_1}, \ldots, k_{j_\ell}$. Then he calculates $r\left(\{k_{j_1}, \ldots, k_{j_\ell}\}\right)$ and sends the result via a secure channel to the device which carries out the desired action if it receives the secret.

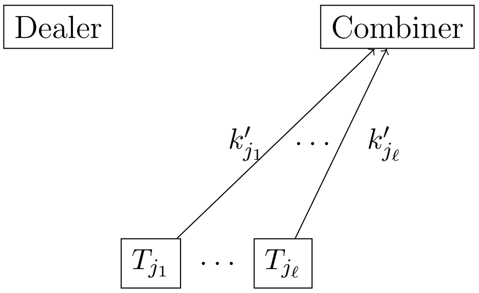


Figure 2.2: Recreation phase part 1 in a combiner driven model

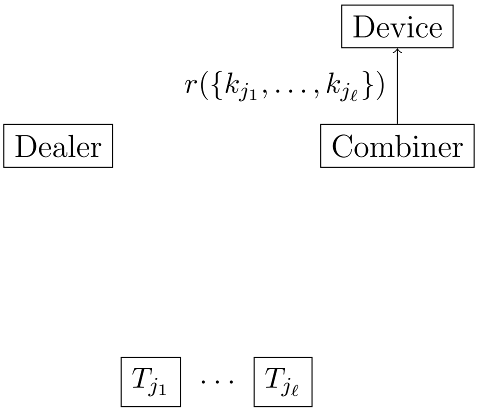


Figure 2.3: Recreation phase part 2 in a combiner driven model

In a combiner driven model the participants do not know the original shares. Furthermore they do not learn the secret, even if they are authorized. Hence the secret sharing scheme can be used for several times with the same secret and the same shares. In addition to that the participants have no longer the possibility to make their own arrangements during the recovery phase.

Chapter 3

Error-Correcting Codes (ECC)

This chapter provides basic knowledge about coding theory which is fundamental for this thesis. We present the basic definitions and concepts and describe some families of codes which play a role in the following chapters. A more detailed introduction into coding theory can be found for example in [5],[43] and [21].

3.1 Basic Definitions and Concepts

The aim of coding is to modify data in a way, such that random errors, that occur during the transmission, can be detected or even corrected. For this purpose redundancy is added to the original data which makes the data more "distinguishable" from each other. This makes it is easier to find out *if* errors have occurred or even *which* errors these were and to restore the original data.

In our context data are words over a given alphabet. The modified data words are called *codewords* and are words over the same alphabet. The set of all these codewords is called *code* and the transition from the original word to the codeword is called *encoding*. In this work we consider only so called block codes, where all codewords have the same length.

Definition 3.1. Let A be a finite set (an alphabet) and $n \in \mathbb{N}$. Then each subset $\mathcal{C}$ of $A^n = \underbrace{A \times \ldots \times A}_{n}$ is a *(block) code* with *length n*. The elements of $\mathcal{C}$ are called *codewords*. In the case $A = \mathbb{Z}_2$ the code $\mathcal{C}$ is a *binary (block) code*.

Example 3.2. Consider the alphabet $A = \mathbb{Z}_2$ and the binary block code

$$\begin{aligned} \mathcal{C} &= \{(0,0,0,0),(0,0,1,1),(0,1,0,1),(0,1,1,0), \\ &\qquad (1,0,0,1),(1,0,1,0),(1,1,0,0),(1,1,1,1)\} \subseteq A^4. \end{aligned}$$

The codewords come from the eight data words $(0,0,0)$, $(0,0,1)$, $(0,1,0)$, $(0,1,1)$, $(1,0,0)$, $(1,0,1)$, $(1,1,0)$, $(1,1,1) \in A^3$ which are encoded by adding the following redundancy bits

$$\begin{array}{ll} (0,0,0) \to (0,0,0,0) & (1,0,0) \to (1,0,0,1) \\ (0,0,1) \to (0,0,1,1) & (1,0,1) \to (1,0,1,0) \\ (0,1,0) \to (0,1,0,1) & (1,1,0) \to (1,1,0,0) \\ (0,1,1) \to (0,1,1,0) & (1,1,1) \to (1,1,1,1). \end{array}$$

$\mathcal{C}$ is a so-called *parity check code* where the original words are encoded by adding a *parity check bit*, such that each codeword has an even number of ones.

In the following we use the term "code" instead of "block code". Now we specify how words can be distinguish from each other.

Definition 3.3. Let A be a finite alphabet and $n \in \mathbb{N}$.

(a) Consider two words $a = (a_1, \dots, a_n)$, $b = (b_1, \dots, b_n) \in A^n$. The number

$$d(a,b) := \# \{i : 1 \le i \le n,\ a_i \ne b_i\}$$

is called *Hamming distance* of a and b.

(b) Let $\mathcal{C} \subseteq A^n$ be an arbitrary code. Then

$$d(\mathcal{C}) = \min \{d(a,b) : a, b \in \mathcal{C}, a \ne b\}$$

is the *minimum distance* of $\mathcal{C}$.

Example 3.4. The codewords of the binary code

$$\begin{aligned} \mathcal{C} \ = \ \{&\underbrace{(0,0,0,0)}_{a}, \underbrace{(0,0,1,1)}_{b}, \underbrace{(0,1,0,1)}_{c}, \underbrace{(0,1,1,0)}_{d}, \\ &\underbrace{(1,0,0,1)}_{e}, \underbrace{(1,0,1,0)}_{f}, \underbrace{(1,1,0,0)}_{g}, \underbrace{(1,1,1,1)}_{h}\}. \end{aligned}$$

from Example 3.2. have the Hamming distances

d	a	b	c	d	e	f	g	h
a	0	2	2	2	2	2	2	4
b	2	0	2	2	2	2	4	2
c	2	2	0	2	2	4	2	2
d	2	2	2	0	4	2	2	2
e	2	2	2	4	0	2	2	2
f	2	2	4	2	2	0	2	2
g	2	4	2	2	2	2	0	2
h	4	2	2	2	2	2	2	0

and the minimum distance is $d(\mathcal{C}) = 2$. In contrast to that there are original words (for example $(0, 0, 1)$ and $(0, 1, 1)$) that differ only in one position. Hence the encoding enlarged the distance between the words.

Now suppose that a codeword c is sent over a channel and the word x is received. The receiver knows that a codeword was sent and when x is a codeword, he assumes that x is the correct codeword. Otherwise he knows that errors have occurred. Depending on the application he than has the possibility to request the codeword c again or has to deduce the sent codeword c from x. The process of assigning a codeword to a received word is called *decoding*.

Definition 3.5. The following decoding algorithm is called *Hamming decoding*. Let $\mathcal{C} \subseteq A^n$ be an arbitrary code. Suppose that a codeword has been sent and the word $x \in A^n$ is received. Then Hamming decoding outputs an arbitrary codeword $c \in \mathcal{C}$ with the property

$$d(c, x) = \min_{c' \in \mathcal{C}} d(c', x).$$

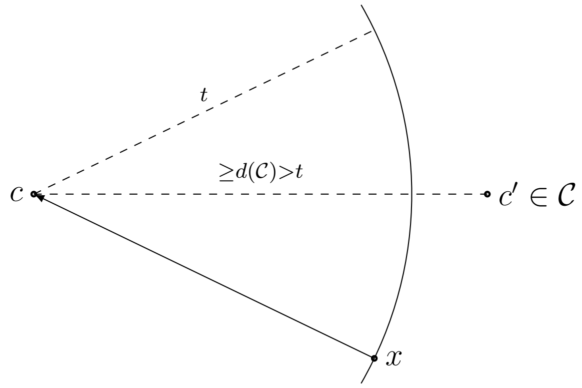
That means Hamming decoding yields one of the codewords which are closest to the received word with respect to the Hamming distance.

Example 3.6. Consider the code $\mathcal{C}$ from Example 3.2. When the word $x = (1, 0, 0, 0) \in \mathbb{Z}_2^4$ is received, Hamming decoding outputs one of the data words $(0, 0, 0)$, $(1, 0, 0)$, $(1, 0, 1)$ and $(1, 1, 0)$ since the related codewords have a Hamming distance of 1 to x.

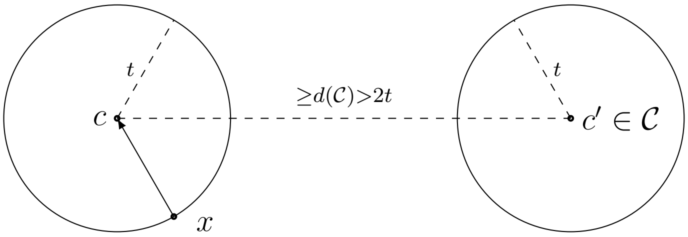
Next we study the impact of the minimum distance of a code on its error-detection and error-correction capability when Hamming decoding is used.

Definition and Remark 3.7. When a codeword $c \in \mathcal{C} \subseteq A^n$ is sent and the word $x \in A^n$ with $d(c, x) = t$ is received, we know that t errors have occurred during transmission. Whether these errors can be detected or even corrected depends on the minimum distance of the code $\mathcal{C}$ in the following way.

- Let $d(\mathcal{C}) \geq t + 1$. Then x cannot be a codeword of $\mathcal{C}$ and we know that errors have occurred. $\mathcal{C}$ is called a *t-error-detecting code*.



- Let $d(\mathcal{C}) \geq 2t+1$. Then c is the codeword lying next to x and Hamming decoding yields the correct codeword. $\mathcal{C}$ is called a *t-error-correcting code*.



That means $\mathcal{C}$ can correct up to $\left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor$ errors, regardless of which codeword was sent and on which positions the errors occurred. That is why $\left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor$ is called *error-correction capability* of $\mathcal{C}$. Nevertheless, there may be codewords and positions such that Hamming decoding still yields the right codeword when more than $\left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor$ errors occur.

Example 3.8. (a) The binary code $\mathcal{C}$ from Example 3.2 has minimum distance $d = 2$ and is a 1-error-detecting and 0-error-correcting code.

(b) In contrast to that the binary code

$$\mathcal{C} \;=\; \{(0,0,0,0,0,0),(0,1,0,1,0,1),(1,0,1,0,1,0),(1,1,1,1,1,1)\}$$

has minimum distance $d(\mathcal{C}) = 3$ and is a 2-error-detecting and 1-error-correcting code. But when the codeword $c = (0,0,0,0,0,0)$ is sent and $x = (1,1,0,0,0,0)$ is received, 2 errors have occurred and Hamming decoding yields nevertheless the sent codeword c.

We now introduce another important parameter of a code: the *covering radius*. It describes the Hamming distance from the code to the furthest word outside the code.

Definition 3.9. Let K be a finite field, $n \in \mathbb{N}$ and $\mathcal{C} \subseteq K^n$ a code. The smallest $r \in \mathbb{N}_0$ with the property that for all words $x \in K^n$ there is a codeword $c \in \mathcal{C}$ with $\mathrm{d}(x,c) \leq r$ is called *covering radius* $\rho(\mathcal{C})$ of $\mathcal{C}$.

That means $\rho(\mathcal{C})$ is the smallest radius r such that the balls with radius r centered in the codewords cover the whole space A^n. It follows directly from the definitions that

$$\rho(\mathcal{C}) \geq \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor .$$

Further details about the covering radius can be found in [15].

Example 3.10. The parity check code from Example 3.2 has covering radius $\rho(\mathcal{C}) = 1$: Let $x = (x_1, x_2, x_3, x_4) \in \mathbb{Z}_2^4$ be arbitrary. Then x or $x' = (x_1, x_2, x_3, x_4 + 1)$ have an even number of ones and belong to $\mathcal{C}$. Therefore the Hamming distance of x to the code is one or zero.

The most frequently used codes are so-called linear codes.

Definition 3.11. Let K be a finite field, $n \in \mathbb{N}$ and $\mathcal{C} \subseteq K^n$ a code. Suppose that $\mathcal{C}$ is a linear subspace of K^n. Then $\mathcal{C}$ is called a *linear code.* Let k be the dimension of $\mathcal{C}$. Then $\mathcal{C}$ is called a $[n,k]$-code or a $[n,k,d(\mathcal{C})]$-code. If K has q elements we also say that $\mathcal{C}$ is a $[n,k,d(\mathcal{C})]_q$-code and for $q = 2$ the code is called a *binary* $[n,k,d(\mathcal{C})]$-code.

Example 3.12. Let $u = (1,1,0,0,0), v = (0,1,1,0,0) \in \mathbb{Z}_2^5$. The linear subspace

$$\mathcal{C} = \langle u, v\rangle_{\mathbb{Z}_2} = \{0, u, v, u+v\} = \{(0,0,0,0,0),(1,1,0,0,0),(0,1,1,0,0),(1,0,1,0,0)\}$$

is a binary $[5,2,2]$-code.

Using a linear code it is very easy to encode the data words or to find out, whether a received word is a codeword or not.

Definition and Remark 3.13. Let $\mathcal{C}$ be a linear $[n,k]$-code over K.

(a) Let $b_1,\dots,b_k$ be a basis of $\mathcal{C}$ and $G = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{pmatrix}$ be the $(k \times n)$-matrix whose rows are these basis vectors. Then G defines an encoding of the original words in K^k by

$$x = (x_1,\dots,x_k) \mapsto x \cdot G = \sum_{i=1}^{k} x_i b_i \quad \text{for all } x \in K^k.$$

G is called a *generator matrix* of $\mathcal{C}$.

Let $c_1,\dots,c_m$ be a generator set of $\mathcal{C}$. Then $G' = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{pmatrix}$ is called *general generator matrix* of $\mathcal{C}$. It has the property $\mathcal{C} = \left\{x \cdot G' : x \in K^k\right\}$.

(b) Since $\mathcal{C}$ is a k-dimensional subspace of K^n, $\mathcal{C}$ is the kernel of a linear function $h : K^n \to K^{n-k}$. Let H be the $(n-k \times n)$-matrix with $h(x) = H \cdot x^\tau$ for all $x \in K^n$ (x^τ denotes the transposed vector of x). Then

$$H \cdot x^\tau = 0 \in K^{n-k} \;\Leftrightarrow\; x \in \mathcal{C}.$$

H is called a *check matrix* of $\mathcal{C}$.

Example 3.14. The linear code $\mathcal{C}$ from Example 3.12 has the following generator matrix G and check matrix H:

$$G = \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Definition 3.15. Let K be a finite field and $n \in \mathbb{N}$.

(a) For all $x = (x_1, \dots, x_n) \in K^n$ the number

$$\mathrm{wt}(x) = \#\{i : 1 \leq i \leq n,\ x_i \neq 0\}$$

is called *(Hamming) weight* of x.

(b) Let $\mathcal{C} \neq \{0\}$ be a code in K^n. Then

$$\min\{\mathrm{wt}(c) : c \in \mathcal{C}, c \neq 0\}$$

is called *minimum weight* of $\mathcal{C}$.

Since the Hamming distance is translation invariant, the minimum distance and the minimum weight of a code are the same when the code is linear. The minimum distance of a linear code can be read from its check matrix:

Proposition 3.16. Let $\mathcal{C}$ be a linear $[n, k]$-code over K with check matrix H. Then

$$\begin{aligned} d(\mathcal{C}) &= \min\{r \in \mathbb{N} : H \text{ has } r \text{ linearly dependent columns}\} \\ &= \max\{r \in \mathbb{N} : \text{each } r-1 \text{ columns of } H \text{ are linearly independent}\}. \end{aligned}$$

In particular that means $d \leq rk(H) + 1 = n - k + 1$. This inequality is called *Singleton bound.*

When the roles of G and H are changed, we obtain a linear $[n, n-k]$-code with generator matrix H and check matrix G, the so-called *dual* code.

Definition and Remark 3.17. Let $\mathcal{C}$ be a linear $[n, k]$-code over K with generator matrix G and check matrix H. Then

$$\mathcal{C}^{\perp} = \left\{x \cdot H : x \in K^{n-k}\right\}$$

is called the *dual* code of $\mathcal{C}$. G is a check matrix of $\mathcal{C}^{\perp}$ since

$$\begin{aligned} & y \in \mathcal{C}^{\perp} \\ \Leftrightarrow\ & y = x \cdot H \text{ for a } x \in K^{n-k} \\ \Leftrightarrow\ & y \cdot c^{\perp} = 0 \text{ for all } c \in \mathcal{C} \\ \Leftrightarrow\ & G \cdot y = 0. \end{aligned}$$

Example 3.18. The dual code $\mathcal{C}^{\perp}$ of the code $\mathcal{C}$ from Example 3.12 is generated by the check matrix H from Example 3.14. Therefore

$$\begin{aligned} \mathcal{C}^{\perp} &= \langle (1,1,1,0,0), (0,0,0,1,0), (0,0,0,0,1) \rangle_{\mathbb{Z}_2} \\ &= \{(0,0,0,0,0), (1,1,1,0,0), (0,0,0,1,0), (0,0,0,0,1) \\ &\qquad (1,1,1,1,0), (1,1,1,0,1), (0,0,0,1,1), (1,1,1,1,1)\}. \end{aligned}$$

Definition 3.19. Let $\mathcal{C}$ be a linear $[n,k]$-code over K.

(a) For all $i = 0, 1, \ldots, n$ let w_i be the number of codewords in $\mathcal{C}$ with weight i. Then the vector

$$w(\mathcal{C}) = (w_0, w_1, \ldots, w_n)$$

is called *weight distribution* $w(\mathcal{C})$.

(b) The polynomial

$$W(\mathcal{C}, x) = \sum_{i=0}^{n} w_i x^i \in \mathbb{R}[x]$$

is called *weight counter* of $\mathcal{C}$.

Example 3.20. The linear code $\mathcal{C}$ from Example 3.12 and its dual code $\mathcal{C}^\perp$ have the weight distributions

$$w(\mathcal{C}) = (1,0,3,0,0,0) \quad \text{and} \quad w(\mathcal{C}^\perp) = (1,2,1,1,2,1)$$

and the weight counters

$$W(\mathcal{C}, x) = 1 + 3x^2 \quad \text{and} \quad W(\mathcal{C}^\perp, x) = 1 + 2x + x^2 + x^3 + 2x^4 + x^5.$$

The weight counters of a linear code and its dual code have the following important relation.

Theorem 3.21 (MacWilliams Identity)**.** Let $\mathcal{C}$ be a $[n,k]_q$-code. Then

$$W(\mathcal{C}^\perp, x) = \frac{(1+(q-1)x)^n}{|\mathcal{C}|} \cdot W\left(\mathcal{C}, \frac{1-x}{1+(q-1)x}\right).$$

(For more details see [26].)

Example 3.22. In our example

$$\begin{aligned}
\frac{(1+(q-1)x)^n}{|\mathcal{C}|} \cdot W(\mathcal{C}, \frac{1-x}{1+(q-1)x}) &= \frac{(1+x)^5}{4} \cdot \left(1 + 3\left(\frac{1-x}{1+x}\right)^2\right) \\
&= \frac{(1+x)^5}{4} + \frac{3}{4}(1+x)^3(1-x)^2 \\
&= \frac{1}{4}(1 + 5x + 10x^2 + 10x^3 + 5x^4 + x^5) + \\
&\quad \frac{3}{4}(1 + x - 2x^2 - 2x^3 + x^4 + x^5) \\
&= 1 + 2x + x^2 + x^3 + 2x^4 + x^5 \\
&= W(\mathcal{C}^\perp, x).
\end{aligned}$$

3.2 Important Families of Linear Codes

In this section we present some of the best-known and frequently used families of linear codes.

3.2.1 Hamming Codes and Simplex Codes

Hamming codes were invented by Hamming in 1950. They are linear codes with minimum distance three, which can be defined over arbitrary finite fields. We describe Hamming codes by constructing their check matrices.

Let K be a finite field with q elements and $\ell \in \mathbb{N}$. The linear space K^ℓ has exactly $\frac{q^\ell-1}{q-1}$ one-dimensional subspaces (each non-zero vector generates one of these subspaces, where the $q-1$ non-zero multiples of each vector generate the same subspace). Define the code length $n = \frac{q^\ell-1}{q-1}$ and the dimension $k = n - \ell$. In order to construct a check matrix for a $[n,k]$-Hamming code we choose one generator of each one-dimensional subspaces of K^ℓ and write these generators as columns in matrix. This yields a $(\ell \times n)$-matrix H over K. In the binary case each non-zero vector generates its own one-dimensional subspace. In this case the check matrix consists of *all* non-zero vectors of $\mathbb{Z}_2^\ell$.

Example 3.23. For $q = 2$ and $\ell = 3$ we obtain $n = \frac{2^3-1}{2-1} = 7$ and $k = n - \ell = 4$.

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

is a check matrix for a $[7,4]$-Hamming code, since each one-dimensional subspaces of $\mathbb{Z}_2^3$ is represented by exactly one column.

Proposition 3.16 shows that all Hamming codes have minimum distance three. We determine $m = \min\{r \in \mathbb{N} : H \text{ has } r \text{ linearly dependent columns}\}$:

- $m \neq 1$ since there is no zero column in H.
- $m \neq 2$ since there are no two columns which are multiples of each other.
- $m = 3$ since the sum of two columns of H generates another one-dimensional subspace of K^ℓ.

$d = 3$ means that Hamming codes can detect up to $d(\mathcal{C}) - 1 = 2$ errors and correct $\left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor = 1$ error. In other words, the balls $B_1(c)$ of radius one (with respect to the Hamming distance) centered at the codewords are disjoint. Furthermore Hamming codes have the property that the union of all balls $B_1(c)$ is already the whole space K^n. Hence the error-correction capacity and the covering radius are equal. This makes Hamming codes so-called *perfect* codes.

The dual code of a $[n, k]_q = [\frac{q^\ell-1}{q-1}, \frac{q^\ell-1}{q-1} - \ell]_q$-Hamming code is called $[\frac{q^\ell-1}{q-1}, \ell]_q$-*Simplex code*. Simplex codes have the property that all non-zero codewords have the weight $q^{\ell-1}$. Hence their minimum distance is also $q^{\ell-1}$. For $q = 2$ Simplex codes have the covering radius $2^{\ell-1} - 1$.

3.2.2 Reed-Solomon Codes

Reed Solomon codes were introduced by Reed and Solomon in 1960 ([32]). These codes are linear and non-binary. They have many applications in everyday life. For example they are used for data storage on CDs, DVDs and for QR-codes.

Let K be a finite field with $q \geq 3$ elements. Choose a code length n and a minimum distance d with $1 \leq d \leq n \leq q$ and an ordered subset $M = (x_1, \dots, x_n)$ of K with pairwise different elements. Then the related Reed-Solomon code $\mathcal{C}$ is defined by

$$\mathcal{C} = \{(f(x_1), \dots, f(x_n)) : f \in K[x],\ \deg(f) \leq n - d\}\,.$$

Each word $a = (a_0, a_1, \dots, a_{n-d}) \in K^{n-d+1}$ is regarded as the polynomial $f_a(x) = a_0 + a_1 x + \ldots + a_{n-d} x^{n-d} \in K[x]$ and is encoded via

$$a \mapsto (f_a(x_1), \dots, f_a(x_n))\,.$$

Each polynomial f_a has at most $n - d$ zeros. Therefore the codewords in $\mathcal{C}$ have at least the weight d. On the other hand, the Singleton bound says $d(\mathcal{C}) \leq n - k + 1 = d$. This yields $d(\mathcal{C}) = d$. Hence $\mathcal{C}$ is a $[n, n-d+1, d]_q$-code.

Depending on the choice of M a Reed-Solomon code can have another important property. $K^* = (K \setminus \{0\}, \cdot)$ is a cyclic group and there is an element $\alpha \in K^*$ with $K^* = \{1 = \alpha^0, \alpha, \dots, \alpha^{q-2}\}$ and $\alpha^{q-1} = 1$. When we choose $M = (1, \alpha, \dots, \alpha^{q-2})$, the related Reed-Solomon code is a so-called *cyclic* code. That means the cyclic shift of any codeword yields another codeword. This property allows faster encoding and decoding algorithms. Furthermore, cyclic codes have the ability to detect burst errors with length $l \leq n - k$, where all errors lie in a segment of the message with length l.

Example 3.24. For $K = \mathbb{Z}_5$ we have $q = 5$ and define $n = q - 1 = 4$. $\alpha = 2$ generates K^* since $(\alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4,) = (x_1, x_2, x_3, x_4) = (1, 2, 4, 3)$. We choose $d = 3$. This yields the Reed-Solomon code

$$\mathcal{C} = \{(f(1), f(2), f(4), f(3)) : f \in \mathbb{Z}_5[x],\ \deg(f) \leq 1\}\,.$$

The data word $a = (2, 3) \in \mathbb{Z}_5$ represents the polynomial $2 + 3x \in \mathbb{Z}_5[x]$ and is encoded to

$$c = (2 + 3 \cdot 1, 2 + 3 \cdot 2, 2 + 3 \cdot 4, 2 + 3 \cdot 3) = (0, 3, 4, 1).$$

3.2.3 Reed-Muller Codes

Reed-Muller codes are a family of binary error-correcting linear codes. They were invented by Reed and Muller in 1954. During the Mariner expeditions 6, 7 and 9 to Mars in 1969-1972 a Reed-Muller code was used for image transmission to earth.

A Reed-Muller Code $RM(r, m)$ is characterized by two variables $r, m \in \mathbb{N}_0$ which determine its parameters. Reed-Muller codes can be defined in many ways. Two of them are the following.

Definition of $\mathbf{RM(r, m)}$ via Boolean polynomials:
A *Boolean polynomial* is a polynomial in $\mathbb{Z}_2[x_1, \ldots, x_m]$. Each Boolean polynomial function $f : \mathbb{Z}_2^m \to \mathbb{Z}_2$ is uniquely characterized by its value table

$$\begin{array}{c|cccccccccccccccccc}
x_m & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\vdots & & & & & & & & & & & & & & & & & \\
x_3 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \ldots & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
x_2 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & \ldots & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
x_1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & \ldots & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
\hline
f(x_1, \ldots, x_m) & * & * & * & * & * & * & * & * & \ldots & * & * & * & * & * & * & * & *.
\end{array}$$

The last row of the table is the vector in $\mathbb{Z}_2^{2^m}$ which contains the function values for all possible assignments of the variables $x_1, \ldots, x_m$ in the given order. This vector is called *evaluation vector* of the Boolean polynomial function f and is denoted with $\underline{f}$. We write $\underline{f} \sim f$ and say that $\underline{f}$ is *related* to f. It can be shown that any vector in $\mathbb{Z}_2^{2^m}$ is the evaluation vector of a Boolean polynomial function.

Now we can define $RM(r, m)$ as the set of all evaluation vectors of Boolean polynomial functions of degree less or equal r in m variables

$$RM(r, m) = \left\{ \underline{f} : f : \mathbb{Z}_2^m \to \mathbb{Z}_2 \text{ Boolean polynomial function with degree } \leq r \right\}.$$

A generator matrix for $RM(r, m)$ can be constructed by writing the evaluation vectors of all monomial functions $m : \mathbb{Z}_2^m \to \mathbb{Z}_2$ of degree $\leq r$ as rows in a matrix.

Example 3.25. Let $r = 2$ and $m = 3$. Then $RM(r, m)$ is generated by the matrix

$$G = \left(\begin{array}{cccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1
\end{array}\right)
\begin{array}{cc}
\leftarrow & \underline{1} \\
\leftarrow & \underline{x_1} \\
\leftarrow & \underline{x_2} \\
\leftarrow & \underline{x_3} \\
\leftarrow & \underline{x_1 \cdot x_2} \\
\leftarrow & \underline{x_1 \cdot x_3} \\
\leftarrow & \underline{x_2 \cdot x_3}
\end{array}.$$

Definition of $\mathbf{RM(r, m)}$ via the Plotkin construction:

Let $n \in \mathbb{N}$ and $A, B \subseteq \mathbb{Z}_2^n$. The *Plotkin construction* of A and B is defined by

$$A \propto B := \big\{ \big(a, a+b\big) \in \mathbb{Z}_2^{2n} : a \in A \text{ and } b \in B \big\}.$$

Starting with $RM(0, m) := \{(0, \dots, 0), (1, \dots, 1)\} \subseteq \mathbb{Z}_2^{2^m}$ for all $m \in \mathbb{N}_0$ we define $RM(r, m)$ by the recursion

$$RM(r, m) := RM(r, m-1) \propto RM(r-1, m-1).$$

Example 3.26.

$$\begin{aligned} RM(1,1) \propto RM(0,1) &= \{(0,0),(0,1),(1,0),(1,1)\} \propto \{(0,0),(1,1)\} \\ &= \{((0,0),(0,0)+(0,0)),((0,0),(0,0)+(1,1)), \\ &\quad ((0,1),(0,1)+(0,0)),((0,1),(0,1)+(1,1)), \\ &\quad ((1,0),(1,0)+(0,0)),((1,0),(1,0)+(1,1)), \\ &\quad ((1,1),(1,1)+(0,0)),((1,1),(1,1)+(1,1))\} \\ &= \{(0,0,0,0),(0,0,1,1),(0,1,0,1),(0,1,1,0), \\ &\quad (1,0,1,0),(1,0,0,1),(1,1,1,1),(1,1,0,0)\} \\ &= RM(1,2). \end{aligned}$$

Both constructions yield exactly the same codes. According to the construction the code length is $n = 2^m$. The dimension is $k = \sum\limits_{i=0}^{r} \binom{m}{i}$ since this is the number of all Boolean monomial functions in m variables with degree $\leq r$. Furthermore it can be shown by induction that the minimum distance is $d = 2^{m-r}$.

The Reed-Muller codes with $r = 1$ are called *first order Reed-Muller codes.* They play an important role in the next chapters and we will need the following properties of this family of codes.

Definitions and Remark 3.27.

(a) $RM(1, m)$ can be constructed from $RM(1, m-1)$ in a very simple way:

$$\begin{aligned} RM(1,m) &= RM(1,m-1) \propto RM(0,m-1) \\ &= RM(1,m-1) \propto \{(\underbrace{0,\dots,0}_{2^{m-1}}),(\underbrace{1,\dots,1}_{2^{m-1}})\} \\ &= \big\{\big(c,c\big) : c \in RM(1,m-1)\big\} \cup \big\{\big(c,\overline{c}\big) : c \in RM(1,m-1)\big\}, \end{aligned}$$

where $\overline{c}$ is the complementary vector of c. The Plotkin construction assigns two codewords (c, c) and $(c, \overline{c})$ to each codeword $c \in RM(1, m-1)$. When we consider c to be the evaluation vector $\underline{f}$ of a Boolean polynomial $f \in \mathbb{Z}_2[x_1, \dots, x_{m-1}]$ the Plotkin construction yields

$$\begin{tikzcd}
 & (c,c) = \big(\underline{f(x_1,\dots,x_{m-1})}\big) \\
\underline{f(x_1,\dots,x_{m-1})} = c \arrow[ur] \arrow[dr] & \\
 & (c,\overline{c}) = \big(\underline{x_m + f(x_1,\dots,x_{m-1})}\big).
\end{tikzcd}$$

(b) Define

$$\begin{aligned}
RM^0(1,m) &= \{\underline{f} : f : \mathbb{Z}_2^m \to \mathbb{Z}_2 \text{ Boolean polynomial function with degree } \le 1 \\
&\qquad \text{without the summand } 1\} \\
&= \{\underline{f} : f : \mathbb{Z}_2^m \to \mathbb{Z}_2,\ f(x_1,\dots,x_m) = x_{i_1} + \dots + x_{i_\ell}, \\
&\qquad i_1,\dots,i_\ell \in \{1,\dots,m\} \text{ pairwise distinct}\} \cup \{(0,\dots,0)\} \\
&= \{c = (c_1,\dots,c_{2^m}) \in RM(1,m) : c_1 = 0\}
\end{aligned}$$

and

$$\begin{aligned}
RM^1(1,m) &= \{\underline{f} : f : \mathbb{Z}_2^m \to \mathbb{Z}_2 \text{ Boolean polynomial function with degree } \le 1 \\
&\qquad \text{with the summand } 1\} \\
&= \{\underline{f} : f : \mathbb{Z}_2^m \to \mathbb{Z}_2,\ f(x_1,\dots,x_m) = 1 + x_{i_1} + \dots + x_{i_\ell}, \\
&\qquad i_1,\dots,i_\ell \in \{1,\dots,m\} \text{ pairwise distinct}\} \cup \{(1,\dots,1)\} \\
&= \{c = (c_1,\dots,c_{2^m}) \in RM(1,m) : c_1 = 1\}.
\end{aligned}$$

Then

$$RM^0(1,m) = RM^0(1,m-1) \propto \mathbb{Z}_2^{2^{m-1}}$$

and

$$RM^1(1,m) = RM^1(1,m-1) \propto \mathbb{Z}_2^{2^{m-1}}.$$

(c) $\mathcal{C} = RM(1,m)$ has the weight distribution

$$w(\mathcal{C}) = (1,0,\dots,0,\underset{\overset{\uparrow}{2^{m-1}}}{2^{m+1}-2},0,\dots,0,1).$$

This follows directly from part (a) by induction over m.

(d) For a binary vector v let $\operatorname{supp}(v)$ be the set of all positions where the vector v has the value one. $\operatorname{supp}(v)$ is called *support* of v. The complement $\overline{\operatorname{supp}(v)}$ consists of all positions where v has the value zero.

Let $c,d \in RM(1,m) \setminus \{(0,\dots,0),(1,\dots,1)\}$ be two different codewords with

$c \neq \overline{d}$. Then

$$\begin{aligned} |\mathrm{supp}(c) \cap \mathrm{supp}(d)| = \left|\mathrm{supp}(c) \cap \overline{\mathrm{supp}(d)}\right| &= \\ \left|\overline{\mathrm{supp}(c)} \cap \mathrm{supp}(d)\right| = \left|\overline{\mathrm{supp}(c)} \cap \overline{\mathrm{supp}(d)}\right| &= 2^{m-2}. \end{aligned}$$

Especially $d(c,d) = 2^{m-1}$. This follows directly from part (a) by induction over m.

(e) $\mathcal{C} = RM(1,m)$ has the covering radius

$$\rho(\mathcal{C}) \begin{cases} = 2^{m-1} - 2^{\frac{m-2}{2}} & \text{if } m \text{ is even} \\ \leq 2^{m-1} - 2^{\frac{m-2}{2}} & \text{if } m \text{ is odd} \end{cases}$$

(see [15]).

Chapter 4

A New Approach to Secret Sharing Using Error-Correcting Codes

There are many ways to construct secret sharing schemes using various mathematical objects and concepts. Shamir for example uses polynomial interpolation over finite fields ([35]). Blakeley as well as Simmons present geometric constructions based on the intersections of hyperplanes in projective spaces and affine spaces ([7],[27]), while Asmuth and Bloom give an algebraic construction based on the Chinese remainder theorem ([2]). In the following chapters we study constructions using error-correcting codes. We begin with an overview of the previous research on secret sharing schemes based on error-correcting codes. Then we present our new approach which differs significantly from the previous constructions.

4.1 Overview of the Current State of Research

McEliece and Sarwate were the first to observe a connection between secret sharing and error-correcting codes [30]. They found out that Shamir's secret sharing scheme is closely related to Reed-Solomon codes. Using the notations of 2.2.1 the shares in Shamir's scheme define a vector $v = \big(f(1), \ldots, f(t)\big) \in \mathbb{Z}_p^t$ for a polynomial $f(x) = \sum_{i=0}^{\alpha-1} a_i x^i \in \mathbb{Z}_p[x]$ of degree $\alpha - 1$. In other words v is a codeword in an α-dimensional Reed-Solomon code over $\mathbb{Z}_p$ with $M = (1, \ldots, t)$ (see 3.2.2). If at least α digits of v are known the corresponding information word $(a_0, \ldots, a_{\alpha-1})$, and therefore the secret $f(0) = a_0$, can be calculated using an errors-and-erasures algorithm.

This construction can be generalized to arbitrary linear $[t,k]_q$ codes (see [33]). Let G denote a generator matrix of such a code with columns $G_1, \ldots, G_t$ and let $v_1 \in \mathbb{F}_q$ be the secret to be shared. Choose randomly $k-1$ values $v_2, \ldots, v_k \in \mathbb{F}_q$ and calculate the corresponding codeword $(c_1, \ldots, c_t) = (v_1, \ldots, v_k) \cdot G$. Then give each c_j as a share to participant T_j. A set $\{T_{j_1}, \ldots, T_{j_s}\}$ can determine the secret by solving the related system of linear equations $(v_1, \ldots, v_k) \cdot \big(G_{j_1}, \ldots, G_{j_s}\big) = (c_{j_1}, \ldots, c_{j_s})$ if the vector $e_1 = (1, 0, \ldots, 0)^\tau$ is a linear combination of the columns $G_{j_1}, \ldots, G_{j_s}$. Otherwise the participants gain no information about the secret. Hence the secret sharing scheme is perfect and ideal. In [33] Renvall and Ding show that each k shares determine the secret if the underlying code is a MDS code. In terms of vector spaces these secret sharing schemes are introduced earlier by Brickell in [9].

A similar construction is proposed in [18] by Ding et al. They use linear $[t,k]_q$ codes to share *multisecrets* $s=(s_1,\ldots,s_k)\in\mathbb{F}_q^k$ consisting of k single secrets $s_1,\ldots,s_k\in\mathbb{F}_q$. Let G be a generator matrix of such a code and s be a multisecret. Then $s\cdot G=(c_1,\ldots,c_t)$ is calculated and the c_j are given as shares to the participants T_j for all $j=1,\ldots,t$. If enough participants join the reconstruction the multisecret can be found using a suitable decoding algorithm. It turns out that special MDS codes yield perfect $[t,k]$-threshold schemes for multisecrets.

Another construction of threshold schemes with linear codes is described in [22] by Karnin et al. In this construction the secret is defined as a part of the codeword and not as a part of the information word. In order to share a secret $c_0\in\mathbb{F}_q$ among t participants a linear $[t+1,k]_q$ code $\mathcal{C}$ is used. The dealer chooses a codeword $c=(c_0,\ldots,c_t)$ with the first component c_0 equal to the secret and distributes the remaining components as shares to the participants. T_j receives the share c_j for all $j=1,\ldots,t$. Suppose that a group of participants wants to recover the secret. When the number of participants which are not in this group is below the error-correction capacity of the code $\mathcal{C}$, the group can recover the secret using a decoding algorithm. Otherwise the recovery may be successful or not. This depends on the structure of the code $\mathcal{C}$. In [33] Renvall and Ding show that this construction also yields a perfect $[k,t]$-threshold scheme if $\mathcal{C}$ is a MDS code.

In [40] Tang et al. present a criterion of whether a monotone access structure Γ can be realized using Karnin's ideal construction. Furthermore they propose an algorithm which outputs a suitable linear code realizing Γ such that the information rate is optimal, if there is no ideal solution.

Bertilsson and Ingemarsson ([6]) extend Karnin's construction for arbitrary monotone access structures. They present an algorithm which generates a suitable generator matrix using the minimal subsets of Γ. The resulting secret sharing schemes are perfect but in general codes of length $>t$ are necessary because some participants need to receive more than one component of the codeword as shares.

In [28], [29] Massey shows an important relationship between the access structures related to a linear code $\mathcal{C}$ and the dual code $\mathcal{C}^\perp$ in Bertilsson's and Ingemarsson's construction. Let $G_0,\ldots,G_t$ denote the columns of the generator matrix G. Suppose that $d=(d_0,\ldots,d_t)$ is a word in the dual code with $d_0=1$ and further $s>0$ nonzero components $d_{j_1},\ldots,d_{j_s}$. Since $d\cdot G^\tau=0$ the first column G_0 can be written as linear combination $G_0=\sum_{j=1}^{s}a_{i_j}G_{i_j}$ and the secret can be computed easily as $c_0=\sum_{j=1}^{s}a_{i_j}c_{i_j}$. Based on this consideration Massey characterizes the minimal authorized sets in terms of minimal codewords of $\mathcal{C}^\perp$. A nonzero codeword d is called *minimal* if there exists no other codeword d' such that $\operatorname{supp}(d)\supset\operatorname{supp}(d')$. Each (minimal) codeword $d=(d_0,\ldots,d_t)\in\mathcal{C}^\perp$ can be associated with a set S of participants by stating $T_j\in S$ iff $d_j\neq 0$ for all $j=1,\ldots,t$. Massey proves that the sets of participants associated to the minimal codewords in $\mathcal{C}^\perp$ starting with one are exactly the minimal subsets of the monotone access structure related to the code $\mathcal{C}$ via Karnin's construction.

Van Dijk ([42]) pointed out that Massey's approach is a special case of the generalized vector space construction introduced by Bertilsson in [6].

Inspired by Massey's results different classes of codes and their duals were studied. Ding et al. apply Karnin's construction to classes of ternary codes ([17]) Li et al. study classes of binary codes [25] and Carlet and Ding use codes from perfect nonlinear mappings ([10]).

Another interesting class of codes are the algebraic-geometric codes. Using these codes Karnin's approach yields ideal ramp schemes ([11], [12], [13], [14], [24]). *Ramp schemes* are a generalization of threshold-schemes with an upper threshold t_2 and a lower threshold t_1 such that any subset of at least t_2 participants can recover the secret and all subsets containing t_1 or less participants are unauthorized. The difference $t_2 - t_1$ is called *threshold gap*. The authors show how the threshold gap depends on the genus of the algebraic curve which defines the code. In [13] Chen et al. show that random error-correcting codes also provide ramp schemes with high information rate.

There is a close relation between the minimal distances d and the dual distance $d^{\perp}$ of the underlying codes $\mathcal{C}$ and the thresholds t_1 and t_2. Sodan shows that Massey's construction yields a ramp scheme with $t_1 = d^{\perp} - 2$ and $t_2 = t - d + 2$ ([38]). In [31] Paterson and Stinson find out that a (not necessarily linear) code with minimal distance d and dual distance $d^{\perp}$ provides a $[d^{\perp} - s - 1, t - d + 1]$ ramp scheme with arbitrary information rate $s \leq d^{\perp} - 2$. Kurihara et al. improve the bounds on t_1 and t_2 using the concept of relative generalized Hamming weights ([23]).

In general it is hard to determine the minimal codewords of a given code. This problem is called covering problem. Even the restriction to minimal words starting with one is no simplification. However the Ashikhmin-Barg lemma gives a criterion that ensures that all nonzero words of a code are minimal [1]. Roughly speaking that lemma tells us that all nonzero codewords are minimal if the weights of all codewords are close to each other. Ding and Yuan show in [20] that the access structure related to $\mathcal{C}$ has some interesting properties when all nonzero words in $\mathcal{C}^{\perp}$ are minimal: With the above notations $\mathcal{C}^{\perp}$ is a $[t+1, t+1-k]_q$ code. Let $H = (H_0, \ldots, H_t)$ denote a generator matrix for $\mathcal{C}^{\perp}$ and assume that no column is the zero vector. Then there are exactly q^{k-1} minimal authorized subsets. Furthermore if H_j is a multiple of H_0 the participant T_j has to be part of any authorized set (T_j is called dictatorial). Otherwise T_j is part of exactly $(q-1)^{k-2}$ minimal authorized sets. In [20] [19], [44] several classes of linear codes are studied. Using the Ashikhmin-Barg lemma the authors show that all nonzero codewords in the dual codes are minimal and obtain secret sharing schemes with the stated properties.

In [39] Tan and Wang improve Massey's scheme such that the participants are able to detect cheating by the dealer.

Tentu et al. provide an ideal computationally perfect secret sharing scheme based on MDS codes realizing *conjunctive hierarchical* access structures ([41]). In such access structures the set of participants consists of disjoint subsets $\mathcal{T} = \bigcup_{i=1}^{m} \mathcal{T}_i$. Each *level*

$\mathcal{T}_i$ is assigned a threshold t_i and set $A \subseteq \mathcal{T}$ is authorized iff $\left|A \cap \bigcup_{j=1}^{i} \mathcal{T}_j\right| \geq t_i$ for all $i = 1, \ldots, m$. The secret s is divided into the sum $s = s_1 + \ldots + s_m$. Then m codewords $c_1, \ldots, c_m$ are constructed such that each c_i has the first component s_i. Some of the remaining components are made public and the other components are distributed as shares to the participants such that any set $A \subseteq \bigcup_{j=1}^{i} \mathcal{T}_j$ of at least t_i participants can recover the codeword c_i and therefore the summand s_i. If a group consists of at least t_i participants for all $i = 1, \ldots, m$, they can determine all components s_i and are able to calculate s.

In [16] Cramer et al. improve Bertilsson's and Ingemarsson's construction by using linear hash functions. In the proposed secret sharing scheme the secret is the image $s = h(x)$ of a suitable vector $x \in \mathbb{F}^k$ under a randomly chosen linear hash function $h : \mathbb{F}^k \to \mathbb{F}^l$. The vector x is encoded to a codeword c of a linear error-correcting code and the entries of c are distributed as shares to the participants. The resulting schemes are ramp schemes and due to the use of the hash function the threshold gap depends only on the rate of the underlying code.

All these previous secret sharing schemes using error-correcting codes have the limitation that they can only realize monotone access structures. In contrast to that our approach yields a secret sharing scheme which can realize *arbitrary* access structures.

First results concerning the properties of the shares were achieved in cooperation with Michael Beiter ([4]).

4.2 The Basic Idea of Our Approach

In the previous constructions the secret and the shares are certain parts of an information word or a codeword. In our secret sharing scheme the secret is a complete codeword of a binary error-correcting code and the shares are binary words of the same length as the secret. When a group of participants is authorized we want the secret to be the codeword next to the sum of their shares, such that Hamming decoding yields the secret. Otherwise, when the participants are unauthorized, we want the sum of their shares to differ strongly enough from the secret such that Hamming decoding outputs the wrong codeword. Let $\mathcal{C}$ be a binary code and $s \in \mathcal{C}$ the secret to be shared. In terms of the minimum distance d of $\mathcal{C}$ the shares $k_1, \ldots, k_t \in \mathbb{Z}_2^n$ distributed to the participants $T_1, \ldots, T_t$ shall have the properties

1. $\mathrm{d}\left(k_{j_1} + \ldots + k_{j_\ell}, s\right) \leq \left\lfloor \frac{d-1}{2} \right\rfloor$ if $\{T_{j_1}, \ldots, T_{j_\ell}\} \in \Gamma$ and
2. For all unauthorized sets $\{T_{j_1}, \ldots, T_{j_\ell}\}$ there is a codeword $c \in \mathcal{C}$, $c \neq s$ such that $\mathrm{d}\left(k_{j_1} + \ldots + k_{j_\ell}, s\right) > \mathrm{d}\left(k_{j_1} + \ldots + k_{j_\ell}, c\right)$.

The first property guarantees that all authorized groups of participant are able to reconstruct the secret. Since the Hamming distance from $k_{j_1} + \ldots + k_{j_\ell}$ to s does not exceed the error correcting capability of $\mathcal{C}$ the secret can be computed with a suitable decoding algorithm. The second requirement ensures that Hamming decoding does not yield the secret when the set is unauthorized.

In a certain way, our approach is related to Karnin's construction. In this construction each participant T_j receives the jth entry c_j of a codeword c. Instead of this, T_j could receive the word $(0, \ldots, 0, c_j, 0, \ldots, 0)$. When enough participants add their words, Hamming decoding yields c and therefore the secret c_0.

The difficulty consists in finding suitable codes $\mathcal{C}$ and secrets $s \in \mathcal{C}$ and in constructing shares with the desired properties. In the next sections we will deal with these problems. We will see that suitable codes, secrets and shares which meet condition 1. and 2. can be found for all access structures. However, in general the resulting secret sharing scheme is neither perfect nor ideal, even when monotone access structures are considered: Using Hamming decoding each unauthorized set receives a codeword which is definitely not the secret. Since these codewords can be excluded, not all secrets are equiprobable.

By now the only known access structures which have perfect realizations using our approach are those of the the form $\Gamma = \{A \subseteq \mathcal{T} : T_j \in A\}$ for a fixed j when the secret is a non-zero codeword. We assign the secret as share to T_j and the zero word to the other participants. Then the unauthorized sets gain no information about the secret and Hamming decoding always yields the zero word which is not the secret. Furthermore, the realization is almost ideal since there are $|\mathcal{C}|$ possible shares and $|\mathcal{C}| - 1$ possible secrets.

So far our secret sharing scheme has the following formal components.

(a) $\mathcal{T} = \{T_1, \ldots, T_t\}$ is the set of participants.

(b) $\Gamma \subseteq \mathcal{P}(\mathcal{T}) \backslash \{\varnothing\}$ is arbitrary. We have to omit the empty set because at least one share is necessary during the recovery of the secret. In the following we consider only access structures which do not contain the empty set.

(c) The possible secrets are certain codewords of a suitable binary error correcting code $\mathcal{C}$ with length n: $\mathcal{S} \subseteq \mathcal{C} \subseteq \mathbb{Z}_2^n$.

(d) $\mathcal{K} = \mathbb{Z}_2^n$ is the set of all possible shares.

(e) The distribution functions will be constructed in the following sections.

(f) $r : \mathcal{P}(\mathbb{Z}_2^n) \to \mathcal{C}$ assigns each set of shares $\{k_{j_1}, \ldots, k_{j_\ell}\}$ a random element of $\operatorname{dec}(k_{j_1} + \ldots + k_{j_\ell})$. $\operatorname{dec} : \mathbb{Z}_2^n \to \mathcal{P}(\mathcal{C})$ is a decoding function for $\mathcal{C}$ and yields the set of all codewords with minimum Hamming distance to the input vector.

In order to find a suitable selection of shares for a given access structure we need to learn more about the structure that the shares must have. This will be done in the next section. We will see that the shares are characterized by a system of linear equations. In Section 4.4 we use that knowledge to prove the existence of a suitable selection of shares for any access structure on an arbitrary number of participants fulfilling condition 1. and 2.

It will turn out that a large code length n is necessary to realize arbitrary access structures. However, large shares must be expected when arbitrary access structures are realized. When there are t participants there are $2^t - 1$ possible authorized subsets. Hence it takes already up to $2^t - 1$ bits of information to declare all authorized subsets.

Furthermore it turns out that in the realization provided by Section 4.4 the distances from the share sums of unauthorized subsets to the secret are rather small. There are only a few codewords closer to these sums than the secret. That is why our secret sharing scheme is far from being perfect, even when monotone access structures are realized. However, since we are going to realize arbitrary access structures which are generally non-monotone, the participants must not receive their shares in plain text and the use of a combiner is vital. In a combiner driven management model the small distances are unproblematic as long as conditions 1. and 2. are satisfied.

Later we will identify access structures which allow smaller code lengths and larger distances from the sums of the shares of unauthorized sets to the secret. For this purpose we will classify all access structures on the same participant set and develop several techniques of how to derive the realization of one access structure from the realizations of others.

4.3 The Structure of the Shares

Let $\mathcal{T} = \{T_1, \ldots, T_t\}$ be a set of t participants and Γ an arbitrary access structure on $\mathcal{T}$. We need to find a suitable error correcting binary code $\mathcal{C}$ of suitable length n with minimal distance d and to construct vectors $k_1, \ldots, k_t \in \mathbb{Z}_2^n$ such that the secret is represented by a codeword $s \in \mathcal{C}$ and the following requirements are satisfied:

1. $\mathrm{d}\left(s, k_{j_1} + \ldots + k_{j_\ell}\right) \leq \left\lfloor \frac{d-1}{2} \right\rfloor \Leftrightarrow \{T_{j_1}, \ldots, T_{j_\ell}\} \in \Gamma$
2. For all unauthorized sets $\{T_{j_1}, \ldots, T_{j_\ell}\}$ there is a codeword $c \in \mathcal{C}$, $c \neq s$ such that $\mathrm{d}\left(s, k_{j_1} + \ldots + k_{j_\ell}\right) > \mathrm{d}\left(c, k_{j_1} + \ldots + k_{j_\ell}\right)$.

In the following we assume that a secret s has already been chosen and suitable shares $k_1, \ldots, k_t \in \mathbb{Z}_2^n$ are already distributed to the participants. We deduce conditions on the code length n and the structure of the shares, such that the requirements 1. and 2. are satisfied. This will lead to a procedure of how to find a suitable code length n and how to construct suitable shares in terms of solutions of a system of linear equations. We develop the description of n and the shares $k_1, \ldots, k_t$ by these linear equations in the following four steps.

4.3.1 Defining Total Orders

In the first step we define total orders on $\mathcal{P}(\mathcal{T})$, on the set of all sums of the distributed shares, on the set of the distances of these sums to the secret and on the binary codes $RM^0(1,t)$ and $RM^1(1,t)$.

(a) At first we define a total order $\preccurlyeq$ on the power set $\mathcal{P}(\mathcal{T})$ of the participant set. We number the participants and order them according to the natural order of the indices:

$$T_1 \leq T_2 \leq \ldots \leq T_t.$$

Then we use this order to define a total order on $\mathcal{P}(\mathcal{T})$ inductively.

- Let $\varnothing$ be the smallest set in $\mathcal{P}(\mathcal{T})$.
- Assume that the power set of the first r participants, $0 \leq r < t$ is already ordered. Then we have the ordered series

$$\varnothing \preccurlyeq \ldots \preccurlyeq S_j \preccurlyeq \ldots \preccurlyeq S_{2^r-1}$$

of all subsets of $\{T_1, \ldots, T_r\}$. We receive the ordered series for $r+1$ participants by extending the series to

$$\begin{aligned} &\varnothing \preccurlyeq \ldots \preccurlyeq S_j \preccurlyeq \ldots \preccurlyeq S_{2^r-1} \preccurlyeq \\ &\{T_{r+1}\} \preccurlyeq \ldots \preccurlyeq S_j \cup \{T_{r+1}\} \preccurlyeq \ldots \preccurlyeq S_{2^r-1} \cup \{T_{r+1}\}. \end{aligned}$$

(b) Now suppose that each participant $T_j \in \mathcal{T}$ has received a share $k_j \in \mathbb{Z}_2^n$. We use the ordered set $(\mathcal{P}(\mathcal{T}), \preccurlyeq)$ as index set to order the set

$$\left\{ \sum_{m=1}^{\ell} k_{j_m} : k_{j_m} \in \{k_1, \ldots k_t\} \right\}$$

of all possible sums of the distributed shares. We define

$$\begin{array}{ccc} k_{j_1} + \ldots + k_{j_\ell} & \preccurlyeq & k_{i_1} + \ldots + k_{i_u} \\ & \Leftrightarrow & \\ \{T_{j_1}, \ldots T_{j_\ell}\} & \preccurlyeq & \{T_{i_1}, \ldots T_{i_u}\}. \end{array}$$

(c) Next we use the ordered set $(\mathcal{P}(\mathcal{T}), \preccurlyeq)$ as index set to order the set

$$\left\{ \mathrm{d}\left(s, \sum_{m=1}^{\ell} k_{j_m} \right) : k_{j_m} \in \{k_1, \ldots k_t\} \right\}$$

of the distances from all possible sums of distributed shares to the secret in the same way. We define

$$\begin{array}{ccc} \mathrm{d}\left(s, k_{j_1} + \ldots + k_{j_\ell}\right) & \preccurlyeq & \mathrm{d}\left(s, k_{i_1} + \ldots + k_{i_u}\right) \\ & \Leftrightarrow & \\ \{T_{j_1}, \ldots T_{j_\ell}\} & \preccurlyeq & \{T_{i_1}, \ldots T_{i_u}\}. \end{array}$$

This order on the set of distances allows us to define the so called distance vector.

Definition 4.1. The *distance vector* corresponding to the secret s and the shares $k_1, \ldots, k_t$ is the vector

$$
\begin{aligned}
b &= b(s, k_1, \ldots, k_t) = \left(b_1, b_2, \ldots, b_{2^t}\right)^{\tau} \\
&:= \begin{pmatrix} \mathrm{d}\,(s, 0) \\ \mathrm{d}\,(s, k_1) \\ \vdots \\ \mathrm{d}\left(s, \sum\limits_{m=1}^{\ell} k_{j_m}\right) \\ \vdots \\ \mathrm{d}\left(s, \sum\limits_{j=1}^{t} k_j\right) \end{pmatrix}
\end{aligned}
$$

such that $b_i \preccurlyeq b_{i+1}$ for all $1 \leq i \leq 2^t - 1$.

Example 4.2. For three participants T_1, T_2, T_3 with shares $k_1, k_2, k_3 \in \mathcal{K} = \mathbb{Z}_2^n$ the total order on $\mathcal{P}(\mathcal{T})$ is given by

$$\varnothing \preccurlyeq \{T_1\} \preccurlyeq \{T_2\} \preccurlyeq \{T_1, T_2\} \preccurlyeq \{T_3\} \preccurlyeq \{T_1, T_3\} \preccurlyeq \{T_2, T_3\} \preccurlyeq \{T_1, T_2, T_3\}\,.$$

The sums of shares are ordered by

$$0 \preccurlyeq k_1 \preccurlyeq k_2 \preccurlyeq k_1 + k_2 \preccurlyeq k_3 \preccurlyeq k_1 + k_3 \preccurlyeq k_2 + k_3 \preccurlyeq k_1 + k_2 + k_3$$

and the distances by

$$
\begin{aligned}
\mathrm{d}\,(s, 0) = \mathrm{wt}(s) &\preccurlyeq \mathrm{d}\,(s, k_1) \preccurlyeq \mathrm{d}\,(s, k_2) \preccurlyeq \mathrm{d}\,(s, k_1 + k_2) \preccurlyeq \mathrm{d}\,(s, k_3) \\
&\preccurlyeq \mathrm{d}\,(s, k_1 + k_3) \preccurlyeq \mathrm{d}\,(s, k_2 + k_3) \preccurlyeq \mathrm{d}\,(s, k_1 + k_2 + k_3)\,.
\end{aligned}
$$

(d) Finally we use $(\mathcal{P}(\mathcal{T}), \preccurlyeq)$ as index set to define total orders on the subsets of the polynomial ring $\mathbb{Z}_2[x_1, \ldots, x_t]$ consisting of Boolean polynomials of degree one with or without the constant summand 1. These orders imply total orders on the binary codes $RM^0(1, t)$ and $RM^1(1, t)$. We define

$$
\begin{aligned}
x_{j_1} + \ldots + x_{j_\ell} &\preccurlyeq x_{i_1} + \ldots + x_{i_u} \\
&\Leftrightarrow \\
\{T_{j_1}, \ldots T_{j_\ell}\} &\preccurlyeq \{T_{i_1}, \ldots T_{i_u}\}
\end{aligned}
$$

and

$$\begin{array}{rcl} 1+x_{j_1}+\ldots+x_{j_\ell} & \preccurlyeq & 1+x_{i_1}+\ldots+x_{i_u} \\ & \Leftrightarrow & \\ \{T_{j_1},\ldots T_{j_\ell}\} & \preccurlyeq & \{T_{i_1},\ldots T_{i_u}\}\,. \end{array}$$

Example 4.3. For $t=3$ the total orders on $RM^0(1,t)$ and $RM^1(1,t)$ are given by the orders on the related Boolean polynomials

$$0 \preccurlyeq x_1 \preccurlyeq x_2 \preccurlyeq x_1+x_2 \preccurlyeq x_3 \preccurlyeq x_1+x_3 \preccurlyeq x_2+x_3 \preccurlyeq x_1+x_2+x_3 \text{ and}$$

$$1 \preccurlyeq 1+x_1 \preccurlyeq 1+x_2 \preccurlyeq 1+x_1+x_2 \preccurlyeq 1+x_3 \preccurlyeq 1+x_1+x_3 \preccurlyeq 1+x_2+x_3 \preccurlyeq 1+x_1+x_2+x_3.$$

This yields the following total orders on $RM^0(1,3)$

$$\begin{array}{llll} & (00000000)\sim 0 & \preccurlyeq (01010101)\sim x_1 & \preccurlyeq (00110011)\sim x_2 \\ \preccurlyeq & (01100110)\sim x_1+x_2 & \preccurlyeq (00001111)\sim x_3 & \preccurlyeq (01011010)\sim x_1+x_3 \\ \preccurlyeq & (00111100)\sim x_2+x_3 & \preccurlyeq (01101001)\sim x_1+x_2+x_3 & \end{array}$$

and on $RM^1(1,3)$

$$\begin{array}{llll} & (11111111)\sim 1 & \preccurlyeq (10101010)\sim 1+x_1 & \preccurlyeq (11001100)\sim 1+x_2 \\ \preccurlyeq & (10011001)\sim 1+x_1+x_2 & \preccurlyeq (11110000)\sim 1+x_3 & \preccurlyeq (10100101)\sim 1+x_1+x_3 \\ \preccurlyeq & (11000011)\sim 1+x_2+x_3 & \preccurlyeq (10010110)\sim 1+x_1+x_2+x_3. & \end{array}$$

At this point we give a representation of the evaluation of a Boolean polynomial $p \in \mathbb{Z}_2[x_1,\ldots,x_t]$ of constant degree one on a vector $w \in \mathbb{Z}_2^t$ in terms of the order $\preccurlyeq$ that we need later on.

Remark 4.4. The interpretation of the elements $(a_0,\ldots,a_{t-1})$ of $\mathbb{Z}_2^t$ as binary representations of natural numbers $\sum\limits_{i=0}^{t-1} a_i 2^i$ yields an order $\leq$ on $\mathbb{Z}_2^t$:

$$(0,\ldots,0) \leq (1,0,\ldots,0) \leq (0,1,0,\ldots,0) \leq (1,1,0,\ldots,0) \leq \ldots \leq (1,\ldots,1).$$

Let $v=(v_1,\ldots,v_t)$ be the ith element of $(\mathbb{Z}_2^t,\leq)$ and p the Boolean polynomial which belongs to the ith element of $(RM^0(1,t),\preccurlyeq)$ for an arbitrary $1 \leq i \leq 2^t$. Then p is related to $v=(v_1,\ldots,v_t)$ in the following way: $v_j=1$ iff the monomial x_j is a term of p. Hence the evaluation of p on an arbitrary vector $w \in \mathbb{Z}_2^t$ can be expressed by calculating the scalar product

$$p(w) = v \cdot w^{\tau}.$$

4.3.2 Characterization of the Distance Vector

In the second step we characterize the distance vector $b(s,k_1,\ldots,k_t)$ in terms of the supports of the secret and the shares.

The shares as well as the secret are binary vectors of length n. Let $I = \{1, \ldots, n\}$ denote the set of all positions in such a vector. In this step we define a partition $I = I_1^t \,\dot\cup\, , \ldots , \,\dot\cup\, I_{2^{t+1}}^t$ such that the support of each sum of shares is the union of a uniquely determined selection of the I_i^t. The term "partition" is used in a general sense since some I_i^t could be empty. Define $s := k_0$. Then each position in I belongs to a unique set of the form

$$\operatorname{supp}(k_{j_0}) \cap \ldots \cap \operatorname{supp}(k_{j_\ell}) \cap \overline{\operatorname{supp}\left(k_{j_{\ell+1}}\right)} \cap \ldots \cap \overline{\operatorname{supp}(k_{j_t})}.$$

with $j_0, \ldots, j_t \in \{0, \ldots, t\}$ pairwise distinct. We will see that this classification of the positions yields a partition of I into 2^{t+1} disjoint sets with the required properties.
Initially consider a scheme with only one participant T_1. We fragment $I = \overline{\operatorname{supp}(s)} \,\dot\cup\, \operatorname{supp}(s)$ into four disjoint subsets

$$\begin{aligned} I &= \left(\overline{\operatorname{supp}(s)} \cap \overline{\operatorname{supp}(k_1)}\right) \,\dot\cup\, \left(\operatorname{supp}(s) \cap \overline{\operatorname{supp}(k_1)}\right) \,\dot\cup\, \\ &\quad \left(\overline{\operatorname{supp}(s)} \cap \operatorname{supp}(k_1)\right) \,\dot\cup\, \left(\operatorname{supp}(s) \cap \operatorname{supp}(k_1)\right) \\ &= I_1^1 \,\dot\cup\, I_2^1 \,\dot\cup\, I_3^1 \,\dot\cup\, I_4^1 \end{aligned}$$

with $I_1^1 := \overline{\operatorname{supp}(s)} \cap \overline{\operatorname{supp}(k_1)}$, $I_2^1 := \operatorname{supp}(s) \cap \overline{\operatorname{supp}(k_1)}$, $I_3^1 := \overline{\operatorname{supp}(s)} \cap \operatorname{supp}(k_1)$ and $I_4^1 := \operatorname{supp}(s) \cap \operatorname{supp}(k_1)$.
When we add a second participant we obtain a refinement of the above partition into eight disjoint subsets

$$\begin{aligned} I_1^2 &= \overline{\operatorname{supp}(s)} \cap \overline{\operatorname{supp}(k_1)} \cap \overline{\operatorname{supp}(k_2)} \\ I_2^2 &= \operatorname{supp}(s) \cap \overline{\operatorname{supp}(k_1)} \cap \overline{\operatorname{supp}(k_2)} \\ I_3^2 &= \overline{\operatorname{supp}(s)} \cap \operatorname{supp}(k_1) \cap \overline{\operatorname{supp}(k_2)} \\ I_4^2 &= \operatorname{supp}(s) \cap \operatorname{supp}(k_1) \cap \overline{\operatorname{supp}(k_2)} \\ I_5^2 &= \overline{\operatorname{supp}(s)} \cap \overline{\operatorname{supp}(k_1)} \cap \operatorname{supp}(k_2) \\ I_6^2 &= \operatorname{supp}(s) \cap \overline{\operatorname{supp}(k_1)} \cap \operatorname{supp}(k_2) \\ I_7^2 &= \overline{\operatorname{supp}(s)} \cap \operatorname{supp}(k_1) \cap \operatorname{supp}(k_2) \\ I_8^2 &= \operatorname{supp}(s) \cap \operatorname{supp}(k_1) \cap \operatorname{supp}(k_2). \end{aligned}$$

Inductively we can partition I for an arbitrary number of t participants. Given the partition $I = I_1^{t-1} \,\dot\cup\, \ldots \,\dot\cup\, I_{2^t}^{t-1}$ for $t-1$ participants define

$$I_i^t := I_i^{t-1} \cap \overline{\operatorname{supp}(k_t)} \quad \text{and} \quad I_{i+2^t}^t := I_i^{t-1} \cap \operatorname{supp}(k_t).$$

for all $1 \leq i \leq 2^t$. This gives a partition $I = I_1^t \,\dot\cup\, \ldots \,\dot\cup\, I_{2^{t+1}}^t$ with the following properties.

Remark 4.5. Let $k_{j_1} + \ldots + k_{j_\ell}$ be an arbitrary sum of shares, $j_m \neq 0$ for all $m = 1, \ldots, \ell$. Then the support $\operatorname{supp}(k_{j_1} + \ldots + k_{j_\ell})$ of the sum is the (disjoint) union of all I_i^t such that $I_i^t \cap \operatorname{supp}(k_{j_m}) \neq \varnothing$ for an odd number of shares $k_{j_m} \in \{k_{j_1}, \ldots, k_{j_\ell}\}$.

Definition 4.6. for $i = 1, ..., 2^{t+1}$ we define

$$a_i = a_i(s, k_1, \ldots, k_t) := |I_i^t| \text{ and}$$

$$a(s, k_1, \ldots, k_t) = (a_1, \ldots, a_{2^{t+1}}).$$

Note that a permutation on the positions has no effect on the a_i. That means for each $s \in \mathbb{Z}_2^n$ with weight $\operatorname{wt}(s) = b_1 \leq n$ all choices $a_1, \ldots, a_{2^{t+1}} \in \mathbb{N}_0^n$ with $\sum\limits_{i=1}^{2^t} a_{2i} = b_1$ and $\sum\limits_{i=1}^{2^t} a_{2i-1} = n - b_1$ determine shares $k_1, \ldots, k_t$ uniquely up to the order of their entries. Since the support of an arbitrary sum of shares is the disjoint union of a suitable selection of the I_i^t we can write the weight of each sum of shares as the sum of the corresponding a_i. Furthermore we have a representation of the distance from each sum of shares to the secret in terms of the a_i.

Remark 4.7. Let $k_{j_1} + \ldots + k_{j_\ell}$ be an arbitrary sum of shares, $j_m \neq 0$ for all $m = 1, \ldots, \ell$. Assume that $\operatorname{supp}(k_{j_1} + \ldots + k_{j_\ell}) = I_{i_1} \ \dot{\cup} \ \ldots \ \dot{\cup} \ I_{i_k}$. Then

(a) $\operatorname{wt}(k_{j_1} + \ldots + k_{j_\ell}) = a_{i_1} + \ldots + a_{i_k}$

(b) $\operatorname{wt}(s) = \sum\limits_{i=1}^{2^t} a_{2i}$

(c) $\operatorname{d}(s, k_{j_1} + \ldots + k_{j_\ell}) = \operatorname{wt}(s + k_{j_1} + \ldots + k_{j_\ell}) = \sum\limits_{\substack{v=1 \\ i_v \text{ odd}}}^{k} a_{i_v} + \sum\limits_{\substack{i \text{ even} \\ i \neq i_1, \ldots, i_k}}^{k} a_i$

The first sum counts the positions where s has the value 0 and $k_{j_1} + \ldots + k_{j_\ell}$ has the value 1. The second sum counts the positions where s has the value 1 and the sum $k_{j_1} + \ldots + k_{j_\ell}$ has the value 0.

Example 4.8. Let $\mathcal{C} = RM(1,3)$ and $t = 2$. Consider the following secret $s \in \mathcal{C} \subseteq \mathbb{Z}_2^8$ and the shares $k_1, k_2 \in \mathcal{K} = \mathbb{Z}_2^8$:

$$\begin{array}{rcl}
\text{positions} & & \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{array} \\
s & = & \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \\
k_1 & = & \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \\
k_2 & = & \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}
\end{array}$$

The supports are

$$\operatorname{supp}(s) = \{1, 2, 3, 4\}, \ \operatorname{supp}(k_1) = \{1, 2, 4, 6, 7, 8\} \text{ and } \operatorname{supp}(k_2) = \{1, 3, 6, 7\}.$$

This yields

$$\begin{array}{lcll}
I_1^2 & = & \overline{\operatorname{supp}(s)} \cap \overline{\operatorname{supp}(k_1)} \cap \overline{\operatorname{supp}(k_2)} = \{5\} & \Rightarrow\ a_1 = 1 \\
I_2^2 & = & \operatorname{supp}(s) \cap \overline{\operatorname{supp}(k_1)} \cap \overline{\operatorname{supp}(k_2)} = \varnothing & \Rightarrow\ a_2 = 0 \\
I_3^2 & = & \overline{\operatorname{supp}(s)} \cap \operatorname{supp}(k_1) \cap \overline{\operatorname{supp}(k_2)} = \{8\} & \Rightarrow\ a_3 = 1 \\
I_4^2 & = & \operatorname{supp}(s) \cap \operatorname{supp}(k_1) \cap \overline{\operatorname{supp}(k_2)} = \{2,4\} & \Rightarrow\ a_4 = 2 \\
I_5^2 & = & \overline{\operatorname{supp}(s)} \cap \overline{\operatorname{supp}(k_1)} \cap \operatorname{supp}(k_2) = \varnothing & \Rightarrow\ a_5 = 0 \\
I_6^2 & = & \operatorname{supp}(s) \cap \overline{\operatorname{supp}(k_1)} \cap \operatorname{supp}(k_2) = \{3\} & \Rightarrow\ a_6 = 1 \\
I_7^2 & = & \overline{\operatorname{supp}(s)} \cap \operatorname{supp}(k_1) \cap \operatorname{supp}(k_2) = \{6,7\} & \Rightarrow\ a_7 = 2 \\
I_8^2 & = & \operatorname{supp}(s) \cap \operatorname{supp}(k_1) \cap \operatorname{supp}(k_2) = \{1\} & \Rightarrow\ a_8 = 1.
\end{array}$$

For example

$$\operatorname{supp}(s + k_1 + k_2) = \operatorname{supp}(10000001) = \{1, 8\} = I_3^2 \ \dot\cup \ I_8^2$$

yields

$$\operatorname{d}(s, k_1 + k_2) = \operatorname{wt}(s + k_1 + k_2) = a_3 + a_8 = 1 + 1 = 2.$$

Furthermore, $\operatorname{wt}(s) = |\operatorname{supp}(s)| = |\,\{1,2,3,4\}\,| = a_2 + a_4 + a_6 + a_8$.

4.3.3 The Connection of the $\mathbf{a_i}$ to the Distance Vector b

In the third step we show that the components a_i are related to the distance vector b by a system of linear equations.

Each participant T_j receives a share $k_j \in \mathbb{Z}_2^n$ and the partition $I = I_1 \ \dot\cup \ \ldots \ \dot\cup \ I_{2^{t+1}}$ enables us to write the distance $\operatorname{d}\left(s, \sum\limits_{m=1}^{\ell} k_{j_m}\right)$ of each sum of shares to the secret as a sum of suitable a_i. Hence there must be a matrix $M(t) \in \mathcal{M}_{2^t, 2^{t+1}}(\mathbb{Z})$ with the entries 0 and 1 depending only on t such that for all possible secrets s and shares $k_1, \ldots, k_t$ and the resulting vectors $a(s, k_1, \ldots, k_t)$ and $b = (s, k_1, \ldots, k_t)$ the equation

$$M(t) \cdot \underbrace{\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{2^{t+1}} \end{pmatrix}}_{=a^\tau} = \begin{pmatrix} \operatorname{wt}(s) \\ \operatorname{d}(s, k_1) \\ \vdots \\ \operatorname{d}\left(s, \sum\limits_{j=1}^{t} k_j\right) \end{pmatrix} = \underbrace{\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_{2^t} \end{pmatrix}}_{=b} \tag{4.1}$$

holds.

In the following we describe the structure of such a matrix $M(t)$. We start with a lemma which shows a close relation between $M(t)$ and the first order Reed Muller codes $RM(1,t)$ and $RM(1,t+1)$. This relation determines $M(t)$ uniquely. In the next section we deal with the question for which types of distance vectors $b \in \mathbb{N}_0^{2^t}$ there is a suitable vector $a \in \mathbb{N}_0^{2^{t+1}}$ coming from the same $s, k_1, \ldots, k_t$ as b such that 4.1 holds.

Lemma 4.9. Let $M(t) \in \mathcal{M}_{2^t,2^{t+1}}(\mathbb{Z})$ be a matrix with entries in $\{0,1\}$ such that Equation 4.1 holds for all $a = a(s, k_1, \ldots, k_t)$ and $b = b(s, k_1, \ldots, k_t)$ coming from the same secret s and the same shares $k_1, \ldots, k_t$. Then $M(t)$ has the following properties:

(a) The odd numbered columns of $M(t)$ are the codewords of $RM^0(1,t)$ and the even numbered columns of $M(t)$ are the codewords of $RM^1(1,t)$. The even and the odd numbered columns appear in ascending order with respect to $\preccurlyeq$ (from left to right).

(b) The rows of $M(t)$ are the codewords of $RM^0(1,t+1)$ corresponding to Boolean polynomials with the term x_1. They appear in ascending order with respect to $\preccurlyeq$ (from top to bottom).

Proof. Proof by induction on t.
Let $t = 1$. For arbitrary s and k_1 we have the partition

$$\begin{aligned} I \;=\; & \underbrace{\left(\overline{\operatorname{supp}(s)} \cap \overline{\operatorname{supp}(k_1)}\right)}_{I_1} \;\dot{\cup}\; \underbrace{\left(\operatorname{supp}(s) \cap \overline{\operatorname{supp}(k_1)}\right)}_{I_2} \;\dot{\cup} \\ & \underbrace{\left(\overline{\operatorname{supp}(s)} \cap \operatorname{supp}(k_1)\right)}_{I_3} \;\dot{\cup}\; \underbrace{\left(\operatorname{supp}(s) \cap \operatorname{supp}(k_1)\right)}_{I_4} \end{aligned}$$

with $a_1(s,k_1) = |I_1|$, $a_2(s,k_1) = |I_2|$, $a_3(s,k_1) = |I_3|$ and $a_4(s,k_1) = |I_4|$.
$b_1 = \operatorname{wt}(s) = a_2(s,k_1) + a_4(s,k_1)$. Hence the first row of $M(1)$ is $\begin{pmatrix}0 & 1 & 0 & 1\end{pmatrix}$. The second row is given by $\begin{pmatrix}0 & 1 & 1 & 0\end{pmatrix}$ since $\mathrm{d}\,(s,k_1) = a_2(s,k_1) + a_3(s,k_1)$ is the number of positions where k and s_1 have different values. We obtain

$$M(1) = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Now, compare the columns and rows of $M(1)$ with the codewords of $RM(1,1)$ and $RM(1,2)$.

$$RM^0(1,1) = \{(0,0),(0,1)\} \text{ with } (0,0) \sim 0 \preccurlyeq x_1 \sim (0,1)$$

These codewords correspond to the odd numbered columns of $M(1)$. The even numbered columns of $M(1)$ correspond to

$$RM^1(1,1) = \{(1,1),(1,0)\} \text{ with } (1,1) \sim 1 \preccurlyeq 1 + x_1 \sim (1,0).$$

Furthermore the codewords of $RM^0(1,2)$ corresponding to Boolean polynomials with summand x_1 are $x_1 \sim (0,1,0,1)$ and $x_1 + x_2 \sim (0,1,1,0)$ with $x_1 \preccurlyeq x_1 + x_2$. These are the rows of $M(1)$. Hence the assertion holds for $t = 1$.
Assume the assertion is true for $t - 1 \in \mathbb{N}$. When we add another participant T_t with an arbitrary share k_t of the same length than $s, k_1, \ldots, k_{t-1}$, the weight vector $b(s, k_1, \ldots, k_{t-1})$ for $t-1$ participants is extended to the weight vector $b(s, k_1, \ldots, k_t)$ for t participants via

$$\underbrace{\begin{pmatrix} \mathrm{d}\,(s,0) \\ \mathrm{d}\,(s,k_1) \\ \vdots \\ \mathrm{d}\left(s, \sum\limits_{m=1}^{\ell} k_{j_m}\right) \\ \vdots \\ \mathrm{d}\left(s, \sum\limits_{j=1}^{t-1} k_j\right) \end{pmatrix}}_{=b(s,k_1,\ldots,k_{t-1})} \to \underbrace{\left(\begin{array}{c} \mathrm{d}\,(s,0) \\ \mathrm{d}\,(s,k_1) \\ \vdots \\ \mathrm{d}\left(s, \sum\limits_{m=1}^{\ell} k_{j_m}\right) \\ \vdots \\ \mathrm{d}\left(s, \sum\limits_{j=1}^{t-1} k_j\right) \\ \hline \mathrm{d}\,(s,k_t) \\ \mathrm{d}\,(s,k_1+k_t) \\ \vdots \\ \mathrm{d}\left(s, \sum\limits_{m=1}^{\ell} k_{j_m} + k_t\right) \\ \vdots \\ \mathrm{d}\left(s, \sum\limits_{j=1}^{t-1} k_j + k_t\right) \end{array}\right)}_{=b(s,k_1,\ldots,k_t)} .$$

The refined partition $I = I_1^t \;\dot\cup\; \ldots \;\dot\cup\; I_{2^{t+1}}^t$ is represented by

$$\underbrace{\begin{pmatrix} a_1(s,k_1,\ldots,k_{t-1}) \\ \vdots \\ a_{2^t}(s,k_1,\ldots,k_{t-1}) \end{pmatrix}}_{=a(s,k_1,\ldots,k_{t-1})^\tau} \to \underbrace{\left(\begin{array}{c} a_1(s,k_1,\ldots,k_t) \\ \vdots \\ a_{2^t}(s,k_1,\ldots,k_t) \\ \hline a_{2^t+1}(s,k_1,\ldots,k_t) \\ \vdots \\ a_{2^{t+1}}(s,k_1,\ldots,k_t) \end{array}\right)}_{=a(s,k_1,\ldots,k_t)^\tau}$$

with $a_i(s,k_1,\ldots,k_t) + a_{i+2^t}(s,k_1,\ldots,k_t) = a_i(s,k_1,\ldots,k_{t-1})$ for all $i = 1,\ldots,2^t$.

At first we examine the rows of $M(t)$. Let $r_i(t-1)$ denote the ith row of $M(t-1)$ and S_i denotes the ith sum of shares with summands in $\{k_1,\ldots,k_{t-1}\}$, $1 \le i \le 2^{t-1}$. Then

$$r_i(t-1) \cdot (a_1(s,k_1,\ldots,k_{t-1}),\ldots,a_{2^t}(s,k_1,\ldots,k_{t-1}))^\tau \;=\; \mathrm{d}\,(s,S_i)$$

This yields the equations

$$\begin{aligned}
& r_i(t-1)\cdot\left(a_1(s,k_1,\ldots,k_t),\ldots,a_{2^t}(s,k_1,\ldots,k_t)\right)^{\tau} \\
= \;& \mathrm{d}\left(s_{|\overline{\mathrm{supp}(k_t)}}, S_{i|\overline{\mathrm{supp}(k_t)}}\right) \\
= \;& \mathrm{d}\left(s_{|\overline{\mathrm{supp}(k_t)}}, (S_i+k_t)_{|\overline{\mathrm{supp}(k_t)}}\right),
\end{aligned}$$

$$\begin{aligned}
& r_i(t-1)\cdot\left(a_{2^t+1}(s,k_1,\ldots,k_t),\ldots,a_{2^{t+1}}(s,k_1,\ldots,k_t)\right)\tau \\
= \;& \mathrm{d}\left(s_{|\mathrm{supp}(k_t)}, S_{i|\mathrm{supp}(k_t)}\right),
\end{aligned}$$

$$\begin{aligned}
& \overline{r_i(t-1)}\cdot\left(a_{2^t+1}(s,k_1,\ldots,k_t),\ldots,a_{2^{t+1}}(s,k_1,\ldots,k_t)\right)^{\tau} \\
= \;& |\mathrm{supp}(k_t)| - \mathrm{d}\left(s_{|\mathrm{supp}(k_t)}, S_{i|\mathrm{supp}(k_t)}\right) \\
= \;& \mathrm{d}\left(s_{|\mathrm{supp}(k_t)}, \overline{S_{i|\mathrm{supp}(k_t)}}\right) \\
= \;& \mathrm{d}\left(s_{|\mathrm{supp}(k_t)}, S_{i|\mathrm{supp}(k_t)}+k_t\right) \\
= \;& \mathrm{d}\left(s_{|\mathrm{supp}(k_t)}, (S_i+k_t)_{|\mathrm{supp}(k_t)}\right).
\end{aligned}$$

Hence on the one hand the distances $\mathrm{d}\,(s, S_i)$ and $\mathrm{d}\,(s, S_i+k_t)$ can be calculated by

$$\begin{aligned}
& \left(r_i(t-1), r_i(t-1)\right)\cdot\left(a_1(s,k_1,\ldots,k_t),\ldots,a_{2^{t+1}}(s,k_1,\ldots,k_t)\right)^{\tau} \\
= \;& \mathrm{d}\left(s_{|\overline{\mathrm{supp}(k_t)}}, S_{i|\overline{\mathrm{supp}(k_t)}}\right) + \mathrm{d}\left(s_{|\mathrm{supp}(k_t)}, S_{i|\mathrm{supp}(k_t)}\right) \\
= \;& \mathrm{d}\,(s, S_i) = b_i(s,k_1,\ldots,k_t)
\end{aligned}$$

and

$$\begin{aligned}
& \left(r_i(t-1), \overline{r_i(t-1)}\right)\cdot\left(a_1(s,k_1,\ldots,k_t),\ldots,a_{2^{t+1}}(s,k_1,\ldots,k_t)\right)^{\tau} \\
= \;& \mathrm{d}\left(s_{|\overline{\mathrm{supp}(k_t)}}, (S_i+k_t)_{|\overline{\mathrm{supp}(k_t)}}\right) + \mathrm{d}\left(s_{|\mathrm{supp}(k_t)}, (S_i+k_t)_{|\mathrm{supp}(k_t)}\right) \\
= \;& \mathrm{d}\,(s, S_i+k_t) = b_{2^t+i}(s,k_1,\ldots,k_t).
\end{aligned}$$

On the other hand these distances are defined by the scalar products $r_i(t)\cdot a(s,k_1,\ldots,k_t)^{\tau}$ and $r_{i+2^{t-1}}(t)\cdot a(s,k_1,\ldots,k_t)^{\tau}$, where $r_i(t)$ is the ith row and $r_{i+2^t}(t)$ is the $i+2^{t-1}$th row of $M(t)$. Therefore we can assume that the rows of $M(t)$ have the form

$$\begin{aligned}
r_i(t) &= \left(r_i(t-1), r_i(t-1)\right) && \text{for all } 1 \le i \le 2^{t-1} \text{ and} \\
r_i(t) &= \left(r_i(t-1), \overline{r_i(t-1)}\right) && \text{for all } 2^{t-1}+1 \le i \le 2^t.
\end{aligned}$$

This means that the rows of $M(t)$ are given by the Plotkin construction on the rows of $M(t-1)$. By induction the rows of $M(t-1)$ correspond to the words of $RM^0(1,t)$ with summand x_1. Therefore the rows of $M(t)$ correspond to the words of $RM^0(1,t+1)$ with summand x_1 in the desired order.

Let $c_j(t-1)$ denote the jth column of $M(t-1)$. The Plotkin construction on the rows yields a Plotkin construction on the columns. We have

$$\begin{aligned} c_j(t) &= \begin{pmatrix} c_j(t-1) \\ c_j(t-1) \end{pmatrix} \quad \text{and} \\ c_{2^t+j}(t) &= \begin{pmatrix} c_j(t-1) \\ \overline{c_j(t-1)} \end{pmatrix} \quad \text{for all } j = 1, \ldots, 2^t. \end{aligned}$$

Let j be odd. According to our assertion, the column $c_j(t-1)$ belongs to a Boolean polynomial $x_{j_1} + \ldots + x_{j_\ell} \in \mathbb{Z}_2[x_1, \ldots, x_{t-1}]$. As $c_j(t)$ is the repetition of $c_j(t-1)$ it corresponds to the same Boolean polynomial $x_{j_1} + \ldots + x_{j_\ell} \in \mathbb{Z}_2[x_1, \ldots, x_t]$, however defined on t variables. Since $(\underbrace{0, \ldots, 0}_{2^{t-1}}, \underbrace{1, \ldots, 1}_{2^{t-1}}) \sim x_t$ the column $c_{j+2^t}(t)$ belongs to the polynomial $x_{j_1} + \ldots + x_{j_\ell} + x_t \in \mathbb{Z}_2[x_1, \ldots, x_t]$. Therefore the assertion holds for the odd numbered columns. By the same argument the even numbered columns correspond to the codewords of $RM^1(1,t)$ ordered by $\preccurlyeq$: When j is even the column $c_j(t-1)$ is related to a Boolean polynomial $1 + x_{j_1} + \ldots + x_{j_\ell} \in \mathbb{Z}_2[x_1, \ldots, x_{t-1}]$. Hence $c_j(t) = \begin{pmatrix} c_j(t-1) \\ c_j(t-1) \end{pmatrix}$ belongs to the Boolean polynomial $1 + x_{j_1} + \ldots + x_{j_\ell} \in \mathbb{Z}_2[x_1, \ldots, x_t]$ and $c_{2^t+j}(t) = \begin{pmatrix} c_j(t-1) \\ \overline{c_j(t-1)} \end{pmatrix}$ is related to $1 + x_{j_1} + \ldots + x_{j_\ell} + x_t \in \mathbb{Z}_2[x_1, \ldots, x_t]$. □

For abbreviation we denote the submatrix of $M(t)$ consisting of the odd numbered columns with $M(t)^{\text{odd}}$ and the submatrix of the even numbered columns with $M(t)^{\text{even}}$.

Example 4.10. For $t = 3$ participants we have the matrix

$$M(3) = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

The rows are the codewords of $RM^0(1,4)$ corresponding to Boolean polynomials with summand x_1:

$$\begin{pmatrix} x_1 \\ x_1+x_2 \\ x_1+x_3 \\ x_1+x_2+x_3 \\ x_1+x_4 \\ x_1+x_2+x_4 \\ x_1+x_3+x_4 \\ x_1+x_2+x_3+x_4 \end{pmatrix}.$$

The columns of

$$M(3)^{\text{odd}} = \begin{pmatrix} 0&0&0&0&0&0&0&0 \\ 0&1&0&1&0&1&0&1 \\ 0&0&1&1&0&0&1&1 \\ 0&1&1&0&0&1&1&0 \\ 0&0&0&0&1&1&1&1 \\ 0&1&0&1&1&0&1&0 \\ 0&0&1&1&1&1&0&0 \\ 0&1&1&0&1&0&0&1 \end{pmatrix}$$

are the codewords of $RM^0(1,3)$ belonging to the Boolean polynomials

$$(0, x_1, x_2, x_1+x_2, x_3, x_1+x_3, x_2+x_3, x_1+x_2+x_3)$$

and the columns of

$$M(3)^{\text{even}} = \begin{pmatrix} 1&1&1&1&1&1&1&1 \\ 1&0&1&0&1&0&1&0 \\ 1&1&0&0&1&1&0&0 \\ 1&0&0&1&1&0&0&1 \\ 1&1&1&1&0&0&0&0 \\ 1&0&1&0&0&1&0&1 \\ 1&1&0&0&0&0&1&1 \\ 1&0&0&1&0&1&1&0 \end{pmatrix}$$

are the codewords of $RM^1(1,3)$ defined by the Boolean polynomials

$$(1, 1+x_1, 1+x_2, 1+x_1+x_2, 1+x_3, 1+x_1+x_3, 1+x_2+x_3, 1+x_1+x_2+x_3).$$

4.3.4 Simplification of Equation 4.1

In this step we transform Equation 4.1 to make the relation between $a(s, k_1, \ldots, k_t)$ and $b(s, k_1, \ldots, k_t)$ clearer. We use the relation of $M(t)$ to the Reed-Muller code $RM(1,t)$ described in Lemma 4.9. At first we define two more useful matrices.

Definition 4.11.

- $\varepsilon(t) \in \mathcal{M}_{2^t,2^t}(\{0,1\})$ is the matrix whose rows correspond to the codewords of $RM^0(1,t)$ ordered by $\preccurlyeq$ in ascending order (from top to bottom).
- $E(t) \in \mathcal{M}_{2^t,2^t}(\{\pm 1\})$ is the matrix generated by replacing the zeros in $\varepsilon(t)$ by ones and the ones by minus ones. $E_i(t)$ denotes the ith row of $E(t)$ for all $i = 1, \dots, 2^t$.

When the number of participants is clear we omit the parameter t. ε and E have the following properties.

Lemma 4.12. (a) ε and E are symmetric. The columns of ε correspond to the codewords of $RM^0(1,t)$ ordered by $\preccurlyeq$, too. Hence $\varepsilon = M^{\text{odd}}$.

(b) E is invertible as matrix over $\mathbb{Q}$.

(c) $\sum_{i=1}^{2^t} E_i = \big(2^t, 0, \dots, 0\big)$.

(d) $\sum_{i=2}^{2^t} E_i = \big(2^t - 1, -1, \dots, -1\big)$.

Proof. (a) Let p_i denote the ith element of $RM^0(1,t)$ and v_j the jth element of $\mathbb{Z}_2^t$ with respect to the order on $\mathbb{Z}_2^t$ defined in Remark 4.4. Per definition the element of ε in the ith row and jth column is $\varepsilon_{i,j} = p_i(v_j)$ and ε has the form

$$\begin{pmatrix} 0(0,\dots,0) & 0(1,0,\dots,0) & \dots & 0(1,\dots,1) \\ x_1(0,\dots,0) & x_1(1,0,\dots,0) & \dots & x_1(1,\dots,1) \\ x_2(0,\dots,0) & x_2(1,0,\dots,0) & \dots & x_2(1,\dots,1) \\ x_1+x_2(0,\dots,0) & x_1+x_2(1,0,\dots,0) & \dots & x_1+x_2(1,\dots,1) \\ \vdots & \vdots & & \vdots \\ x_1+\dots+x_t(0,\dots,0) & x_1+\dots+x_t(1,0,\dots,0) & \dots & x_1+\dots+x_t(1,\dots,1) \end{pmatrix}.$$

As stated in Remark 4.4, $p_i(v_j) = v_i \cdot v_j^\top = v_j \cdot v_i^\top = p_j(v_i)$. Hence ε is symmetric.

(b) E is invertible since $E \cdot E = 2^t \cdot E_{2^t}$ (where E_{2^t} denotes the identity matrix). With part (a) the diagonal entries are clear since 1 and -1 are the only entries in E. The zeroes come from the fact two different codewords in $RM^0(1,t)$ differ in the half of their entries. (see 3.27 (d))

(c),(d) The first entries are clear since the first column of ε is the zero word. The other columns come from words in $RM^0(1,t) \setminus \{(0\dots0)\}$ which have weight 2^{t-1} and start with a zero. (see 3.27 (c))

□

Example 4.13. For $t = 3$ participants we have

$$\varepsilon(3) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

The rows are related to the Boolean polynomials

$$0,\ x_1,\ x_2,\ x_1 + x_2,\ x_3,\ x_1 + x_3,\ x_2 + x_3\ x_1 + x_2 + x_3.$$

$$E(3) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

Based on these preliminary thoughts we find a simplification of the linear system 4.1.

Lemma 4.14. Let $a = a(s, k_1, \dots, k_t) = (a_1, a_2, \dots, a_{2^{t+1}})$ and $b = b(s, k_1, \dots, k_t)$. Then Equation 4.1 is equivalent to the following system of linear equations:

$$\begin{aligned} \sum_{i=1}^{2^t} a_{2i} &= b_1 \\ a_4 - a_3 &= \frac{1}{2^{t-1}} E_2 \cdot b \\ &\vdots \\ a_{2i} - a_{2i-1} &= \frac{1}{2^{t-1}} E_i \cdot b \\ &\vdots \\ a_{2^{t+1}} - a_{2^{t+1}-1} &= \frac{1}{2^{t-1}} E_{2^t} \cdot b. \end{aligned} \tag{4.2}$$

Proof. Let $a^{\text{odd}} = (a_1, a_3, \dots, a_{2^{t+1}-1})$ and $a^{\text{even}} = (a_2, a_4, \dots, a_{2^{t+1}})$. Then

$$\begin{aligned} & & M \cdot a^\tau &= b \\ \Leftrightarrow & & M^{\text{odd}} \cdot (a^{\text{odd}})^\tau + M^{\text{even}} \cdot (a^{\text{even}})^\tau &= b \\ \Leftrightarrow & & E \cdot M^{\text{odd}} \cdot (a^{\text{odd}})^\tau + E \cdot M^{\text{even}} \cdot (a^{\text{even}})^\tau &= E \cdot b \end{aligned} \tag{4.3}$$

Since E is invertible (see Lemma 4.12 (b)) the last two equations are equivalent. Next we compute the matrices $E \cdot M^{\text{odd}}$ and $E \cdot M^{\text{even}}$ separately using the information about the columns of M given in Lemma 4.9 and the properties of first order Reed-Muller codes stated in 3.27.

- For $j = 1, \ldots, 2^t$ let M_j^{odd} denote the jth column of M^{odd}. Then M_j^{odd} corresponds to the jth element of $RM^0(1,t)$. The ith row E_i of E corresponds to the ith element of $RM^0(1,t)$. Now we calculate all scalar products $E_i \cdot M_j^{\text{odd}}$. We have to distinguish four cases.

  1. $j = 1$.
  $$E_i \cdot M_1^{\text{odd}} = E_i \cdot (0, \ldots, 0)^\tau = 0$$

  2. $i = 1$, $j \neq 1$.
  $$E_1 \cdot M_j^{\text{odd}} = (1, \ldots, 1) \cdot M_j^{\text{odd}} = \text{wt}\left(M_j^{\text{odd}}\right) = 2^{t-1}$$
  since all codewords in $RM^0(1,t)$ except for the zero vector have weight 2^{t-1}.

  3. Let $i, j \neq 1$, $i \neq j$. E_i has the values ± 1 and M_j^{odd} has the values 0 and 1. Therefore each multiplication during the calculation of $E_i \cdot M_j^{\text{odd}}$ has the form $1 \cdot 0$, $-1 \cdot 0$, $1 \cdot 1$ or $-1 \cdot 1$. In this case E_i and M_j^{odd} correspond to different nonzero codewords in $RM^0(1,t)$. These codewords have both 2^{t-1} times the value 0 and 2^{t-1} times the value 1 such that they coincide exactly in 2^{t-2} positions with value 0 and 1, respectively. This yields

E_i	1	-1	1	-1
M_j^{odd}	0	0	1	1
#	2^{t-2}	2^{t-2}	2^{t-2}	2^{t-2}

  .

  where # denotes the number of positions with the specified combinations. Thus
  $$E_i \cdot M_j^{\text{odd}} = 2^{t-2} - 2^{t-2} = 0.$$

  4. Let $i = j \neq 1$. Then E_i and M_j^{odd} belong to the same nonzero codeword of $RM^0(1,t)$ and we have

E_i	1	-1	1	-1
M_i^{odd}	0	0	1	1
#	2^{t-1}	0	0	2^{t-1}

  .

Therefore

$$E_i \cdot M_i^{\text{odd}} = -2^{t-1}.$$

This yields

$$E \cdot M^{\text{odd}} = \left(\begin{array}{c|cccc} 0 & 2^{t-1} & & \dots & 2^{t-1} \\ \hline 0 & -2^{t-1} & & & \\ \vdots & & & \ddots & \\ 0 & & & & -2^{t-1} \end{array} \right).$$

- For $j = 1, \dots, 2^t$ let M_j^{even} denote the jth column of M^{even}. Then M_j^{even} corresponds to the jth element of $RM^1(1,t)$. Again we calculate all scalar products $E_i \cdot M_j^{\text{even}}$. There are five different cases.

  1. $i = j = 1$.
  $$E_1 \cdot M_1^{\text{even}} = (1, \dots, 1) \cdot (1, \dots, 1)^\tau = 2^t$$

  2. $i \neq 1$, $j = 1$.
  $$E_i \cdot M_1^{\text{even}} = E_i \cdot (1, \dots, 1)^\tau = 0$$
  since E_i has exactly 2^{t-1} ones and 2^{t-1} minus ones.

  3. $i = 1$, $j \neq 1$.
  $$E_1 \cdot M_j^{\text{even}} = (1, \dots, 1) \cdot M_j^{\text{even}} = \text{wt}\left(M_j^{\text{even}}\right) = 2^{t-1}$$
  since all codewords in $RM^1(1,t) \setminus \{(1, \dots, 1)\}$ have the weight 2^{t-1}.

  4. Let $i, j \neq 1$, $i \neq j$. Then the vectors E_i and M_j^{even} belong to different codewords in $c, d \in RM(1,t) \setminus \{(0, \dots, 0), (1, \dots, 1)\}$ with $c \neq \overline{d}$. This yields

E_i	1	-1	1	-1
M_j^{even}	0	0	1	1
#	2^{t-2}	2^{t-2}	2^{t-2}	2^{t-2}

  and
  $$E_i \cdot M_j^{\text{even}} = 2^{t-2} - 2^{t-2} = 0.$$

  5. Let $i = j \neq 1$. Then there is a polynomial $p \in \mathbb{Z}_2[x_1, \dots, x_t]$ of degree one without the summand 1 such that E_i is related to p and $M_i^{\text{even}} \sim 1 + p$. p and $1 + p$ have exactly 2^{t-1} times the value 0 and the value 1 and differ for all inputs. Therefore

E_i	1	-1	1	-1
M_i^{even}	0	0	1	1
#	0	2^{t-1}	2^{t-1}	0

  and
  $$E_i \cdot M_i^{\text{even}} = 2^{t-1}.$$

We obtain

$$E \cdot M^{\text{even}} = \left(\begin{array}{c|ccc} 2^t & 2^{t-1} & \dots & 2^{t-1} \\ \cline{2-4} 0 & 2^{t-1} & & \\ \vdots & & \ddots & \\ 0 & & & 2^{t-1} \end{array}\right).$$

Using these results on $E \cdot M^{\text{odd}}$ and $E \cdot M^{\text{even}}$, Equation 4.3 is equivalent to

$$\begin{pmatrix} 2^{t-1} \cdot \sum_{i=2}^{2^t} a_i^{\text{odd}} \\ -2^{t-1} a_2^{\text{odd}} \\ \vdots \\ -2^{t-1} a_{2^t}^{\text{odd}} \end{pmatrix} + \begin{pmatrix} 2^{t-1} \left(a_1^{\text{even}} + \sum_{i=1}^{2^t} a_i^{\text{even}} \right) \\ 2^{t-1} a_2^{\text{even}} \\ \vdots \\ 2^{t-1} a_{2^t}^{\text{even}} \end{pmatrix} = \begin{pmatrix} E_1 \cdot b \\ E_2 \cdot b \\ \vdots \\ E_{2^t} \cdot b \end{pmatrix}.$$

Replace the first row by the sum of all rows. Then

$$\begin{pmatrix} 0 \\ -2^{t-1} a_2^{\text{odd}} \\ \vdots \\ -2^{t-1} a_{2^t}^{\text{odd}} \end{pmatrix} + \begin{pmatrix} 2^t \cdot \sum_{i=1}^{2^t} a_i^{\text{even}} \\ 2^{t-1} a_2^{\text{even}} \\ \vdots \\ 2^{t-1} a_{2^t}^{\text{even}} \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^{2^t} E_i \cdot b \\ E_2 \cdot b \\ \vdots \\ E_{2^t} \cdot b \end{pmatrix}.$$

According to Lemma 4.12 (c), this is equivalent to

$$\begin{pmatrix} \sum_{i=1}^{2^t} a_{2i} \\ 2^{t-1} (a_4 - a_3) \\ \vdots \\ 2^{t-1} (a_{2^{t+1}} - a_{2^{t+1}-1}) \end{pmatrix} = \begin{pmatrix} b_1 \\ E_2 \cdot b \\ \vdots \\ E_{2^t} \cdot b \end{pmatrix}.$$

□

Example 4.15. Consider a scheme on $t = 3$ participants.

$$E \cdot M^{\text{odd}} \cdot (a^{\text{odd}})^\tau + E \cdot M^{\text{even}} \cdot (a^{\text{even}})^\tau$$

$$= \begin{pmatrix} 0 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 0 & -4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -4 \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_3 \\ a_5 \\ a_7 \\ a_9 \\ a_{11} \\ a_{13} \\ a_{15} \end{pmatrix} + \begin{pmatrix} 8 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix} \cdot \begin{pmatrix} a_2 \\ a_4 \\ a_6 \\ a_8 \\ a_{10} \\ a_{12} \\ a_{14} \\ a_{16} \end{pmatrix} \to \begin{pmatrix} \sum_{j=1}^{8} a_{2j} \\ 4(a_4 - a_3) \\ 4(a_6 - a_5) \\ 4(a_8 - a_7) \\ 4(a_{10} - a_9) \\ 4(a_{12} - a_{11}) \\ 4(a_{14} - a_{13}) \\ 4(a_{16} - a_{15}) \end{pmatrix}$$

$$E \cdot b$$

$$= \begin{pmatrix} b_1+b_2+b_3+b_4+b_5+b_6+b_7+b_8 \\ b_1-b_2+b_3-b_4+b_5-b_6+b_7-b_8 \\ b_1+b_2-b_3-b_4+b_5+b_6-b_7-b_8 \\ b_1-b_2-b_3+b_4+b_5-b_6-b_7+b_8 \\ b_1+b_2+b_3+b_4-b_5-b_6-b_7-b_8 \\ b_1-b_2+b_3-b_4-b_5+b_6-b_7+b_8 \\ b_1+b_2-b_3-b_4-b_5-b_6+b_7+b_8 \\ b_1-b_2-b_3+b_4-b_5+b_6+b_7-b_8 \end{pmatrix} \rightarrow \begin{pmatrix} b_1 \\ b_1-b_2+b_3-b_4+b_5-b_6+b_7-b_8 \\ b_1+b_2-b_3-b_4+b_5+b_6-b_7-b_8 \\ b_1-b_2-b_3+b_4+b_5-b_6-b_7+b_8 \\ b_1+b_2+b_3+b_4-b_5-b_6-b_7-b_8 \\ b_1-b_2+b_3-b_4-b_5+b_6-b_7+b_8 \\ b_1+b_2-b_3-b_4-b_5-b_6+b_7+b_8 \\ b_1-b_2-b_3+b_4-b_5+b_6+b_7-b_8 \end{pmatrix}$$

We obtain the equations

$$a_2+a_4+a_6+a_8+a_{10}+a_{12}+a_{14}+a_{16} = b_1 \qquad \text{and}$$

$$\begin{aligned} a_4-a_3 &= \frac{1}{4}(b_1-b_2+b_3-b_4+b_5-b_6+b_7-b_8) \\ a_6-a_5 &= \frac{1}{4}(b_1+b_2-b_3-b_4+b_5+b_6-b_7-b_8) \\ a_8-a_7 &= \frac{1}{4}(b_1-b_2-b_3+b_4+b_5-b_6-b_7+b_8) \\ a_{10}-a_9 &= \frac{1}{4}(b_1+b_2+b_3+b_4-b_5-b_6-b_7-b_8) \\ a_{12}-a_{11} &= \frac{1}{4}(b_1-b_2+b_3-b_4-b_5+b_6-b_7+b_8) \\ a_{14}-a_{13} &= \frac{1}{4}(b_1+b_2-b_3-b_4-b_5-b_6+b_7+b_8) \\ a_{16}-a_{15} &= \frac{1}{4}(b_1-b_2-b_3+b_4-b_5+b_6+b_7-b_8). \end{aligned}$$

Remark 4.16. (a) We are only interested in solutions $a \in \mathbb{N}_0^{2^{t+1}}$ for Equation 4.2 because the a_i represent the cardinalities of the sets I_i^t and cannot be negative.

(b) a_1 is the number of all positions where the secret and all shares have the value zero. These positions still contain only zeros when sums of shares are considered. Hence a_1 has no effect on the distances of these sums to the secret and on whether a group of participants is authorized or not. That is why a_1 does not appear in the system of linear equations 4.2. a_1 can be regarded as a free parameter which can be used to adjust to a given code length $n \geq \underbrace{\sum_{i=1}^{2^t} a_{2i}}_{b_1} + \sum_{i=2}^{2^t} a_{2i-1}$.

So far we expressed the structure of the shares in terms of the cardinalities $a_1, \ldots,$ $a_{2^{t+1}}$ of sets determined by the supports of the shares and the secret. Furthermore we found out that for a given secret s the distance vector $b(s, k_1, \ldots, k_t)$ is possible if there is a solution $(a_1, \dots, a_{2^{t+1}}) \in \mathbb{N}_0^{2^{t+1}}$ of the system of linear equations in 4.2. This solution determines the shares uniquely up to the order of their entries.

4.4 The Existence of an Universal Realization

In this section we show that *any* access structure can be realized using our construction. For the sake of simplicity we restrict ourselves to the case that there are only two possible distances from the sums to the secret: one small distance k and one large distance g. When a set of participants is authorized the distance of the related sum to the secret shall be k. Otherwise we want the distance to be g. We develop non-negative integer solutions of Equation 4.2 for such distance vectors.

Remark 4.17. Suppose that $\mathcal{C}$ is a binary code with length n and minimum distance d. Let $s \in \mathcal{C}$ be the secret to be shared with our construction.

(a) The secret s is a codeword in $\mathcal{C}$. Therefore its weight b_1 has to be at least as large as the minimum weight of $\mathcal{C}$.

(b) When the small distance k fulfills the inequality $d \geq 2k + 1$, then k does not exceed the error-correction capacity of $\mathcal{C}$. That guarantees that the secret is the codeword lying next to the sum of the shares of each authorized set. Using Hamming decoding the secret can be found and condition 1 from Section 4.2 is fulfilled.

(c) The large distance g can be regarded as the *security distance* of our scheme. It is the number of positions in which the sum of the shares of each unauthorized subset differ from the secret and has to be larger than the error-correction capability. Hence we require $g > \left\lfloor \frac{d-1}{2} \right\rfloor$. This condition is necessary, but not sufficient, to guarantee that no unauthorized set is able to reconstruct the secret using Hamming decoding. Depending on the structure of $\mathcal{C}$, the secret may still be the codeword next to the sum of the shares. Condition 2 from Section 4.2 is definitely met when, for instance, g exceeds the covering radius of $\mathcal{C}$.

In the following we show that for all access structures there are suitable codes and distances $b_1, k, g \in \mathbb{N}$ depending only on the number t of the participants such that for all codewords s with weight b_1 there are shares $k_1, \dots, k_t \in \mathbb{Z}_2^n$ with the following properties:

- $b_j = \mathrm{d}(s, S_j) = k$ if the jth set in $\mathcal{P}(\mathcal{T})$ is authorized. S_j denotes the jth sum of shares which belong to the jth set of participants.
- $b_j = \mathrm{d}(s, S_j) = g > k$ if the jth set in $\mathcal{P}(\mathcal{T})$ is unauthorized.

$b = (b_1, \dots, b_{2^t})^\tau$ is the distance vector $b(s, k_1, \dots, k_t)$. Using specific values for n, b_1, g and k we prove the existence of a solution $a = (a_1, \dots, a_{2^{t+1}}) \in \mathbb{N}_0^{2^{t+1}}$ for the linear system 4.2. Since $a_i = |I_i^t|$ for all $i = 1, \ldots, 2^{t+1}$, these solutions determine suitable shares $k_1, \ldots, k_t$ uniquely up to permutations of the positions.

Unfortunately the price for this generality is a large word length n and a relatively small security distance g. Later we will see that special classes of access structures allow choices of b_1, g and k which have significantly more efficient and secure realizations.

4.4.1 First Definitions

The linear system 4.2 states requirements for the *differences* $a_{2i} - a_{2i-1}$, $i = 2, \ldots, 2^t$, and not for the single a_i. Thus, for the sake of simplicity, we can consider solutions with $a_{2i} = 0$ or $a_{2i-1} = 0$.

Definition 4.18. Let Γ be an arbitrary access structure on t participants and let $b_1, g \in \mathbb{N}$ and $k \in \mathbb{N}_0$ such that $b_1, g > k$.

(a) The distance vector $b = (b_1, b_2, \ldots, b_{2^t})^\tau$ defined by

$$b_j = \begin{cases} k & \text{if the } j\text{th subset of } \mathcal{T} \text{ is authorized} \\ g & \text{if the } j\text{th subset of } \mathcal{T} \text{ is unauthorized} \end{cases} \quad \text{for all } j = 2, 3, \ldots, 2^t.$$

is called *elementary distance vector for* Γ *with respect to* (b_1, g, k).

(b) Consider the system of linear equations 4.2:

$$\begin{aligned} \sum_{i=1}^{2^t} a_{2i} &= b_1 \\ a_{2i} - a_{2i-1} &= \frac{1}{2^{t-1}} E_i \cdot b \quad \text{for all } i = 2, 3, \ldots, 2^t \end{aligned}$$

For $i = 2, 3, \ldots, 2^t$ let

$$a_{2i} = \frac{1}{2^{t-1}} E_i \cdot b \text{ and } a_{2i-1} = 0 \text{ if } \frac{1}{2^{t-1}} E_i \cdot b > 0$$

and

$$a_{2i} = 0 \text{ and } a_{2i-1} = -\frac{1}{2^{t-1}} E_i \cdot b \text{ if } \frac{1}{2^{t-1}} E_i \cdot b \le 0.$$

Then $a_3, \ldots, a_{2^{t+1}} \in \mathbb{N}_0$ solve all equations of 4.2 but the first one. If additionally the inequality

$$\sum_{i=2}^{2^t} a_{2i} \le b_1$$

holds, we define $a_2 = b_1 - \sum_{i=2}^{2^t} a_{2i} \ge 0$ and obtain a solution $(a_2, a_3, \ldots, a_{2^{t+1}}) \in \mathbb{N}_0^{2^{t+1}-1}$ for all equations of 4.2. In this case we say that (b_1, g, k) *realizes* Γ *elementarily* and call $(a_2, a_3, \ldots, a_{2^{t+1}})$ an *elementary solution for* (Γ, b_1, g, k).

Now we have a look at the structure of $E \cdot b$ for an elementary distance vector b with respect to arbitrary parameters b_1, g, k. The following lemma gives us three important properties.

Lemma 4.19. Let Γ be an access structure on t participants and let $b = (b_1, b_2, \ldots, b_{2^t})^\tau$ be an elementary distance vector for Γ with respect to (b_1, g, k). Suppose that there are u non-empty unauthorized sets. Let E_i denote the ith row of the matrix $E(t)$. Define c_i to be the number of ones in E_i being multiplied with g while calculating $E_i \cdot b$ and d_i to be the number of minus ones being multiplied with g . Then

(a) $E_i \cdot b = b_1 - k + (2c_i - u)(g - k) = b_1 - k + (u - 2d_i)(g - k)$ for all $i = 2, 3, \ldots, 2^t$

(b) $\sum\limits_{i=2}^{2^t} E_i \cdot b = (2^t - 1)(b_1 - k) - u(g - k)$

(c) $2c_i - u \geq -2^{t-1}$ for all $i = 2, 3, \ldots, 2^t$

Proof. (a) By construction each row E_i, $i \geq 2$, consists of 2^{t-1} ones and 2^{t-1} minus ones and starts with one. Therefore

$$\begin{aligned} E_i \cdot b &= b_1 + c_i \cdot g - (u - c_i)g + (2^{t-1} - c_i - 1)k - (2^{t-1} - (u - c_i))k \\ &= b_1 - k + (2c_i - u)(g - k) \\ &= b_1 - k + (u - 2d_i)(g - k) \quad \text{since } c_i = u - d_i \end{aligned}$$

(b) Lemma 4.12 (d) yields

$$\sum_{i=2}^{2^t} E_i \cdot b = (2^t - 1)b_1 - ug - (2^t - u - 1)k = (2^t - 1)(b_1 - k) - u(g - k).$$

(c) Let $i \geq 2$. If $u < 2^{t-1}$, the smallest possible value for c_i is 0 since each row E_i contains exactly 2^{t-1} ones and we have

$$2c_i - u \geq -u > -2^{t-1}.$$

If $u \geq 2^{t-1}$, we write $u = 2^{t-1} + u'$ for a suitable $0 \leq u' < 2^{t-1}$. Since E_i contains 2^{t-1} ones and 2^{t-1} minus ones, c_i is at least u'. This yields

$$2c_i - u \geq 2u' - u = u' - 2^{t-1} \geq -2^{t-1}.$$ □

Next we specify what we mean by a “suitable” code.

Definition 4.20. Let $\mathcal{C}$ be a binary code with length n. Suppose that $(a_2, \ldots, a_{2^{t+1}})$ is a (not necessary elementary) solution for the linear system 4.2 with respect to an access structure Γ and a distance vector $b = (b_1, \ldots, b_{2^t})^\tau$. Then $\mathcal{C}$ is called *suitable for* (s, Γ, b) iff

(a) s is a codeword in $\mathcal{C}$ with weight b_1.

(b) The inequality

$$n \geq b_1 + \sum_{i=2}^{2^t} a_{2i-1}$$

holds.

(c) There are shares $k_1, \ldots, k_t$ defined by $(a_2, \ldots, a_{2^{t+1}})$ and s with the following properties: For all $j = 2, 3, \ldots, 2^t$ let S_j be the sum of the shares of the jth set A_j in $\mathcal{P}(\mathcal{T})$.

i. When A_j is authorized, then

$$\mathrm{d}\,(s, S_j) = b_j$$

and there is no other codeword $c \in \mathcal{C}$ with $\mathrm{d}\,(c, S) \leq b_j$.

ii. When A_j is unauthorized, then

$$\mathrm{d}\,(s, S_j) = b_j$$

and there is at least one other codeword $c \in \mathcal{C}$ with

$$\mathrm{d}\,(c, S_j) < \mathrm{d}\,(s, S_j)\,.$$

We define $a_1 = n - b_1 - \sum_{i=2}^{2^t} a_{2i-1}$ and call $(a_1, a_2, \ldots, a_{2^{t+1}}) \in \mathbb{N}_0^{2^{t+1}}$ a *solution for* (Γ, b) *with respect to* $\mathcal{C}$.
If additionally b is an elementary distance vector for Γ with respect to (b_1, g, k) and $(a_2, \ldots, a_{2^{t+1}})$ is an elementary solution for (Γ, b_1, g, k), we say that $\mathcal{C}$ *is suitable for* (s, Γ, b_1, g, k) and call $(a_1, a_2, \ldots, a_{2^{t+1}}) \in \mathbb{N}_0^{2^{t+1}}$ an *elementary solution for* (Γ, b_1, g, k) *with respect to* $\mathcal{C}$.

Remark 4.21. (a) When $\mathcal{C}$ is suitable for (s, Γ, b), s can be shared with our construction such that the conditions 1. and 2. of section 4.2 are fulfilled.

(b) Let $u \leq 2^t - 1$ be the number of the non-empty unauthorized sets and $g \leq b_1$. When $(a_2, \ldots, a_{2^{t+1}})$ is an elementary solution for (Γ, b_1, g, k), condition (b) in Definition 4.20 is definitely fulfilled when $n \geq 2b_1 - a_2$ holds: The equation

$$\begin{aligned} \underbrace{\sum_{i=2}^{2^t} a_{2i}}_{b_1 - a_2} - \sum_{i=2}^{2^t} a_{2i-1} &= \sum_{i=2}^{2^t} (a_{2i} - a_{2i-1}) \\ &= \frac{1}{2^{t-1}} \big((2^t - 1)(b_1 - k) - u(g - k) \big) \quad \text{(see Lemma 4.19 (b))} \end{aligned}$$

yields

$$\sum_{i=2}^{2^t} a_{2i-1} = b_1 - a_2 - \frac{1}{2^{t-1}}\Big((2^t-1)(b_1-k) - \underbrace{u}_{\leq 2^t-1}\underbrace{(g-k)}_{\leq(b_1-k)}\Big) \leq b_1 - a_2.$$

That means $n \geq 2b_1 - a_2 \geq b_1 + \sum_{i=2}^{2^t} a_{2i-1}$.

(c) For all $j = 2, 3, \ldots, 2^t$ let A_j be the jth set in $\mathcal{P}(\mathcal{T})$. Define

$$k^* = \max_{A_j \in \Gamma}\{b_j\} \text{ and } g^* = \min_{A_j \in \overline{\Gamma}}\{b_j\}.$$

i. The first requirement of condition (c) in Definition 4.20 is fulfilled when the minimum distance $d(\mathcal{C})$ satisfies $2k^*+1 \leq d(\mathcal{C})$. In this case the maximum error k^* does not exceed the error-correction capability of $\mathcal{C}$.

ii. The second requirement of condition (c) in Definition 4.20 is fulfilled when the minimum security distance g^* is larger than the covering radius $\rho(\mathcal{C})$.

4.4.2 The Universal Realization

Now we are ready to state our main theorem about the existence of an universal elementary realization (b_1, g, k) depending only on the number t of the involved participants, which can be used for all access structures. Furthermore we prove the existence of suitable binary codes for these realizations.

Theorem 4.22. Let $t \in \mathbb{N}$ be arbitrary and Γ an arbitrary access structure on t participants.

(a) Suppose that the parameters b_1, g, k have the following properties.

- $b_1 \in \mathbb{N}$, $b_1 \geq 2^{2t} - 2^t$ such that $2^t \mid b_1$
- $k = \frac{b_1}{2} - 2^{t-1}$
- $g \in \mathbb{N}$, $\frac{b_1}{2} < g \leq b_1\left(\frac{1}{2} + \frac{1}{2^t}\right) - 2^{t-1}$ such that $2^{t-1} \mid g$

Then (b_1, g, k) realizes Γ elementarily.

(b) Let b_1, g, k be defined as in part (a) and let $\mathcal{C}$ be an arbitrary binary (not necessary linear) code with minimum distance $d(\mathcal{C}) = b_1$ which contains the zero word. Then $\mathcal{C}$ is suitable for (s, Γ, b_1, g, k) for all codewords $s \in \mathcal{C}$ with weight b_1.

It will turn out that the conditions stated in part (a) are sufficient, but generally not necessary (see Example 5.23).

Proof. (a) With the results and notations from Lemma 4.19 (a) Equation 4.2 can be written as

$$\begin{array}{rcl} E\cdot b & = & E\cdot M^{\text{odd}}\cdot(a^{\text{odd}})^\tau + E\cdot M^{\text{even}}\cdot(a^{\text{even}})^\tau \\ \Leftrightarrow \begin{pmatrix} b_1 \\ \\ b_1-k+(2c_2-u)(g-k) \\ \vdots \\ b_1-k+(2c_i-u)(g-k) \\ \vdots \\ b_1-k+(2c_{2^t}-u)(g-k) \end{pmatrix} & = & \begin{pmatrix} \sum\limits_{i=1}^{2^t} a_{2i} \\ \\ 2^{t-1}\,(a_4-a_3) \\ \vdots \\ 2^{t-1}\,(a_{2i}-a_{2i-1}) \\ \vdots \\ 2^{t-1}\,(a_{2^{t+1}}-a_{2^{t+1}-1}) \end{pmatrix} \end{array}.$$

Hence for all $i \geq 2$ the following inequality holds

$$\begin{array}{rcll} b_1-k+(2c_i-u)(g-k) & \geq & b_1-k-2^{t-1}(g-k) & \text{(Lemma 4.19 (c))} \\ & \geq & b_1-k-2^{t-1}\cdot\dfrac{b_1}{2^t} & \text{since } g-k\leq\dfrac{b_1}{2^t} \\ & = & \dfrac{b_1}{2}-k & \\ & = & 2^{t-1}>0 & \text{as } k=\dfrac{b_1}{2}-2^{t-1}. \end{array}$$

That means $a_{2i}-a_{2i-1}=\frac{1}{2^{t-1}}\left(b_1-k+(2c_i-u)(g-k)\right)>0$ for all $i\geq 2$. We obtain an elementary solution by choosing

$$a_{2i}=\frac{1}{2^{t-1}}\left(b_1-k+(2c_i-u)(g-k)\right) \text{ and } a_{2i-1}=0 \text{ for all } i\geq 2.$$

(Note that $a_j\in\mathbb{N}_0$ for all $j=3,4,\ldots,2^{t+1}$ since $2^{t-1}\mid(b_1-k)$ and $2^{t-1}\mid(g-k)$.)
Next we show that the inequality $\sum\limits_{i=1}^{2^t} a_{2i}\leq b_1$ holds.

$$\begin{array}{rcll} \sum\limits_{i=1}^{2^t} a_{2i} & = & a_2+\dfrac{1}{2^{t-1}}\sum\limits_{i=2}^{2^t}\left(b_1-k+(2c_i-u)(g-k)\right) & \\ & = & a_2+\dfrac{1}{2^{t-1}}\big((2^t-1)(b_1-k)-u(g-k)\big) & \text{(Lemma 4.19 (b))} \\ & = & a_2+2b_1-\dfrac{1}{2^{t-1}}\left(b_1+ug+\left(2^t-u-1\right)k\right) & \end{array}$$

Since the sum $\sum\limits_{i=1}^{2^t} a_{2i}$ has to be b_1 and a_2 cannot be negative the following inequality has to be satisfied.

$$\begin{array}{rcl} \underbrace{\dfrac{1}{2^{t-1}}\left(b_1+ug+\left(2^t-u-1\right)k\right)-b_1}_{a_2} & \geq & 0 \\ \Leftrightarrow \qquad u(g-k) & \geq & (2^{t-1}-1)\,b_1-(2^t-1)\,k \end{array}$$

If this equation holds for $u = 0$ it holds for all $u \geq 0$. For $u = 0$ we have

$$\begin{aligned} 0 &\geq \left(2^{t-1} - 1\right) b_1 - \left(2^t - 1\right) k \\ &= \left(2^{t-1} - 1\right) b_1 - \left(2^t - 1\right) \left(\frac{b_1}{2} - 2^{t-1}\right) \\ &= -\frac{b_1}{2} + 2^{t-1}(2^t - 1) \end{aligned}$$

which is true for $b_1 \geq 2^{2t} - 2^t$. We define $a_2 = b_1 - \sum_{i=2}^{2^t} a_{2i}$ and obtain the elementary solution $(a_2, a_3, \ldots, a_{2^{t+1}})$ for (Γ, b_1, g, k).

(b) According to part (a), the parameters b_1, g, k provide an elementary solution $(a_2, a_3, \ldots, a_{2^{t+1}})$ for (Γ, b_1, g, k) where all odd numbered components are zero. Let $\mathcal{C}$ be a binary code with $d(\mathcal{C}) = b_1$ and let $s \in \mathcal{C}$ be a codeword with weight b_1. This fulfills condition (a) of Definition 4.20. The code length n has to be at least the minimum distance b_1. This length is sufficient since

$$n \geq b_1 = \underbrace{\sum_{i=1}^{2^t} a_{2i}}_{=b_1} + \sum_{i=2}^{2^t} \underbrace{a_{2i-1}}_{=0}.$$

Thus condition (b) of Definition 4.20 is fulfilled. Furthermore the first part of condition (c) is fulfilled since

$$d(\mathcal{C}) = b_1 > b_1 - 2^t = 2k + 1$$

(see Remark 4.21 (c)). Now let $a_1 = n - b_1$ and consider shares $k_1, \ldots, k_t$ given by $(a_1, a_2, \ldots, a_{2^{t+1}})$. Since all odd numbered components of the elementary solution $(a_2, a_3, \ldots, a_{2^{t+1}})$ are zero there are no positions where s has the value zero and one of the shares or a share sum has the value one. Let S be the share sum of an arbitrary unauthorized set. Then there are exactly $g > \frac{b_1}{2}$ positions where s and S differ. In these positions s has the value one and S has the value zero. Hence S has the weight $b_1 - g < \frac{b_1}{2}$ and Hamming decoding yields the zero word.

□

Example 4.23. The following parameters fulfill the conditions of Theorem 4.22 (a):

$$b_1 = 2^{2t}, \; k = 2^{2t-1} - 2^{t-1} \text{ and } g = 2^{2t-1} + 2^{t-1}.$$

A possible suitable code for the universal realization is the following.

Corollary 4.24. Let $a \in \mathbb{N}$, $a \geq 2t$. Choose

- $b_1 = 2^a$
- $k = \frac{b_1}{2} - 2^{t-1} = 2^{a-1} - 2^{t-1}$
- $g = b_1 \left(\frac{1}{2} + \frac{1}{2^t}\right) - 2^{t-1} = 2^{a-1} + 2^{a-t} - 2^{t-1}$
- $\mathcal{C} = RM(1, a+1)$

Then $\mathcal{C}$ is suitable for (s, Γ, b_1, g, k) for all access structures Γ on t participants and all codewords $s \in \mathcal{C} \setminus \{(0, \ldots, 0), (1, \ldots, 1)\}$.

Proof. b_1, g, k fulfill the conditions of Theorem 4.22 (a). $\mathcal{C}$ has minimum distance $d = b_1$, contains the zero word and all codewords $s \in \mathcal{C} \setminus \{(0, \ldots, 0), (1, \ldots, 1)\}$ have the weight $b_1 = 2^a$. Hence condition (b) is also met. □

Example 4.25. For $t = 3$ participants let

$$\Gamma = \{\{T_1\}, \{T_3\}, \{T_1, T_2\}, \{T_2, T_3\}\}.$$

The non-empty unauthorized sets are

$$\{T_2\}, \{T_1, T_3\}, \{T_1, T_2, T_3\}.$$

These are the 3rd, the 6th, and the 8th element of $\mathcal{P}(\mathcal{T})$. Define the parameters b_1, g, k as in Example 4.23:

$$b_1 = 2^{2t} = 64, \ k = \frac{b_1}{2} - 2^{t-1} = 28, \ g = \frac{b_1}{2} + \frac{b_1}{2^t} - 2^{t-1} = 36.$$

The corresponding distance vector is given by

$$b = \big(64, 28, \underset{\overset{\uparrow}{3}}{36}, 28, 28, \underset{\overset{\uparrow}{6}}{36}, 28, \underset{\overset{\uparrow}{8}}{36}\big)^\tau.$$

Since

$$\frac{1}{4} \cdot E \cdot b = (71, 7, 7, 7, 7, 15, 7, 7)^\tau$$

we are looking for an elementary solution $a = (a_1, \ldots, a_{16}) \in \mathbb{N}_0^{16}$ such that

$$\begin{aligned} a_2 + a_4 + \ldots + a_{16} &= 64 \\ a_4 - a_3 &= 7 \\ a_6 - a_5 &= 7 \\ a_8 - a_7 &= 7 \\ a_{10} - a_9 &= 7 \\ a_{12} - a_{11} &= 15 \\ a_{14} - a_{13} &= 7 \\ a_{16} - a_{15} &= 7. \end{aligned}$$

We define

$$\begin{aligned} a_2 = a_4 = a_6 = a_8 = a_{10} = a_{14} = a_{16} &= 7 \\ a_3 = a_5 = a_7 = a_9 = a_{11} = a_{13} = a_{15} &= 0 \\ a_{12} = 15. \end{aligned}$$

As in Corollary 4.24 for $a = 2t = 6$ we choose the binary code

$$\mathcal{C} = RM(1, a+1) = RM(1, 7).$$

The code length is $n = 128$ and we have to choose $a_1 = 64$. Let

$$\begin{array}{rcllllllll} s & = & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 \\ & & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 \\ & & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 \\ & & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & \in \mathcal{C}. \end{array}$$

the secret to be shared. Next we construct the shares.

- $$a_1 = |I_1^3| = \left|\overline{\text{supp}(s)} \cap \overline{\text{supp}(k_1)} \cap \overline{\text{supp}(k_2)} \cap \overline{\text{supp}(k_3)}\right| = 64$$

  means that s, k_1, k_2 and k_3 have all the value zero in exactly 64 positions.

- $$I_1^3 \cup I_3^3 \cup I_5^3 \cup I_7^3 \cup I_9^3 \cup I_{11}^3 \cup I_{13}^3 \cup I_{15}^3 = \overline{\text{supp}(s)}$$

  Therefore $a_3 = a_5 = a_7 = a_9 = a_{11} = a_{13} = a_{15} = 0$ means that there are no positions with zeros in s and a one in one of the shares.

- $$a_2 = |I_2^3| = \left|\text{supp}(s) \cap \overline{\text{supp}(k_1)} \cap \overline{\text{supp}(k_2)} \cap \overline{\text{supp}(k_3)}\right| = 7$$

  implies that there are exactly 7 positions with ones in s and zeros in k_1, k_2 and k_3. Choose the first 7 positions.

- $$a_{12} = |I_{12}^3| = \left|\text{supp}(s) \cap \text{supp}(k_1) \cap \overline{\text{supp}(k_2)} \cap \text{supp}(k_3)\right| = 15$$

  implies that there are exactly 15 positions with ones in s, k_1 and k_3 and zeros in k_2. Choose positions $8, \ldots, 22$.

- The remaining positions are chosen in the same way by

i	a_i	I_i^3	positions	s	k_1	k_2	k_3
4	7	$\mathrm{supp}(s) \cap \mathrm{supp}(k_1) \cap \overline{\mathrm{supp}(k_2)} \cap \overline{\mathrm{supp}(k_3)}$	$23-29$	1	1	0	0
6	7	$\mathrm{supp}(s) \cap \overline{\mathrm{supp}(k_1)} \cap \mathrm{supp}(k_2) \cap \overline{\mathrm{supp}(k_3)}$	$30-32$, $65-68$	1	0	1	0
8	7	$\mathrm{supp}(s) \cap \mathrm{supp}(k_1) \cap \mathrm{supp}(k_2) \cap \overline{\mathrm{supp}(k_3)}$	$69-75$	1	1	1	0
10	7	$\mathrm{supp}(s) \cap \overline{\mathrm{supp}(k_1)} \cap \overline{\mathrm{supp}(k_2)} \cap \mathrm{supp}(k_3)$	$76-82$	1	0	0	1
14	7	$\mathrm{supp}(s) \cap \overline{\mathrm{supp}(k_1)} \cap \mathrm{supp}(k_2) \cap \mathrm{supp}(k_3)$	$83-89$	1	0	1	1
16	7	$\mathrm{supp}(s) \cap \mathrm{supp}(k_1) \cap \mathrm{supp}(k_2) \cap \mathrm{supp}(k_3)$	$90-96$	1	1	1	1

We obtain the shares

$$\begin{array}{rcllllllll}
k_1 & = & 0000 & 0001 & 1111 & 1111 & 1111 & 1111 & 1111 & 1000 \\
 & & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 \\
 & & 0000 & 1111 & 1110 & 0000 & 0000 & 0000 & 0111 & 1111 \\
 & & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000
\end{array}$$

$$\begin{array}{rcllllllll}
k_2 & = & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0111 \\
 & & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 \\
 & & 1111 & 1111 & 1110 & 0000 & 0011 & 1111 & 1111 & 1111 \\
 & & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000
\end{array}$$

$$\begin{array}{rcllllllll}
k_3 & = & 0000 & 0001 & 1111 & 1111 & 1111 & 1100 & 0000 & 0000 \\
 & & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 \\
 & & 0000 & 0000 & 0001 & 1111 & 1111 & 1111 & 1111 & 1111 \\
 & & 0000 & 0000 & 0000 & 0000 & 0000 & 1111 & 0000 & 0000
\end{array}$$

and the sums

$$\begin{array}{rcllllllll}
k_1+k_2 & = & 0000 & 0001 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 \\
 & & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 \\
 & & 1111 & 0000 & 0000 & 0000 & 0011 & 1111 & 1000 & 0000 \\
 & & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000
\end{array}$$

$$\begin{array}{rcllllllll}
k_1+k_3 & = & 0000 & 0000 & 0000 & 0000 & 0000 & 0011 & 1111 & 1000 \\
 & & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 \\
 & & 0000 & 1111 & 1111 & 1111 & 1111 & 1111 & 1000 & 0000 \\
 & & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000
\end{array}$$

$$\begin{array}{rcllllllll}
k_2+k_3 & = & 0000 & 0001 & 1111 & 1111 & 1111 & 1100 & 0000 & 0111 \\
 & & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 \\
 & & 1111 & 1111 & 1111 & 1111 & 1100 & 0000 & 0000 & 0000 \\
 & & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000
\end{array}$$

$$\begin{array}{rcllllllll}
k_1+k_2+k_3 & = & 0000 & 0000 & 0000 & 0000 & 0000 & 0011 & 1111 & 1111 \\
 & & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 \\
 & & 1111 & 0000 & 0001 & 1111 & 1100 & 0000 & 0111 & 1111 \\
 & & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000.
\end{array}$$

$\mathcal{C} = RM(1,7)$ has minimum distance $d = 2^6$ and can correct up to $\left\lfloor \frac{2^6-1}{2} \right\rfloor = 31$ errors. Since

$$\mathrm{d}\,(s,k_1) = \mathrm{d}\,(s,k_3) = \mathrm{d}\,(s,k_1+k_2) = \mathrm{d}\,(s,k_2+k_3) = 28 \leq 31,$$

Hamming decoding yields the secret s when the set is authorized. Furthermore

$$\mathrm{wt}(k_2) = \mathrm{wt}(k_1+k_3) = \mathrm{wt}(k_1+k_2+k_3) = 28$$

means

$$\mathrm{d}\,(0,k_2) = \mathrm{d}\,(0,k_1+k_3) = \mathrm{d}\,(0,k_1+k_2+k_3) = 28 \leq 31.$$

Hence Hamming decoding yields the zero word when the set is unauthorized.

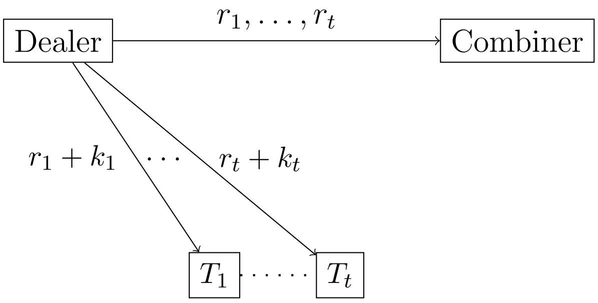
In general Γ is non-monotone and the use of a combiner is necessary in any case. But there is another reason why the participants must not have their shares in plain text. It is public knowledge that the zero word cannot be the secret since $b_1 > 0$. So the members of an unauthorized set may look for the codeword lying next to their sum which is not the zero word. Since g is rather small it is very likely that they find s.

Example 4.26. For s, k_1, k_2, k_3 and $\mathcal{C}$ from Example 4.25 the following table shows the results of Hamming decoding of the share sums of the unauthorized sets. We see that the closest code word, which is not the zero word, is already the secret s.

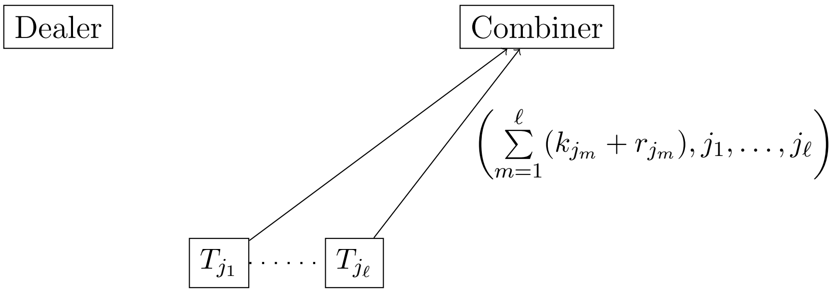
unauthorized sum S	$c \in \mathcal{C}$ with $\mathrm{d}\,(S,c) < 36$	$c \in \mathcal{C}$ with $\mathrm{d}\,(S,c) = 36$	next $c \in \mathcal{C}$ with $\mathrm{d}\,(S,c) > 36$
k_2	$c \sim 0$	$c = s \sim 1 + x_6$	$c \sim x_7$, $c \sim x_6 + x_7$; d= 42
$k_1 + k_2$	$c \sim 0$	$c = s$	$c \sim x_7$, $c \sim x_6 + x_7$; d= 50
$k_1 + k_2 + k_3$	$c \sim 0$	$c = s$	$c \sim x_4$, $c \sim x_4 + x_6$, $c \sim x_3 + x_4 + x_7$, $c \sim x_3 + x_4 + x_6 + x_7$; d= 52

This problem can be overcome by the use of a combiner. The following management model may be used.

1. For a given secret the dealer chooses a codeword s in a suitable binary code of length n which represents it. Then he constructs suitable shares $k_1, \ldots, k_t$ in $\mathbb{Z}_2^n$ such that conditions 1. and 2. from Section 4.2 are satisfied. In addition to that he chooses random vectors $r_1, \ldots, r_t \in \mathbb{Z}_2^n$ and distributes the vectors $k_1 + r_1, \ldots, k_t + r_t$ as shares to the participants. Since the r_i are chosen randomly the shares are also random vectors and provide no information about s to the participants. The dealer gives $(r_1, \ldots, r_t)$ to the combiner.



2. When a group $\{T_{j_1}, \dots, T_{j_\ell}\}$ of participants wants to reconstruct the secret they calculate the sum $\sum_{m=1}^{\ell}(k_{j_m} + r_{j_m})$ of their shares and send it together with their numbers $j_1, \dots, j_\ell$ to the combiner.


Dealer
Combiner
$\left(\sum_{m=1}^{\ell} (k_{j_m} + r_{j_m}), j_1, \dots, j_\ell\right)$
T_{j_1}
T_{j_ℓ}

3. The combiner adds $\sum_{m=1}^{\ell} r_{j_m}$ to the received sum and obtains $\sum_{m=1}^{\ell} k_{j_m}$. Then he applies a Hamming decoding algorithm on $\sum_{m=1}^{\ell} k_{j_m}$. If the participants are authorized the algorithm outputs the secret since condition 1 is satisfied. Otherwise the output is another codeword since condition 2 is satisfied.

4. The dealer sends the output of the decoding algorithm to the device which carries out the desired action if it receives the secret.

However, if an unauthorized group gets to know their random vectors r_j, they have their shares in plain text. Then it is very likely that they gain the secret by looking for the nearest codeword with weight b_1 (see Example 4.26). Furthermore, the problem of the large code length n, which has a negative impact on the effectiveness of the scheme, remains.

In the following chapters we identify access structures which allow smaller code lengths and larger security distances. We start with the classification of access structures on the same number of participants, such that the access structures lying in the same class allow the same parameters b_1, g, k and also have the same suitable codes when some additional conditions are met.

Chapter 5

Classification of Access Structures

As in the previous section we consider the case that the sums of the subsets have either distance k or distance g to the secret, depending on whether the subset is authorized or not. This chapter identifies an invariant which enables us to classify all access structures on the same number of participants such that each class allows the same valid parameters b_1, g and k. Furthermore we present a refinement of this classification such that all access structures lying in the same refined class have the same suitable codes and are able to share the same secrets.

Throughout this section we consider access structures on t participants. We start with an important definition.

Definition 5.1. Consider an access structure $\Gamma \neq \mathcal{P}(\mathcal{T}) \setminus \{\varnothing\}$. The set

$$\overline{\Gamma} = \mathcal{P}(\mathcal{T}) \setminus (\Gamma \cup \{\varnothing\})$$

of all non-empty unauthorized sets is called *dual access structure* of Γ.

Now we have a closer look at the matrix ε defined in 4.11. The first row of ε is the zero vector. Hence the first entry of each column is zero. For all $j = 1, \ldots, 2^t$ we denote the jth column with the first entry deleted by ε_j.

Definition 5.2. Consider an access structure $\Gamma \neq \mathcal{P}(\mathcal{T}) \setminus \{\varnothing\}$ with the dual access structure $\overline{\Gamma} = \mathcal{P}(\mathcal{T}) \setminus (\Gamma \cup \{\varnothing\}) = \{A_1, \ldots, A_u\}$. Assume that A_j is the ℓ_jth element in $\mathcal{P}(\{T_1, \ldots, T_t\})$ with respect to $\preccurlyeq$ for all $j = 1, \ldots, u$ and that $A_j \preccurlyeq A_{j+1}$ for all $j = 1, \ldots, u-1$. Define $\varepsilon_{\overline{\Gamma}}$ to be the following binary $(2^t - 1 \times u)$-matrix:

$$\varepsilon_{\overline{\Gamma}} = \left(\varepsilon_{\ell_1}, \ldots, \varepsilon_{\ell_u}\right).$$

Suppose that b is an elementary weight vector with respect to the parameters b_1, g, k. Since $\overline{\Gamma} = \{A_1, \ldots, A_u\}$, $b_{\ell_j} = g$ for all $j = 1, \ldots, u$. The first component of b is b_1 and all other components have the value k. Hence a column ε_{ℓ_j} occurs in $\varepsilon_{\overline{\Gamma}}$ iff the ℓ_jth column of E is multiplied with g while calculating $\frac{1}{2^{t-1}} E \cdot b$.

Example 5.3. Let $\Gamma = \{\{T_1\}, \{T_2\}, \{T_1, T_3\}, \{T_1, T_2, T_3\}\}$ be an access structure on 3 participants. Then

$$\overline{\Gamma} = \{\underbrace{\{T_1, T_2\}}_{=A_1}, \underbrace{\{T_3\}}_{=A_2}, \underbrace{\{T_2, T_3\}}_{=A_3}\}.$$

A_1 is the 4th element, A_2 the 5th element and A_3 the 7th element of $(\mathcal{P}(\mathcal{T}), \preccurlyeq)$. Hence $\varepsilon_{\overline{\Gamma}}$ consists of the 4th, the 5th and the 7th column of ε without the first entry.

$$\varepsilon = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \text{ and } \varepsilon_{\overline{\Gamma}} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

For all $i = 2, 3, \ldots, 2^t$ the number of ones in the $(i-1)$th row of $\varepsilon_{\overline{\Gamma}}$ is exactly the number of summands $-g$ in the equation $a_{2i} - a_{2i-1} = \frac{1}{2^{t-1}} E_i \cdot b$ in the linear system 4.2. The number of zeros in the ith row of $\varepsilon_{\overline{\Gamma}}$ says how many summands of the form $+g$ occur in that equation. Each row of ε, except for the first row, consists of 2^{t-1} ones and 2^{t-1} zeros and starts with a one. Therefore the number of summands k, $-k$ in the equation $a_{2i} - a_{2i-1} = \frac{1}{2^{t-1}} E_i \cdot b$ is also determined by the weight of the ith row of $\varepsilon_{\overline{\Gamma}}$. That means the weight distribution of the rows characterize equations 2 up to 2^t of the linear system 4.2 uniquely.

In the next step we identify a class of permutations on the indices of the rows of $\varepsilon_{\overline{\Gamma}}$ such that the first t rows of the resulting matrix represent the non-empty unauthorized sets $A_1, \ldots, A_u$. For all $j = 1, \ldots, u$ the jth column of this $(t \times u)$-submatrix should represent the unauthorized set A_j. That means a vector in $\mathbb{Z}_2^t$ has to characterize a subset of $\{T_1, \ldots, T_t\}$. This can be done as follows.

Definition 5.4. Let A be an arbitrary subset of $\{T_1, \ldots, T_t\}$. Define $v = (v_1, \ldots, v_t)^\tau \in \mathbb{Z}_2^t$ by

$$v_i = \begin{cases} 1 & \text{if } T_i \in A \\ 0 & \text{if } T_i \notin A \end{cases} \quad \text{for all } i = 1, \ldots, t.$$

v is called the *characteristic vector* of A.

Example 5.5. The characteristic vectors of the non-empty unauthorized sets $A_1 = \{T_1, T_2\}$, $A_2 = \{T_3\}$, $A_3 = \{T_2, T_3\}$ in Example 5.3 are

$$\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}.$$

For a permutation P on the indices of the rows of $\varepsilon_{\overline{\Gamma}}$ we denote the resulting matrix with the permuted rows by $P(\varepsilon_{\overline{\Gamma}})$. That means we have to find a class of permutations P such that the columns of the submatrix consisting of the first t rows of $P(\varepsilon_{\overline{\Gamma}})$ are the characteristic vectors of the non-empty unauthorized sets. The following lemma provides such a class of permutations.

Lemma 5.6. Let $\overline{\Gamma} = \{A_1, \ldots, A_u\}$ and let $P : \{1, 2, \ldots, 2^t - 1\} \to \{1, 2, \ldots, 2^t - 1\}$ be an arbitrary permutation such that

$$P(2^{l-1}) = l \text{ for all } l = 1, \ldots, t.$$

For each subset A_j, $j = 1, \ldots, u$, let v_j be the characteristic vector. Then $P\left(\varepsilon_{\overline{\Gamma}}\right)$ has the form

$$P(\varepsilon_{\overline{\Gamma}}) = \left(\begin{array}{ccc} v_1 & \ldots & v_u \\ \hline * & \ldots & * \\ \vdots & & \vdots \\ * & \ldots & * \end{array}\right) \begin{array}{l} \}\, t \\ \left.\begin{array}{l} \\ \\ \\ \end{array}\right\} 2^t - t - 1 \end{array}$$

where the first t rows are given by the column vectors $v_1, \ldots, v_u$ and the remaining $2^t - t - 1$ rows consist of the remaining $2^t - t - 1$ non-trivial linear combinations modulo 2 of the first t rows.

Proof. 1. At first we have a look at the structure of the rows of the matrices ε and $\varepsilon_{\overline{\Gamma}}$. Let p_j denotes the Boolean polynomial corresponding to the jth codeword in $RM^0(1, t)$. According to Lemma 4.12 (a), the jth column of ε is the evaluation vector of p_j for all $j = 1, \ldots, 2^t$. Therefore each row of ε consists of all possible evaluations

$$\left(p_1\left(\sum_{i=1}^{t} a_i e_i\right), \ldots, p_{2^t}\left(\sum_{i=1}^{t} a_i e_i\right)\right)$$

on one specific element $\sum\limits_{i=1}^{t} a_i e_i \in \mathbb{Z}_2^t$ ($e_1, \ldots, e_t$ denote the canonical basis vectors of $\mathbb{Z}_2^t$). The order of the vectors $\sum\limits_{i=1}^{t} a_i e_i$ which characterize the rows of ε corresponds to the order $\leq$ on $\mathbb{Z}_2^t$ mentioned in Remark 4.4. Hence the $(2^{l-1} + 1)$th row belongs to the canonical basis vector e_l for all $l = 1, \ldots, t$ and has the form $(p_1(e_l), \ldots, p_{2^t}(e_l))$. Due to the linearity

$$\left(p_1\left(\sum_{i=1}^{t} a_i e_i\right), \ldots, p_{2^t}\left(\sum_{i=1}^{t} a_i e_i\right)\right) = \sum_{i=1}^{t} a_i \left(p_1(e_i), \ldots, p_{2^t}(e_i)\right)$$

the remaining rows are the remaining linear combinations of the rows belonging to the canonical basis vectors $e_1, \ldots, e_t$.

Suppose that $A_1, \ldots, A_u$ are the l_1th, ..., l_uth element of $\mathcal{P}(\mathcal{T})$ with $l_1 < \ldots < l_u$. When we delete the first row and all columns of ε which do not belong to the non-empty unauthorized sets we obtain the matrix $\varepsilon_{\overline{\Gamma}}$ with the rows

$$\left(p_{l_1}\left(\sum_{i=1}^{t} a_i e_i\right), \ldots, p_{l_u}\left(\sum_{i=1}^{t} a_i e_i\right)\right)$$

for all sums $\sum_{i=1}^{t} a_i e_i \neq 0$. For all $l = 1, \ldots, t$ the 2^{l-1}th row has the form $\big(p_1(e_1), \ldots, p_{2^t}(e_l)\big)$ as the first row is missing.

2. In this step we identify the positions in the columns of $\varepsilon_{\overline{\Gamma}}$ which belong to the characteristic vectors $v_1, \ldots, v_u$. Since all p_{l_j}, $j = 1, \ldots, u$, are Boolean polynomials of degree one without the constant summand 1, $p_{l_j}(e_i) = 1$ iff the monomial x_i is a summand of p_{l_j}. According to Remark 4.4, this happens exactly if $T_i \in A_j$. Hence $(p_{l_j}(e_1), \ldots, p_{l_j}(e_t))^\tau = v_j$ for all $j = 1, \ldots, u$.

Now we apply the permutation P on $\varepsilon_{\overline{\Gamma}}$. Because of the observations in 1. and 2. the first t rows of the resulting matrix are

$$\begin{pmatrix} p_{l_1}(e_1) & \ldots & p_{l_u}(e_1) \\ p_{l_1}(e_2) & \ldots & p_{l_u}(e_2) \\ \vdots & & \vdots \\ p_{l_1}(e_t) & \ldots & p_{l_u}(e_t) \end{pmatrix} = \big(v_1, \ldots, v_u\big)$$

and the remaining $2^t - t - 1$ rows of $\varepsilon_{\overline{\Gamma}}$ are the remaining non-trivial linear combinations of the first t rows. □

Example 5.7. $\overline{\Gamma} = \Big\{ \underbrace{\{T_1, T_2\}}_{=A_1}, \underbrace{\{T_3\}}_{=A_2}, \underbrace{\{T_2, T_3\}}_{=A_3} \Big\}$ from Example 5.3 corresponds to the Boolean polynomials $p_4 = x_1 + x_2$, $p_5 = x_3$, $p_7 = x_2 + x_3 \in \mathbb{Z}_2[x_1, \ldots, x_t]$. Therefore

$$\varepsilon_{\overline{\Gamma}} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} p_4(100) & p_5(100) & p_7(100) \\ p_4(010) & p_5(010) & p_7(010) \\ p_4(110) & p_5(110) & p_7(110) \\ p_4(001) & p_5(001) & p_7(001) \\ p_4(101) & p_5(101) & p_7(101) \\ p_4(011) & p_5(011) & p_7(011) \\ p_4(111) & p_5(111) & p_7(111) \end{pmatrix} \begin{array}{l} \leftarrow x_1 \\ \leftarrow x_2 \\ \\ \leftarrow x_3. \\ \\ \\ \\ \end{array}$$

We apply the candidate $P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 3 & 5 & 6 & 7 \end{pmatrix}$ for a permutation described in Lemma 5.6 on $\varepsilon_{\overline{\Gamma}}$ and receive the matrix

$$P(\varepsilon_{\overline{\Gamma}}) = \left(\begin{array}{ccc} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{array}\right) = \left(\begin{array}{c} \\ v_1 \qquad v_2 \qquad v_3 \\ \\ \hline \text{row } 1 + \text{row } 2 \\ \text{row } 1 + \text{row } 3 \\ \text{row } 2 + \text{row } 3 \\ \text{row } 1 + \text{row } 2 + \text{row } 3 \end{array}\right).$$

As already mentioned we are interested in the weight distribution of the rows of $\varepsilon_{\overline{\Gamma}}$ because these weights characterize the equations in the linear system 4.2. These weights can be written in a vector, the so called weight vector of $\varepsilon_{\overline{\Gamma}}$, which is defined as follows.

Definition 5.8. Let A be an arbitrary $(x \times y)$-matrix over $\mathbb{Z}_2$. For $j = 0, \dots, y$ let w_j be the number of rows with exactly j ones. The *weight vector of* A is the vector

$$w_A := (w_j)_{j=0}^{y}\,.$$

For $A = \varepsilon_{\overline{\Gamma}}$ the weight vector $w_{\varepsilon_{\overline{\Gamma}}} =: w_{\overline{\Gamma}}$ is called *weight vector of the access structure* Γ.

Obviously the order of the rows (and columns) of a matrix has no effect on its weight vector. Hence the permutation P, which brings the characteristic vectors of the unauthorized sets in the first t rows, does not change the weight vector.

Example 5.9. The weight vector of the access structure Γ from Example 5.3 is

$$w_{\overline{\Gamma}} = (0, 3, 3, 1).$$

For abbreviation we denote the matrix consisting of the first t rows of $P(\varepsilon_{\overline{\Gamma}})$ with $\varepsilon^1_{\overline{\Gamma}}$. According to our construction, the columns of this matrix are the characteristic vectors of the unauthorized sets in $\overline{\Gamma}$ ordered by $\preccurlyeq$.

Using the weight vector $w_{\overline{\Gamma}}$ we can specify how $\varepsilon_{\overline{\Gamma}}$ determines the equations of the linear system 4.2.

Remark 5.10. The weight vector $w_{\overline{\Gamma}}$ describes the equations of the linear system 4.2 up to the order. Let $w_{\overline{\Gamma}} = (w_0, w_1, \dots, w_u)$. Then there are exactly w_j equations with exactly j minus ones being multiplied with g. According to Lemma 4.19 (a) these equations have the form

$$a_{2i} - a_{2i-1} \quad = \quad \frac{1}{2^{t-1}}(b_1 - k + (u - 2j)(g - k)).$$

Example 5.11. The weight vector $w_{\overline{\Gamma}} = (0, 3, 3, 1)$ of the access structure in Example

5.3 yields the following system of linear equations:

$$\begin{array}{lclcll}
\sum_{i=1}^{8} a_{2i} & = & b_1 & & & \\
a_{2i} - a_{2i-1} & = & \frac{1}{4}(b_1 - k + (3 - 2 \cdot 1)(g - k)) & = & \frac{1}{4}(b_1 + g - 2k) & \text{3 times} \\
 & & & & & (i = 2, 4, 8) \\
a_{2i} - a_{2i-1} & = & \frac{1}{4}(b_1 - k + (3 - 2 \cdot 2)(g - k)) & = & \frac{1}{4}(b_1 - g) & \text{3 times} \\
 & & & & & (i = 3, 5, 7) \\
a_{2i} - a_{2i-1} & = & \frac{1}{4}(b_1 - k + (3 - 2 \cdot 3)(g - k)) & = & \frac{1}{4}(b_1 - 3g + 2k) & \text{once } (i = 6)
\end{array}$$

When two access structures Γ, Γ' have the same weight vectors, the right hand sides of the related equations 2 to 2^t of the linear system 4.2 are the same. Only their orders may be different. However, a change in the order of the right hand sides has no impact on the validity of the parameters b_1, g, k. Hence the same parameters (b_1, g, k) realize Γ and Γ' elementarily. For this reason we classify the set of all access structures in the following way.

Definition 5.12. Two access structures Γ and Γ' on the same set of t participants *belong to the same class of access structures* iff

$$w_{\overline{\Gamma}} = w_{\overline{\Gamma'}}.$$

Example 5.13. Let $\overline{\Gamma'} = \{\{T_1\}, \{T_2\}, \{T_1, T_2\}\}$, $\overline{\Gamma''} = \{\{T_1, T_2\}, \{T_3\}, \{T_1, T_2, T_3\}\}$ be access structures on the same participant set $\mathcal{T} = \{T_1, T_2, T_3\}$. Then

$$\varepsilon^1_{\overline{\Gamma'}} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \varepsilon^1_{\overline{\Gamma''}} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

The related weight vectors are

$$w_{\overline{\Gamma'}} = w_{\overline{\Gamma''}} = (1, 0, 6, 0).$$

Hence Γ' and Γ'' belong to the same class. The access structure Γ from Example 5.3 belongs to another class since the weight vector $w_{\overline{\Gamma}} = (0, 3, 3, 1)$ is different.

The following proposition summarizes our previous considerations. It says that we have achieved our first aim to classify the access structures such that each class allows the same parameters b_1, g, k.

Proposition 5.14. Let Γ, Γ' be two access structures in the same class. Suppose that (b_1, g, k) realizes Γ elementarily. Then (b_1, g, k) realizes Γ' elementarily, too.

When we want to find out, whether two access structures belong to the same class or not, we can do this by determining the weight vectors of the related ε-matrices. In this context the following remark is very helpful for the following course of this work.

Remark 5.15. Let A be an $(x \times 2^x - 1)$-matrix over $\mathbb{Z}_2$ which contains each non-zero vector in $\mathbb{Z}_2^x$ as column. Then A is a generator matrix of a binary simplex code $\mathcal{I}$ of dimension x. $\mathcal{I}$ has the weight distribution

$$w(\mathcal{I}) = (1, 0, \dots, 0, \underset{\overset{\uparrow}{2^{x-1}}}{2^x - 1}, 0, \dots, 0).$$

Therefore the $(2^x - 1 \times 2^x - 1)$-matrix B over $\mathbb{Z}_2$, whose rows are all possible non-trivial linear combination of the rows of A (which are the non-zero codewords of $\mathcal{I}$), has the weight vector

$$w_B = (0, \dots, 0, \underset{\overset{\uparrow}{2^{x-1}}}{2^x - 1}, 0, \dots, 0).$$

Our next aim is to find a refinement of the classification explained above, such that all access structures in the same refined class allow not only the same parameters b_1, g, k, but also have the same suitable codes and possible secrets. To achieve this we give another presentation of our classification in terms of linear algebra. For this purpose we introduce an invariant of binary matrices of the same size, the so-called linearity type of the matrix.

Definition 5.16. (a) Let A be an arbitrary $(x \times y)$-matrix over $\mathbb{Z}_2$. For $i = 1, \dots, y$ let ℓ_i denote the number of all sets of i pairwise different columns $A_{j_1}, \dots, A_{j_i}$ of A such that $A_{j_1} + \ldots + A_{j_i} = 0$. Define $\ell_A := (\ell_1, \dots, \ell_y)$. ℓ_A is called *linearity vector* of A.

(b) We say that two binary $(x \times y)$-matrices A, A' have the same *linearity type* if they have the same linearity vector $\ell_A = \ell_{A'}$.

(c) Denote $\ell_{\varepsilon^1_{\overline{\Gamma}}}$ by $\ell_{\overline{\Gamma}}$. We say that two access structures Γ, Γ' have the same *linearity type*, if $\ell_{\overline{\Gamma}} = \ell_{\overline{\Gamma'}}$.

Example 5.17. Consider the access structure Γ from Example 5.3. The first 3 rows of $P(\varepsilon_{\overline{\Gamma}})$ are

$$\varepsilon^1_{\overline{\Gamma}} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

$\ell_1 = 0$, since there is no zero vector.
$\ell_2 = 0$, since no column occurs twice.
$\ell_3 = 0$, since the columns are linearly independent.
We obtain the linearity vector $\ell_{\overline{\Gamma}} = (0, 0, 0)$.

In contrast to that the access structures Γ', Γ'' from Example 5.13 with

$$\overline{\Gamma'} = \{\{T_1\}, \{T_2\}, \{T_1, T_2\}\}, \quad \overline{\Gamma''} = \{\{T_1, T_2\}, \{T_3\}, \{T_1, T_2, T_3\}\}$$

and

$$\varepsilon^1_{\overline{\Gamma'}} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad \varepsilon^1_{\overline{\Gamma''}} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

both have the linearity vector $(0, 0, 1)$:
$\ell_1 = 0$, since there is no zero vector.
$\ell_2 = 0$, since no column occurs twice.
$\ell_3 = 1$, since the sum of the three columns is the zero vector.

Since the columns of $\varepsilon^1_{\overline{\Gamma}}$ are the characteristic vectors of the unauthorized sets, they are pairwise different and non-zero. That means $\ell_1 = \ell_2 = 0$ for all $\varepsilon^1_{\overline{\Gamma}}$.

In Example 5.17 it is noticeable, that the access structures Γ' and Γ'', which belong to the same class according to Example 5.13, have the same linearity vector. The access structure Γ belongs to another class and also has another linearity type. This is not a coincidence. In the next step we show that two access structures have the same weight vector iff they have the same linearity type.

To achieve this we have a look at the matrix $\varepsilon_{\overline{\Gamma}}$ from a different perspective: Suppose that the $(t \times u)$-submatrix $\varepsilon^1_{\overline{\Gamma}}$ has the rank r. Then $\varepsilon^1_{\overline{\Gamma}}$ has r linearly independent rows and can be considered as a general generator matrix of a binary linear $[u, r]$-code $\mathcal{D}$. The rows of $\varepsilon_{\overline{\Gamma}}$ and the zero word of length u are the codewords of $\mathcal{D}$ because they are all possible linear combinations of the rows of $\varepsilon^1_{\overline{\Gamma}}$ (see Lemma 5.6). Depending on the rank r each codeword occurs several times.

Lemma 5.18. *Consider an arbitrary $(x \times y)$-matrix A over $\mathbb{Z}_2$ with $rk(A) = r$. Let U be the r-dimensional linear subspace of $\mathbb{Z}_2^y$ generated by the rows of A. Then each vector in U can be written as linear combination of the rows of A in 2^{x-r} different ways.*

Proof. Let $R_1, \ldots, R_x$ denote the rows of A.

For $r = x$ all rows are linearly independent and $U = \langle R_1, \ldots, R_x \rangle$ is a r-dimensional subspace of $\mathbb{Z}_2^y$ with the basis $\{R_1, \ldots, R_x\}$. Hence each vector in U has a unique representation as linear combination of the rows $R_1, \ldots, R_x$ and can be represented in $1 = 2^{x-r}$ ways.

Let $r < x$. The rank is the maximal number of linearly independent rows and we can assume w.l.o.g. that the rows $R_1, \ldots, R_r$ are linearly independent and that the rows $R_{r+1}, \ldots, R_x$ are linear combinations of the first r rows. Let $u \in U$ and $b_{r+1}, \ldots, b_x \in \mathbb{Z}_2$ be arbitrary. Then $u + \sum\limits_{i=r+1}^{x} b_i R_i$ is a vector in U and there are uniquely determined coefficients $b_1, \ldots, b_r$ such that

$$u + \sum_{i=r+1}^{x} b_i R_i = \sum_{i=1}^{r} b_i R_i.$$

Since there are 2^{x-r} possibilities to choose $b_{r+1}, \ldots, b_x$ the assertion holds. □

Lemma 5.18 yields

Lemma 5.19. Consider an arbitrary $(x \times y)$-matrix A over $\mathbb{Z}_2$ with $rk(A) = r$. Let B be a $(z \times y)$-submatrix of A consisting of $z \leq x$ rows of A which also has rank r. Define N to be the binary $(2^x \times y)$-matrix whose rows are all possible linear combinations of the rows of A and M to be the $(2^z \times y)$-matrix consisting of all possible linear combinations of the rows of B. Then

$$w_N = 2^{x-z} w_M.$$

Proof. There must be r linearly independent rows which appear in the matrix A as well as in B. Hence the linear subspace U generated by the rows of A is the same as the subspace generated by the rows of B. Lemma 5.18 says that each vector in U can be written as a linear combination of rows of A in exactly 2^{x-r} ways and as a linear combination of rows of B in exactly 2^{z-r} ways. Let P be the binary $(2^r \times y)$-matrix whose rows are the vectors of U. Then

$$w_N = 2^{x-r} w_P \quad \text{and} \quad w_M = 2^{z-r} w_P.$$

This yields $w_N = 2^{x-z} w_M$. □

Going back to the code $\mathcal{D}$ generated by the rows of $\varepsilon^1_{\overline{\Gamma}}$ Lemma 5.18 says that each codeword, except for the zero word, occurs exactly 2^{t-r} times as a row of the matrix $\varepsilon_{\overline{\Gamma}}$. The zero word occurs $2^{t-r} - 1$ times since the first row of ε, which contains only zeros, has been removed during the construction of $\varepsilon_{\overline{\Gamma}}$.

Lemma 5.19 gives the following relation between the weight distribution $w(\mathcal{D})$ of $\mathcal{D}$ and the weight vector $w_{\overline{\Gamma}}$ of the matrix $\varepsilon_{\overline{\Gamma}}$:

$$w_{\overline{\Gamma}} = 2^{t-r} \cdot w(\mathcal{D}) - (1, 0, \ldots, 0).$$

In other words, the weight vector $w_{\overline{\Gamma}}$ of each access structure Γ and the weight distribution of the binary code generated by $\varepsilon^1_{\overline{\Gamma}}$ determine each other uniquely.

The following lemma explains the connection between the weight distribution of the dual $[u, u-r]$-code $\mathcal{D}^\perp$ and the linearity vector $\ell_{\overline{\Gamma}}$ of $\varepsilon^1_{\overline{\Gamma}}$.

Lemma 5.20. Let A be an arbitrary $(x \times y)$-matrix over $\mathbb{Z}_2$ of rank r with the columns $C_1, \ldots, C_y$ and the rows $R_1, \ldots, R_x$. Let $\mathcal{E}$ be the binary $[y, r]$-code generated by A. Then

(a) A is a check matrix of the dual code $\mathcal{E}^\perp$ and

(b) $\ell_A = w(\mathcal{E}^\perp)$.

Proof. Part (a) is a well known fact, so we only prove part (b).
Let $d = (d_1, \ldots, d_y)$ be a binary vector with weight w. Then there are positions

$i_1, \dots, i_w$ where d has the value one. In all other position d has the value zero. Furthermore

$$d \in \mathcal{D}^{\perp} \;\Leftrightarrow\; \sum_{i=1}^{y} d_i C_i = 0 \;\Leftrightarrow\; \sum_{j=1}^{w} d_{i_j} C_{i_j} = 0.$$

That means each codeword $d \in \mathcal{D}^{\perp}$ with weight w corresponds to a selection of w pairwise different columns of A whose sum is the zero vector and vice versa. □

We also know that, due to the MacWilliams identity stated in Theorem 3.21, $w(\mathcal{D}^{\perp})$ determines $w(\mathcal{D})$ uniquely and vice versa. With these preliminary thoughts we can prove the following proposition.

Proposition 5.21. Let Γ, Γ' be arbitrary access structures on t participants. Then

$$w_{\overline{\Gamma}} = w_{\overline{\Gamma'}} \;\Leftrightarrow\; \ell_{\overline{\Gamma}} = \ell_{\overline{\Gamma'}}.$$

Proof. Let $\mathcal{D}$ be the binary code generated by the rows of $\varepsilon^1_{\overline{\Gamma}}$ and $\mathcal{D}'$ be the binary code generated by the rows of $\varepsilon^1_{\overline{\Gamma'}}$.

"$\Rightarrow$" Suppose that $w_{\overline{\Gamma}} = (w_0, \dots, w_u) = (w'_0, \dots, w'_u) = w_{\overline{\Gamma'}}$. For $rk(\varepsilon^1_{\overline{\Gamma}}) = r$ we have $2^{t-r} - 1 = w_0 = w'_0$. Hence $rk(\varepsilon^1_{\overline{\Gamma'}}) = r$, too, and both codes have the same dimension r and the same weight distributions

$$w(\mathcal{D}) = \frac{1}{2^{t-r}}\left(w_{\overline{\Gamma}} + (1, 0, \dots, 0)\right) = \frac{1}{2^{t-r}}\left(w_{\overline{\Gamma'}} + (1, 0, \dots, 0)\right) = w(\mathcal{D}').$$

Using the MacWilliams identity we see that the weight distributions $\ell_{\overline{\Gamma}}$ and $\ell_{\overline{\Gamma'}}$ of the dual codes $\mathcal{D}^{\perp}$ and $(\mathcal{D}')^{\perp}$ are also the same.

"$\Leftarrow$" Suppose that the dual codes $\mathcal{D}^{\perp}$ and $(\mathcal{D}')^{\perp}$ have the same weight distribution $\ell_{\overline{\Gamma}} = \ell_{\overline{\Gamma'}}$. The sum of all entries in $\ell_{\overline{\Gamma}}$ determines the dimension of $\mathcal{D}^{\perp}$ and therefore the dimension of $\mathcal{D}$. Hence the codes $\mathcal{D}$ and $\mathcal{D}'$ have the same dimension r. Furthermore $w(\mathcal{D}) = w(\mathcal{D}')$ due to the MacWilliams identity. This yields

$$w_{\overline{\Gamma}} = 2^{t-r} \cdot w(\mathcal{D}) - (1, 0, \dots, 0) = 2^{t-r} \cdot w(\mathcal{D}') - (1, 0, \dots, 0) = w_{\overline{\Gamma'}}.$$

□

The equivalence stated in Proposition 5.21 provides a linear algebraic view on the classification of the access structure. This yields one possible refinement of the classification such that all access structures of the same refined class have the same suitable codes and allow the same secrets.

Proposition 5.22. Consider two access structures Γ, Γ'. Suppose that there is an invertible binary $(t \times t)$-matrix B with

$$B \cdot \varepsilon^1_{\overline{\Gamma}} = \varepsilon^1_{\overline{\Gamma'}}.$$

(a) Then Γ and Γ' lie in the same class.

(b) Let (b_1, g, k) be an elementary realization for Γ (and thus also for Γ') and $\mathcal{C}$ a binary code which is suitable for (s, Γ, b_1, g, k) for a codeword $s \in \mathcal{C}$ with weight b_1. Then $\mathcal{C}$ is also suitable for (s, Γ', b_1, g, k).

Proof. Since $B \cdot \varepsilon^1_{\overline{\Gamma}} = \varepsilon^1_{\overline{\Gamma'}}$ for an invertible matrix B, the rows of $\varepsilon^1_{\overline{\Gamma'}}$ are linear combinations of the rows of $\varepsilon^1_{\overline{\Gamma}}$ and vice versa. Therefore the matrices $\varepsilon_{\overline{\Gamma}}$ and $\varepsilon_{\overline{\Gamma'}}$ have the same rows. Only the orders of these rows may be different. Hence there is a permutation $\pi : \{1, 2, \ldots, 2^t - 1\} \to \{1, 2, \ldots, 2^t - 1\}$ such that the ith row of $\varepsilon_{\overline{\Gamma}}$ is the $\pi(i)$th row of $\varepsilon_{\overline{\Gamma'}}$ for all $i = 1, 2, \ldots, 2^t - 1$. This yields:

(a) $w_{\overline{\Gamma}} = w_{\overline{\Gamma'}}$.

(b) The right hand sides of the related equations of the linear system 4.2 differ only in their order. Hence an elementary solution $a' = (a'_2, a'_3, \ldots, a'_{2^t+1})$ for (Γ', b_1, g, k) can be gained from an elementary solution $(a_2, a_3, \ldots, a_{2^t+1})$ for (Γ, b_1, g, k) by permuting the even and the odd numbered components separately using the permutation π:

$$a_{2i} = a'_{2(\pi(i-1)+1)} \text{ and } a_{2i-1} = a'_{2(\pi(i-1)+1)-1} \text{ for all } i = 2, 3, \ldots, 2^t.$$

We check the requirements of Definition 4.20.

- By assumption requirement (a) is fulfilled.
- Requirement (b) is met since $n \geq b_1 + \sum_{i=1}^{2^t} a_{2i-1} = b_1 + \sum_{i=1}^{2^t} a'_{2i-1}$.
- Let $a = (a_1, \ldots, a_{2^t+1})$ be an elementary solution for (Γ, b_1, g, k) with respect to $\mathcal{C}$. Consider shares $k_1, \ldots, k_t$ defined by a and s which share the secret s according to Γ and let $K = \begin{pmatrix} k_1 \\ \vdots \\ k_t \end{pmatrix}$ be the matrix whose rows are these shares. We define
$$K' = \begin{pmatrix} k'_1 \\ \vdots \\ k'_t \end{pmatrix} = (B^{-1})^\tau \cdot K$$
and give the rows $k'_1, \ldots, k'_t$ as shares to the participants $T_1, \ldots, T_t$. These shares have the following properties:
    - Let $S_1, \ldots, S_{2^t}$ be all possible sums of the shares $k_1, \ldots, k_t$ and $S'_1, \ldots, S'_{2^t}$ be all possible sums of the shares $k'_1, \ldots, k'_t$. Since $(B^{-1})^\tau$ is invertible, each sum of the shares $k_1, \ldots, k_t$ can be by represented as a suitable sum of the shares $k'_1, \ldots, k'_t$ and vice versa. That means $(S_1, \ldots, S_{2^t})$ and $(S'_1, \ldots, S'_{2^t})$ differ only in the order of their components.
    - Let $S_{i_1}, \ldots, S_{i_u}$ be the sums related to the unauthorized sets in $\overline{\Gamma}$ and

$S'_{i'_1}, \ldots, S'_{i'_u}$ be the sums related to the unauthorized sets in $\overline{\Gamma'}$. Then

$$\begin{aligned}
\begin{pmatrix} S'_{i_1} \\ \vdots \\ S'_{i_u} \end{pmatrix} &= \left(\varepsilon^1_{\overline{\Gamma'}}\right)^\tau \cdot K' \\
&= \left(\varepsilon^1_{\overline{\Gamma'}}\right)^\tau \cdot (B^{-1})^\tau \cdot K \\
&= \left(\varepsilon^1_{\overline{\Gamma}}\right)^\tau \cdot K \\
&= \begin{pmatrix} S_{i_1} \\ \vdots \\ S_{i_u} \end{pmatrix}.
\end{aligned}$$

Hence the sums of the shares $k_1, \ldots, k_t$ of the (un)authorized sets in $\overline{\Gamma}$ are the same as the sums of the shares $k'_1, \ldots, k'_t$ for the (un)authorized sets in $\overline{\Gamma'}$. Since $k_1, \ldots, k_t$ fulfills the requirements of Definition 4.20 (c) the same is true for $k'_1, \ldots, k'_t$.

□

Indeed, we receive a refinement of our classification by saying that two access structures Γ, Γ' belong to the same (refined) class, iff there is an invertible binary matrix B with $B \cdot \varepsilon_{\overline{\Gamma}} = \varepsilon_{\overline{\Gamma'}}$: Proposition 5.22 says that access structures with this property have the same weight distributions. But the converse is not true. For example consider the access structures Γ, Γ' with the ε^1-matrices

$$\varepsilon^1_{\overline{\Gamma}} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \text{ and } \varepsilon^1_{\overline{\Gamma'}} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Both access structures have the same weight distribution $(0, 0, 2, 4, 1, 0)$, but there is no matrix B with the properties stated above.

However, when there is no such matrix B, the same code $\mathcal{C}$ and the same secret $s \in \mathcal{C}$ can be suitable for both access structures. This depends on the structure of $\mathcal{C}$, on k and on g.

Example 5.23. Consider the access structures Γ, Γ' with

$$\overline{\Gamma} = \{\{T_1, T_2\}, \{T_3\}, \{T_2, T_3\}\}, \quad \overline{\Gamma'} = \{\{T_1\}, \{T_2\}, \{T_1, T_2, T_3\}\}.$$

Then there is an invertible (3×3)-matrix B such that

$$\underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}}_{B} \cdot \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}}_{\varepsilon^1_{\overline{\Gamma}}} = \underbrace{\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}}_{\varepsilon^1_{\overline{\Gamma'}}}.$$

The parameters $b_1 = g = 6$ and $k = 2$ realize Γ elementarily since for these parameters there is an elementary solution for the linear system in Example 5.11. According to Proposition 5.14 $b_1 = g = 6$ and $k = 2$ also realize Γ' elementarily. The related ε-matrices and elementary solutions $(a_2, \ldots, a_{16})$, $(a'_2, \ldots, a'_{16})$ are

$$\begin{array}{l} a_4 = 2, a_3 = 0 \\ a_6 = 0, a_5 = 0 \\ a_8 = 2, a_7 = 0 \\ a_{10} = 0, a_9 = 0 \\ a_{12} = 0, a_{11} = 2 \\ a_{14} = 0, a_{13} = 0 \\ a_{16} = 2, a_{15} = 0 \end{array} \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}}_{=\varepsilon_{\overline{\Gamma}}} \xrightarrow{\pi} \underbrace{\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}}_{=\varepsilon_{\overline{\Gamma'}}} \begin{array}{l} a'_4 = 0, a'_3 = 0 \\ a'_6 = 0, a'_5 = 0 \\ a'_8 = 0, a'_7 = 0 \\ a'_{10} = 2, a'_9 = 0 \\ a'_{12} = 2, a'_{11} = 0 \\ a'_{14} = 2, a'_{13} = 0 \\ a'_{16} = 0, a'_{15} = 2 \end{array} ,$$

where π is the permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 4 & 2 & 7 & 3 & 6 \end{pmatrix}$ of the rows of $\varepsilon_{\overline{\Gamma}}$.

For $a_1 = a'_1 = a_2 = a'_2 = 0$ we receive the word length

$$n = \sum_{i=1}^{8} a_{2i} + \sum_{i=1}^{8} a_{2i-1} = \sum_{i=1}^{8} a'_{2i} + \sum_{i=1}^{8} a'_{2i-1} = 8.$$

We choose the code $\mathcal{C} = \{ \underbrace{(1,1,1,1,1,1,0,0)}_{s}, \underbrace{(1,1,0,0,0,0,1,1)}_{c} \}$ and the secret s.

For all $i \in \{4, 8, 11, 16\}$ the components a_i of the elementary solution a are nonzero. We choose the following positions to be defined by the a_i:

$$\begin{aligned} I_4 &= |\mathrm{supp}(s) \cap \mathrm{supp}(k_1) \cap \overline{\mathrm{supp}(k_2)} \cap \overline{\mathrm{supp}(k_3)}| : && \text{positions } 1, 2 \\ I_8 &= |\mathrm{supp}(s) \cap \mathrm{supp}(k_1) \cap \mathrm{supp}(k_2) \cap \overline{\mathrm{supp}(k_3)}| : && \text{positions } 5, 6 \\ I_{11} &= |\overline{\mathrm{supp}(s)} \cap \mathrm{supp}(k_1) \cap \overline{\mathrm{supp}(k_2)} \cap \mathrm{supp}(k_3)| : && \text{positions } 7, 8 \\ I_{16} &= |\mathrm{supp}(s) \cap \mathrm{supp}(k_1) \cap \mathrm{supp}(k_2) \cap \mathrm{supp}(k_3)| : && \text{positions } 3, 4 \end{aligned}$$

This yields the shares $k_1, \ldots, k_8$. The shares $k'_1, \ldots, k'_8$ are defined by

$$k'_j = (B^{-1})^{\tau} \cdot k_j \text{ for all } j = 1, \ldots, 8.$$

We obtain the following sums:

$$\begin{array}{llllllllll}
S_1 & = s & = & 1\,1\,1\,1\,1\,1\,0\,0 & = & 1\,1\,1\,1\,1\,1\,0\,0 & = & s & = & S_1' \\
S_2 & = k_1 & = & 1\,1\,1\,1\,1\,1\,1\,1 & & \boxed{1\,1\,0\,0\,0\,0\,1\,1} & = & k_1' & = & S_2' \\
S_3 & = k_2 & = & 0\,0\,1\,1\,1\,1\,0\,0 & & \boxed{0\,0\,1\,1\,0\,0\,1\,1} & = & k_2' & = & S_3' \\
S_5 & = k_3 & = & \boxed{0\,0\,1\,1\,0\,0\,1\,1} & & 1\,1\,1\,1\,1\,1\,1\,1 & = & k_3' & = & S_5' \\
S_4 & = k_1 + k_2 & = & \boxed{1\,1\,0\,0\,0\,0\,1\,1} & & 1\,1\,1\,1\,0\,0\,0\,0 & = & k_1' + k_2' & = & S_4' \\
S_6 & = k_1 + k_3 & = & 1\,1\,0\,0\,1\,1\,0\,0 & & 0\,0\,1\,1\,1\,1\,0\,0 & = & k_1' + k_3' & = & S_6' \\
S_7 & = k_2 + k_3 & = & \boxed{0\,0\,0\,0\,1\,1\,1\,1} & & 1\,1\,0\,0\,1\,1\,0\,0 & = & k_2' + k_3' & = & S_7' \\
S_8 & = k_1 + k_2 & = & 1\,1\,1\,1\,0\,0\,0\,0 & & \boxed{0\,0\,0\,0\,1\,1\,1\,1} & = & k_1' + k_2' & = & S_8' \\
 & \quad +k_3 & & & & & & +k_3' & &
\end{array}$$

We see that the same sums occur for both access structures. Only their order is different. Furthermore the matrices K, K' whose rows are the shares have the relation

$$\underbrace{\begin{pmatrix}1&1&0\\0&0&1\\1&0&0\end{pmatrix}}_{(B^{-1})^{\top}} \cdot \underbrace{\begin{pmatrix}1&1&1&1&1&1&1&1\\0&0&1&1&1&1&0&0\\0&0&1&1&0&0&1&1\end{pmatrix}}_{K} = \underbrace{\begin{pmatrix}1&1&0&0&0&0&1&1\\0&0&1&1&0&0&1&1\\1&1&1&1&1&1&1&1\end{pmatrix}}_{K'}.$$

A look at the distances of the sums to the secret s and to the wrong codeword c shows that $\mathcal{C}$ is suitable for both access structures.

	$d(S_i, s)$	$d(S_i, c)$
$S_2 = S_5'$	2	4
$S_3 = S_6'$	2	8
$S_4 = S_2'$	6	0
$S_5 = S_3'$	6	4
$S_6 = S_7'$	2	4
$S_7 = S_8'$	6	4
$S_8 = S_4'$	2	4

Remark 5.24. Let Γ, Γ' be two access structures in the same class realized elementarily by (b_1, g, k) and let $\mathcal{C}$ be a binary code which is suitable for (s, Γ, b_1, g, k) for a codeword $s \in \mathcal{C}$ with weight b_1. Suppose that additionally

$$2k + 1 \leq d(\mathcal{C}) \quad \text{and} \quad g > \rho(\mathcal{C})$$

holds. Then $\mathcal{C}$ is also suitable for (s, Γ', b_1, g, k) and the existence of a matrix B with the properties stated above is not necessary. In this case $w_{\overline{\Gamma}} = w_{\overline{\Gamma'}}$ holds by assumption and in the proof of Proposition 5.22 only part (c) of Definition 4.20 requires the existence of the matrix B. But with the additional requirements on k and g part (c) is already satisfied according to remark 4.21 (c).

Even when Γ and Γ' belong to different classes, they can nevertheless have the same elementary realization (b_1, g, k). Under certain conditions the same code $\mathcal{C}$ and the same secret $s \in \mathcal{C}$ are suitable for both access structures.

Lemma 5.25. Consider two access structures Γ, Γ' which allow the same parameters (b_1, g, k) with $g \leq b_1$. Assume that there are $u' \leq 2^t - 1$ unauthorized sets with regard to Γ' and let $a' = (a'_2, a'_3, \ldots, a'_{2^{t+1}})$ be an elementary solution for (Γ', b_1, g, k). Consider a binary code $\mathcal{C}$ with length n, minimal distance $d(\mathcal{C})$ and covering radius $\rho(\mathcal{C})$, which is suitable for (s, Γ, b_1, g, k) for a secret $s \in \mathcal{C}$ with weight b_1. Suppose that

- $n \geq 2b_1 - a'_2$
- $2k + 1 \leq d(\mathcal{C})$
- $g > \rho(\mathcal{C})$.

Then $\mathcal{C}$ is also suitable for (s, Γ', b_1, g, k).

Proof. We check the conditions of Definition 4.20:
Condition (a) holds by definition of s.
Remark 4.21 (b) shows that the elementary solution $a' = (a'_2, \ldots, a'_{2^{t+1}})$ for (Γ', b_1, g, k) has the property $\sum_{i=2}^{2^t} a'_{2i-1} \leq b_1 - a'_2$. Hence $b_1 + \sum_{i=2}^{2^t} a'_{2i-1} \leq 2b_1 - a'_2 \leq n$. This satisfies condition (b).
Finally, condition (c) is met because of Remark 4.21 (c). □

In this chapter we dealt with the question under which conditions two different access structures Γ, Γ' on the same set of participants have the same elementary realizations or even the same suitable codes and secrets. The following graphic summarizes our results.

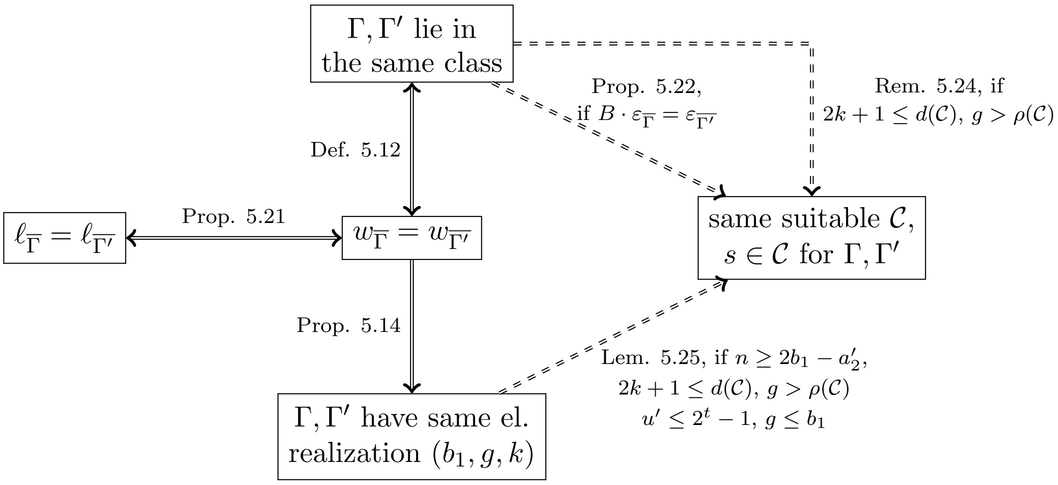

Γ, Γ' lie in the same class
Prop. 5.22, if $B \cdot \varepsilon_{\overline{\Gamma}} = \varepsilon_{\overline{\Gamma'}}$
Rem. 5.24, if $2k+1 \leq d(\mathcal{C})$, $g > \rho(\mathcal{C})$
Def. 5.12
$\ell_{\overline{\Gamma}} = \ell_{\overline{\Gamma'}}$
Prop. 5.21
$w_{\overline{\Gamma}} = w_{\overline{\Gamma'}}$
same suitable $\mathcal{C}$, $s \in \mathcal{C}$ for Γ, Γ'
Prop. 5.14
Lem. 5.25, if $n \geq 2b_1 - a'_2$, $2k+1 \leq d(\mathcal{C})$, $g > \rho(\mathcal{C})$ $u' \leq 2^t - 1$, $g \leq b_1$
Γ, Γ' have same el. realization (b_1, g, k)

Figure 5.1: Results of Chapter 5

At the end of this chapter we present two kinds of especially favorable parameters.

Lemma 5.26. Let Γ be an arbitrary access structure with an elementary realization (b_1, g, k) and a (not necessarily elementary) solution $a = (a_2, a_3, \ldots, a_{2^t+1})$ for (Γ, b_1, g, k).

(a) Suppose that $k = 0 < g$. Let $n \in \mathbb{N}$ be arbitrary with $n \geq b_1 + \sum_{i=2}^{2^t} a_{2i-1}$ and let $s \in \mathbb{Z}_2^n$ be arbitrary with weight b_1. Then $\mathcal{C} = \mathbb{Z}_2^n$ is suitable for (s, Γ, b_1, g, k). Especially for $n \geq 2b_1$ the code $\mathcal{C} = \mathbb{Z}_2^n$ is suitable for (s, Γ, b_1, g, k) for all $s \in \mathbb{Z}_2^n$ with weight b_1.

(b) Assume that there are $u \leq 2^t - 1$ unauthorized sets. Suppose that $b_1 = 2^e \geq g > 2^e - 2^{\frac{e-1}{2}}$ and $k < \frac{b_1}{2} = 2^{e-1}$ for an arbitrary $e \in \mathbb{N}$. Then the first order Reed Muller code $\mathcal{C} = RM(1, e+1)$ is suitable for (s, Γ, b_1, g, k) for all codewords $s \in \mathcal{C} \setminus \{(0. \ldots, 0), (1, \ldots, 1)\}$.

Proof. We check the requirements of Definition 4.20.

(a) Requirement (a) is obviously fulfilled. Requirement (b) holds because of Remark 4.21 (b).
(c) i. is fulfilled since $k = 0$ yields $1 = 2k + 1 \leq d(\mathcal{C}) = 1$ (see Remark 4.21 (c)).
(c) ii. holds since the sum of the shares of each unauthorized set is already a codeword $\neq s$.

(b) Requirement (a) is fulfilled since all codewords in $RM(1, e + 1)$ except for the zero word and the word $(1, \ldots, 1)$ have the weight $2^e = b_1$.
The code length of $\mathcal{C}$ is $n = 2^{e+1} = 2b_1$ and according to Remark 4.21 (b) requirement (b) is fulfilled.
According to Remark 4.21 (c), requirement (c) holds since $2k + 1 \leq 2^e = d(\mathcal{C})$ and since $g > 2^e - 2^{\frac{e-1}{2}}$ exceeds the covering radius of $\mathcal{C}$ (see 3.27).

□

One advantage of variant (a) is that no decoding is necessary. The authorized sets receive the secret s directly by adding their shares. Furthermore the knowledge of n yields neither the weight of the secret b_1 nor the number g of the incorrect positions. Hence the members of the unauthorized sets learn only very little about the secret from the sums of their shares.

Variant (b) has the advantage that g exceeds the covering radius of $\mathcal{C}$. When a set is unauthorized, Hamming decoding yields a wrong codeword. In contrast to the general solution stated in Theorem 4.22 this codeword is generally not the zero word.

For both variants the additional properties $2k+1 \leq d(\mathcal{C})$ and $g > \rho(\mathcal{C})$ are fulfilled. That means, if one access structure of an arbitrary class allows the given parameters, all other access structures of that class allow the same parameters and the given codes are suitable for all access structures of that class (see Remark 5.24).

In the next chapter we examine how specific operations on the access structures influence the elementary realizations. The classification of the access structures described above will become a very useful tool for this task.

Chapter 6

Operations on the Access Structures

For many access structures there are elementary realizations (b_1, g, k) which are superior to the universal realization provided by Theorem 4.22. The security distance g might be larger or the weight of the secret b_1 smaller, such that smaller code lengths are possible. For instance in Example 5.23 the parameters $b_1 = g = 6$ and $k = 2$ and the code length $n = 8$ are possible for an access structure on $t = 3$ participants. In contrast to that Theorem 4.22 provides parameters $b_1 \geq 2^{2t} - 2^t = 56$, $g \leq b_1 \left(\frac{1}{2} + \frac{1}{2^t}\right) - 2^{t-1} = \frac{5}{8} b_1 - 4$ and $k = \frac{b_1}{2} - 2^{t-1} = \frac{b_1}{2} - 4$ and a code length $n \geq b_1 = 56$.

In this chapter we study how certain operations performed on the access structures influence the possible elementary realizations and solutions. Starting with an access structure with favorable parameters this gives us the possibility to identify further access structures which allow parameters that are superior to the parameters of the universal solution.

Again we consider access structures on t participants and restrict ourselves to the case that there are only two different distances g, k from the sums of the shares to the secret.

6.1 The Dual Access Structure

At first we have a look at access structures and their duals. In order to find a relation between their elementary realizations we start with some fundamental considerations.

Remark 6.1. Let $\Gamma \subsetneq \mathcal{P}(\mathcal{T}) \setminus \{\varnothing\}$ be an arbitrary access structure and $\overline{\Gamma} = \mathcal{P}(\mathcal{T}) \setminus (\{\varnothing\} \cup \Gamma)$ the dual access structure.

(a) $\Gamma \cup \overline{\Gamma} = \mathcal{P}(\mathcal{T}) \setminus \{\varnothing\}$

(b) $\overline{\overline{\Gamma}} = \Gamma$

(c) Let $u = |\overline{\Gamma}|$. Then $u > 0$ since $\overline{\Gamma} \neq \varnothing$. We know that all rows of the matrix ε, except for the first row, contains 2^{t-1} ones and 2^{t-1} zeros. Furthermore the first column of ε is the zero vector. Hence the weight vector $w_{\overline{\Gamma}} = (w_0, \dots, w_u)$ of Γ determines the weight vector $w_\Gamma = (w'_0, \dots, w'_{2^t-u-1})$ of the dual access structure $\overline{\Gamma}$ uniquely by

$$w'_j = \begin{cases} w_{2^{t-1}-j} & \text{for all } j = 2^{t-1}-u, \dots, 2^{t-1} \\ 0 & \text{else} \end{cases} .$$

(d) Let $\Gamma, \Gamma' \subsetneq \mathcal{P}(\mathcal{T}) \setminus \{\varnothing\}$ be access structures on the same set of t participants. Then Γ and Γ' belong to the same class of access structures iff the matrices $\varepsilon^1_{\overline{\Gamma}}$ and $\varepsilon^1_{\overline{\Gamma'}}$ have the same linearity type, or equivalently iff the access structures have the same weight vector $w_{\overline{\Gamma}} = w_{\overline{\Gamma'}}$ (see Proposition 5.21). Using part (b) we see that this is equivalent to the dual access structures $\overline{\Gamma}$ and $\overline{\Gamma'}$ having the same weight vector $w_\Gamma = w_{\Gamma'}$. Equivalently the matrices ε^1_Γ and $\varepsilon^1_{\Gamma'}$ have the same linearity type which means that $\overline{\Gamma}$ and $\overline{\Gamma'}$ belong to the same class of access structures.

We will see that in some cases the same parameters b_1, g, k can be used for realizing the access structure Γ and also its dual $\overline{\Gamma}$. Furthermore the same codes can be suitable for both access structures.

Proposition 6.2. Let $\Gamma \subsetneq \mathcal{P}(\mathcal{T}) \setminus \{\varnothing\}$ be an arbitrary access structure realized elementarily by (b_1, g, k) such that $2b_1 - g - k \geq 0$ and $2^{t-1}|(2b_1 - g - k)$. Let $a = (a_2, \dots, a_{2^{t+1}})$ be an elementary solution for (Γ, b_1, g, k).
Define x to be the number characterized by equation 2 up to 2^t of the linear system 4.2 in the following way:

- $a_{2i} < \frac{1}{2^{t-1}}(2b_1 - g - k)$ for x different indices i and
- $a_{2i} \geq \frac{1}{2^{t-1}}(2b_1 - g - k)$ for $2^t - 1 - x$ different indices i

and define

$$S := \sum_{\substack{i=2 \\ 0 \leq a_{2i} < \frac{2b_1-g-k}{2^{t-1}}}}^{2^t} a_{2i}.$$

Suppose that

$$x \cdot \frac{2b_1 - g - k}{2^{t-1}} - S \leq b_1 - \sum_{i=2}^{2^t} a_{2i-1}$$

holds. Then (b_1, g, k) realizes $\overline{\Gamma}$ elementarily, too.

Proof. All non-empty sets which are unauthorized with regard to Γ are authorized with regard to $\overline{\Gamma}$ and vice versa. Hence the elementary weight vector $\overline{b}$ for $(\overline{\Gamma}, b_1, g, k)$ can be gained from the elementary weight vector b for (Γ, b_1, g, k) by interchanging all

g's and k's. For $u = |\overline{\Gamma}|$ and $\overline{u} = |\overline{\overline{\Gamma}}| = |\Gamma|$ we have $\overline{u} = 2^t - u - 1$. Furthermore there are exactly $\overline{c}_i = 2^{t-1} - c_i - 1$ ones in the ith row of E being multiplied with g while calculating $E \cdot \overline{b}$, where c_i is the number of ones in the ith row of E being multiplied with g in the calculation of $E \cdot b$.

Hence an elementary solution $\overline{a} = (\overline{a}_2, \ldots, \overline{a}_{2^{t+1}})$ for $(\overline{\Gamma}, b_1, g, k)$ is related to a as follows:

$$\begin{aligned}
a_{2i} - a_{2i-1} &= \frac{1}{2^{t-1}} E_i \cdot b \quad \text{(see Lemma 4.19 (a))} \\
&= \frac{1}{2^{t-1}} \left(b_1 - k + (2c_i - u)(g - k)\right) \\
&\qquad\qquad \downarrow \\
\overline{a}_{2i} - \overline{a}_{2i-1} &= \frac{1}{2^{t-1}} E_i \cdot \overline{b} \\
&= \frac{1}{2^{t-1}} \Big(b_1 - k + \big(2 \cdot (\underbrace{2^{t-1} - 1 - c_i}_{\overline{c}_i}) \underbrace{-2^t + u + 1}_{-\overline{u}}\big)(g - k)\Big) \\
&= \frac{1}{2^{t-1}} \left(b_1 - g - (2c_i - u)(k - g)\right) \\
&= \frac{1}{2^{t-1}} \left(2b_1 - g - k - (b_1 - k + (2c_i - u)(g - k))\right) \\
&= \frac{2b_1 - g - k}{2^{t-1}} - a_{2i} + a_{2i-1} \quad \text{for all } i = 2, \ldots, 2^t.
\end{aligned}$$

There are two cases to consider:

- Let $0 \leq a_{2i} < \frac{1}{2^{t-1}}(2b_1 - g + k)$, $a_{2i-1} \geq 0$. Then $\overline{a}_{2i} - \overline{a}_{2i-1} > 0$. We define $\overline{a}_{2i} = \frac{2b_1 - g - k}{2^{t-1}} - a_{2i} + a_{2i-1}$ and $\overline{a}_{2i-1} = 0$. This case occurs for x times.
- Let $a_{2i} \geq \frac{1}{2^{t-1}}(2b_1 - g + k) > 0$. Then $a_{2i-1} = 0$. Hence $\overline{a}_{2i} - \overline{a}_{2i-1} \leq 0$. We define $\overline{a}_{2i} = 0$ and $\overline{a}_{2i-1} = a_{2i} - \frac{2b_1 - g - k}{2^{t-1}}$.

$(\overline{a}_3, \overline{a}_4, \ldots, \overline{a}_{2^{t+1}} \in \mathbb{N}_0$ since $2^{t-1} | (2b_1 - g - k)$.) With these results we calculate

$$\begin{aligned}
\sum_{i=2}^{2^t} \overline{a}_{2i} &= \sum_{\substack{i=2 \\ 0 \leq a_{2i} < \frac{2b_1 - g - k}{2^{t-1}}}}^{2^t} \overline{a}_{2i} + \underbrace{\sum_{\substack{i=2 \\ a_{2i} \geq \frac{2b_1 - g - k}{2^{t-1}}}}^{2^t} \overline{a}_{2i}}_{=0} \\
&= x \cdot \frac{2b_1 - g - k}{2^{t-1}} - \underbrace{\sum_{\substack{i=2 \\ 0 \leq a_{2i} < \frac{2b_1 - g - k}{2^{t-1}}}}^{2^t} a_{2i}}_{= S} + \sum_{i=2}^{2^t} a_{2i-1} \\
&= \underbrace{x \cdot \frac{2b_1 - g - k}{2^{t-1}} - S}_{\leq b_1 - \sum_{i=2}^{2^t} a_{2i-1}} + \sum_{i=2}^{2^t} a_{2i-1} \leq b_1.
\end{aligned}$$

For $\overline{a}_2 = b_1 - \sum_{i=2}^{2^t} \overline{a}_{2i}$ we obtain $\sum_{i=1}^{2^t} \overline{a}_{2i} = b_1$. Hence $(\overline{a}_2, \overline{a}_3, \ldots, \overline{a}_{2^{t+1}})$ is an elementary solution for $(\overline{\Gamma}, b_1, g, k)$ and (b_1, g, k) realizes $\overline{\Gamma}$ elementarily. □

Remark 6.3. (a) Suppose that the conditions of Proposition 6.2 are satisfied and additionally $g \leq b_1$ holds. Let $\mathcal{C}$ be a binary code with the properties $2k+1 \leq d(\mathcal{C})$, $g > \rho(\mathcal{C})$ and $n \geq 2b_1 - \overline{a}_2$, which is suitable for (s, Γ, b_1, g, k) for a secret $s \in \mathcal{C}$. According to Lemma 5.25, $\mathcal{C}$ is also suitable for $(s, \overline{\Gamma}, b_1, g, k)$.

(b) Suppose that Γ allows the security distance $g = b_1$. Then all differences $a_{2i} - a_{2i-1}$ have to be multiples of $\frac{g-k}{2^{t-1}}$. Hence the inequality $a_{2i} < \frac{2b_1-g-k}{2^{t-1}}$ yields $a_{2i} < \frac{g-k}{2^{t-1}}$ which means $a_{2i} = 0$. Therefore $S = 0$. In this case x counts the number of equations with $a_{2i} = 0$. That means the parameters $b_1, g = b_1, k$ realize the dual access structure elementarily if $2b_1 - g - k = g - k$ is divisible by 2^{t-1} and if the inequality

$$x \leq \frac{2^{t-1}}{g-k}\left(b_1 - \sum_{i=2}^{2^t} a_{2i-1}\right)$$

holds.

Example 6.4. For $t = 3$ participants let

$$\Gamma = \{\{T_1\}, \{T_2\}, \{T_3\}, \{T_1, T_2, T_3\}\}.$$

The dual access structure is

$$\overline{\Gamma} = \{\{T_1, T_2\}, \{T_1, T_3\}, \{T_2, T_3\}\}.$$

We show that any parameters (b_1, g, k) with $b_1 = g$ and $k < g$ realize the access structure Γ. If additionally $g \leq 3k$ holds, (b_1, g, k) is also an elementary realization for $\overline{\Gamma}$. Furthermore we show that any binary simplex code with length $n = 2^l - 1$ for $l \geq 6$ is suitable for both access structures. We have

$$u = 3,\ \varepsilon^1_{\overline{\Gamma}} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \text{ and } w_{\overline{\Gamma}} = (1, 0, 6, 0).$$

Therefore the equations given in 4.2 are the following: For exactly one $i \in \{2, 3, \ldots, 8\}$ we have $c_i = 3$ and therefore the equation

$$\begin{aligned} a_{2i} - a_{2i-1} &= \frac{1}{4}(b_1 - k + (2c_i - u)(g - k)) \\ &= \frac{1}{4}((g - k) + (2 \cdot 3 - 3)(g - k)) \\ &= g - k. \end{aligned}$$

We define $a_{2i} = g - k$ and $a_{2i-1} = 0$.

In the remaining six equations $c_i = 1$ and the equations have the form

$$\begin{aligned} a_{2i} - a_{2i-1} &= \frac{1}{4}\left(b_1 - k + (2c_i - u)(g-k)\right) \\ &= \frac{1}{4}\left((g-k) + (2\cdot 1 - 3)(g-k)\right) = 0. \end{aligned}$$

In this cases we define $a_{2i} = a_{2i-1} = 0$. This yields

$$\sum_{i=2}^{8} a_{2i} \;=\; g - k \;\le\; g \;=\; b_1.$$

This shows that arbitrary parameters (g, g, k) with $k \le g$ realize Γ elementarily.

According to Remark 6.3 (b), the number of the components a_{2i} for $i = 2, \dots, 8$ in the range from 0 to $\frac{1}{2^{t-1}}(2b_1 - g - k)$ is $x = 6$ and the sum of these a_{2i} is $S = 0$. This yields

$$\begin{aligned} x &\le \tfrac{2^{t-1}}{g-k}\left(b_1 - \sum_{i=2}^{2^t} a_{2i-1}\right) \\ \Leftrightarrow\; 6 &\le \tfrac{4}{g-k}\cdot g \\ \Leftrightarrow\; g &\le 3k. \end{aligned}$$

Hence $\overline{\Gamma}$ is realized elementarily by any (g, g, k), too, provided that $g \le 3k$ and $4|g-k$.

Now choose an arbitrary $l \in \mathbb{N}$, $l \ge 6$, and consider a binary simplex code $\mathcal{C}$ with length $n = 2^l - 1$. All codewords in $\mathcal{C}$, except for the zero word, have weight 2^{l-1}. The minimal distance is $d(\mathcal{C}) = 2^{l-1}$ and the covering radius $\rho(\mathcal{C}) = 2^{l-1} - 1$.
We define $g = b_1 = 2^{l-1}$ and $k = 2^{l-2} - 4$. This yields $g > \rho(\mathcal{C})$ and $2k + 1 \le d(\mathcal{C})$. Furthermore $g \le 3k$ holds and $4|(g-k)$. Hence $(2^{l-1}, 2^{l-1}, 2^{l-2} - 4)$ is an elementary realization for both access structures. We have

$$a_2 = b_1 - \sum_{i=1}^{2^t} a_{2i} = g - (g-k) = k \quad\text{and}\quad a_1 = n - b_1 - \underbrace{\sum_{i=1}^{2^t} a_{2i-1}}_{0} = g - 1.$$

According to Remark 4.21, $\mathcal{C}$ is suitable for (s, Γ, b_1, g, k) for all nonzero codewords $s \in \mathcal{C}$. It remains to show that $n \ge 2b_1 - \overline{a}_2$ holds. In this case Remark 6.3 (a) says that $\mathcal{C}$ is also suitable for $(s, \overline{\Gamma}, b_1, g, k)$.

$$
\begin{aligned}
2b_1 - \overline{a}_2 &= 2b_1 - \left(b_1 - \sum_{i=2}^{2^t} \overline{a}_{2i} \right) \\
&= b_1 + \sum_{i=2}^{2^t} \overline{a}_{2i} \\
&= b_1 + (\underbrace{x}_{6} \cdot \frac{2b_1 - g - k}{2^{t-1}} - \underbrace{S}_{0} + \underbrace{\sum_{i=2}^{2^t} a_{2i-1}}_{0}) \\
&= b_1 + \frac{3}{2}(g-k) \\
&= 2^{l-1} + \frac{3}{2} \cdot (2^{l-2} + 4) \\
&= \underbrace{2^l - 1}_{n} \underbrace{-2^{l-3} + 7}_{\leq 0} \ \leq \ n.
\end{aligned}
$$

6.2 Embedding of Access Structures

Let Γ be an access structure on a set $\mathcal{T}$ of participants. Consider an arbitrary superset $\mathcal{T}'$ of $\mathcal{T}$. Then Γ is also an element of the power set $\mathcal{P}(\mathcal{T}')$ and therefore an access structure on the superset $\mathcal{T}'$. We denote it $\Gamma_{\mathcal{T}'}$ and call this access structure the *embedding of* Γ *in* $\mathcal{P}(\mathcal{T}')$.

In this section we show under which conditions an elementary realization (b_1, g, k) for Γ is also suitable for all its embeddings $\Gamma_{\mathcal{T}'}$.

Example 6.5. Consider the access structure $\Gamma = \{\{T_1, T_2\}\} \subseteq \mathcal{P}(\underbrace{\{T_1, T_2\}}_{=\mathcal{T}})$ with the non-empty unauthorized sets $\{T_1\}$ and $\{T_2\}$.
The embedding $\Gamma_{\mathcal{T}'}$ of Γ in $\mathcal{P}(\underbrace{\{T_1, T_2, T_3, T_4\}}_{\mathcal{T}'})$ consists also of the authorized set $\{T_1, T_2\}$. The non-empty unauthorized sets are

$$
\begin{aligned}
&\{T_1\}, \{T_2\}, \{T_3\}, \{T_1, T_3\}, \{T_2, T_3\}, \{T_1, T_2, T_3\}, \{T_4\}, \{T_1, T_4\}, \\
&\{T_2, T_4\}, \{T_1, T_2, T_4\}, \{T_3, T_4\}, \{T_1, T_3, T_4\}, \{T_2, T_3, T_4\}, \{T_1, T_2, T_3, T_4\}.
\end{aligned}
$$

Proposition 6.6. Consider an access structure Γ on a set $\mathcal{T}$ of t participants and its embedding $\Gamma_{\mathcal{T}'}$ in the power set of a participants set $\mathcal{T}' \supseteq \mathcal{T}$ with $t' \geq t$ participants. Suppose that there are u non-empty unauthorized sets with regard to Γ and that (b_1, g, k) realizes Γ elementarily such that

$$b_1 - k \leq (2^t - u)(g - k)$$

holds. Then (b_1, g, k) is also an elementary realization for $\Gamma_{\mathcal{T}'}$.

Proof. Consider the matrix ε^1_Γ whose columns are the characteristic vectors of the authorized sets with regard to Γ. Suppose that the matrix ε_Γ, whose rows are the non-trivial linear combinations of the rows of ε^1_Γ, has the weight vector

$$w_\Gamma = (w_0, \ldots, w_{2^t-u-1}).$$

For $\mathcal{T}' = \{T_{t+1}, \ldots, T_{t'}\}$ the matrix $\varepsilon^1_{\Gamma_{\mathcal{T}'}}$, which consists of the characteristic vectors of the authorized sets in $\Gamma_{\mathcal{T}'}$, has the form.

$$\varepsilon^1_{\Gamma_{\mathcal{T}'}} = \underbrace{\begin{pmatrix} & \varepsilon^1_\Gamma & \\ 0 & \ldots & 0 \\ \vdots & & \vdots \\ 0 & \ldots & 0 \end{pmatrix}}_{2^t-u-1} \begin{matrix} \}\, t \\ \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} t'-t \end{matrix}.$$

Hence the matrix $\varepsilon_{\Gamma_{\mathcal{T}'}}$ has the weight vector

$$w_{\Gamma_{\mathcal{T}'}} = (2^{t'-t} - 1 + 2^{t'-t}w_0, 2^{t'-t}w_1, \ldots, 2^{t'-t}w_{2^t-u-1})$$

(see Lemma 5.19). There are $u' = 2^{t'} - 1 - (2^t - u - 1) = 2^{t'} - 2^t + u$ non-empty unauthorized sets with regard to $\Gamma_{\mathcal{T}'}$ and the matrix $\varepsilon_{\overline{\Gamma_{\mathcal{T}'}}}$ has the following row weights:
$2^{t'-t} - 1 + 2^{t'-t}w_0$ rows have the weight $2^{t'-1}$ and
$2^{t'-t}w_j$ rows have the weight $2^{t'-1} - j$ for all $j = 1, 2, \ldots, 2^t - u - 1$.
Let $(a_2, a_3, \ldots, a_{2^t+1})$ be an elementary solution for (Γ, b_1, g, k). In the first case there are indices i such that

$$\begin{aligned} a'_{2i} - a'_{2i-1} &= \frac{1}{2^{t'-1}}\Big(b_1 - k + (2^{t'} - 2^t + u - 2\cdot 2^{t'-1})(g-k)\Big) \\ &= \frac{1}{2^{t'-1}}\underbrace{\big(b_1 - k + (u - 2^t)(g-k)\big)}_{\leq 0} \\ &= \frac{1}{2^{t'-t}}(a_{2i} - a_{2i-1}) \end{aligned}$$

and we define $a'_{2i} = 0$ and $a'_{2i-1} = -\frac{1}{2^{t'-1}}\left(b_1 - k + (u - 2^t)(g-k)\right)$.
In the second case there are indices i such that

$$\begin{aligned} a'_{2i} - a'_{2i-1} &= \frac{1}{2^{t'-1}}\Big(b_1 - k + (2^{t'} - 2^t + u - 2\cdot(2^{t'-1} - j))(g-k)\Big) \\ &= \frac{1}{2^{t'-1}}\big(b_1 - k + (u - 2\cdot(2^{t-1} - j))(g-k)\big) \\ &= \frac{1}{2^{t'-t}}(a_{2i} - a_{2i-1}) \end{aligned}$$

and we define $a'_{2i} = \frac{1}{2^{t'-t}}a_{2i}$ and $a'_{2i-1} = \frac{1}{2^{t'-t}}a_{2i-1}$.

This yields $\sum\limits_{i=2}^{2^{t'}} a'_{2i} = 2^{t'-t}\frac{1}{2^{t'-t}}\sum\limits_{i=2}^{2^t} a_{2i} = b_1 - a_2$ and we define $a'_2 = a_2$ and obtain the elementary solution $(a'_2, a'_3, \ldots, a'_{2^{t'}+1})$ for $(\Gamma_{\mathcal{T}'}, b_1, g, k)$. □

There is also another kind of embedding. Γ defines an access structure Γ' on the superset $\mathcal{T}'$ with the property that each subset A of $\mathcal{T}'$ is (un-)authorized iff the intersection $A \cap \mathcal{T}$ is (un-)authorized. That means

$$\Gamma' = \{A \cup B : A \in \Gamma, B \in \mathcal{P}(\mathcal{T}' \setminus \mathcal{T})\} \subseteq \mathcal{P}(\mathcal{T}').$$

In this access structure the participants of $\mathcal{T}' \setminus \mathcal{T}$ have no influence on whether a subset is authorized or not.

Example 6.7. Consider the access structure

$$\Gamma = \{\{T_1, T_2\}\} \subseteq \mathcal{P}(\underbrace{\{T_1, T_2\}}_{=\mathcal{T}}).$$

Then Γ' in $\mathcal{P}(\underbrace{\{T_1, T_2, T_3, T_4\}}_{\mathcal{T}'})$ is just the access structure

$$\Gamma' = \left\{ \{T_1, T_2\}, \{T_1, T_2, T_3\}, \{T_1, T_2, T_4\}, \{T_1, T_2, T_3, T_4\} \right\}.$$

Suppose that there are shares for the participants in $\mathcal{T} = \{T_1, \ldots, T_t\}$, which can be used to share a secret s in a suitable code $\mathcal{C}$ of length n according to Γ. By assigning the participants of $\mathcal{T}' \setminus \mathcal{T}$ the zero word of length n as shares, the secret s can be shared among the participants of $\mathcal{T}'$ according to Γ'.

6.3 Symmetric Difference

The next technique is to replace all authorized sets A of an access structure Γ^1 by the symmetric differences $A \vartriangle B$ for a given unauthorized subset $B \in \overline{\Gamma^1}$. This leads to an interesting access structure Γ with the same number of authorized sets. We will see that the transition from $\varepsilon^1_{\Gamma^1}$ to the matrix ε^1_{Γ} related to the new access structure is characterized by adding the characteristic vector of B to all columns of $\varepsilon^1_{\Gamma^1}$. Only the column related to B remains unchanged. With that knowledge we identify pairs (Γ^1, B) such that both ε^1-matrices have the same linearity type. Where this is the case the access structures Γ^1 and Γ belong to the same class and can be realized using the same parameters.

Definition 6.8. Consider an arbitrary set M and a set $B \subseteq M$ and let $U \subseteq \mathcal{P}(M)$. Define the *symmetric difference of* U and B to be the set

$$U \vartriangle B := \{A \vartriangle B : A \in U\}.$$

We consider the case that M is the set $\mathcal{T}$ of the participants $T_1, \ldots, T_t$, U is an access structure Γ^1 and B is an unauthorized set in $\overline{\Gamma^1}$.

Example 6.9. Let $\Gamma^1 = \{\{T_2\}, \{T_3\}, \{T_1, T_3\}, \{T_2, T_3\}\}$ and $B = \{T_1\} \in \overline{\Gamma^1}$. Then

$$\begin{aligned} \Gamma = \Gamma^1 \vartriangle B &= \{\{T_2\} \vartriangle \{T_1\}, \{T_3\} \vartriangle \{T_1\}, \{T_1, T_3\} \vartriangle \{T_1\}, \{T_2, T_3\} \vartriangle \{T_1\}\} \\ &= \{\{T_1, T_2\}, \{T_1, T_3\}, \{T_3\}, \{T_1, T_2, T_3\}\}. \end{aligned}$$

Next we study the effect of the symmetric difference on the dual access structure. For this we need the following lemma.

Lemma 6.10. Let M be an arbitrary set and $B \subseteq M$ a subset. Then

$$\mathcal{P}(M) = \{A \vartriangle B : A \subseteq M\} = \mathcal{P}(M) \vartriangle B.$$

Proof. $\mathcal{P}(M) \supseteq \mathcal{P}(M) \vartriangle B$ is clear since $B \subseteq M$. Additionally

$$\begin{aligned} \mathcal{P}(M) &= \{A : A \subseteq M\} \\ &= \{(A \vartriangle B) \vartriangle B : A \subseteq M\} \\ &\subseteq \mathcal{P}(M) \vartriangle B. \end{aligned}$$

□

We use Lemma 6.10 to describe the dual access structure $\overline{\Gamma^1 \vartriangle B}$.

Lemma 6.11. Let $\Gamma^1 \subsetneq \mathcal{P}(\mathcal{T}) \setminus \{\varnothing\}$ be an arbitrary access structure and $B \in \overline{\Gamma^1}$ an unauthorized set. Define $\Gamma = \Gamma^1 \vartriangle B$. Then $\overline{\Gamma} = \Big((\overline{\Gamma^1} \setminus \{B\}) \vartriangle B)\Big) \cup \{B\}$.

Proof.

$$\begin{aligned} \overline{\Gamma} &= (\mathcal{P}(\mathcal{T}) \setminus \Gamma) \setminus \{\varnothing\} \\ &= ((\mathcal{P}(\mathcal{T}) \vartriangle B) \setminus \Gamma) \setminus \{\varnothing\} \quad \text{(Lemma 6.10)} \\ &= \big((\mathcal{P}(\mathcal{T}) \vartriangle B) \setminus (\Gamma^1 \vartriangle B)\big) \setminus \{\varnothing\} \\ &= \big((\mathcal{P}(\mathcal{T}) \setminus \Gamma^1) \vartriangle B\big) \setminus \{\varnothing\} \\ &= \big((\overline{\Gamma^1} \cup \{\varnothing\}) \vartriangle B\big) \setminus \{\varnothing\} \\ &= \big(((\overline{\Gamma^1} \setminus \{B\}) \vartriangle B) \cup (\underbrace{\{B\} \vartriangle B}_{\{\varnothing\}}) \cup (\underbrace{\{\varnothing\} \vartriangle B}_{\{B\}})\big) \setminus \{\varnothing\} \\ &= \big((\overline{\Gamma^1} \setminus \{B\}) \vartriangle B)\big) \cup \{B\} \end{aligned}$$

□

Example 6.12. For Γ^1, B as in Example 6.9 we have

$$\begin{aligned} &\Big((\overline{\Gamma^1} \setminus \{B\}) \vartriangle B)\Big) \cup \{B\} \\ = \; &(\{\{T_1, T_2\}, \{T_1, T_2, T_3\}\} \vartriangle \{T_1\}) \cup \{\{T_1\}\} \\ = \; &\{\{T_2\}, \{T_2, T_3\}\} \cup \{\{T_1\}\} \\ = \; &\{\{T_1\}, \{T_2\}, \{T_2, T_3\}\} \\ = \; &\overline{\Gamma}. \end{aligned}$$

Remark 6.13. Let $A, B \subseteq \mathcal{T}$ with the characteristic vectors $x = (x_1, \ldots, x_t)^\tau$, $y = (y_1, \ldots, y_t)^\tau \in \mathbb{Z}_2^t$ and let $z = (z_1, \ldots, z_t) \in \mathbb{Z}_2^t$ be the characteristic vector of $A \vartriangle B$. Then $z = x + y$, since for all $j = 1, \ldots, t$

$$\begin{aligned} z_j = 1 &\Leftrightarrow T_j \in A \vartriangle B \\ &\Leftrightarrow T_j \in A \;\; XOR \;\; T_j \in B \\ &\Leftrightarrow x_j = 1 \;\; XOR \;\; y_j = 1 \\ &\Leftrightarrow x_j + y_j = 1. \end{aligned}$$

In terms of the ε^1-matrices the transition from Γ^1 to $\Gamma = \Gamma^1 \vartriangle B$ means the following.

Lemma 6.14. Let $v_1, \ldots, v_u \in \mathbb{Z}_2^t$ be the characteristic vectors of the unauthorized sets in $\overline{\Gamma^1}$. W.l.o.g. assume that $v_1 = b$ is the characteristic vector of B. Let $\Gamma = \Gamma^1 \vartriangle B$. Then the columns of $\varepsilon^1_{\overline{\Gamma}}$ are $b, v_2 + b, \ldots, v_u + b$.

Proof. According to Lemma 6.11, the columns of $\varepsilon^1_{\overline{\Gamma}}$ have to be the characteristic vectors of the set B and of all sets $A \vartriangle B$ with $A \in \overline{\Gamma^1}$, $A \neq B$. These vectors are exactly b and $v_2 + b, \ldots, v_u + b$ by Remark 6.13. □

In general the access structures Γ^1 and $\Gamma^1 \vartriangle B$ have different linearity types.

Example 6.15. For $t = 3$ participants let $\overline{\Gamma^1} = \{\{T_1\}, \{T_1, T_2\}, \{T_3\}, \{T_1, T_2, T_3\}\}$ and $B = \{T_1\}$. Then

$$\varepsilon^1_{\overline{\Gamma^1}} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad \text{and} \quad \varepsilon^1_{\overline{\Gamma}} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

The linearity vectors are $\ell_{\overline{\Gamma^1}} = (0, 0, 1, 0) \neq \ell_{\overline{\Gamma}} = (0, 0, 0, 1)$.

However, there are cases where Γ^1 and $\Gamma^1 \vartriangle B$ belong to the same class. In these cases the same parameters can be used for both access structures. The following proposition describes pairs of access structures Γ^1 and unauthorized sets B with this property.

Proposition 6.16. Let $\Gamma^1 \subsetneq \mathcal{P}(\mathcal{T}) \setminus \{\varnothing\}$ be an access structure and $B \in \overline{\Gamma^1}$ an unauthorized set with the characteristic vector $b \in \mathbb{Z}_2^t$. Let $v_1 = b, v_2, \ldots, v_u$ be the columns of $\varepsilon^1_{\overline{\Gamma^1}}$. Suppose that $\sum\limits_{p=1}^{n} v_{j_p} = 0$ implies

- $b \notin \{v_{j_1}, \ldots, v_{j_n}\}$ and n even or
- $b \in \{v_{j_1}, \ldots, v_{j_n}\}$ and n odd.

Then Γ^1 and $\Gamma = \Gamma^1 \vartriangle B$ belong to the same class.

Proof. According to Lemma 6.14, the columns of ε^1_Γ are $v'_1 = b$, $v'_2 = v_2 + b, \dots, v'_u = v_u + b$. Since their order has no effect on the linearity type we assume w.l.o.g. that $\varepsilon^1_\Gamma = \big(v'_1, \dots, v'_u\big) = \big(b, v_2 + b, \dots, v_u + b\big)$. We show that

$$\sum_{p=1}^{n} v_{j_p} = 0 \quad \Leftrightarrow \quad \sum_{p=1}^{n} v'_{j_p} = 0$$

holds for all $n = 1, \dots, u$ and all choices $\{j_1, \dots, j_n\} \subseteq \{1, \dots, u\}$. Then both matrices have the same linearity type and belong to the same class (see Proposition 5.21). According to the restrictions in the proposition, there are two cases with $\sum\limits_{p=1}^{n} v_{j_p} = 0$:

1. Suppose that $b \notin \{v_{j_1}, \dots, v_{j_n}\}$ and n is even. Then

$$\sum_{p=1}^{n} v_{j_p} = \underbrace{nb}_{=0} + \sum_{p=1}^{n} v_{j_p} = \sum_{p=1}^{n} (v_{j_p} + b) = \sum_{p=1}^{n} v'_{j_p}.$$

2. Let $b \in \{v_{j_1}, \dots, v_{j_n}\}$ and n be odd. W.l.o.g assume that $v_{j_1} = b$. Since $b = v_1$ that means $j_1 = 1$. Then

$$\sum_{p=1}^{n} v_{j_p} = \underbrace{b}_{v_{j_1}} + \sum_{p=2}^{n} v_{j_p} = \underbrace{(n-1)b}_{=0} + b + \sum_{p=2}^{n} v_{j_p} = \underbrace{b}_{v'_{j_1}} + \sum_{p=2}^{n} \underbrace{(v_{j_p} + b)}_{=v'_{j_p}} = \sum_{p=1}^{n} v'_{j_p}.$$

Now suppose that $\sum\limits_{p=1}^{n} v'_{j_p} = 0$.

1. Let $b \notin \big\{v'_{j_1}, \dots, v'_{j_n}\big\}$. Then

$$0 = \sum_{p=1}^{n} v'_{j_p} = nb + \sum_{p=1}^{n} v_{j_p}.$$

If n is even, this implies $\sum\limits_{p=1}^{n} v_{j_p} = 0$. Otherwise, when n is odd, we have $0 = b + \sum\limits_{p=1}^{n} v_{j_p}$. This is a contradiction since the summand b occurs and the number of summands (including b) is even.

2. Let $b \in \big\{v'_{j_1}, \dots, v'_{j_n}\big\}$. W.l.o.g assume that $v'_{j_1} = b$. Then

$$0 = \sum_{p=1}^{n} v'_{j_p} = nb + \sum_{p=2}^{n} v_{j_p}.$$

If n is even, $\sum\limits_{p=2}^{n} v_{j_p} = 0$. This is a contradiction since the number of summands is odd and the summand b is not involved. When n is odd, we receive $0 = b + \sum\limits_{p=2}^{n} v_{j_p} = \sum\limits_{p=1}^{n} v_{j_p}$.

□

Remark 6.17. Let Γ^1 be an access structure with an unauthorized set B such that the requirements of Proposition 6.16 are met. Then Γ^1 and $\Gamma = \Gamma^1 \triangle B$ have the same elementarily realizations (see Proposition 5.14).
Additionally, if there is an invertible binary matrix M such that $\varepsilon^1_{\overline{\Gamma^1}} = M \cdot \varepsilon^1_{\overline{\Gamma}}$ holds, the same codes are suitable for both access structures (see Proposition 5.22).

Example 6.18. The access structure Γ^1 and the unauthorized set B from Example 6.9 yield

$$\varepsilon^1_{\overline{\Gamma^1}} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = (v_1, v_2, v_3) = (b, v_2, v_3)$$

and

$$\varepsilon^1_{\overline{\Gamma}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = (v'_1, v'_2, v'_3) = (b, v_2 + b, v_3 + b).$$

Since v_1, v_2, v_3 are linearly independent, there are no sums $\sum\limits_{p=1}^{n} v_{j_p} = 0$ and the requirements of Proposition 6.16 are fulfilled. Hence both access structures belong to the same class. Furthermore there is an invertible (3×3)-matrix M such that $\varepsilon^1_{\overline{\Gamma^1}} = M \cdot \varepsilon^1_{\overline{\Gamma}}$:

$$\underbrace{\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}}_{\varepsilon^1_{\overline{\Gamma^1}}} = \underbrace{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{M} \cdot \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}}_{\varepsilon^1_{\overline{\Gamma}}}$$

and Γ^1 and Γ have the same suitable codes.

Sometimes it is easier to determine the characteristic vectors of the authorized sets, than the characteristic vectors of the unauthorized sets, and it is easier to find the matrix $\varepsilon^1_{\Gamma^1}$ than the matrix $\varepsilon^1_{\overline{\Gamma^1}}$. Furthermore, in some cases it is easier to find out, which sums of the columns of $\varepsilon^1_{\Gamma^1}$ yield the zero vector, than to check the sums of the columns of $\varepsilon^1_{\overline{\Gamma^1}}$. The following remark shows the connection between the columns of $\varepsilon^1_{\Gamma^1}$ and $\varepsilon^1_{\overline{\Gamma^1}}$. Moreover, we give a criterion concerning the columns of $\varepsilon^1_{\Gamma^1}$ for Γ^1 and Γ belonging to the same class.

Remark 6.19. (a) Let $\Gamma = \Gamma^1 \triangle B$, $B \in \overline{\Gamma^1}$. Suppose that $\varepsilon^1_{\Gamma^1}$ consists of the columns $v_{u+2}, \ldots, v_{2^t}$. Let $v_1 = b$ be the characteristic vector of B and let $v_2, \ldots, v_u$ denote the remaining nonzero vectors of $\mathbb{Z}_2^t$. Using Lemma 6.10 the set $\mathbb{Z}_2^t$ of all characteristic vectors of the subsets of $\mathcal{T}$ can be written as

$$\begin{aligned}\mathbb{Z}_2^t &= \Big\{ \underbrace{v_1, \dots, v_u}_{\text{columns of } \varepsilon^1_{\overline{\Gamma^1}}}, 0, \underbrace{v_{u+2}, \dots, v_{2^t}}_{\text{columns of } \varepsilon^1_{\Gamma^1}} \Big\} \\ &= \Big\{ 0, \underbrace{v_2 + b, \dots, v_u + b, b}_{\text{columns of } \varepsilon^1_{\overline{\Gamma}}}, \underbrace{v_{u+2} + b, \dots, v_{2^t} + b}_{\text{columns of } \varepsilon^1_{\Gamma}} \Big\}.\end{aligned}$$

We know from Lemma 6.14 that the vectors $v_2 + b, \dots, v_u + b, b$ characterize the elements of $\overline{\Gamma}$. Hence the remaining nonzero vectors $v_{u+2} + b, \dots, v_{2^t} + b$ must be the columns of ε^1_{Γ}.

(b) Suppose that the columns $v_{u+2}, \dots, v_{2^t}$ of the matrix $\varepsilon^1_{\Gamma^1}$ have the property that a sum of pairwise distinct columns $v_{j_1}, \dots, v_{j_n}$ can only be the zero vector when the number n of the summands is even. The columns of ε^1_{Γ} have the form $v_{u+2} + b, \dots, v_{2^t} + b$ and the equivalence

$$\sum_{p=1}^{n} (v_{j_p} + b) = 0 \;\Leftrightarrow\; \sum_{p=1}^{n} v_{j_p} = 0$$

holds. That means $\varepsilon^1_{\Gamma^1}$ and ε^1_{Γ} have the same linearity type. Therefore $\overline{\Gamma^1}$ and $\overline{\Gamma}$ lie in the same class. According to Remark 6.1 (d), their duals Γ^1 and Γ lie in the same class, too.

6.4 The Intersection of Access Structures

Another technique to create new access structures is to intersect two initial access structures Γ_1 and Γ_2 on the same set $\mathcal{T}$ of t participants. At first we show how solutions for the initial access structures provide a solution for their intersection if the dual access structures $\overline{\Gamma_1}$ and $\overline{\Gamma_2}$ are disjoint. Then we generalize our results to arbitrary dual access structures.

First we analyze the dual of the intersection Γ. It turns out that it is the union of the dual access structures $\overline{\Gamma_1}$ and $\overline{\Gamma_2}$:

$$\begin{aligned}\overline{\Gamma} &= (\mathcal{P}(\mathcal{T}) \setminus \{\varnothing\}) \setminus (\Gamma_1 \cap \Gamma_2) \\ &= ((\mathcal{P}(\mathcal{T}) \setminus \{\varnothing\}) \setminus \Gamma_1) \cup ((\mathcal{P}(\mathcal{T}) \setminus \{\varnothing\}) \setminus \Gamma_2) \\ &= \overline{\Gamma}_1 \cup \overline{\Gamma}_2.\end{aligned}$$

In terms of the related ε-matrices this means that the columns of $\varepsilon_{\overline{\Gamma}}$ are exactly the columns which occur in $\varepsilon_{\overline{\Gamma_1}}$ or in $\varepsilon_{\overline{\Gamma_2}}$. When $\overline{\Gamma_1}$ and $\overline{\Gamma_2}$ are disjoint then $\varepsilon_{\overline{\Gamma}}$ is the concatenation of $\varepsilon_{\overline{\Gamma_1}}$ and $\varepsilon_{\overline{\Gamma_2}}$, except for the order of the columns. We use this fact to construct a solution for Γ from solutions for Γ_1 and Γ_2.

Proposition 6.20. Let $\Gamma_1, \Gamma_2 \subsetneq \mathcal{P}(\mathcal{T}) \setminus \{\varnothing\}$ be access structures on the same set of t participants with disjoint dual access structures.

(a) Suppose that (b_1, g, k) realizes Γ_1 elementarily and that (b_1', g', k') realizes Γ_2 elementarily with $g - k = g' - k'$. Then

$$(\hat{b}_1, \hat{g}, \hat{k}) = (b_1 + b_1', g + k', k + k')$$

realizes Γ elementarily.

(b) Additionally, let $\mathcal{C} \subseteq \mathbb{Z}_2^n$ be a suitable code for (s, Γ_1, b_1, g, k) for a codeword $s \in \mathcal{C}$ with weight b_1 and $\mathcal{C}' \subseteq \mathbb{Z}_2^{n'}$ be suitable for $(s', \Gamma_2, b_1', g', k')$ for a codeword $s' \in \mathcal{C}'$ with weight b_1'. Then the concatenation $\hat{\mathcal{C}}$ of $\mathcal{C}$ and $\mathcal{C}'$ is suitable for $(\hat{s}, \Gamma, \hat{b_1}, \hat{g}, \hat{k})$, where $\hat{s}$ is the concatenation of the codewords s and s'.

Proof. (a) Let $|\overline{\Gamma}_1| = u$ and $|\overline{\Gamma}_2| = u'$. Then $\overline{\Gamma}$ has $\hat{u} = u + u'$ elements since $\overline{\Gamma_1} \cap \overline{\Gamma_2} = \varnothing$. The matrix $\varepsilon_{\overline{\Gamma}}$ consists of the columns of $\varepsilon_{\overline{\Gamma_1}}$ and of $\varepsilon_{\overline{\Gamma_2}}$. Hence the number $\hat{c}_i$ of zeros in the ith column of $\varepsilon_{\overline{\Gamma}}$ is the sum $c_i + c_i'$ of zeros in the ith columns of $\varepsilon_{\overline{\Gamma_1}}$ and $\varepsilon_{\overline{\Gamma_2}}$.

We are looking for an elementary solution $\hat{a} = (\hat{a}_2, \ldots, \hat{a}_{2^{t+1}})$ for $(\Gamma, \hat{b}_1, \hat{g}, \hat{k}) = (\Gamma_1 \cap \Gamma_2, b_1 + b_2, g + k', k + k')$. Let $a = (a_2, \ldots, a_{2^{t+1}})$ and $a' = (a_2', \ldots, a_{2^{t+1}}')$ be elementary solutions for (Γ_1, b_1, g, k) and (Γ_2, b_1', g', k'), respectively. Then $\hat{a}$, a and a' have the following relations given by Equation 4.2:

$$\begin{aligned}
\hat{a}_{2i} - \hat{a}_{2i-1} &= \frac{1}{2^{t-1}} \left(\hat{b}_1 - \hat{k} + (2\hat{c}_i - \hat{u})(\hat{g} - \hat{k})\right) \\
&= \frac{1}{2^{t-1}} \left(b_1 + b_1' - (k + k') + (2(c_i + c_i') - (u + u'))\underbrace{(g + k' - (k + k'))}_{=g-k=g'-k'}\right) \\
&= \frac{1}{2^{t-1}} (b_1 - k + (2c_i - u)(g - k) + (b_1' - k' + (2c_i' - u')(g' - k')) \\
&= a_{2i} - a_{2i-1} + a_{2i}' - a_{2i-1}' \quad \text{for all } i = 2, 3, \ldots, 2^t.
\end{aligned}$$

We have to distinguish the following cases.

- If $a_{2i} > 0$ and $a_{2i}' > 0$ then $a_{2i-1} = a_{2i-1}' = 0$ and $\hat{a}_{2i} - \hat{a}_{2i-1} = a_{2i} + a_{2i}' > 0$. Hence
$$\hat{a}_{2i} = a_{2i} + a_{2i}' \quad \text{and} \quad \hat{a}_{2i-1} = 0 = a_{2i-1} + a_{2i-1}'.$$
- If $a_{2i} = a_{2i}' = 0$ then $a_{2i-1},\ a_{2i-1}' \geq 0$ and $\hat{a}_{2i} - \hat{a}_{2i-1} = -a_{2i-1} - a_{2i-1}' \leq 0$. Hence
$$\hat{a}_{2i} = 0 = a_{2i} + a_{2i}' \quad \text{and} \quad \hat{a}_{2i-1} = a_{2i-1} + a_{2i-1}' \geq 0.$$
- Let $a_{2i} > 0$ and $a_{2i}' = 0$. Then $a_{2i-1} = 0$, $a_{2i-1}' \geq 0$ and $\hat{a}_{2i} - \hat{a}_{2i-1} = a_{2i} - a_{2i-1}'$.

If $a_{2i} - a'_{2i-1} > 0$ then

$$\hat{a}_{2i} = a_{2i} - a'_{2i-1} \leq a_{2i} + a'_{2i} \text{ and } \hat{a}_{2i-1} = 0 \leq a_{2i-1} + a'_{2i-1}.$$

If $a_{2i} - a'_{2i-1} \leq 0$ then

$$\hat{a}_{2i} = 0 \leq a_{2i} + a'_{2i} \text{ and } \hat{a}_{2i-1} = a'_{2i-1} - a_{2i} \leq a_{2i-1} + a'_{2i-1}.$$

($a_{2i} = 0$ and $a'_{2i} > 0$ analogously)

In all cases the following equations are satisfied

$$\hat{a}_{2i} \leq a_{2i} + a'_{2i} \text{ and } \hat{a}_{2i-1} \leq a_{2i-1} + a'_{2i-1}.$$

Therefore

$$\begin{aligned}\sum_{i=2}^{2^t} \hat{a}_{2i} &\leq \sum_{i=2}^{2^t}(a_{2i} + a'_{2i}) \\ &= \sum_{i=2}^{2^t} a_{2i} + \sum_{i=2}^{2^t} a'_{2i} \leq b_1 + b'_1 = \hat{b}_1.\end{aligned}$$

This shows that $(b_1 + b'_1, g + k', k + k')$ realizes Γ elementarily.

(b) Let $\hat{\mathcal{C}}$ be the concatenation of the codes $\mathcal{C}$ and $\mathcal{C}'$ and $\hat{s}$ the concatenation of the codewords s and s'. We check the requirements of Definition 4.20.

- Requirement (a) is met since $\hat{s}$ is a codeword in $\hat{\mathcal{C}}$ with weight $b_1 + b'_1 = \hat{b}_1$.
- The code length of $\hat{\mathcal{C}}$ is

$$\begin{aligned}\hat{n} &= n + n' \\ &\geq b_1 + \sum_{i=2}^{2^t} a_{2i-1} + b'_1 + \sum_{i=2}^{2^t} a'_{2i-1} \\ &\quad \text{(since } \mathcal{C} \text{ is suitable for } (s, \Gamma_1, b_1, g, k) \text{ and} \\ &\quad \mathcal{C}' \text{ is suitable for } (s', \Gamma_2, b'_1, g', k')\text{)} \\ &= \underbrace{b_1 + b'_1}_{\hat{b}_1} + \sum_{i=2}^{2^t} \underbrace{(a_{2i-1} + a'_{2i-1})}_{\geq \hat{a}_{2i-1}} \\ &\geq \hat{b}_1 + \sum_{i=2}^{2^t} \hat{a}_{2i-1} \text{ (see proof of part (a))},\end{aligned}$$

which satisfies requirement (b) of Definition 4.20.

- Let $k_1, \ldots, k_t$ and $k'_1, \ldots, k'_t$ be shares which satisfy the conditions of Definition 4.20 (c) for s, Γ_1, b_1, g, k and $s', \Gamma_2, b'_1, g', k'$, respectively. Define the shares $\hat{k_1}, \ldots, \hat{k_t}$ for $\Gamma, \hat{b_1}, \hat{g}, \hat{k}$ to be the concatenations $\hat{k_i} = (k_i, k_i')$ for all $i = 1, \ldots, t$. For all $j = 1, \ldots, 2^t$ let $S_j, S_j', \hat{S}_j$ be the sums of the shares of the jth set $A_j \in \mathcal{P}(\mathcal{T})$ with respect to the shares k_i, the k_i' and $\hat{k_i}$.

- Suppose that $A_j \in \Gamma$. Then $A_j \in \Gamma_1$ and $A_j \in \Gamma_2$. Therefore $\mathrm{d}\left(S_j, s\right) = k$, $\mathrm{d}\left(S_j', s'\right) = k'$ and there are no codewords $c \in \mathcal{C}$, $c' \in \mathcal{C}'$ with $\mathrm{d}\left(S_j, c\right) \leq k$ and $\mathrm{d}\left(S_j', c'\right) \leq k'$. That means

$$\mathrm{d}\left(\hat{S}_j, \hat{s}\right) = \mathrm{d}\left(S_j, s\right) + \mathrm{d}\left(S_j', s'\right) = k + k' = \hat{k}$$

  and there is no other codeword $\hat{c} \in \hat{\mathcal{C}}$ with $\mathrm{d}\left(\hat{S}_j, \hat{c}\right) \leq \hat{k}$.

- For $A_j \in \overline{\Gamma}$, $A_j \in \overline{\Gamma_1} \cap \Gamma_2$ or $A_j \in \Gamma_1 \cap \overline{\Gamma_2}$. W.l.o.g we assume that the first case occurs. Then $\mathrm{d}\left(S_j, s\right) = g$ and $\mathrm{d}\left(S_j', s'\right) = k'$. We also know that there must be a codeword $c \in \mathcal{C}$ with $\mathrm{d}\left(S_j, c\right) < g$. Hence

$$\mathrm{d}\left(\hat{S}_j, \hat{s}\right) = \mathrm{d}\left(S_j, s\right) + \mathrm{d}\left(S_j', s'\right) = g + k' = \hat{g}.$$

  Let $\hat{c} \in \hat{\mathcal{C}}$ be the concatenation of c and s'. Then

$$\mathrm{d}\left(\hat{S}_j, \hat{c}\right) = \mathrm{d}\left(S_j, c\right) + \mathrm{d}\left(S_j', s'\right) < g + k' = \hat{g}.$$

This satisfies condition (c) of Definition 4.20.

□

Example 6.21. Consider the access structures

$$\begin{aligned} \Gamma_1 &= \{\{T_3\}, \{T_1, T_2\}, \{T_2, T_3\}, \{T_1, T_3\}, \{T_1, T_2, T_3\}\} \quad \text{and} \\ \Gamma_2 &= \{\{T_1\}, \{T_2\}, \{T_3\}, \{T_2, T_3\}, \{T_1, T_2, T_3\}\} \end{aligned}$$

on the participants set $\mathcal{T} = \{T_1, T_2, T_3\}$. The dual access structures

$$\begin{aligned} \overline{\Gamma_1} &= \{\{T_1\}, \{T_2\}\} \quad \text{and} \\ \overline{\Gamma_2} &= \{\{T_1, T_2\}, \{T_1, T_3\}\} \end{aligned}$$

are disjoint. Define

$$\Gamma = \Gamma_1 \cap \Gamma_2 = \{\{T_3\}, \{T_2, T_3\}, \{T_1, T_2, T_3\}\}.$$

Then

$$\overline{\Gamma} = \{\{T_1\}, \{T_2\}, \{T_1, T_2\}, \{T_1, T_3\}\} = \overline{\Gamma_1} \cup \overline{\Gamma_2}.$$

At first we show that the parameters $(b_1, g, k) = (b_1', g', k') = (64, 64, 28)$ realize Γ_1 and Γ_2 elementarily. Then we find suitable codes for Γ_1 and Γ_2 and apply Proposition

6.20 to find an elementary realization and a suitable code for Γ.

$$\varepsilon^1_{\overline{\Gamma_1}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad w_{\overline{\Gamma_1}} = (1, 4, 2)$$

The numbers d_i of the ones in the ith row of $\varepsilon_{\overline{\Gamma_1}}$ are

$$d_i = \begin{cases} 0 & \text{once} \\ 1 & \text{4 times} \\ 2 & \text{2 times} \end{cases}.$$

Hence the equations 2 to 8 in the linear system 4.2 equations are

- $a_{2i} - a_{2i-1} = \frac{1}{4}(b_1 - k + (u - 2d_i)(g - k)) = \frac{1}{4}(64 - 28 + (2 - 2 \cdot 0)(64 - 28)) = 27$ for one time. In this case we choose $a_{2i} = 27$ and $a_{2i-1} = 0$.
- $a_{2i} - a_{2i-1} = \frac{1}{4}(b_1 - k + (u - 2d_i)(g - k)) = \frac{1}{4}(64 - 28 + (2 - 2 \cdot 1)(64 - 28)) = 9$ for four times. We choose $a_{2i} = 9$ and $a_{2i-1} = 0$.
- $a_{2i} - a_{2i-1} = \frac{1}{4}(b_1 - k + (u - 2d_i)(g - k)) = \frac{1}{4}(64 - 28 + (2 - 2 \cdot 2)(64 - 28)) = -9$ for two times and we choose $a_{2i} = 0$ and $a_{2i-1} = 9$.

This yields

$$\sum_{i=2}^{8} a_{2i} \;=\; 27 + 4 \cdot 9 \;=\; 63 \;\leq\; 64 = b_1.$$

Hence $(64, 64, 28)$ realizes Γ_1 elementarily. In order to show that $(64, 64, 28)$ is also an elementary realization for Γ_2 we have a look at the matrix

$$\varepsilon^1_{\overline{\Gamma_2}} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

It also consists of two linearly independent columns. That means $\varepsilon^1_{\overline{\Gamma_1}}$ and $\varepsilon^1_{\overline{\Gamma_2}}$ have the same linearity type and Γ_1 and Γ_2 belong to the same class of access structures. Hence $(64, 64, 28)$ realizes Γ_2 elementarily, too.

Lemma 5.26 (b) tells us that the first order Reed Muller code $RM(1, 7)$ is suitable for $(s, \Gamma_1, 64, 64, 28)$ and for $(s', \Gamma_1, 64, 64, 28)$ for all codewords $s, s' \in RM(1, 7) \setminus \{(0, \ldots, 0), (1, \ldots, 1)\}$.

According to Proposition 6.20 (a), Γ is realized elementary by

$$(\hat{b}_1, \hat{g}, \hat{k}) = (b_1 + b'_1, g + k', k + k') = (128, 92, 56).$$

Finally Proposition 6.20 (b) says that the concatenation

$$\hat{\mathcal{C}} = \{(c, c') : c, c' \in RM(1, 7)\}$$

is suitable for $(\hat{s}, \Gamma, 128, 92, 56)$ for all codewords $\hat{s} \in \hat{\mathcal{C}}$, $\hat{s} \neq (\underbrace{0, \ldots, 0}_{128}, \underbrace{1, \ldots, 1}_{128})$, $(\underbrace{1, \ldots, 1}_{128}, \underbrace{0, \ldots, 0}_{128})$, with weight 128.

Let us now consider the general case where $\overline{\Gamma_1}$ and $\overline{\Gamma_2}$ are not disjoint. Suppose that $\Gamma_1, \Gamma_2 \subsetneq \mathcal{P}(\mathcal{T}) \setminus \{\varnothing\}$ such that $\Gamma_1 \not\subseteq \Gamma_2$ and $\Gamma_2 \not\subseteq \Gamma_1$. Then $\overline{\Gamma_1} \cup \overline{\Gamma_2}$ consists of the three non-empty and pairwise disjoint sets $\overline{\Gamma_1} \setminus \overline{\Gamma_2}$, $\overline{\Gamma_2} \setminus \overline{\Gamma_1}$ and $\overline{\Gamma_1} \cap \overline{\Gamma_2}$. In order to find a realization for $\Gamma_1 \cap \Gamma_2$ we apply Proposition 6.20 twice:

- on $\overline{\overline{\Gamma_1} \setminus \overline{\Gamma_2}} = \Gamma_1 \cup \overline{\Gamma_2}$ and $\overline{\overline{\Gamma_2} \setminus \overline{\Gamma_1}} = \overline{\Gamma_1} \cup \Gamma_2$, this yields an elementary realization for $(\Gamma_1 \cup \overline{\Gamma_2}) \cap (\overline{\Gamma_1} \cup \Gamma_2) = (\Gamma_1 \cap \Gamma_2) \cup (\overline{\Gamma_1} \cap \overline{\Gamma_2})$;

- on $(\Gamma_1 \cap \Gamma_2) \cup (\overline{\Gamma_1} \cap \overline{\Gamma_2})$ and $\overline{\overline{\Gamma_1} \cap \overline{\Gamma_2}} = \Gamma_1 \cup \Gamma_2$, this yields an elementary realization for $((\Gamma_1 \cap \Gamma_2) \cup (\overline{\Gamma_1} \cap \overline{\Gamma_2})) \cap (\Gamma_1 \cup \Gamma_2) = \Gamma_1 \cap \Gamma_2$.

Corollary 6.22. Let $\Gamma_1, \Gamma_2 \subsetneq \mathcal{P}(\mathcal{T}) \setminus \{\varnothing\}$ be access structures on the same set of t participants such that $\Gamma_1 \not\subseteq \Gamma_2$ and $\Gamma_2 \not\subseteq \Gamma_1$. Suppose that the dual access structures are not disjoint. Let $\Gamma_1' := \Gamma_1 \cup \overline{\Gamma_2}$, $\Gamma_2' := \overline{\Gamma_1} \cup \Gamma_2$ and $\Gamma_3 = \Gamma_1 \cup \Gamma_2$.

(a) Suppose that (b_1, g, k), (b_1', g', k') and (b_1'', g'', k'') are elementary realizations for Γ_1', Γ_2' and Γ_3, respectively, such that $g - k = g' - k' = g'' - k''$ holds. Then

$$(\hat{b}_1, \hat{g}, \hat{k}) = (b_1 + b_1' + b_1'', g + k' + k'', k + k' + k'')$$

realizes $\Gamma_1 \cap \Gamma_2$ elementarily.

(b) Additionally, let $\mathcal{C} \subseteq \mathbb{Z}_2^n$ be a suitable code for $(s, \Gamma_1', b_1, g, k)$ for a codeword $s \in \mathcal{C}$ with weight b_1, $\mathcal{C}' \subseteq \mathbb{Z}_2^{n'}$ be a suitable code for $(s', \Gamma_2', b_1', g', k')$ for a codeword $s' \in \mathcal{C}'$ with weight b_1' and $\mathcal{C}'' \subseteq \mathbb{Z}_2^{n''}$ be suitable for $(s'', \Gamma_3, b_1'', g'', k'')$ for a codeword $s'' \in \mathcal{C}''$ with weight b_1''. Then the concatenation $\hat{\mathcal{C}}$ of $\mathcal{C}$, $\mathcal{C}'$ and $\mathcal{C}''$ is suitable for $(\hat{s}, \Gamma_1 \cap \Gamma_2, \hat{b}_1, \hat{g}, \hat{k})$, where $\hat{s}$ is the concatenation of the codewords s, s' and s''.

Remark 6.23. Let $\Gamma \neq \mathcal{P}(\mathcal{T}) \setminus \{\varnothing\}$ be an arbitrary access structure such that there are $u > 0$ unauthorized sets. The dual access structure $\overline{\Gamma}$ can be partitioned into at most u disjoint smaller sets, which can be regarded as the duals of some suitable access structures. This yields another approach towards an universal solution for all access structures on the same number of participants: We partition the dual access structure into u pairwise different sets, each containing one unauthorized set. Then we apply Proposition 6.20 for $u - 1$ times. Unfortunately, access structures with dual access structures of size one do not allow small code lengths and large security distances. This has the consequence that the alternative approach based on Proposition 6.20 does not improve the universal solution given in Theorem 4.22 with regard to the code length and the security distance.

Let us take a detailed look at this construction. Let Γ_1 be an arbitrary access structure with one unauthorized set. Then $u = 1$ and $w_{\overline{\Gamma_1}} = (2^{t-1} - 1, 2^{t-1})$ yields $c_i = 1$ for $2^{t-1} - 1$ times and $c_i = 0$ for 2^{t-1} times. We obtain the equations

$$a_{2i} - a_{2i-1} = \begin{cases} \frac{1}{2^{t-1}}(b_1 - k + (g-k)) & 2^{t-1} - 1 \text{ times} \\ \frac{1}{2^{t-1}}(b_1 - k - (g-k)) & 2^{t-1} \text{ times} \end{cases}.$$

We choose $b_1 = g$ and $b_1\left(\frac{1}{2} - \frac{1}{2^{t-2}}\right) \le k < \frac{b_1}{2}$ such that $2^{t-2}|b_1 - k$. Then

$$\begin{array}{rrcl} & \sum_{i=2}^{2^t} a_{2i} & \le & b_1 \\ \Leftrightarrow & \frac{1}{2^{t-1}}\left((2^{t-1}-1)\cdot 2 \cdot (b_1 - k)\right) & \le & b_1 \\ \Leftrightarrow & b_1 \cdot (2^{t-2} - 1) & \le & k \cdot (2^{t-1} - 1) \\ \Leftrightarrow & b_1 \cdot \left(\frac{1}{2} - \frac{1}{2^{t-2}}\right) & \le & k. \end{array}$$

Hence the parameters (b_1, b_1, k) with the properties described above realize Γ_1 elementarily. In order to guarantee that $2^{t-2}|b_1 - k$ we choose $k = \frac{b_1}{2} - 2^{t-2}$ and b_1 to be divisible by 2^{t-1}. However, a consequence of this is that b_1 has to be at least $2^{2t-2} - 2^{t-1}$.

For $b_1 = 2^{2t-2}$ the first order Reed Muller code $RM(1, 2t-1)$ is suitable for $(s, \Gamma_1, b_1, b_1, k)$ for all codewords in $s \in RM(1, 2t-1) \setminus \{(0, \dots, 0), (1, \dots, 1)\}$ (see Lemma 5.26 (b)).

Now let Γ be an access structure with $u > 0$ unauthorized sets. We split the dual access structure into u disjoint sets with one element and apply Proposition 6.20 (a) for $u - 1$ times. This yields the following elementary realizations depending on the size u of $\overline{\Gamma}$.

$$\begin{array}{rl} u = 1: & (b_1, b_1, k) \\ u = 2: & (2b_1, b_1 + k, 2k) \\ \vdots & \\ 1 \le u \le 2^t - 1: & (ub_1, b_1 + (u-1)k, uk) = (\hat{b}_{1,u}, \hat{g}_u, \hat{k}_u) \\ \vdots & \\ u = 2^t - 1: & ((2^t - 1)b_1, b_1 + (2^t - 2)k, (2^t - 1)k) = (\hat{b}_1, \hat{g}, \hat{k}) \end{array}$$

For all $u = 1, \dots, 2^t - 1$ Proposition 6.20 (b) says that the u-fold concatenation $\mathcal{C}$ of $RM(1, 2t-1)$ is suitable for $(\hat{s}, \Gamma, ub_1, b_1 + (u-1)k, uk)$ for all secrets $\hat{s} \in \mathcal{C}$, which are concatenations of codewords in $RM(1, 2t-1) \setminus \{(0, \dots, 0), (1, \dots, 1)\}$.

Let $(\tilde{b}_1, \tilde{g}, \tilde{k})$ be the parameters provided by theorem 4.22 for t participants. That means especially

$$\tilde{b}_1 \ge 2^{2t} - 2^t \text{ and } \tilde{g} \le \tilde{b}_1 \left(\frac{1}{2} + \frac{1}{2^t}\right) - 2^{t-1}.$$

In the worst case the alternative construction yields

$$\hat{b}_1 = (2^t - 1)b_1 \ge 2^{3t-2} - 3 \cdot 2^{2t-2} + 2^{t-1}$$

and fails to improve the efficiency of the scheme. In order to make a statement about the security provided by the two different realizations we study the "relative security distances" $\frac{\hat{g}}{\hat{b}_1}$ and $\frac{\tilde{g}}{\tilde{b}_1}$. We know from Remark 4.21 (b) that the code lengths $2\hat{b}_1$ and $2\tilde{b}_1$, respectively, are arithmetically possible. Hence the relative security distance measure the proportions of digits in the share sums of the unauthorized sets which differ from the secret. Unfortunately the new approach means no essential improvement with regard to the security either since both relative security distances are below the (very small) bound $\frac{1}{2}+\frac{1}{2^t}$:
The relative security distance provided by the universal solution is

$$\frac{\tilde{b}_1}{\tilde{g}} = \frac{1}{2} + \frac{1}{2^t} - \frac{2^{t-1}}{\tilde{b}_1} \leq \frac{1}{2} + \frac{1}{2^t}.$$

In the worst case $u = 2^t - 1$ we have $\hat{g} = b_1 + (2^t - 2)k = 2^{t-1}b_1 - 2^{2t-2} + 2^{t-1}$ and therefore

$$\frac{\hat{g}}{\hat{b}_1} = \frac{1}{2} + \underbrace{\frac{1}{2^{t+1}-2}}_{\leq\frac{1}{2^t}} \underbrace{- \frac{2^{2t-2}}{(2^t-1)b_1} + \frac{2^{t-1}}{(2^t-1)b_1}}_{\leq 0} \leq \frac{1}{2} + \frac{1}{2^t}.$$

However, for smaller numbers u of unauthorized sets, the weights $\hat{b}_{1,u}$ are considerably smaller than $\tilde{b}_1$ and relative security distances above the bound $\frac{1}{2}+\frac{1}{2^t}$ are possible:

$$\begin{aligned}
\frac{\hat{g}_u}{\hat{b}_{1,u}} &= \frac{b_1 + (u-1)k}{ub_1} \\
&= \frac{b_1\left(1+\frac{u-1}{2}\right)}{ub_1} - \frac{u-1}{u} \cdot \frac{2^{t-2}}{b_1} \\
&\geq \frac{u+1}{2u} - \frac{u-1}{u} \cdot \frac{2^{t-2}}{2^{2t-2} - 2^{t-1}} \\
&= \frac{1}{2} + \frac{1}{2u} - \frac{u-1}{u} \underbrace{\left(\frac{1}{2^t} + \frac{1}{2^{2t-1} - 2t}\right)}_{\leq\frac{1}{2^{t-1}}} \\
&\geq \frac{1}{2} + \frac{1}{2u} - \frac{u-1}{2^{t-1}u}
\end{aligned}$$

which is larger than $\frac{1}{2}+\frac{1}{2^t}$ for all $u < \frac{2^{t-1}+2}{3}$.

6.5 Removal of One Authorized Subset

This section deals with very small changes in the access structure. We study the effect on the possible parameters when one single set of the access structure is removed.

Let Γ' be an access structure realized elementarily by (b_1, g, k). It will turn out that any authorized set, which is disjoint to all unauthorized sets, can be removed from Γ' such that the resulting access structure Γ is also realized elementarily by (b_1, g, k).

Proposition 6.24. Let $\Gamma' \subsetneq \mathcal{P}(\mathcal{T}) \setminus \{\varnothing\}$ be an arbitrary access structure on t participants. Consider a set of participants $V \in \Gamma'$ which is disjoint to all unauthorized sets in $\overline{\Gamma'}$.

(a) Suppose that $(a'_2, \dots, a'_{2^{t+1}})$ is an elementarily solution for (Γ, b_1, g, k) such that there is no pair (a'_{2i}, a'_{2i-1}) with
$$0 \leq |a'_{2i} - a'_{2i-1}| < \frac{g-k}{2^{t-1}}.$$
Then (b_1, g, k) realizes the access structure
$$\Gamma := \Gamma' \setminus \{V\}.$$
elementarily, too.

(b) Let $\mathcal{C}$ be suitable for (s, Γ', b_1, g, k) for a codeword $s \in \mathcal{C}$ with weight b_1. Suppose that the minimum distance $d(\mathcal{C})$ and the covering radius $\rho(\mathcal{C})$ satisfy $d(\mathcal{C}) \geq 2k+1$ and $\rho(\mathcal{C}) < g$. Then $\mathcal{C}$ is also suitable for (s, Γ, b_1, g, k).

Proof. (a) Without loss of generality let $V = \{T_1, \dots, T_v\}$. Let $|\overline{\Gamma'}| = u'$. $\overline{\Gamma} = \overline{\Gamma'} \cup \{V\}$ yields $|\overline{\Gamma}| = u = u' + 1$ and

$$\varepsilon^1_{\overline{\Gamma'}} = \underbrace{\begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \\ & * & \end{pmatrix}}_{u'} \begin{matrix} \left.\vphantom{\begin{matrix}0\\ \vdots\\ 0\end{matrix}}\right\} v \\ \} \, t-v \end{matrix} \quad \text{and} \quad \varepsilon^1_{\overline{\Gamma}} = \underbrace{\begin{pmatrix} 1 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & * & \\ 0 & & & \end{pmatrix}}_{u=u'+1} \begin{matrix} \left.\vphantom{\begin{matrix}1\\ \vdots\\ 1\end{matrix}}\right\} v \\ \left.\vphantom{\begin{matrix}0\\ \vdots\\ 0\end{matrix}}\right\} t-v \end{matrix}$$

for a suitable $(t - v \times u')$-matrix $(*)$. The rows of the matrices $\varepsilon_{\overline{\Gamma'}}$ and $\varepsilon_{\overline{\Gamma}}$ consist of all possible sums of the rows of the matrices $\varepsilon^1_{\overline{\Gamma'}}$ and $\varepsilon^1_{\overline{\Gamma}}$, respectively, with at least one summand. Let c'_i denote the number of zeros in the ith row of $\varepsilon_{\overline{\Gamma'}}$. The number c_i of zeros in the ith row of $\varepsilon_{\overline{\Gamma}}$ is characterized by the matrix $(*)$ and has the following relation to c'_i:

- Suppose that the ith row of $\varepsilon_{\overline{\Gamma'}}$ is the sum of at least one of the last $t-v$ rows of $\varepsilon^1_{\overline{\Gamma'}}$. Then this row is the sum of a sum R' of the last $t-v$ rows and a multiple $m \cdot (0, \dots, 0)$, $m = 0, \dots, v$, of the zero row. Since there are 2^v combinations of the first v rows, there are 2^v rows like the ith row.

  Let R be the vector consisting of R' with an additional leading zero. Then

the ith row of $\varepsilon_{\overline{\Gamma}}$ is the sum $R + m \cdot (1, 0, \ldots, 0)$. If m is even (possibly zero), then the ith row is just R. In this case $c_i = c'_i + 1$. This happens 2^{v-1} times. If m is odd, the ith row looks like R with the first bit flipped. In this case $c_i = c'_i$. This also happens 2^{v-1} times.
Hence each c'_i occurs for a multiple of 2^v times and there are 2^{v-1} rows of $\varepsilon_{\overline{\Gamma}}$ with $c_i = c'_i + 1$ zeros and 2^{v-1} rows with $c_i = c'_i$ zeros.

$$\begin{tikzcd}
 & 2^{v-1} \text{ times } c_i = c'_i + 1 \\
2^v \text{ times } c'_i \arrow[ur] \arrow[dr] & \\
 & 2^{v-1} \text{ times } c_i = c'_i
\end{tikzcd}$$

- Let the ith row of $\varepsilon_{\overline{\Gamma'}}$ be a sum of the first v rows of $\varepsilon^1_{\overline{\Gamma'}}$. Then the row is a multiple $m \cdot (0, \ldots, 0)$, $m = 1, \ldots v$. Since there are $2^v - 1$ possibilities to choose at least one of the first v rows, there are $2^v - 1$ rows in $\varepsilon_{\overline{\Gamma'}}$ of that form. The ith row of $\varepsilon_{\overline{\Gamma}}$ is $m \cdot (1, 0, \ldots, 0)$. When m is even, the row is also the zero vector and $c_i = c'_i + 1$. This happens $2^{v-1} - 1$ times. Otherwise, when m is odd, the ith row of $\varepsilon_{\overline{\Gamma}}$ is the vector $(1, 0, \ldots, 0)$ and $c_i = c'_i$. This happens 2^{v-1} times.

$$\begin{tikzcd}
 & 2^{v-1} - 1 \text{ times } c_i = c'_i + 1 = u \\
2^v - 1 \text{ times } c'_i = u' \arrow[ur] \arrow[dr] & \\
 & 2^{v-1} \text{ times } c_i = c'_i = u - 1
\end{tikzcd}$$

These observations show that there are indices $i_1, \ldots, i_{2^{t-v}-1}$ such that for all $j \in \{i_1, \ldots, i_{2^{t-v}-1}\}$ there are exactly 2^v rows of $\varepsilon_{\overline{\Gamma'}}$ with c'_j zeros. In $\varepsilon_{\overline{\Gamma}}$ there are exactly 2^{v-1} rows with $c_j = c'_j$ zeros and 2^{v-1} rows with $c_j = c'_j + 1$ zeros. Furthermore there are $2^v - 1$ rows of $\varepsilon_{\overline{\Gamma'}}$ with u' zeros, $2^{v-1} - 1$ rows of $\varepsilon_{\overline{\Gamma}}$ with $u = u' + 1$ zeros and 2^{v-1} rows of $\varepsilon_{\overline{\Gamma}}$ with $u - 1 = u'$ zeros. Let $i_{2^{t-v}}$ be the index of such a row of $\varepsilon_{\overline{\Gamma'}}$.

Hence the elementary solution a' for (Γ', b_1, g, k) yields an elementary solution $a = (a_2, \ldots, a_{2^{t+1}})$ for (Γ, b_1, g, k):

Consider the case $c_i = c'_i + 1$:

$$\begin{aligned} a_{2i} - a_{2i-1} &= \frac{1}{2^{t-1}} (b_1 - k + (2c_i - u)(g-k)) \\ &= \frac{1}{2^{t-1}} (b_1 - k + (2c_i' + 2 - u' - 1)(g-k)) \\ &= a_{2i}' - a_{2i-1}' + \frac{g-k}{2^{t-1}}. \end{aligned}$$

In the other case $c_i = c_i'$ and we have

$$\begin{aligned} a_{2i} - a_{2i-1} &= \frac{1}{2^{t-1}} (b_1 - k + (2c_i - u)(g-k)) \\ &= \frac{1}{2^{t-1}} (b_1 - k + (2c_i' - u' - 1)(g-k)) \\ &= a_{2i}' - a_{2i-1}' - \frac{g-k}{2^{t-1}}. \end{aligned}$$

According to our hypothesis $|a_{2i}' - a_{2i-1}'| \geq \frac{g-k}{2^{t-1}}$ for all $i = 2, \ldots, 2^t$, we have to distinguish two cases:

- Suppose that $a_{2i}' > 0$. Then $a_{2i-1}' = 0$ and $a_{2i}' \geq \frac{g-k}{2^{t-1}}$. Furthermore

$$a_{2i} - a_{2i-1} = a_{2i}' + \frac{g-k}{2^{t-1}} > 0 \text{ yields } a_{2i} = a_{2i}' + \frac{g-k}{2^{t-1}},\ a_{2i-1} = 0,$$

$$a_{2i} - a_{2i-1} = a_{2i}' - \frac{g-k}{2^{t-1}} \geq 0 \text{ yields } a_{2i} = a_{2i}' - \frac{g-k}{2^{t-1}},\ a_{2i-1} = 0$$

- If $a_{2i}' = 0$ and $a_{2i-1}' > 0$ then $a_{2i-1}' \geq \frac{g-k}{2^{t-1}}$ and

$$a_{2i} - a_{2i-1} = -a_{2i-1}' + \frac{g-k}{2^{t-1}} \leq 0 \text{ yields } a_{2i} = 0,\ a_{2i-1} = a_{2i-1}' - \frac{g-k}{2^{t-1}},$$

$$a_{2i} - a_{2i-1} = -a_{2i-1}' - \frac{g-k}{2^{t-1}} < 0 \text{ yields } a_{2i} = 0,\ a_{2i-1} = a_{2i-1}' + \frac{g-k}{2^{t-1}}$$

Using these results we calculate

$$\begin{aligned} \sum_{i=2}^{2^t} a_{2i} &= 2^{v-1} \sum_{l=1}^{2^{t-v}-1} \left(a_{2i_l}' - \frac{g-k}{2^{t-1}} \right) + 2^{v-1} \sum_{l=1}^{2^{t-v}-1} \left(a_{2i_l}' + \frac{g-k}{2^{t-1}} \right) \\ &\quad + 2^{v-1} \left(a_{2i_{2^{t-v}}}' - \frac{g-k}{2^{t-1}} \right) + (2^{v-1} - 1) \left(a_{2i_{2^{t-v}}}' + \frac{g-k}{2^{t-1}} \right) \\ &= 2^v \sum_{l=1}^{2^{t-v}-1} a_{2i_l}' + (2^v - 1) a_{2i_{2^{t-v}}}' - \frac{g-k}{2^{t-1}} \end{aligned}$$

$$= \underbrace{\sum_{i=2}^{2^t} a'_{2i}}_{=b_1 - a'_2} - \frac{g-k}{2^{t-1}} \;\leq\; b_1.$$

That means (b_1, g, k) realizes Γ elementarily, too and $(a_2, \ldots, a_{2^{t+1}})$ is an elementary solution for (Γ, b_1, g, k).

(b) We have to check the requirements of Definition 4.20. Condition (a) is obviously met and condition (c) is fulfilled because of remark 4.21 (c). It remains to show that the length n of $\mathcal{C}$ is sufficient.

$$\begin{aligned} n &\geq b_1 + \sum_{i=2}^{2^t} a'_{2i_l - 1} \\ &= b_1 + 2^{v-1} \sum_{l=1}^{2^{t-v}-1} \left(a'_{2i_l - 1} - \frac{g-k}{2^{t-1}} \right) + 2^{v-1} \sum_{l=1}^{2^{t-v}-1} \left(a'_{2i_l - 1} + \frac{g-k}{2^{t-1}} \right) \\ &\quad + (2^v - 1) \underbrace{a'_{2i_{2^{t-v}} - 1}}_{=0} \\ &= b_1 + \sum_{i=2}^{2^t} a_{2i_l - 1} \end{aligned}$$

Hence $\mathcal{C}$ is also suitable for (s, Γ, b_1, g, k).

□

Example 6.25. Let

$$\Gamma' = \{\{T_1\}, \{T_3\}, \{T_1, T_2\}, \{T_1, T_3\}, \{T_1, T_2, T_3\}\}, \; \overline{\Gamma'} = \{\{T_2\}, \{T_2, T_3\}\}.$$

$V = \{T_1\}$ is disjoint to all unauthorized sets in $\overline{\Gamma'}$. Define

$$\Gamma = \Gamma' \setminus \{V\} = \{\{T_3\}, \{T_1, T_2\}, \{T_1, T_3\}, \{T_1, T_2, T_3\}\}.$$

Then

$$\overline{\Gamma} = \overline{\Gamma'} \cup \{V\} = \{\{T_1\}, \{T_2\}, \{T_2, T_3\}\}.$$

The ε^1-matrices and weight vectors are

$$\varepsilon^1_{\overline{\Gamma'}} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad w_{\overline{\Gamma'}} = (1, 4, 2)$$

and

$$\varepsilon^1_{\overline{\Gamma}} = \begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}, \quad w_{\overline{\Gamma}} = (0,3,3,1).$$

At first we illustrate how the numbers c'_i of zeros in the ith row of $\varepsilon_{\overline{\Gamma'}}$ determine the numbers c_i of zeros in the ith row of $\varepsilon_{\overline{\Gamma}}$ using the same notations as in the proof of Proposition 6.24.

The rows of the matrices $\varepsilon_{\overline{\Gamma'}}$ and $\varepsilon_{\overline{\Gamma}}$ are the following linear combinations of the rows of $\varepsilon^1_{\overline{\Gamma'}}$ and $\varepsilon^1_{\overline{\Gamma}}$:

$$\begin{array}{r}i_4\to i=2\\ i_1\to i=3\\ i=4\\ i_2\to i=5\\ i=6\\ i_3\to i=7\\ i=8\end{array}
\underbrace{\begin{pmatrix}0&0\\1&1\\1&1\\0&1\\0&1\\1&0\\1&0\end{pmatrix}}_{=\varepsilon_{\overline{\Gamma'}}}
\begin{array}{c}\text{row 1}\\ \text{row 2}\\ \text{row 1 + row 2}\\ \text{row 3}\\ \text{row 1 + row 3}\\ \text{row 2 + row 3}\\ \text{row 1 + row 2 + row 3}\end{array}
\underbrace{\begin{pmatrix}1&0&0\\0&1&1\\1&1&1\\0&0&1\\1&0&1\\0&1&0\\1&1&0\end{pmatrix}}_{=\varepsilon_{\overline{\Gamma}}}
\begin{array}{l}i=2\\ i=3\\ i=4\\ i=5\\ i=6\\ i=7\\ i=8\end{array}$$

Let $i_1 = 3$, $i_2 = 5$, $i_3 = 7$ and $i_4 = 2$. Then $c'_{i_1} = 0$, $c'_{i_2} = 1$, $c'_{i_3} = 1$ and $c'_{i_4} = 2$. For all $j \in \{i_1, i_2, i_3\}$ there are $2^v = 2$ rows in $\varepsilon_{\overline{\Gamma'}}$ with c'_j zeros:

$j = i_1$: row 2 and row 3 have $c'_j = 0$ zeros
$j = i_2$: row 4 and row 5 have $c'_j = 1$ zero
$j = i_3$: row 6 and row 7 have $c'_j = 1$ zero

$\varepsilon_{\overline{\Gamma}}$ has $2^{v-1} = 1$ row with $c'_j + 1$ zeros and $2^{v-1} = 1$ row with c'_j zeros:

$j = i_1$: row 2 has 1 zero and row 3 has 0 zeros
$j = i_2$: row 4 has 2 zero and row 5 has 1 zero
$j = i_3$: row 6 has 2 zero and row 7 has 1 zeros

For $j = i_4$ there is $2^v - 1 = 1$ row in $\varepsilon_{\overline{\Gamma'}}$ with $c'_j = u' = 2$ zeros: row 1. $\varepsilon_{\overline{\Gamma}}$ has $2^{v-1} - 1 = 0$ rows with $u' + 1 = 3$ zeros and $2^{v-1} = 1$ row with $u' = 2$ zeros: row 1.

Next we have a look at the equations 2 to 8 in the linear system 4.2 for elementary solutions $(a'_2, \dots, a'_{16})$ for (Γ', b_1, g, k) and $(a_2, \dots, a_{16})$ for (Γ, b_1, g, k) defined by the numbers $c'_2, \dots, c'_8$ and $c_2, \dots, c_8$ of zeros in the rows of $\varepsilon_{\overline{\Gamma'}}$ and $\varepsilon_{\overline{\Gamma}}$. Consider the case $b_1 = g$.

$$\begin{aligned}
a'_3 &= 0, & a_3 &= 0\\
a'_4 &= \frac{3}{4}(g-k), & a_4 &= \frac{1}{2}(g-k)\\
a'_5 &= \frac{1}{4}(g-k), & a_5 &= 0\\
a'_6 &= 0, & a_6 &= 0\\
a'_7 &= \frac{1}{4}(g-k), & a_7 &= \frac{1}{2}(g-k)\\
a'_8 &= 0, & a_8 &= 0\\
a'_9 &= 0, & a_9 &= 0\\
a'_{10} &= \frac{1}{4}(g-k), & a_{10} &= \frac{1}{2}(g-k)\\
a'_{11} &= 0, & a_{11} &= 0\\
a'_{12} &= \frac{1}{4}(g-k), & a_{12} &= 0\\
a'_{13} &= 0, & a_{13} &= 0\\
a'_{14} &= \frac{1}{4}(g-k), & a_{14} &= \frac{1}{2}(g-k)\\
a'_{15} &= 0, & a_{15} &= 0\\
a'_{16} &= \frac{1}{4}(g-k), & a_{16} &= 0
\end{aligned}$$

Just like in the proof we obtain

$$\begin{aligned}
\frac{3}{2}(g-k) &= \sum_{i=2}^{8} a_{2i}\\
&= \underbrace{a_4}_{a'_4-\frac{1}{4}(g-k)} + \underbrace{a_6}_{a'_6=0} + \underbrace{a_8}_{a'_8=0} + \underbrace{a_{10}}_{a'_{10}+\frac{1}{4}(g-k)} + \underbrace{a_{12}}_{a'_{10}-\frac{1}{4}(g-k)} + \underbrace{a_{14}}_{a'_{14}+\frac{1}{4}(g-k)} + \underbrace{a_{16}}_{a'_{14}-\frac{1}{4}(g-k)}\\
&= 2(a'_6+a'_{10}+a'_{14}) + a'_4 - \frac{1}{4}(g-k)
\end{aligned}$$

$$\begin{aligned}
&= 2\cdot\sum_{l=1}^{3} a'_{2i_l} + a'_{2i_4} - \frac{1}{4}(g-k)\\
&= \underbrace{\sum_{i=2}^{8} a'_{2i}}_{\frac{7}{4}(g-k)} - \frac{1}{4}(g-k)
\end{aligned}$$

and

$$\begin{aligned}
\frac{1}{2}(g-k) &= \sum_{i=2}^{8} a_{2i-1} \\
&= \underbrace{a_3}_{a_3'=0} + \underbrace{a_5}_{a_5'-\frac{1}{4}(g-k)} + \underbrace{a_7}_{a_5'+\frac{1}{4}(g-k)} + \underbrace{a_9}_{a_9'=0} + \underbrace{a_{11}}_{a_{11}'=0} + \underbrace{a_{13}}_{a_{13}'=0} + \underbrace{a_{15}}_{a_{15}'=0} \\
&= 2(a_5' + a_9' + a_{13}') + a_3' \\
&= 2 \cdot \sum_{l=1}^{3} a'_{2i_l-1} \\
&= \sum_{i=2}^{8} a'_{2i-1}.
\end{aligned}$$

In the general case, when the participant set $V \in \Gamma'$ is not disjoint to all unauthorized sets in $\overline{\Gamma'}$, the summands $\pm\frac{g-k}{2^{t-1}}$ may be distributed differently. For an elementarily solution $(a_2', \ldots, a_{2^{t+1}}')$ for (Γ', b_1, g, k) there may be an elementarily solution $(a_2, \ldots, a_{2^{t+1}})$ for $(\Gamma' \setminus \{V\}, b_1, g, k)$ such that

$$\sum_{i=2}^{2^t} a_{2i} > \sum_{i=2}^{2^t} a_{2i}'.$$

But one can say at least the following.

Proposition 6.26. Let $\Gamma' \subsetneq \mathcal{P}(\mathcal{T}) \setminus \{\varnothing\}$ be an arbitrary access structure on t participants and $V \in \Gamma'$. Suppose that $(a_2', \ldots, a_{2^{t+1}}')$ is an elementarily solution for (Γ, b_1, g, k) such that

$$a_2' \geq (g-k)\left(1 - \frac{1}{2^{t-1}}\right).$$

Then (b_1, g, k) realizes the access structure $\Gamma := \Gamma' \setminus \{V\}$ elementarily, too.

Proof. Without loss of generality let $V = \{T_1, \ldots, T_v\}$. Let $|\overline{\Gamma'}| = u'$. $\overline{\Gamma} = \overline{\Gamma'} \cup \{V\}$ yields $|\overline{\Gamma}| = u = u'+1$ and $\varepsilon^1_{\overline{\Gamma}}$ consists of the columns of $\varepsilon^1_{\overline{\Gamma}}$ with the additional column $(1, \ldots, 1, 0, \ldots, 0)^\tau$ which represents V. Up to the order of the columns $\varepsilon^1_{\overline{\Gamma}}$ has the form

$$\underbrace{\begin{pmatrix} 1 & \\ \vdots & \\ 1 & \varepsilon^1_{\overline{\Gamma'}} \\ 0 & \\ \vdots & \\ 0 & \end{pmatrix}}_{u=u'+1} \begin{array}{l} \left.\vphantom{\begin{matrix}1\\ \vdots\\ 1\end{matrix}}\right\} v \\ \left.\vphantom{\begin{matrix}0\\ \vdots\\ 0\end{matrix}}\right\} t-v \end{array}$$

The rows of the matrix $\varepsilon_{\overline{\Gamma}}$ look like the rows of $\varepsilon_{\overline{\Gamma}}$ with an additional leading zero or an additional leading one. $2^{t-1} - 1$ rows are the sums of an even number of columns

of $\varepsilon_{\overline{\Gamma}}^{1}$. In this case the row starts with a zero. The remaining 2^{t-1} rows of $\varepsilon_{\overline{\Gamma}}$ belong to sums with an odd number of summands and start with one.
Suppose that $a_2, \ldots, a_{2^{t+1}}$ solve equations 2 up to 2^t of the linear system 4.2 for Γ, b_1, g, k. Then there are $2^{t-1} - 1$ indices i such that

$$a_{2i} - a_{2i-1} = a'_{2i} - a'_{2i-1} + \frac{g-k}{2^{t-1}}$$

and 2^{t-1} indices i such that

$$a_{2i} - a_{2i-1} = a'_{2i} - a'_{2i-1} - \frac{g-k}{2^{t-1}}.$$

Hence

$$\begin{aligned} \sum_{i=2}^{2^t} a_{2i} &\leq \underbrace{\sum_{i=2}^{2^t} a'_{2i}}_{b_1 - a'_2} + (2^{t-1} - 1) \cdot \frac{g-k}{2^{t-1}} \\ &= b_1 \underbrace{- a'_2 + (g-k)\left(1 - \frac{1}{2^{t-1}}\right)}_{\leq 0} \leq b_1. \end{aligned}$$

Therefore $(a_2, \ldots, a_{2^{t+1}})$ is an elementary solution for (Γ, b_1, g, k). □

Chapter 7

Special Access Structures

In this chapter we apply the results and techniques of the previous chapters on special classes of access structures. This yields access structures which are far superior with regard to efficiency and security to the general realization provided by Theorem 4.22

We start with access structures whose elementary distance vectors come from the evaluation vectors of special Boolean polynomials by replacing 0 by k and 1 by g.

Then we deal with access structures which are defined by so-called necessary sets and veto sets of different types.

7.1 Access Structures Related to Boolean Polynomials

In this section we present an interesting connection between access structures on t participants and Boolean polynomials with t variables. This connection comes from the fact that any access structure Γ is completely characterized by the indices $j \geq 2$ where it's elementary weight vector has the value g (or k, respectively). Hence the distance vector b corresponds to the vector $(v_2, \ldots, v_{2^t})$ in $\mathbb{Z}_2^{2^t-1}$ with $v_j = 1$ iff $b_j = g$. Adding another bit v_1 we receive one of the vectors $(0, v_2, \ldots, v_{2^t})$ or $(1, v_2, \ldots, v_{2^t}) \in \mathbb{Z}_2^{2^t}$ which both characterize the access structure. We know that any vector in $\mathbb{Z}_2^{2^t}$ can be considered as the evaluation vector of a Boolean polynomial. Hence there are two Boolean polynomials which are related to $(v_1, v_2, \ldots, v_{2^t})$ and therefore related to b and to Γ.

This approach enables us to identify classes of access structures with considerable better parameters than the parameters provided by Theorem 4.22. We will see that access structures related to Boolean polynomials which belong to codewords in $RM^1(1,t)$ allow the parameters $g = b_1$ and arbitrary small code lengths $n \geq b_1$. Furthermore we study elementary realizations for access structures related to Boolean monomials depending on the degree of the monomial.

Definition 7.1. Let Γ be an access structure on t participants and $b = (b_1, \ldots, b_{2^t})^\tau$ the elementary distance vector for Γ with respect to (b_1, g, k). If there is a Boolean polynomial $p : \mathbb{Z}_2^t \to \mathbb{Z}_2$ with evaluation vector $\underline{p} = (\underline{p}_1, \ldots, \underline{p}_{2^t})$ such that

$$(b_2, \ldots, b_{2^t}) = g \cdot (\underline{p}_2, \ldots, \underline{p}_{2^t}) + k \cdot \big((1, \ldots, 1) - (\underline{p}_2, \ldots, \underline{p}_{2^t})\big)$$

we say that b and Γ are *related to p*, $b \sim p$ and $\Gamma \sim p$.

That means b is related to a Boolean polynomial p when

$$b^\tau = \begin{cases} g \cdot \underline{p} + k \cdot ((1, \ldots, 1) - \underline{p}) + (b_1 - g) \cdot e_1 & \text{if } p(0, \ldots, 0) = 1 \\ g \cdot \underline{p} + k \cdot ((1, \ldots, 1) - \underline{p}) + (b_1 - k) \cdot e_1 & \text{if } p(0, \ldots, 0) = 0. \end{cases}$$

Example 7.2. Consider the access structure $\Gamma = \{\{T_1\}, \{T_1, T_2\}, \{T_3\}, \{T_2, T_3\}\}$ from Example 4.25. Γ is related to the Boolean polynomial $p : \mathbb{Z}_2^3 \to \mathbb{Z}_2$ defined by $(x_1, x_2, x_3) \mapsto 1 + x_1 + x_3$ of degree one. The evaluation vector of p is calculated as follows

x_3	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_1	0	1	0	1	0	1	0	1
$\underline{p}$	1	0	1	0	0	1	0	1.

Since the 2nd, the 4th, the 5th and the 7th element of $(\mathcal{P}(\{T_1, T_2, T_3\}), \preccurlyeq)$ are authorized, any elementary distance vector of Γ has the form

$$\begin{aligned} b^\tau &= (b_1, \underset{\overset{\uparrow}{2}}{k}, g, \underset{\overset{\uparrow}{4}}{k}, \underset{\overset{\uparrow}{5}}{k}, g, \underset{\overset{\uparrow}{7}}{k}, g) \\ &= g \cdot \underbrace{(1,0,1,0,0,1,0,1)}_{\underline{p}} + k \cdot \underbrace{(0,1,0,1,1,0,1,0)}_{(1,\ldots,1)-\underline{p}} + (b_1 - g) \cdot e_1. \end{aligned}$$

Γ is also related to the Boolean polynomial $q : \mathbb{Z}_2^t \to \mathbb{Z}_2$, defined by $(x_1, x_2, x_3) \mapsto 1 + x_1 + x_3 + (1 + x_1)(1 + x_2)(1 + x_3)$ with the following evaluation vector

x_3	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_1	0	1	0	1	0	1	0	1
$\underline{q}$	0	0	1	0	0	1	0	1

as

$$b^\tau = g \cdot \underbrace{(0,0,1,0,0,1,0,1)}_{\underline{q}} + k \cdot \underbrace{(1,1,0,1,1,0,1,0)}_{(1,\ldots,1)-\underline{q}} + (b_1 - k) \cdot e_1.$$

The dual access structure is $\overline{\Gamma} = \{\{T_2\}, \{T_1, T_3\}, \{T_1, T_2, T_3\}\}$ and it is remarkable that the vectors $(x_1, x_2, x_3)^\tau$ in the positions ≥ 2, where $\underline{p}$ or $\underline{q}$ have the value one, are exactly the characteristic vectors the unauthorized sets. The other positions ≥ 2 of the evaluation vectors belong to the characteristic vectors of the authorized sets. There the evaluation vectors have the value zero. This is not a coincidence. The following lemma describes the connection between the authorized subsets and the zeros of the related Boolean polynomials.

Lemma 7.3. Suppose that the access structure Γ is related to the Boolean polynomial $p : \mathbb{Z}_2^t \to \mathbb{Z}_2$. Then the set $A = \{T_{i_1}, \dots, T_{i_l}\}$ is authorized iff

$$p(y_1, \dots, y_t) = 0 \quad \text{for} \quad y_i = \begin{cases} 1 & \text{if } T_i \in A \\ 0 & \text{if } T_i \notin A \end{cases}.$$

Proof. Since Γ is related to p, the elementary weight vector $b = (b_1, \dots, b_{2^t})^\tau$ for Γ with respect to (b_1, g, k) has the property

$$(b_2, b_3, \dots, b_{2^t}) = g \cdot (\underline{p}_2, \dots, \underline{p}_{2^t}) + k \cdot \Big((1, \dots, 1) - (\underline{p}_2, \dots, \underline{p}_{2^t})\Big).$$

Let $\{T_{i_1}, \dots, T_{i_l}\}$ be the jth element of $\mathcal{P}(\mathcal{T})$. By construction of b

$$\{T_{i_1}, \dots, T_{i_l}\} \in \Gamma \;\Leftrightarrow\; b_j = k \;\Leftrightarrow\; \underline{p}_j = 0.$$

$\underline{p}_j$ is the value of p when the argument is the jth vector of $\mathbb{Z}_2^t$ with regard to the order defined in Remark 4.4. This is exactly the desired vector y. □

Remark 7.4. Lemma 7.3 yields the following connection between the Boolean polynomials of an access structure and it's dual access structure:

$$\Gamma \sim p \;\Leftrightarrow\; \overline{\Gamma} \sim p + 1.$$

Now we use the observations above to find classes of access structures which allow favorable parameters. We start with access structures related to Boolean polynomials of degree ≤ 1 like the access structure in Example 7.2. Indeed, these access structures turn out to have very good realizations.

Example 7.5. Again we consider the access structure

$$\Gamma = \{\{T_1\}, \{T_3\}, \{T_1, T_2\}, \{T_2, T_3\}\}$$

on $t = 3$ participants with the elementary distance vector $b = (b_1, k, g, k, k, g, k, g)^\tau$. Let b_1 be an arbitrary natural number, $g = b_1$, and $k \in \mathbb{N}_0$ arbitrary with $k < \frac{b_1}{2}$.

$$\varepsilon_{\overline{\Gamma}} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \quad \text{yields } d_i = \begin{cases} 2 & \text{6 times} \\ 0 & \text{once,} \end{cases}$$

where d_i is the number of ones in the ith row of $\varepsilon_{\overline{\Gamma}}$ for all $i = 1, \dots, 2^t - 1$. We obtain the following equations for an elementary solution $a = (a_2, \dots, a_8)$:

$$a_{2i} - a_{2i-1} = \begin{cases} \frac{1}{4}(b_1 - k - (g-k)) = 0 & \text{6 times} \\ \frac{1}{4}(b_1 - k + 3(g-k)) = g - k & \text{once} \end{cases}$$

Define $a_2 = k$. Then

$$\sum_{i=1}^{8} a_{2i} = k + g - k = g = b_1$$

shows that the chosen parameters realize Γ elementarily. Even the choice $k = 0$ is possible. In this case Lemma 5.26 (a) implies that $\mathbb{Z}_2^n$, $n \geq b_1 + \sum_{i=2}^{2^t} \underbrace{a_{2i-1}}_{=0} = b_1$, is suitable for $(s, \Gamma, b_1, b_1, 0)$ for all words $s \in \mathbb{Z}_2^n$ with weight b_1.

The elementary solution a has the property that all its odd numbered components are zero. Hence there are no positions where the secret has the value 0 and at least one share has the value 1. Furthermore exactly one entry in $\{a_4, a_6, a_8, \dots, a_{16}\}$ is non-zero and has the value $g - k$. This entry has to be

$$a_{12} = \operatorname{supp}(s) \cap \operatorname{supp}(k_1) \cap \operatorname{supp}(\overline{k_2}) \cap \operatorname{supp}(k_3).$$

Otherwise $\{T_1\}$ and $\{T_3\}$ could not be authorized and $\{T_2\}$ unauthorized. Apart from the order of the positions, the secret and the shares have the following structure.

1...1	1........1	0........0	s
1...1	1........1	0........0	k_1
1...1	0........0	0........0	k_2
1...1	1........1	0........0	k_3
$a_2 = k \geq 0$	$a_{12} = g - k$	$a_1 \geq 0$	

Hence T_1 and T_3 receive the secret s as shares and T_2 receives the zero vector.

We will see that it is not a coincidence that the access structure in Example 7.2 has such a good realization. The following proposition states that all access structures related to Boolean polynomials of degree ≤ 1, which have the constant summand 1, have these realizations. Furthermore access structures related to Boolean polynomials of degree ≤ 1 without the constant summand 1 allow significantly better elementarily solutions than the universal solution provided by Theorem 4.22.

Proposition 7.6. Let Γ be an access structure on t participants such that the elementary distance vectors are related to a Boolean polynomial p of degree ≤ 1. Then the following parameters b_1, g, k are possible.

(a) Let $\underline{p} = (0, \ldots, 0)$. Then $\Gamma = \mathcal{P}(\mathcal{T}) \setminus \{\varnothing\}$ and (b_1, g, k) is an elementary realization for Γ if

- $2^{t-1} | (b_1 - k)$
- $b_1 > k \geq b_1 \left(\frac{1}{2} - \frac{1}{2^{t+1}-2}\right)$.

(One possible elementary realization is (b_1, g, k) with $b_1 = 2^{e+t+1}$, $k = 2^{e+t} - 2^e$ for $e \in \mathbb{N}$, $e \geq t-1$, g arbitrary.)
Furthermore the minimum code length of each suitable code is b_1.

(b) Let $\underline{p} = (1, \ldots, 1)$. Then all subsets are unauthorized and the parameters $b_1 = g$ are possible for all $b_1 \in \mathbb{N}$. For all $n \geq b_1$ all subsets of $\mathbb{Z}_2^n$, which contain a word s with weight b_1 and a word c with weight $< b_1$, are suitable codes for (s, Γ, b_1, g, k).

(c) Let $p : \mathbb{Z}_2^t \to \mathbb{Z}_2$ be a Boolean polynomial with $\underline{p} \in RM^0(1, t) \setminus \{(0, \ldots, 0)\}$. Then (b_1, g, k) realizes Γ elementarily if

- $2^{t-1} | (b_1 - k)$
- $b_1 > k \geq b_1 \left(\frac{1}{2} - \frac{1}{2^t-2}\right)$.
- $b_1 \geq g \geq k + \frac{b_1-k}{2^{t-1}}$.

(One possible elementary realization is (b_1, g, k) with $b_1 = g = 2^{h+t}$ and $k = 2^{h+t-1} - 2^{h+1}$ for all $h \in \mathbb{N}$, $h \geq t-2$.)
Furthermore the minimum code length of each suitable code is at least $b_1 + g - k - \frac{b_1-k}{2^{t-1}}$.

(d) Let $p : \mathbb{Z}_2^t \to \mathbb{Z}_2$ be a Boolean polynomial with $\underline{p} \in RM^1(1, t) \setminus \{(1, \ldots, 1)\}$. Then (b_1, g, k) realizes Γ elementarily if

- $2^{t-1} | (b_1 - k)$
- $2^{t-1} | (g - k)$
- $b_1 > k \geq b_1 \left(\frac{1}{2} - \frac{1}{2^t-2}\right)$.
- $b_1 \geq g \geq b_1 - \frac{2^{t-1}}{2^{t-1}-1} k$.

(One possible elementary realization is (b_1, g, k) with $b_1 = g$ and $k = 0$.)
Furthermore the minimum code length of each suitable code is b_1.

Proof. (a) Let $\underline{p} = (0, \ldots, 0)$. Choose parameters b_1, k with the properties stated in the proposition. Since all nonempty sets of participants are authorized, equations 2 up to 2^t in the linear system 4.2 have the form

$$a_{2i} - a_{2i-1} = \frac{1}{2^{t-1}}(b_1 - k) > 0.$$

Hence we define $a_{2i} = \frac{1}{2^{t-1}}(b_1 - k)$, which is a natural number since $2^{t-1}|b_1 - k$, and $a_{2i-1} = 0$ for all $i = 2, 3, \dots 2^t$. Then

$$\begin{aligned}\sum_{i=2}^{2^t} a_{2i} &= (2^t - 1)\frac{1}{2^{t-1}}(b_1 - k) \\ &\leq (2^t - 1)\frac{1}{2^{t-1}}\left(\frac{b_1}{2} + \frac{b_1}{2^{t+1} - 2}\right) = b_1,\end{aligned}$$

which shows that $a = (a_2, \dots, a_{2^{t+1}})$ is an elementary solution for (Γ, b_1, g, k) for $a_2 = b_1 - (2^t - 1)\frac{1}{2^{t-1}}(b_1 - k)$.
Furthermore the code length of each suitable code has to be at least

$$\underbrace{\sum_{i=1}^{2^t} a_{2i}}_{=b_1} + \sum_{i=2}^{2^t} \underbrace{a_{2i-1}}_{=0} = b_1.$$

(b) When all sets of participants are unauthorized, we choose an arbitrary code length $n \geq b_1$ and consider an arbitrary subset $\mathcal{C} \subseteq \mathbb{Z}_2^n$ which contains a word s with weight b_1 and a word c with weight $< b_1$. Then we give the zero word of length n as share to all participants. The consequence is that all sums S of shares are also the zero vector and fulfill

$$\mathrm{d}(s, S) > \mathrm{d}(c, S).$$

Hence Hamming decoding yields the wrong codeword.

(c) In this case b is related to a Boolean polynomial p of degree 1 without the constant summand 1. W.l.o.g. let $p(x_1, \dots, x_t) = x_1 + \dots + x_v$, $v \leq t$. According to Lemma 7.3, a vector $y = (y_1, \dots, y_t)^\tau \in \mathbb{Z}_2^t$ is the characteristic vector of an unauthorized set iff $p(y_1, \dots, y_t) = y_1 + \dots + y_v = 1$. That means the set V of the characteristic vectors of the unauthorized sets is the preimage of 1 under the linear transformation $(y_1, \dots, y_t)^\tau \mapsto y_1 + \dots + y_v$ of rank 1. Hence V is an affine subspace of $\mathbb{Z}_2^t$ with dimension $t - 1$ which does not contain the zero vector. Because of Proposition 5.21 we can assume w.l.o.g. that $V = e_t + \langle e_1, \dots, e_{t-1}\rangle$. This yields

$$\varepsilon_{\overline{\Gamma}}^1 = \underbrace{\begin{pmatrix} & * & \\ 1 & \dots & 1\end{pmatrix}}_{u=2^{t-1}} \}\, t-1$$

where the submatrix $(*)$ consists of all possible columns with $t - 1$ entries. According to Remark 5.15, the number d_i of ones in the ith row of $\varepsilon_{\overline{\Gamma}}$ is

$$d_i = \begin{cases} 2^{t-2} & 2^t - 2 \text{ times} \\ 2^t - 1 & \text{once}\end{cases}$$

and we obtain the equations

$$\begin{array}{rcll} a_{2i}-a_{2i-1} & = & \dfrac{1}{2^{t-1}}(b_1-k) & 2^t-2 \text{ times} \\ a_{2i}-a_{2i-1} & = & \dfrac{1}{2^{t-1}}(b_1-k-2^{t-1}(g-k)) & \text{once.} \end{array}$$

We choose parameters b_1, g, k with the properties stated in the proposition. In the first case we define $a_{2i} = \frac{1}{2^{t-1}}(b_1-k)$ which is > 0 since $b_1 > k$, and integer since $2^{t-1}|(b_1-k)$. In this case $a_{2i-1} = 0$. In the second case we define $a_{2i} = 0$ and $a_{2i-1} = -\frac{1}{2^{t-1}}(b_1-k-2^{t-1}(g-k))$ because $b_1-k-2^{t-1}(g-k) < 0$ for $g \geq k + \frac{b_1-k}{2^{t-1}}$. Hence

$$\begin{array}{rcl} \sum_{i=2}^{2^t} a_{2i} & = & (2^t-2)\dfrac{1}{2^{t-1}}(b_1-k) \\ & \leq & (2^t-2)\dfrac{1}{2^{t-1}}\left(\dfrac{b_1}{2}+\dfrac{b_1}{2^t-2}\right) \;=\; b_1. \end{array}$$

Define $a_2 = b_1 - (2^t-2)\frac{1}{2^{t-1}}(b_1-k)$. Then $(a_2, \ldots, a_{2^{t+1}})$ is an elementary solution for (Γ, b_1, g, k).
Furthermore the code length of each suitable code has to be at least

$$\underbrace{\sum_{i=1}^{2^t} a_{2i}}_{=b_1} + \underbrace{\sum_{i=2}^{2^t} a_{2i-1}}_{=g-k-\frac{b_1-k}{2^{t-1}}} \;=\; b_1+g-k-\frac{b_1-k}{2^{t-1}}.$$

(d) b is related to a Boolean polynomial p of degree one with the constant summand 1. W.l.o.g. let $p(x_1, \ldots, x_t) = x_1 + \ldots + x_v + 1$, $v \leq t$. Then a vector $y = (y_1, \ldots, y_t)^\tau \in \mathbb{Z}_2^t$ is the characteristic vector of an unauthorized set iff $p(y_1, \ldots, y_t) = y_1 + \ldots + y_v + 1 = 1$, which is equivalent to $y_1 + \ldots + y_v = 0$. That means the set V of the characteristic vectors of the unauthorized sets is a linear subspace of $\mathbb{Z}_2^t$ of dimension $t-1$. Because of Proposition 5.21 we can assume w.l.o.g. that $V = \langle e_1, \ldots, e_{t-1} \rangle$. This yields

$$\varepsilon^1_{\overline{\Gamma}} = \underbrace{\begin{pmatrix} & * & \\ 0 & \ldots & 0 \end{pmatrix}}_{u=2^{t-1}-1} \}\, t-1$$

where the submatrix $(*)$ consists of all possible columns with $t-1$ entries without the zero column. According to Remark 5.15, the number d_i of ones in the ith row of $\varepsilon_{\overline{\Gamma}}$ is

$$d_i = \begin{cases} 2^{t-2} & 2^t-2 \text{ times} \\ 0 & \text{once} \end{cases}$$

and we obtain the equations

$$\begin{array}{rcll} a_{2i} - a_{2i-1} & = & \frac{1}{2^{t-1}}(b_1 - k - (g-k)) & 2^t - 2 \text{ times} \\ a_{2i} - a_{2i-1} & = & \frac{1}{2^{t-1}}(b_1 - k + (2^{t-1}-1)(g-k)) & \text{once.} \end{array}$$

We choose parameters b_1, g, k with the properties stated in the proposition. In the first case we define $a_{2i} = \frac{1}{2^{t-1}}(b_1 - k - (g-k))$ which is ≥ 0 and $a_{2i-1} = 0$. In the second case we define $a_{2i} = \frac{1}{2^{t-1}}(b_1 - k + (2^{t-1}-1)(g-k)) \geq 0$ and $a_{2i-1} = 0$. This yields

$$\begin{array}{rcl} \sum\limits_{i=2}^{2^t} a_{2i} & = & \frac{1}{2^{t-1}}\left((2^t - 1)(b_1 - k) - (2^t - 2)(g-k) + (2^{t-1}-1)(g-k)\right) \\ & = & b_1\left(2 - \frac{1}{2^{t-1}}\right) - g\left(1 - \frac{1}{2^{t-1}}\right) - k \\ & \leq & b_1\left(2 - \frac{1}{2^{t-1}}\right) - \left(b_1 - \frac{2^{t-1}}{2^{t-1}-1}k\right)\left(1 - \frac{1}{2^{t-1}}\right) - k \\ & = & b_1. \end{array}$$

Choose $a_2 = \sum\limits_{i=2}^{2^t} a_{2i} - b_1$. Then $(a_2, \ldots, a_{2^{t+1}})$ is an elementary solution for (Γ, b_1, g, k).

Furthermore the code length of each suitable code has to be at least

$$\underbrace{\sum_{i=1}^{2^t} a_{2i}}_{=b_1} + \sum_{i=2}^{2^t} \underbrace{a_{2i-1}}_{=0} = b_1.$$

□

Remark 7.7. (a) If p is a Boolean polynomial of degree ≤ 1 with constant summand 1, Proposition 7.6 says that $(b_1, g, k) = (b_1, b_1, 0)$ is an elementary realization. According to Lemma 5.26 (a), $\mathcal{C} = \mathbb{Z}_2^n$ is suitable for (s, Γ, b_1, g, k) for all $n \geq b_1$ and all $s \in \mathbb{Z}_2^n$ with weight b_1.

(b) Suppose that p is a Boolean polynomial of degree 1 without the constant summand 1. Proposition 7.6 yields the following elementary realization (b_1, g, k):

$$b_1 = 2^{h+t} = g \text{ and } k = 2^{h+t-1} - 2^{h+1} \text{ for an arbitrary } h \in \mathbb{N},\ h \geq t-2.$$

According to Lemma 5.26 (b), the first order Reed Muller code $RM(1, h+t+1)$ is suitable for (s, Γ, b_1, g, k) for all codewords $s \in RM(1, h+t+1)$, $s \neq (0, \ldots, 0), (1, \ldots, 1)$.

In the general solution provided by Theorem 4.22 we have the restrictions

$$b_1 \geq 2^{2t} - 2^t \text{ and } g \leq b_1 \left(\frac{1}{2} + \frac{1}{2^t} \right) - 2^{t-1}.$$

Hence the solutions provided by Proposition 7.6 mean an improvement concerning the code length and therefore the efficiency of the scheme. With regard to the security of the scheme, the parameters provided by Proposition 7.6 are far superior to the universal parameters, since g exceeds the covering radius.

At this point we want to mention another approach towards the elementary realizations of access structures related to Boolean polynomials of degree one. This approach uses the fact that the structure of the matrix E defined in 4.11 is also given by Boolean polynomials of degree one (see Lemma 4.12).

Remark 7.8. Each Boolean polynomial $p : \mathbb{Z}_2^t \to \mathbb{Z}_2$ of degree one represents a codeword in $RM(1,t)$. If it has the summand 1, then $\underline{p}$ is contained in $RM^1(1,t)$. Otherwise $\underline{p}$ lies in $RM^0(1,t)$.
Recall that the matrix $E = E(t)$ is also related to codewords in $RM(1,t)$. It's rows are defined by the codewords of $RM^0(1,t)$ ordered by $\preccurlyeq$ in the way that all zeros in the codewords are replaced by ones and all ones by minus ones.
These observations yield an alternative way to prove Proposition 7.6 (c) and (d): Equation 2 up to equation 2^t in the linear system 4.2 come from the equation

$$E \cdot b = \begin{pmatrix} a_4 - a_3 \\ a_6 - a_5 \\ \vdots \\ a_{2^{t+1}} - a_{2^{t+1}-1} \end{pmatrix}.$$

If b is related to a Boolean polynomial p with $\underline{p} = c \in RM(1,t)$ we have

$$\begin{aligned} E \cdot b &= E \cdot (g \cdot c + k \cdot \overline{c} + (b_1 - k)e_1)^\tau \\ &= g \cdot Ec^\tau + k \cdot E\overline{c}^\tau + (b_1 - k) \cdot Ee_1^\tau \\ &= (g - k) \cdot Ec^\tau + (b_1 - k) \cdot (1, \ldots, 1)^\tau \end{aligned}$$

for $c \in RM^0(1,t)$ and

$$\begin{aligned} E \cdot b &= E \cdot (g \cdot c + k \cdot \overline{c} + (b_1 - g)e_1)^\tau \\ &= g \cdot Ec^\tau + k \cdot E\overline{c}^\tau + (b_1 - g) \cdot Ee_1^\tau \\ &= (g - k) \cdot Ec^\tau + (b_1 - g) \cdot (1, \ldots, 1)^\tau \end{aligned}$$

for $c \in RM^1(1,t)$.
Since the rows of E belong to the codewords in $RM^0(1,t)$ ordered by $\preccurlyeq$, it can be

shown that

$$E \cdot c^{\tau} = \begin{cases} (0,\dots,0,\overset{\uparrow}{-2^{t-1}},0,\dots,0) & \text{if } c \text{ is the } l\text{th codeword in } RM^0(1,t) \\ \qquad\qquad\quad l & \\ \qquad\qquad\quad \downarrow & \\ (0,\dots,0,2^{t-1},0,\dots,0) & \text{if } c \text{ is the } l\text{th codeword in } RM^1(1,t). \end{cases}$$

These calculations yield the same elementary solutions $(a_2,\dots,a_{2^{t+1}})$ as the proof of Proposition 7.6 (c) and (d):
For $c \in RM^0(1,t)$ we have

$$a_{2i} - a_{2i-1} = \begin{cases} \frac{1}{2^{t-1}}(-2^{t-1}(g-k) + b_1 - k) & \text{if } i = l \\ \frac{1}{2^{t-1}}(b_1 - k) & \text{if } i \neq l. \end{cases}$$

$c \in RM^1(1,t)$ yields

$$a_{2i} - a_{2i-1} = \begin{cases} \quad \frac{1}{2^{t-1}}(2^{t-1}(g-k) + b_1 - g) & \\ = \frac{1}{2^{t-1}}(b_1 - k + (2^{t-1}-1)(g-k)) & \text{if } i = l \\ \quad \frac{1}{2^{t-1}}(b_1 - g) & \\ = \frac{1}{2^{t-1}}(b_1 - k - (g-k)) & \text{if } i \neq l. \end{cases}$$

We have seen that access structures related to Boolean polynomials of degree ≤ 1 have very nice realizations. But how do these access structures look like? We have a look at these access structures for $t = 3$ participants.

Example 7.9. For $t = 3$ we have the following access structures related to Boolean polynomials p of degree ≤ 1:

p	b^{τ}	Γ
0	(b_1,k,k,k,k,k,k,k)	$\mathcal{P}(\mathcal{T}) \setminus \{\varnothing\}$
x_1	(b_1,g,k,g,k,g,k,g)	$\{A \neq \varnothing : T_1 \notin A\}$
x_2	(b_1,k,g,g,k,k,g,g)	$\{A \neq \varnothing : T_2 \notin A\}$
$x_1 + x_2$	(b_1,g,g,k,k,g,g,k)	$\{A \neq \varnothing : T_1, T_2 \in A \text{ or } T_1, T_2 \notin A\}$
x_3	(b_1,k,k,k,g,g,g,g)	$\{A \neq \varnothing : T_3 \notin A\}$
$x_1 + x_3$	(b_1,g,k,g,g,k,g,k)	$\{A \neq \varnothing : T_1, T_3 \in A \text{ or } T_1, T_3 \notin A\}$
$x_2 + x_3$	(b_1,k,g,g,g,g,k,k)	$\{A \neq \varnothing : T_2, T_3 \in A \text{ or } T_2, T_3 \notin A\}$
$x_1 + x_2 + x_3$	(b_1,g,g,k,g,k,k,g)	$\{A \neq \varnothing : \lvert A \rvert \text{ even}\}$

p	$b^\mathcal{T}$	Γ
1	$(b_1, g, g, g, g, g, g, g)$	$\varnothing$
$1 + x_1$	$(b_1, k, g, k, g, k, g, k)$	$\{A : T_1 \in A\}$
$1 + x_2$	$(b_1, g, k, k, g, g, k, k)$	$\{A : T_2 \in A\}$
$1 + x_1 + x_2$	$(b_1, k, k, g, g, k, k, g)$	$\{A \neq \varnothing : T_1 \in A \text{ XOR } T_2 \in A\}$
$1 + x_3$	$(b_1, g, g, g, k, k, k, k)$	$\{A : T_3 \in A\}$
$1 + x_1 + x_3$	$(b_1, k, g, k, k, g, k, g)$	$\{A \neq \varnothing : T_1 \in A \text{ XOR } T_3 \in A\}$
$1 + x_2 + x_3$	$(b_1, g, k, k, k, k, g, g)$	$\{A \neq \varnothing : T_2 \in A \text{ XOR } T_3 \in A\}$
$1 + x_1 + x_2 + x_3$	$(b_1, k, k, g, k, g, g, k)$	$\{A : \lvert A\rvert \text{ odd}\}$

In Chapter 4 we considered the access structure $\Gamma = \{A : T_j \in A\}$ for a fixed j. We now know that this access structure is related to the Boolean polynomial $1 + x_j$. The special feature of this access structure is, that it can be realized using only the secret s itself and the zero vector as shares. There are only a few access structures which allow these shares and we are able to describe them in terms of Boolean polynomials.

Proposition 7.10. Let Γ be an access structure on the participant set $\mathcal{T} = \{T_1, \ldots, T_t\}$. Then the following statements are equivalent:

(a) Γ is related to a Boolean polynomial p with $\underline{p} \in RM^1(1,t)$.

(b) Γ can be realized by assigning the following shares:

$$T_j \text{ receives } \begin{cases} \text{the secret } s & \text{if } \{T_j\} \in \Gamma \\ \text{the zero vector} & \text{if } \{T_j\} \in \overline{\Gamma} \end{cases} \quad \text{for all } j = 1, \ldots, t.$$

Proof. "$\Rightarrow$" Suppose that (a) holds. For $p = 1$ this is Proposition 7.6 (b).
W.l.o.g. let $p(x_1, \ldots, x_t) = x_1 + \ldots + x_v + 1$. Lemma 7.3 yields

$$\begin{aligned} & A = \{T_{i_1}, \ldots, T_{i_l}\} \in \Gamma \\ \Leftrightarrow\; & p(y_1, \ldots, y_t) = y_1 + \ldots + y_v + 1 = 0 \\ & \text{for } y_i = \begin{cases} 1 & \text{if } T_i \in A \\ 0 & \text{if } T_i \notin A \end{cases} \text{ for all } i = 1, \ldots, t \\ \Leftrightarrow\; & A \text{ contains an odd number of participants of the set } \{T_1, \ldots, T_v\}\,. \end{aligned}$$

When we give the secret s as share to each participant in $\{T_1, \ldots, T_v\}$ and the zero vector to all other participants, this access structure is realized.

"$\Leftarrow$" Suppose that (b) holds. When there is no $T_j \in \Gamma$, all participants receive the zero word and $\Gamma \sim 1$. Now assume that w.l.o.g. exactly for $j = 1, \ldots, v$ the sets $\{T_j\}$ are the authorized sets with one element. Let $V = \{T_1, \ldots, T_v\}$. Consider an arbitrary non-empty set $A \subseteq \mathcal{T}$ and the related sum S of the shares.

- If $A \cap V = \varnothing$, $S = 0$ and A is unauthorized.

- If $A \cap V = \{T_{i_1}, \ldots, T_{i_l}\}$, $S = \begin{cases} s & \text{if } l \text{ is odd} \\ 0 & \text{if } l \text{ is even} \end{cases}$ and $A \in \begin{cases} \Gamma & \text{if } l \text{ is odd} \\ \overline{\Gamma} & \text{if } l \text{ is even} \end{cases}$.

Hence $\Gamma \sim 1 + x_1 + \ldots + x_v$.

□

Next we have a look at access structures related to Boolean monomials of higher degree and their duals.

Proposition 7.11. Let Γ be an access structure on t participants related to a Boolean monomial $p : \mathbb{Z}_2^t \to \mathbb{Z}_2$ of degree v, $1 \leq v \leq t$.

(a) (b_1, g, k) is an elementary realization for Γ if

- $b_1 \geq 2^{2t-1} - 2^t$ and $2^t | b_1$
- $k = \frac{b_1}{2} - 2^{t-1}$
- $b_1 \left(\frac{1}{2} + \frac{1}{2^{t-v+1}}\right) - 2^{t-1}(2^{t-v} - 1) \leq g \leq b_1 \left(\frac{1}{2} + \frac{1}{2^{t-v+1}}\right)$ such that $2^{v-1} | g - k$.

Furthermore the minimum code length of each suitable code is $n \geq b_1 + g - k - \frac{b_1 - k}{2^{t-v}}$.

(b) The dual access structure $\overline{\Gamma}$ is related to the Boolean polynomial $p + 1$ and (b_1, g, k) is an elementary realization if

- $k < b_1$
- $b_1 \geq g \geq \max\left\{b_1 - k, k + \frac{b_1 - k}{2^{t-v}+1}\right\}$.
- $2^{t-1} | (b_1 - k)$, $2^{t-1} | (g - k)$.

The parameters $b_1 = g$ and $k = 0$ are possible for all $b_1 \in \mathbb{N}$ with $2^{v-1} | b_1$.
The minimum code length of each suitable code is
$\frac{1}{2^{t-1}} \left((2^{t-1} - 2^{v-1} + 1)b_1 + (2^{t-1} + 2^{v-1} - 2^{t-v} - 1)g - (2^{t-1} - 2^{t-v})k\right)$.

Proof. (a) W.l.o.g. we assume that $p(x_1, \ldots, x_t) = x_1 \cdot \ldots \cdot x_v$. According to Lemma 7.3 the vector $y = (y_1, \ldots, y_t)^\tau \in \mathbb{Z}_2^t$ is the characteristic vector of a subset in Γ iff $p(y_1, \ldots, y_t) = 0$. This is equivalent to $y_1 \cdot \ldots \cdot y_v = 0$ and happens iff there is at least one $y_j = 0$ for $1 \leq j \leq v$. Only $y_1 = \ldots = y_v = 1$ yields $y_1 \cdot \ldots \cdot y_v = 1$. That is why we know that $\Gamma = \{A \subseteq \mathcal{T} : \{T_1, \ldots, T_v\} \subseteq A\}$. $\varepsilon^1_{\overline{\Gamma}}$ consists of all possible columns in $\mathbb{Z}_2^t$ which have the form $(\underbrace{1, \ldots, 1}_{v}, \underbrace{*, \ldots, *}_{t-v})^\tau$. This means that there are $u = 2^{t-v}$ unauthorized sets and

$$\varepsilon^1_{\overline{\Gamma}} = \underbrace{\begin{pmatrix} 1 & \ldots & 1 \\ \vdots & & \vdots \\ 1 & \ldots & 1 \\ & * & \end{pmatrix}}_{2^{t-v}} \begin{matrix} \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} v \\ \}\, t - v \end{matrix}$$

where the columns of the matrix $(*)$ are all vectors in $\mathbb{Z}_2^{t-v}$. The matrix $\varepsilon_{\overline{\Gamma}}$, which consists of all possible linear combinations of the rows of $\varepsilon^1_{\overline{\Gamma}}$, has the weight vector

$$w_{\overline{\Gamma}} = (\underset{\overset{\uparrow}{0}}{2^{v-1} - 1}, 0, \ldots, 0, \underset{\overset{\uparrow}{2^{t-v-1}}}{2^t - 2^v}, 0, \ldots, 0, \underset{\overset{\uparrow}{2^{t-v}}}{2^{v-1}})$$

(see Remark 5.15). The related equations of the linear system 4.2 are

$$a_{2i} - a_{2i-1} \;=\; \begin{cases} \frac{1}{2^{t-1}}\left(b_1 - k + 2^{t-v}(g-k)\right) & 2^{v-1} - 1 \text{ times,} \\ \frac{1}{2^{t-1}}\left(b_1 - k\right) & 2^t - 2^v \text{ times,} \\ \frac{1}{2^{t-1}}\left(b_1 - k - 2^{t-v}(g-k)\right) & 2^{v-1} \text{ times.} \end{cases}$$

Choose b_1, g, k as stated in the proposition. Then $b_1 - k - 2^{t-v}(g-k) \leq 0$. For all $i = 2, \ldots, 2^t$ define a_{2i} to be the right hand side of the equation and $a_{2i-1} = 0$, if this side is positive. When the right hand side is negative we choose $a_{2i} = 0$ and define a_{2i-1} to be the absolute value of the right hand side. This yields an elementary solution $(a_2, \ldots, a_{2^{t+1}})$ for (Γ, b_1, g, k) since $\sum_{i=2}^{2^t} a_{2i} \leq b_1$ holds:

$$\begin{aligned} \sum_{i=2}^{2^t} a_{2i} &= \frac{1}{2^{t-1}}\left((2^t - 2^{v-1} - 1)\underbrace{(b_1 - k)}_{=\frac{b_1}{2}+2^{t-1}} + (2^{v-1} - 1)2^{t-v}\underbrace{(g-k)}_{\leq\frac{b_1}{2^{t-v+1}}+2^{t-1}}\right) \\ &\leq \frac{1}{2^{t-1}}\left(b_1(2^{t-1} - 1) + 2^{t-1}(2^t - 2)\right) \\ &= b_1 + 2^t - 2 - \underbrace{\frac{b_1}{2^{t-1}}}_{\geq 2^t - 2} \;\leq\; b_1. \end{aligned}$$

Furthermore

$$\begin{aligned} \sum_{i=2}^{2^t} a_{2i-1} &= \frac{1}{2^{t-1}} \cdot 2^{v-1}\left(2^{t-v}(g-k) - (b_1 - k)\right) \\ &= g - k - \frac{b_1 - k}{2^{t-v}} \end{aligned}$$

shows that the length of each suitable code has to be $\geq b_1 + g - k - \frac{b_1 - k}{2^{t-v}}$.

(b) In the proof of part (a) we determined the weight vector $w_{\overline{\Gamma}}$ of the matrix $\varepsilon_{\overline{\Gamma}}$. $\varepsilon_{\overline{\overline{\Gamma}}} = \varepsilon_\Gamma$ contains the remaining columns of the matrix ε with the first row and first column removed, and we deduce that the weight vector of ε_Γ has to be

$$w_\Gamma = (0,\dots,0,\underset{\substack{\uparrow\\ 2^{t-1}-2^{t-v}}}{2^{v-1}},0,\dots,0,\underset{\substack{\uparrow\\ 2^{t-1}-2^{t-v-1}}}{2^t-2^v},0,\dots,0,\underset{\substack{\uparrow\\ 2^{t-1}}}{2^{v-1}-1},0,\dots,0).$$

Γ contains $2^t - 2^{t-v} - 1$ sets and the related equations of the linear system 4.2 are

$$a_{2i} - a_{2i-1} \;=\; \begin{cases} \frac{1}{2^{t-1}}\left(b_1 - k + (2^{t-v}-1)(g-k)\right) & 2^{v-1} \text{ times,}\\ \frac{1}{2^{t-1}}\left(b_1 - k - (g-k)\right) & 2^t - 2^v \text{ times,}\\ \frac{1}{2^{t-1}}\left(b_1 - k - (2^{t-v}+1)(g-k)\right) & 2^{v-1}-1 \text{ times.}\end{cases}$$

Choose b_1, g, k as stated in the proposition. Then $b_1 - k - (2^{t-v}+1)(g-k)$ is negative as $g \geq k + \frac{b_1-k}{2^{t-v}+1}$. For all $i = 2,\dots,2^t$ we define a_{2i} and a_{2i-1} as described in part (a). This yields an elementary solution $(a_2,\dots,a_{2^{t+1}})$ for $(\overline{\Gamma}, b_1, g, k)$ since

$$\begin{aligned}\sum_{i=2}^{2^t} a_{2i} &= \frac{1}{2^{t-1}}\left((2^t - 2^{v-1})(b_1-k) + (2^{v-1}(2^{t-v}-1) - (2^t-2^v))(g-k)\right)\\ &= b_1 - k + \frac{1}{2^{t-1}}(2^{t-1}-2^{v-1})\underbrace{(b_1-g)}_{\leq k}\\ &\leq b_1 - \frac{1}{2^{t-v}}k \;\leq\; b_1.\end{aligned}$$

The parameters $b_1 = g$, $k = 0$ have the property that $k < \frac{b_1}{2}$ and $g \geq \max\{b_1 - k, k + \frac{b_1-k}{2^{t-v}+1}\}$. In this case the requirements $2^{t-1}|(b_1 - k = g - k = b_1)$ can be weakened: For all $i = 2,\dots,2^t$ we have $a_{2i} - a_{2i-1} \in \left\{0, \pm\frac{b_1}{2^{v-1}}\right\}$ and the requirement $2^{v-1}|b_1$ is sufficient.

Furthermore

$$\begin{aligned}\sum_{i=2}^{2^t} a_{2i-1} &= \frac{1}{2^{t-1}}(2^{v-1}-1)\left((2^{t-v}+1)(g-k) - (b_1-k)\right)\\ &= \frac{1}{2^{t-1}}\left((2^{t-1}+2^{v-1}-2^{t-v}-1)g - (2^{t-1}-2^{t-v})k - (2^{v-1}-1)b_1\right)\end{aligned}$$

shows that the length of each suitable code has to be

$$\begin{aligned} n &\geq b_1 + \frac{1}{2^{t-1}}\left((2^{t-1}+2^{v-1}-2^{t-v}-1)g - (2^{t-1}+2^{t-v})k - (2^{v-1}-1)b_1\right)\\ &= \frac{1}{2^{t-1}}\left((2^{t-1}-2^{v-1}+1)b_1 + (2^{t-1}+2^{v-1}-2^{t-v}-1)g - (2^{t-1}+2^{t-v})k\right).\end{aligned}$$

□

Example 7.12. Let Γ be an access structure on $t = 4$ participants which is related to the Boolean polynomial $p(x_1, x_2, x_3, x_4) = 1 + x_1x_2x_3$. Then

$$\Gamma = \{\{T_1.T_2, T_3\}, \{T_1, T_2, T_3, T_4\}\}$$

and

$$\varepsilon_{\overline{\Gamma}} = \underbrace{\begin{pmatrix}
1&0&1&0&1&0&0&1&0&1&0&1&0\\
0&1&1&0&0&1&0&0&1&1&0&0&1\\
1&1&0&0&1&1&0&1&1&0&0&1&1\\
0&0&0&1&1&1&0&0&0&0&1&1&1\\
1&0&1&1&0&1&0&1&0&1&1&0&1\\
0&1&1&1&1&0&0&0&1&1&1&1&0\\
1&1&0&1&0&0&0&1&1&0&1&0&0\\
0&0&0&0&0&0&1&1&1&1&1&1&1\\
1&0&1&0&1&0&1&0&1&0&1&0&1\\
0&1&1&0&0&1&1&1&0&0&1&1&0\\
1&1&0&0&1&1&1&0&0&1&1&0&0\\
0&0&0&1&1&1&1&1&1&1&0&0&0\\
1&0&1&1&0&1&1&0&1&0&0&1&0\\
0&1&1&1&1&0&1&1&0&0&0&0&1\\
1&1&0&1&0&0&1&0&0&1&0&1&1
\end{pmatrix}}_{u=13}
\begin{array}{c}
6\\6\\8\\6\\8\\8\\6\\7\\7\\7\\7\\7\\7\\7\\7
\end{array}.$$

The additional row contains the weights of the rows. Choose $b_1 = g = 8$ and $k = 0$. The related equations of the linear system 4.2 are

$$\begin{aligned}
a_{2i} - a_{2i-1} &= \frac{1}{8}\left(b_1 + (13 - 2\cdot 6)b_1\right)\\
&= \frac{b_1}{4} \text{ for } i = 2, 3, 5, 8
\end{aligned}$$

$$\begin{aligned}
a_{2i} - a_{2i-1} &= \frac{1}{8}\left(b_1 + (13 - 2\cdot 7)b_1\right)\\
&= 0 \text{ for } i = 9, 10, \ldots, 16
\end{aligned}$$

$$\begin{aligned}
a_{2i} - a_{2i-1} &= \frac{1}{8}\left(b_1 + (13 - 2\cdot 8)b_1\right)\\
&= -\frac{b_1}{4} \text{ for } i = 4, 6, 7.
\end{aligned}$$

We choose $a_4 = a_6 = a_{10} = a_{16} = a_7 = a_{11} = a_{13} = \frac{b_1}{4} = 2$ and the remaining $a_j = 0$. Then $\sum_{i=2}^{16} a_{2i} = b_1$ and $\sum_{i=2}^{16} a_{2i-1} = \frac{3}{4}b_1$ and we choose $a_2 = 0$ and $a_1 = \frac{1}{4}b_1 = 2$. Let $s = (1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0)$ be the secret to be shared. That means $\mathrm{supp}(s) = \{1, 2, \ldots, 8\}$.

$$\begin{aligned}
I_1^4 &= \overline{\mathrm{supp}(s)} \cap \overline{\mathrm{supp}(k_1)} \cap \overline{\mathrm{supp}(k_2)} \cap \overline{\mathrm{supp}(k_3)} \cap \overline{\mathrm{supp}(k_4)}\\
I_4^4 &= \mathrm{supp}(s) \cap \mathrm{supp}(k_1) \cap \overline{\mathrm{supp}(k_2)} \cap \overline{\mathrm{supp}(k_3)} \cap \overline{\mathrm{supp}(k_4)}\\
I_6^4 &= \mathrm{supp}(s) \cap \overline{\mathrm{supp}(k_1)} \cap \mathrm{supp}(k_2) \cap \overline{\mathrm{supp}(k_3)} \cap \overline{\mathrm{supp}(k_4)}\\
I_7^4 &= \overline{\mathrm{supp}(s)} \cap \mathrm{supp}(k_1) \cap \mathrm{supp}(k_2) \cap \overline{\mathrm{supp}(k_3)} \cap \overline{\mathrm{supp}(k_4)}\\
I_{10}^4 &= \mathrm{supp}(s) \cap \overline{\mathrm{supp}(k_1)} \cap \overline{\mathrm{supp}(k_2)} \cap \mathrm{supp}(k_3) \cap \overline{\mathrm{supp}(k_4)}\\
I_{11}^4 &= \overline{\mathrm{supp}(s)} \cap \mathrm{supp}(k_1) \cap \overline{\mathrm{supp}(k_2)} \cap \mathrm{supp}(k_3) \cap \overline{\mathrm{supp}(k_4)}\\
I_{13}^4 &= \overline{\mathrm{supp}(s)} \cap \overline{\mathrm{supp}(k_1)} \cap \mathrm{supp}(k_2) \cap \mathrm{supp}(k_3) \cap \overline{\mathrm{supp}(k_4)}\\
I_{16}^4 &= \mathrm{supp}(s) \cap \mathrm{supp}(k_1) \cap \mathrm{supp}(k_2) \cap \mathrm{supp}(k_3) \cap \overline{\mathrm{supp}(k_4)}
\end{aligned}$$

Let a_4, a_6, a_{10}, a_{16} determine the positions $\{1,2\}$, $\{3,4\}$, $\{5,6\}$, $\{7,8\}$ and a_1, a_9, a_{11}, a_{13} the positions $\{9,10\}$, $\{11,12\}$, $\{13,14\}$, $\{15,16\}$, respectively- This yields the following shares:

$$\begin{aligned}
k_1 &= (1,1,0,0,0,0,1,1,0,0,1,1,1,1,0,0)\\
k_2 &= (0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1)\\
k_3 &= (0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1)\\
k_4 &= (0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)
\end{aligned}$$

Remark 7.13. (a) For $\Gamma \sim x_{i_1} \cdot \ldots \cdot x_{i_v}$ the parameters provided by Proposition 7.11 (a) represent a slight improvement on the parameters provided by Theorem 4.22: b_1 is improved from

$$b_1 \geq 2^{2t} - 2^t \quad \text{to} \quad b_1 \geq 2^{2t-1} - 2^t$$

and g is improved from

$$\begin{aligned}
\frac{b_1}{2} &< g \leq b_1\left(\frac{1}{2} + \frac{1}{2^t}\right) - 2^{t-1}\\
&\text{to}\\
b_1\left(\frac{1}{2} + \frac{1}{2^{t-v+1}}\right) - 2^{t-1}(2^{t-v} - 1) &\leq g \leq b_1\left(\frac{1}{2} + \frac{1}{2^{t-v+1}}\right).
\end{aligned}$$

k is subject to the same condition $k = \frac{b_1}{2} - 2^{t-1}$.

(b) For $\Gamma \sim x_{i_1} \cdot \ldots \cdot x_{i_v} + 1$ the parameters $b_1 = g$ and $k = 0$ are possible. Proposition 7.11 (b) and Lemma 5.26 (a) imply, that for all $n \geq b_1\left(2 - \frac{1}{2^{v-1}}\right)$ the code $\mathcal{C} = \mathbb{Z}_2^n$ is suitable for $(s, \Gamma, b_1, b_1, 0)$ for all words $s \in \mathbb{Z}_2^n$ with weight b_1.

When an access structure Γ is related to a Boolean polynomial of the form $p = x_{i_1} \cdot \ldots \cdot x_{i_v} + 1$, a set is authorized iff it contains the set $\{T_{i_1}, \ldots, T_{i_v}\}$. That means $\{T_{i_1}, \ldots, T_{i_v}\}$ is a *necessary* subset of all authorized sets and Γ is defined by this necessary set. The dual access structure $\overline{\Gamma}$ consists of all non-empty sets which do not contain the whole set $\{T_{i_1}, \ldots, T_{i_v}\}$. For this access structure one can say that the participants $T_{i_1}, \ldots, T_{i_v}$ have veto power. When they work together and collectively join the reconstruction process, they prevent the recovery of the secret. $\overline{\Gamma}$ is characterized uniquely by the *veto set* $\{T_{i_1}, \ldots, T_{i_v}\}$.

This motivates us to have a closer look at access structures defined by necessary sets and veto sets and their realizations.

7.2 Access Structures Defined by Necessary Sets and Veto Sets

In this section we deal with classes of access structures defined by so-called necessary sets and veto sets. It will turn out that some of these classes match perfectly to our approach using error-correcting codes and allow large security distances g and small code lengths n.

By a *necessary set* we mean a subset $N \subseteq \mathcal{T}$ such that a set of participants can only be authorized if it contains certain participants of N. A subset $V \subseteq \mathcal{T}$ is called a *veto set* when all sets of participants, which contain certain participants of V, are unauthorized. In other words these certain participants are able to compromise the correct reconstruction of the secret: They have veto power.

In [8] Blundo et al. also consider access structures with veto capability, which can be realized using error-correcting codes. However, the way in which the participants use their vetoes is different and the resulting access structures cannot be described by veto sets. Additionally the use of the error-correcting code is completely different from our approach. Blundo et al. study threshold access structures with veto capability. In such a (r, m, t)-access structure on a set of t participants a set is authorized iff it contains at least r participants from whom at most $m - 1$ members want to prevent the correct reconstruction of the secret. Each participant can decide whether he wants to recover the secret or whether he wants to compromise the reconstruction. For this purpose he has two different shares: one share to enable the reconstruction of the secret and another share to prevent it. This means, strictly speaking, this is not an access structure in the sense of Definition 2.1.

Blundo et al. show how these access structures can be realized using Reed Solomon codes. They start with a realization for the case $m = 1$ where all sets with at least r participant are authorized if no participant uses his veto. Their method is an expansion of Shamir's scheme and works as follows.

Consider a secret $s \in GF(p^m)$, p prime, and choose random elements $s_1, s_2 \in GF(p^m)$ such that $s = s_1 + s_2$ (componentwise addition modulo p). Choose two polynomials $f, g \in GF(p^m)[x]$ randomly with $deg(f) = 2r - 2$ and $deg(g) = r - 1$ such that $f(0) = s_1$ and $g(0) = s_2$. Let c be the codeword of a Reed Solomon code over $GF(p^m)$ which belongs to the polynomial f. The shares of each participant consist of some correct digits of the codeword c, some random elements of $GF(p^m)$, which are not components of c, and one interpolation point of g. In the recreation process each participant provides his interpolation point. When he wants to recover the secret, he also provides his correct parts of c. Otherwise, when he wants to prevent the reconstruction, he uses his veto by giving his random elements. When at least r participants join the reconstruction process, their interpolation points yield the polynomial g and therefore $g(0) = s_2$. Fewer than r interpolation points provide no information about s_2. This is Shamir's scheme. In addition to that, when no participant uses his veto, there are enough correct digits to recover c with an errors-and-erasures algorithm. The codeword c yields $s_1 = f(0)$ and therefore the secret $s = s_1 + s_2$. When at least one participant refuses to give his correct digits, there are too few digits to decode c and s_1 cannot be found.

For $m > 1$ a (r, m, t)-access structures can be derived from $(r, 1, t)$-access structures in the following way. Choose a random polynomial $f \in GF(p^m)[x]$ of degree $t - m$ such that $s = f(0)$ is the secret and choose t further interpolation points $s_1, \ldots, s_t$ of f such that each participant T_j has the power to prevent the reconstruction of one interpolation point s_j by providing his random elements instead of the correct components. In the reconstruction process the participants try to recreate as many as possible of the interpolation points of f and use them to recover s just as in Shamir's scheme. When less than r participants join the reconstruction, no interpolation point can be found and s cannot be recovered. Suppose that at least r participants take part. When m or more participants use their vetoes, at most $t - m$ interpolation points can be reconstructed- too few to recover f and s. Otherwise the secret can be found, since at least $r - m + 1$ interpolation points can be recovered.

Now we return to access structures defined by necessary sets and veto sets. At first we have a closer look on those defined by necessary sets. We consider two kinds:

Definition 7.14. Let $\mathcal{T}$ be a set of participants, Γ an access structure on $\mathcal{T}$ and $N \subseteq \mathcal{T}$, $N \neq \varnothing$.

- N is called *strongly necessary*, when all authorized sets contain the whole set N. That means the whole set N is necessary for reconstructing the secret.
- We call N *weakly necessary*, when each authorized set contains at least one participant of N. Here at least one participant of N is necessary for reconstruction.

Note that there can be unauthorized sets containing N or participants from N. Access structures with necessary sets are generally non-monotone.

Example 7.15. Let $\mathcal{T} = \{T_1, T_2, T_3, T_4\}$ and $N = \{T_1, T_2\}$. For

$$\Gamma = \{\{T_1, T_2\}, \{T_1, T_2, T_4\}\}$$

N is strongly necessary and for

$$\Gamma = \{\{T_1, T_2, T_3\}, \{T_2, T_4\}\}$$

N is weakly necessary.

Note that a strongly necessary set N is also weakly necessary, since all authorized sets have to contain N and therefore at least one element of N.

Definition and Remark 7.16. Let $\mathcal{T}$ be a set of participants and $N \subseteq \mathcal{T}$. The largest access structure (e.g. the access structure with the largest cardinality) on $\mathcal{T}$ with N being strongly necessary is

$$\Gamma_{sn}(\mathcal{T}, N) := \{A \subseteq \mathcal{T} : N \subseteq A\} .$$

The largest access structure on $\mathcal{T}$ with N being weakly necessary is

$$\Gamma_{wn}(\mathcal{T}, N) := \{A \subseteq \mathcal{T} : N \cap A \neq \varnothing\} .$$

When the participant set $\mathcal{T}$ is clear, we omit the parameter $\mathcal{T}$.

Remark 7.17. We have the inclusion $\Gamma_{sn}(\mathcal{T}, N) \subseteq \Gamma_{wn}(\mathcal{T}, N)$ because

$$\begin{aligned} A \in \Gamma_{sn}(\mathcal{T}, N) &\Rightarrow N \subseteq A \\ &\Rightarrow A \cap N \neq \varnothing \\ &\Rightarrow A \in \Gamma_{wn}(\mathcal{T}, N). \end{aligned}$$

Example 7.18. For $\mathcal{T} = \{T_1, T_2, T_3, T_4\}$ and $N = \{T_1, T_2\}$

$$\Gamma_{sn}(N) = \{\{T_1, T_2\}, \{T_1, T_2, T_3\}, \{T_1, T_2, T_4\}, \{T_1, T_2, T_3, T_4\}\}$$

and

$$\begin{aligned} \Gamma_{wn}(N) = \; &\{ \{T_1\}, \{T_1, T_3\}, \{T_1, T_4\}, \{T_1, T_3, T_4\}, \\ &\{T_2\}, \{T_2, T_3\}, \{T_2, T_4\}, \{T_2, T_3, T_4\}, \\ &\{T_1, T_2\}, \{T_1, T_2, T_3\}, \{T_1, T_2, T_4\}, \{T_1, T_2, T_3, T_4\} \}. \end{aligned}$$

Now we will have a closer look at access structures defined by veto sets. Again we consider two kinds:

Definition 7.19. Let $\mathcal{T}$ be a set of participants, Γ an access structure on $\mathcal{T}$ and $V \subseteq \mathcal{T}$, $V \neq \varnothing$.

- We say that V is a *strong veto set* , when all sets of participants, which contain at least one participant of V, are unauthorized. That means each single participant of V has veto power.
- We say that V is a *weak veto set* , when all sets containing the whole set V are unauthorized. Here the participants of V have veto power when all of them collaborate.

When a set V is a strong veto set, it is also a weak veto set: Suppose that all subsets containing at least one element of V are unauthorized. Then all sets containing the whole set V must be unauthorized, too.

Example 7.20. Let $\mathcal{T} = \{T_1, T_2, T_3, T_4\}$ and $V = \{T_1, T_2\}$. For

$$\Gamma = \{\{T_3\}, \{T_3, T_4\}\}$$

V is a strong veto set, since all sets containing T_1 or T_2 are unauthorized. For

$$\Gamma = \{\{T_1, T_3\}, \{T_2, T_4\}\}$$

V is a weak veto set, since all sets , which contain T_1 and T_2, are unauthorized.

Definition and Remark 7.21. Let $\mathcal{T}$ be a set of participants and $V \subseteq \mathcal{T}$. Then

$$\Gamma_{sv}(\mathcal{T}, N) := \{A \subseteq \mathcal{T} : A \neq \varnothing,\ V \cap A = \varnothing\}$$

is the largest access structure on $\mathcal{T}$ with V being a strong veto set.

$$\Gamma_{wv}(\mathcal{T}, N) := \{A \subseteq \mathcal{T} : A \neq \varnothing,\ V \nsubseteq A\}.$$

is the largest access structure on $\mathcal{T}$ with V being a weak veto set. When the participant set $\mathcal{T}$ is clear, we omit the parameter $\mathcal{T}$.

Remark 7.22. We have the inclusion $\Gamma_{sv}(\mathcal{T}, V) \subseteq \Gamma_{wv}(\mathcal{T}, V)$ because

$$\begin{aligned} A \in \Gamma_{sv}(\mathcal{T}, V) \quad &\Rightarrow \quad A \cap V = \varnothing \\ &\Rightarrow \quad V \nsubseteq A \\ &\Rightarrow \quad A \in \Gamma_{wv}(\mathcal{T}, V). \end{aligned}$$

There is an interesting connection between the access structures defined by necessary sets and those define by veto sets.

Remark 7.23. Let $\mathcal{T}$ be an arbitrary set of participants and $N \subseteq \mathcal{T}$. Then

- $\Gamma_{sn}(\mathcal{T}, N) = \{A : N \subseteq A\}$ is dual to $\Gamma_{wv}(\mathcal{T}, N) = \{A \neq \varnothing : N \nsubseteq A\}$ and
- $\Gamma_{wn}(\mathcal{T}, N) = \{A : N \cap A \neq \varnothing\}$ is dual to $\Gamma_{sv}(\mathcal{T}, N) = \{A \neq \varnothing : N \cap A = \varnothing\}$.

Example 7.24. Let $\mathcal{T} = \{T_1, T_2, T_3, T_4\}$ and $V = \{T_1, T_2\}$. Then

$$\Gamma_{sv}(V) = \overline{\Gamma_{wn}(V)} = \{\{T_3\}, \{T_4\}, \{T_3, T_4\}\}$$

and

$$\begin{aligned}\Gamma_{wv}(V) &= \overline{\Gamma_{sn}(V)}\\ &= \big\{ \{T_3\}, \{T_4\}, \{T_3, T_4\},\\ &\quad\ \{T_1\}, \{T_1, T_3\}, \{T_1, T_4\}, \{T_1, T_3, T_4\},\\ &\quad\ \{T_2\}, \{T_2, T_3\}, \{T_2, T_4\}, \{T_2, T_3, T_4\} \big\}.\end{aligned}$$

In the following we will study the access structures $\Gamma_{sn}(N)$, $\Gamma_{wn}(N)$, $\Gamma_{sv}(V)$ and $\Gamma_{wv}(V)$ with regard to elementary realizations and suitable error-correcting codes.

7.2.1 Access Structures Defined by Necessary Sets

Elementary Realizations and Suitable Codes for $\mathbf{\Gamma_{sn}(N)}$

Let $N \subsetneq \mathcal{T}$ be a subset of participants, $N \neq \varnothing$, and let

$$\Gamma = \Gamma_{sn}(N) = \{A \subseteq \mathcal{T} : N \subseteq A\}.$$

Then a subset is authorized iff it contains all members of N. We can assume without loss of generality that $N = \{T_1, \ldots, T_v\}$, $1 \leq v \leq t$. That means a vector $y = (y_1, \ldots, y_t)^\tau \in \mathbb{Z}_2^t$ is the characteristic vector of an unauthorized set iff there is at least one j, $1 \leq j \leq v$, with $y_j = 0$. Hence Γ is related to the Boolean polynomial $p(x_1, \ldots, x_t) = 1 + x_1 \cdot \ldots \cdot x_v$ (see Lemma 7.3). According to Proposition 7.11, the only restrictions on the parameters are the following.

Parameters for $\Gamma_{sn}(N)$

- $k < b_1$
- $b_1 \geq g \geq \max\left\{b_1 - k, k + \frac{b_1 - k}{2^{t-v}+1}\right\}$
- $2^{t-1} | (b_1 - k)$, $2^{t-1} | (g - k)$

In particular, the parameters $b_1 = g$ divisible by 2^{v-1} and $k = 0$ are possible. Furthermore the code $\mathcal{C} = \mathbb{Z}_2^n$ is suitable for $(s, \Gamma, b_1, b_1, 0)$ for all words $s \in \mathbb{Z}_2^n$ with weight b_1 for all $n \in \mathbb{N}$, $n \geq b_1 \left(2 - \frac{1}{2^{v-1}}\right)$ (see Remark 7.13 (b)) .

Elementary Realizations and Suitable Codes for $\mathbf{\Gamma_{wn}(N)}$

Let $N \subsetneq \mathcal{T}$, $N \neq \varnothing$, and define

$$\Gamma = \Gamma_{wn}(N) = \{A \subseteq \mathcal{T} : N \cap A \neq \varnothing\}.$$

Here a set is authorized iff it contains at least one member of N. For an arbitrary $h \in \mathbb{N}$ with $h \geq v - 1$ the following calculations show that (b_1, g, k) realizes Γ elementarily if the following restrictions hold:

Parameters for $\Gamma_{wn}(N)$

- $b_1 = g$
- $k = \frac{g}{2} - 2^h$
- $g \geq 2^{v+h+1} - 2^{h+1}$
- $2^v | g$

Again let w.l.o.g. $N = \{T_1, \dots, T_v\}$ with $v < t$. Then the dual access structure is $\overline{\Gamma} = \Gamma_{sv}(N) = \{B : B \subseteq \{T_{v+1}, \dots, T_t\}\} \setminus \{\varnothing\}$ (see Remark 7.23) and

$$\varepsilon^1_{\overline{\Gamma}} = \underbrace{\begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \\ & * & \end{pmatrix}}_{u=2^{t-v}-1} \begin{matrix} \left.\vphantom{\begin{matrix}0\\ \vdots\\ 0\end{matrix}}\right\} v \\ \}\, t-v \end{matrix} .$$

The submatrix $(*)$ consists of all columns in $\mathbb{Z}_2^{t-v}$ except for the zero vector. The related weight vector is given by

$$w_{\overline{\Gamma}} = (\underset{\overset{\uparrow}{0}}{2^v - 1}, 0, \dots, 0, \underset{\overset{\uparrow}{2^{t-v-1}}}{2^t - 2^v}, 0, \dots, 0)$$

(see Remark 5.15).

Hence we have the following types of equations

$$\begin{aligned} a_{2i} - a_{2i-1} &= \frac{1}{2^{t-1}} (b_1 - k + (u - 2 \cdot 0)(g - k)) \\ &= \frac{1}{2^{t-1}} \big(b_1 - k + (2^{t-v} - 1)(g - k)\big) \quad 2^v - 1 \text{ times,} \\ a_{2i} - a_{2i-1} &= \frac{1}{2^{t-1}} \big(b_1 - k + (u - 2 \cdot 2^{t-v-1})(g - k)\big) \\ &= \frac{1}{2^{t-1}} (b_1 - k - (g - k)) \qquad\qquad 2^t - 2^v \text{ times.} \end{aligned}$$

For an arbitrary $h \in \mathbb{N}$, $h \geq v - 1$, let $b_1 = g \geq 2^{v+h+1} - 2^{h+1}$ be divisible by 2^v and $k = \frac{g}{2} - 2^h$. We define

$$\begin{array}{lll} a_{2i} = \frac{1}{2^{v-1}}(g - k) = \frac{g}{2^v} + 2^{h-v+1}, & a_{2i-1} = 0 & 2^v - 1 \text{ times and} \\ a_{2i} = a_{2i-1} = 0 & & 2^t - 2^v \text{ times.} \end{array}$$

Note that $a_2, a_3, \dots, a_{2^{t+1}} \in \mathbb{N}_0$ since $2^{v-1} | g - k = \frac{g}{2} - 2^h$. Let $a_2 = \frac{g}{2^v} - 2^{h+1} + 2^{h-v+1}$. Then $a_2 \geq 0$ since $g \geq 2^{h+v+1} - 2^{h+1}$ and we have

$$\begin{aligned}\sum_{i=1}^{2^t} a_{2i} &= a_2 + (2^v - 1) \cdot \frac{1}{2^{v-1}} \cdot (g-k) \\ &= \frac{g}{2^v} - 2^{h+1} + 2^{h-v+1} + \underbrace{\left(2 - \frac{1}{2^{v-1}}\right) \cdot \left(\frac{g}{2} + 2^h\right)}_{g - \frac{g}{2^v} + 2^{h+1} - 2^{h-v+1}} = g = b_1.\end{aligned}$$

Hence $(a_2, \ldots, a_{2^{t+1}})$ is an elementary solution for (Γ, b_1, b_1, k). Additionally, the first order Reed-Muller code $RM(1, v+h+2)$ is suitable for $(s, \Gamma, 2^{v+h+1}, 2^{v+h+1}, 2^{v+h} - 2^h)$ for all secrets $s \in RM(1, v+h+2) \setminus \{(0, \ldots, 0), (1, \ldots, 1)\}$ (see Lemma 5.26 (b)).

7.2.2 Access Structures Defined by Veto Sets

Elementary Realizations and Suitable Codes for $\mathbf{\Gamma_{wv}(V)}$

Let V be a subset of $\mathcal{T}$ with $0 < v < 2^t$ elements. Consider the access structure

$$\Gamma = \Gamma_{wv}(V) = \{A \subseteq \mathcal{T} : A \neq \varnothing, V \nsubseteq A\}.$$

Here a subset is unauthorized iff it contains all participants of V. That means the participants of the veto set V have a collective veto right.

As pointed out in Remark 7.23, this access structure is dual to the access structure $\Gamma_{sn}(V)$, where V acts as a strongly necessary set. We assume without loss of generality that $V = \{T_1, \ldots, T_v\}$. We have seen above that $\Gamma_{sn}(V)$ is related to the Boolean polynomial $1 + x_1 \cdot \ldots \cdot x_v$. Hence the dual access structure $\Gamma_{wv}(V)$ must be related to the Boolean monomial $x_1 \cdot \ldots \cdot x_v$ of degree v. Proposition 7.11 (a) yields the following parameters:

Parameters for $\Gamma_{wv}(V)$

- $b_1 \geq 2^{2t-1} - 2^t$
- $k = \frac{b_1}{2} - 2^{t-1}$
- $b_1\left(\frac{1}{2} + \frac{1}{2^{t-v+1}}\right) - 2^{t-1}(2^{t-v} - 1) \leq g \leq b_1\left(\frac{1}{2} + \frac{1}{2^{t-v+1}}\right)$
- $2^{t-1} | g - k$, $2^t | b_1$

We also know from Proposition 7.11 (a) that the minimum length of a suitable code is $b_1 + g - k - \frac{b_1 - k}{2^{t-v}}$.

Elementary Realizations and Suitable Codes for $\mathbf{\Gamma_{sv}(V)}$

Again let $V \subseteq \mathcal{T}$ be a subset with $0 < v < 2^t$ elements. Define

$$\Gamma = \Gamma_{sv}(V) = \{A \subseteq \mathcal{T} : A \neq \varnothing, A \cap V = \varnothing\}.$$

Here all subsets are authorized iff they do not contain any participant of V. That means each member of the veto set V has the power to impede the reconstruction of the secret.

According to Remark 7.23, this access structure is dual to the access structure $\Gamma_{wn}(V)$. Using Proposition 6.2 we can find an elementary realization (b_1, g, k) and an elementary solution $(\overline{a}_2, \dots, \overline{a}_{2^{t+1}})$ for $(\Gamma_{sv}(V), b_1, g, k)$.

We have seen above that (b_1, g, k) with $b_1 = g$ divisible by 2^v, $k = \frac{g}{2} - 2^h$ and $g \geq 2^{v+h+1} - 2^{h+1}$ for an arbitrary $h \in \mathbb{N}$, $h \geq v - 1$, realize $\Gamma_{wn}(V)$ elementarily. For applying Proposition 6.2 we need $g - k$ to be divisible by 2^{t-1}. Furthermore we require $b_1 \geq 2^{t-v+h+1} - 2^{h+1}$. This yields the following parameters.

Parameters for $\Gamma_{sv}(V)$

- $b_1 = g$
- $k = \frac{g}{2} - 2^h$
- $g \geq \max\left\{2^{v+h+1} - 2^{h+1}, 2^{t-v+h+1} - 2^{h+1}\right\}$
- $2^t | g$

Suppose that $(a_2, \dots, a_{2^{t+1}})$ is an elementary solution for $(\Gamma_{wn}(V), b_1, b_1, k)$. The linear system 4.2 for $\Gamma_{wn}(V)$ provides two types of equations for $a_3, \dots, a_{2^{t+1}}$:

$$\begin{array}{ll} a_{2i} = \frac{1}{2^{v-1}}(g-k) = \frac{g}{2^v} + 2^{h-v+1}, \quad a_{2i-1} = 0 & 2^v - 1 \text{ times and} \\ a_{2i} = a_{2i-1} = 0 & 2^t - 2^v \text{ times.} \end{array}$$

Using the notations of Proposition 6.2 the number x of all pairs (a_{2i}, a_{2i-1}) with $a_{2i} - a_{2i-1} < \frac{1}{2^{t-1}}(2b_1 - g - k)$ is $x = 2^t - 2^v$ and $S = \sum\limits_{\substack{i=2 \\ 0 \leq a_{2i} < \frac{2b_1 - g - k}{2^{t-1}}}}^{2^t} a_{2i} = 0$. Furthermore we know from the observations about $\Gamma_{wn}(V)$ that $\sum\limits_{i=2}^{2^t} \underbrace{a_{2i-1}}_{=0} = 0$. Therefore

$$\begin{array}{rcl} x \cdot \dfrac{2b_1 - g - k}{2^{t-1}} - \underbrace{S}_{=0} & = & (2^t - 2^v) \cdot \dfrac{g-k}{2^{t-1}} \\ & = & (2^t - 2^v) \cdot \dfrac{\frac{g}{2} + 2^h}{2^{t-1}} \\ & = & g - \dfrac{g}{2^{t-v}} + 2^{h+1} - 2^{h-t+v+1} \\ & \leq & g - \dfrac{2^{t-v+h+1} - 2^{h+1}}{2^{t-v}} + 2^{h+1} - 2^{h-t+v+1} \\ & = & g \; = \; b_1 - \underbrace{\sum_{i=2}^{2^t} a_{2i-1}}_{=0}. \end{array}$$

This means that all requirements of Proposition 6.2 are met and (b_1, b_1, k) with the stronger restrictions stated above is an elementary realization for both access structures, $\Gamma_{wn}(V)$ and $\Gamma_{sv}(V)$.
According Lemma 5.26 (b), the first order Reed-Muller code $RM(1, v+h+2)$ is also suitable for $(s, \Gamma_{sv}(V), 2^{v+h+1}, 2^{v+h+1}, 2^{v+h} - 2^h)$ for all secrets $s \in RM(1, v+h+2) \setminus \{(0, \dots, 0), (1, \dots, 1)\}$.

It is also possible to define access structures by necessary sets *and* veto sets at the same time. Finally, we have a look at their realizations.

7.2.3 Access Structures Defined by Necessary Sets and Veto Sets

Definition and Remark 7.25. Let $\mathcal{T}$ be a set of participants and $N, V \subsetneq \mathcal{T}$ disjoint non-empty subsets. Then

- $$\Gamma_{sn,sv}(N, V) := \{A \subseteq \mathcal{T} : N \subseteq A,\ A \cap V = \varnothing\}$$
  is the largest access structure on $\mathcal{T}$ with N being strongly necessary and V being a strong veto set.

- $$\Gamma_{sn,wv}(N, V) := \{A \subseteq \mathcal{T} : N \subseteq A,\ V \nsubseteq A\}$$
  is the largest access structure on $\mathcal{T}$ with N being strongly necessary and V being a weak veto set.

- $$\Gamma_{wn,sv}(N, V) := \{A \subseteq \mathcal{T} : N \cap A \neq \varnothing,\ A \cap V = \varnothing\}$$
  is the largest access structure on $\mathcal{T}$ with N being weakly necessary and V being a strong veto set.

- $$\Gamma_{wn,wv}(N, V) := \{A \subseteq \mathcal{T} : N \cap A \neq \varnothing,\ V \nsubseteq A\}$$
  is the largest access structure on $\mathcal{T}$ with N being weakly necessary and V being a weak veto set.

Elementary Realizations and Suitable Codes for $\mathbf{\Gamma_{sn,sv}(N, V)}$

Let
$$\Gamma = \Gamma_{sn,sv}(N, V) = \{A \subseteq \mathcal{T} : N \subseteq A \text{ and } V \cap A = \varnothing\}.$$

That means a set of participants is authorized iff it contains all members of the necessary set N and no member of the veto set V. We will see that Γ allows the same favorable parameters as the access structure $\Gamma_{sn}(N \cup V)$. This comes from the fact that $\Gamma_{sn,sv}(N,V) = \Gamma_{sn}(N \cup V) \vartriangle V$:

- Let A be arbitrary with $(N \cup V) \subseteq A$. Then

$$A \vartriangle V = (\underbrace{A \cup V}_{=A}) \setminus \underbrace{A \cap V}_{=V} = A \setminus V \in \Gamma_{sn,sv}(N,V)$$

  since $N \subseteq A \setminus V$. This means $\Gamma_{sn,sv}(N,V) \supseteq \Gamma_{sn}(N \cup V) \vartriangle V$.

- Let A be arbitrary with $N \subseteq A$ and $A \cap V = \varnothing$. Then

$$A = A \setminus V = \underbrace{(A \cup V) \cup V}_{=A \cup V} \setminus \underbrace{(A \cup V) \cap V}_{=V} = \underbrace{(A \cup V)}_{\supseteq N \dot{\cup} V} \vartriangle V$$

  Hence $\Gamma_{sn,sv}(N,V) \subseteq \Gamma_{sn}(N \cup V) \vartriangle V$.

$\Gamma_{sn}(N \cup V)$ consists of all sets of participants, which contain all members of $N \cup V$. Without loss of generality assume that $V = \{T_1, \ldots, T_v\}$ and $N = \{T_{v+1}, \ldots, T_{v+w}\}$. We obtain the matrices

$$\varepsilon^1_{\Gamma_{sn}(N \cup V)} = \underbrace{\begin{pmatrix} 1 & \dots & 1 \\ \vdots & & \vdots \\ 1 & \dots & 1 \\ 1 & \dots & 1 \\ \vdots & & \vdots \\ 1 & \dots & 1 \\ & * & \end{pmatrix}}_{2^{t-v-w}} \begin{matrix} \left.\vphantom{\begin{matrix}1\\ \vdots\\ 1\end{matrix}}\right\} v \\ \left.\vphantom{\begin{matrix}1\\ \vdots\\ 1\end{matrix}}\right\} w \\ \} \, t-v-w \end{matrix} \quad \text{and} \quad \varepsilon^1_{\Gamma_{sn,sv}(N,V)} = \underbrace{\begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \\ 1 & \dots & 1 \\ \vdots & & \vdots \\ 1 & \dots & 1 \\ & * & \end{pmatrix}}_{2^{t-v-w}} \begin{matrix} \left.\vphantom{\begin{matrix}1\\ \vdots\\ 1\end{matrix}}\right\} v \\ \left.\vphantom{\begin{matrix}1\\ \vdots\\ 1\end{matrix}}\right\} w \\ \} \, t-v-w \end{matrix} ,$$

where the submatrix $(*)$ contains all vectors in $\mathbb{Z}_2^{t-v-w}$ as columns.

According to Remark 6.19 (b) the access structures $\Gamma_{sn}(N \cup V)$ and $\Gamma_{sn,sv}(N,V)$ have the same linearity type and we can use the same parameters for realizing both of them. These are

Parameters for $\Gamma_{sn,sv}(N,V)$

- $k < b_1$
- $b_1 \geq g \geq \max\left\{b_1 - k, k + \frac{b_1 - k}{2^{t-v}+1}\right\}$
- $2^{t-1} | (b_1 - k)$, $2^{t-1} | (g - k)$.

For $k = 0$ and $b_1 = g$ divisible by 2^{v-1} the code $\mathcal{C} = \mathbb{Z}_2^n$ is suitable for $(s, \Gamma, b_1, b_1, 0)$ for all words $s \in \mathbb{Z}_2^n$ with weight b_1 for all $n \in \mathbb{N}$, $n \geq b_1 + \frac{b_1}{2^{v-1}}$. (see Remark 7.13) (b).

Elementary Realizations and Suitable Codes for $\mathbf{\Gamma_{sn,wv}(N,V)}$

Let

$$\Gamma = \Gamma_{sn,wv}(N,V) = \{A \subseteq \mathcal{T} : N \subseteq A \text{ and } V \not\subseteq A\}\,.$$

That means a set of participants is authorized iff it contains all members of the necessary set N and not all members of the veto set V. W.l.o.g. assume that $N = \{T_1, \ldots, T_w\}$ and $V = \{T_{w+1}, \ldots, T_{w+v}\}$.
The columns of the matrix ε_Γ^1 are

$$\begin{array}{r} N \\ \\ \\ V \\ \mathcal{T}\backslash(N\cup V) \end{array} \underbrace{\left(\begin{array}{ccc} 1 & \ldots & 1 \\ \vdots & & \vdots \\ 1 & \ldots & 1 \\ \hline & & \\ & * & \\ & & \end{array}\right)}_{2^{t-w}} \begin{array}{l} \left.\vphantom{\begin{array}{c}1\\ \vdots\\ 1\end{array}}\right\} w \\ \left.\vphantom{\begin{array}{c}1\\ *\\ 1\end{array}}\right\} t-w \end{array} \quad \text{without the columns} \quad \begin{array}{r} N \\ \\ \\ V \\ \\ \\ \mathcal{T}\backslash(N\cup V) \end{array} \underbrace{\left(\begin{array}{ccc} 1 & \ldots & 1 \\ \vdots & & \vdots \\ 1 & \ldots & 1 \\ \hline 1 & \ldots & 1 \\ \vdots & & \vdots \\ 1 & \ldots & 1 \\ \hline & *' & \end{array}\right)}_{2^{t-w-v}} \begin{array}{l} \left.\vphantom{\begin{array}{c}1\\ \vdots\\ 1\end{array}}\right\} w \\ \left.\vphantom{\begin{array}{c}1\\ \vdots\\ 1\end{array}}\right\} v \\ \}\, t-w-v \end{array}$$

where the columns of the submatrices $(*)$ and $(*')$ are all possible vectors in $\mathbb{Z}_2^{t-w}$ and $\mathbb{Z}_2^{t-v-w}$, respectively. The number of the unauthorized sets is $u = 2^t - 2^{t-w} + 2^{t-w-v} - 1$. In order to find the weight distribution $w_{\overline{\Gamma}}$ of the rows of $\varepsilon_{\overline{\Gamma}}$ we determine the weights of all non-trivial linear combinations of the rows of ε_Γ^1. In this context, linear combinations are regarded as different, when their coefficients are different, even when the resulting vectors are equal. We use Remark 5.15 and have to consider the following cases:

linear combinations of rows belonging to ...	number	weight	
N	$2^{w\ \ 1} - 1$ $2^{w\ \ 1}$	0 $2^{t\ \ w} - 2^{t\ \ w\ \ v}$	# rows even # rows odd
V	$2^{v\ \ 1} - 1$ $2^{v\ \ 1}$	$2^{t\ \ w\ \ 1}$ $2^{t\ \ w\ \ 1} - 2^{t\ \ w\ \ v}$	# rows even # rows odd
$\mathcal{T} \setminus (N \cup V)$	$2^{t\ \ w\ \ v} - 1$	$2^{t\ \ w\ \ 1} - 2^{t\ \ w\ \ v\ \ 1}$	
N, V	$(2^{w\ \ 1} - 1)(2^{v\ \ 1} - 1)$ $(2^{w\ \ 1} - 1) \cdot 2^{v\ \ 1}$ $2^{w\ \ 1} \cdot (2^{v\ \ 1} - 1)$ $2^{w\ \ 1} \cdot 2^{v\ \ 1}$	$2^{t\ \ w\ \ 1}$ $2^{t\ \ w\ \ 1} - 2^{t\ \ w\ \ v}$ $2^{t\ \ w\ \ 1} - 2^{t\ \ w\ \ v}$ $2^{t\ \ w\ \ 1}$	# rows of N even, # rows of V even # rows of N even, # rows of V odd # rows of N odd, # rows of V even # rows of N odd, # rows of V odd
$N, \mathcal{T} \setminus (N \cup V)$	$(2^w - 1)(2^{t\ \ w\ \ v} - 1)$	$2^{t\ \ w\ \ 1} - 2^{t\ \ w\ \ v\ \ 1}$	
$V, \mathcal{T} \setminus (N \cup V)$	$(2^v - 1)(2^{t\ \ w\ \ v} - 1)$	$2^{t\ \ w\ \ 1} - 2^{t\ \ w\ \ v\ \ 1}$	
$N, V, \mathcal{T} \setminus (N \cup V)$	$(2^w - 1)(2^v - 1)(2^{t\ \ w\ \ v} - 1)$	$2^{t\ \ w\ \ 1} - 2^{t\ \ w\ \ v\ \ 1}$	

(# means the number of the rows.)

Overall the row weight of ε_Γ are

$$\begin{array}{rl}
0 & 2^{w-1}-1 \text{ times,}\\
2^{t-w}-2^{t-w-v} & 2^{w-1} \text{ times,}\\
2^{t-w-1} & 2^{w+v-1}-2^{w-1} \text{ times,}\\
2^{t-w-1}-2^{t-w-v} & 2^{w+v-1}-2^{w-1} \text{ times,}\\
2^{t-w-1}-2^{t-w-v-1} & 2^{t}-2^{w+v} \text{ times.}
\end{array}$$

This yields the following row weights d_i of $\varepsilon_{\overline{\Gamma}}$:

$$\begin{array}{rl}
2^{t-1} & 2^{w-1}-1 \text{ times,}\\
2^{t-1}-2^{t-w}+2^{t-w-v} & 2^{w-1} \text{ times,}\\
2^{t-1}-2^{t-w-1} & 2^{w+v-1}-2^{w-1} \text{ times,}\\
2^{t-1}-2^{t-w-1}+2^{t-w-v} & 2^{w+v-1}-2^{w-1} \text{ times,}\\
2^{t-1}-2^{t-w-1}+2^{t-w-v-1} & 2^{t}-2^{w+v} \text{ times.}
\end{array}$$

If there is an elementary solution $(a_2, a_3, \dots, a_{2^{t+1}})$ for (Γ, b_1, g, k), the following equations provided by the linear system 4.2 have to be fulfilled:

$$\begin{aligned}
&a_{2i}-a_{2i-1}\\
&=\tfrac{1}{2^{t-1}}(b_1-k+(\underbrace{2^t-2^{t-w}+2^{t-w-v}-1}_{u}-2\cdot\underbrace{2^{t-1}}_{d_i})(g-k))\\
&=\tfrac{1}{2^{t-1}}(b_1-k+(-2^{t-w}+2^{t-w-v}-1)(g-k)) && 2^{w-1}-1 \text{ times,}
\end{aligned}$$

$$\begin{aligned}
&a_{2i}-a_{2i-1}\\
&=\tfrac{1}{2^{t-1}}(b_1-k+(u-2\cdot(2^{t-1}-2^{t-w}+2^{t-w-v}))(g-k))\\
&=\tfrac{1}{2^{t-1}}(b_1-k+(2^{t-w}-2^{t-w-v}-1)(g-k)) && 2^{w-1} \text{ times,}
\end{aligned}$$

$$\begin{aligned}
&a_{2i}-a_{2i-1}\\
&=\tfrac{1}{2^{t-1}}(b_1-k+(u-2\cdot(2^{t-1}-2^{t-w-1}))(g-k))\\
&=\tfrac{1}{2^{t-1}}(b_1-k+(2^{t-w-v}-1)(g-k)) && 2^{w+v-1}-2^{w-1} \text{ times,}
\end{aligned}$$

$$\begin{aligned}
&a_{2i}-a_{2i-1}\\
&=\tfrac{1}{2^{t-1}}(b_1-k+(u-2\cdot(2^{t-1}-2^{t-w-1}+2^{t-w-v}))(g-k))\\
&=\tfrac{1}{2^{t-1}}(b_1-k-(2^{t-w-v}+1)(g-k)) && 2^{w+v-1}-2^{w-1} \text{ times,}
\end{aligned}$$

$$\begin{aligned}
&a_{2i}-a_{2i-1}\\
&=\tfrac{1}{2^{t-1}}(b_1-k+(u-2\cdot(2^{t-1}-2^{t-w-1}+2^{t-w-v-1}))(g-k))\\
&=\tfrac{1}{2^{t-1}}(b_1-k-(g-k)) && 2^{t}-2^{w+v} \text{ times.}
\end{aligned}$$

For $b_1 = g$ that means

$$\begin{aligned}\sum_{i=2}^{2^t} a_{2i} &= \frac{1}{2^{t-1}}\left(2^{w-1}\cdot(2^{t-w}-2^{t-w-v}) + (2^{w+v-1}-2^{w-1})\cdot 2^{t-w-v}\right)(g-k)\\ &= \frac{1}{2^{t-1}}(2^t - 2^{t-v})(g-k).\end{aligned}$$

Let $\frac{g}{2} > k \geq \left(\frac{1}{2} - \frac{1}{2^{v+1}-2}\right) g$. Then

$$\sum_{i=2}^{2^t} a_{2i} \;\leq\; \frac{1}{2^{t-1}}(2^t - 2^{t-v})\left(\frac{1}{2} + \frac{1}{2^{v+1}-2}\right) g \;=\; g \;=\; b_1.$$

Hence there is an elementary solution for $(\Gamma_{sn,wv}(N,V), b_1, g, k)$ for the following parameters.

Parameters for $\Gamma_{sn,wv}(N,V)$

- $b_1 = g$
- $\frac{g}{2} > k \geq \left(\frac{1}{2} - \frac{1}{2^{v+1}-2}\right) g$
- $2^{w+v-1} | g - k$

For example $(2^e, 2^e, 2^{e-1} - 2^{t-1})$ realize $\Gamma_{sn,wv}(N,V)$ elementarily for all $e \in \mathbb{N}$, $e \geq t + v$. According to Lemma 5.26 (b), the first order Reed-Muller code $RM(1, e+1)$ is suitable for $(s, \Gamma_{sn,wv}(N,V), 2^e, 2^e, 2^e - 2^{t-1})$ for all codewords $s \in RM(1, e+1) \setminus \{(0,\ldots,0),(1,\ldots,1)\}$.

Elementary Realizations and Suitable Codes for $\Gamma_{\mathbf{wn,sv}}(\mathbf{N},\mathbf{V})$

We consider the access structure

$$\Gamma = \Gamma_{wn,sv}(N,V) = \{A \subseteq \mathcal{T} : N \cap A \neq \varnothing \text{ and } V \cap A = \varnothing\}.$$

Here a set of participants is authorized iff it contains at least one member of the necessary set N and no member of the veto set V. This access structure allows the same parameters as the access structure $\Gamma_{sn,wv}(V,N)$ since $\Gamma_{wn,sv}(N,V)$ is the symmetric difference $\Gamma_{sn,wv}(V,N) \vartriangle (N \cup V)$:

- Let $A \in \Gamma_{sn,wv}(V,N)$ be arbitrary. Then $V \subseteq A$, $N \not\subseteq A$ and

$$\begin{aligned}A \vartriangle (N \cup V) &= (\underbrace{A \cup V}_{=A} \cup N) \setminus (A \cap (N \cup V))\\ &= A \cup N \setminus (A \cap N \cup \underbrace{A \cap V}_{=V})\\ &= (A \vartriangle N) \setminus V \in \Gamma_{wn,sv}(N,V),\end{aligned}$$

since $((A \vartriangle N) \setminus V) \cap V = \varnothing$ and $((A \vartriangle N) \setminus V) \cap N \neq \varnothing$.
This means $\Gamma_{wn,sv}(N,V) \supseteq \Gamma_{sn,wv}(V,N) \vartriangle (N \cup V)$.

- Let $A \in \Gamma_{wn,sv}(N,V)$ be arbitrary. Then $A \cap N \neq \varnothing$, $A \cap V = \varnothing$ and

$$\begin{aligned} A &= (A \cup V) \setminus V \\ &= \underbrace{(((A \setminus N) \cup V) \cup (N \cup V))}_{=A \cup V} \setminus \underbrace{(((A \setminus N) \cup V) \cap (N \cup V))}_{=V} \\ &= ((A \setminus N) \cup V) \vartriangle (N \cup V) \in \Gamma_{sn,wv}(V,N) \vartriangle (N \cup V), \end{aligned}$$

since $V \subseteq ((A \setminus N) \cup V)$ and $N \not\subseteq ((A \setminus N) \cup V)$. Hence $\Gamma_{wn,sv}(N,V) \subseteq \Gamma_{sn,wv}(V,N) \vartriangle (N \cup V)$.

W.l.o.g. let $V = \{T_1, \ldots, T_v\}$ and $N = \{T_{v+1}, \ldots, T_{v+w}\}$. The columns of the matrix $\varepsilon_{\Gamma_{sn,wv}(V,N)}$ are

$$\begin{array}{c} V \\ \\ N \\ \mathcal{T}\setminus(N\cup V) \end{array} \underbrace{\left(\begin{array}{ccc} 1 & \ldots & 1 \\ \vdots & & \vdots \\ 1 & \ldots & 1 \\ \hline & & \\ & * & \\ & & \end{array}\right)}_{2^{t-v}} \begin{array}{l} \left.\vphantom{\begin{array}{c}1\\ \vdots\\ 1\end{array}}\right\} v \\ \left.\vphantom{\begin{array}{c}1\\ *\\ 1\end{array}}\right\} t-v \end{array} \quad \text{without the columns} \quad \begin{array}{c} V \\ \\ N \\ \mathcal{T}\setminus(N\cup V) \end{array} \underbrace{\left(\begin{array}{ccc} 1 & \ldots & 1 \\ \vdots & & \vdots \\ 1 & \ldots & 1 \\ \hline 1 & \ldots & 1 \\ \vdots & & \vdots \\ 1 & \ldots & 1 \\ \hline & *' & \end{array}\right)}_{2^{t-w-v}} \begin{array}{l} \left.\vphantom{\begin{array}{c}1\\ \vdots\\ 1\end{array}}\right\} v \\ \left.\vphantom{\begin{array}{c}1\\ \vdots\\ 1\end{array}}\right\} w \\ \}\, t-w-v \end{array}$$

where the columns of the submatrices $(*)$ and $(*')$ are all possible vectors in $\mathbb{Z}_2^{t-v}$ and $\mathbb{Z}_2^{t-v-w}$, respectively. That means a linear combination of the columns can only be the zero vector, if the number of the summands is even. By Remark 6.19 (b) the access structures $\Gamma_{wn,sv}(N,V)$ and $\Gamma_{sn,wv}(V,N)$ have the same linearity type and we can use the same parameters for realizing $\Gamma_{wn,sv}(N,V)$ and $\Gamma_{sn,wv}(V,N)$. These are

Parameters for $\Gamma_{wn,sv}(N,V)$

- $b_1 = g$
- $\frac{g}{2} > k \geq \left(\frac{1}{2} - \frac{1}{2^{w+1}-2}\right) g$
- $2^{w+v-1} | g-k$.

Also here $(2^e, 2^e, 2^{e-1} - 2^{t-1})$ realize $\Gamma_{wn,sv}(N,V)$ elementarily for all $e \in \mathbb{N}$, $e \geq t+w$. According to Lemma 5.26 (b), the first order Reed-Muller code $RM(1, e+1)$ is suitable for $(s, \Gamma_{wn,sv}(N,V), 2^e, 2^e, 2^e - 2^{t-1})$ for all codewords $s \in RM(1, e+1) \setminus \{(0, \ldots, 0), (1, \ldots, 1)\}$.

Elementary Realizations and Suitable Codes for $\mathbf{\Gamma_{wn,wv}(N,V)}$

Let

$$\Gamma = \Gamma_{wn,wv}(N,V) = \{A \subseteq \mathcal{T} : N \cap A \neq \varnothing \text{ and } V \not\subseteq A\}\,.$$

In this access structure a set of participants is authorized iff it contains at least one member of the necessary set N and not all members of the veto set V. The columns of the matrix $\varepsilon^1_{\overline{\Gamma}}$ are

$$\begin{array}{r} N \\ \\ \\ V \\ \\ \mathcal{T}\backslash(N\cup V) \end{array} \left(\begin{array}{ccc|ccc} 0 & \dots & 0 & & & \\ \vdots & & \vdots & & * & \\ 0 & \dots & 0 & & & \\ \hline & & & 1 & \dots & 1 \\ & & & \vdots & & \vdots \\ & *' & & 1 & \dots & 1 \\ \cline{4-6} & & & & *'' & \\ \multicolumn{3}{c}{\underbrace{\qquad\qquad}_{2^{t-w}-1}} & \multicolumn{3}{c}{\underbrace{\qquad\qquad}_{2^{t-v}}} \end{array}\right) \begin{array}{l} \left.\right\}w \\ \\ \left.\right\}v \\ \left.\right\}t-w-v \end{array} \quad \text{without} \quad \left(\begin{array}{ccc} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \\ \hline 1 & \dots & 1 \\ \vdots & & \vdots \\ 1 & \dots & 1 \\ \hline & *''' & \\ \multicolumn{3}{c}{\underbrace{\qquad\qquad}_{2^{t-w-v}}} \end{array}\right) \begin{array}{l} \left.\right\}w \\ \\ \left.\right\}v \\ \left.\right\}t-w-v \end{array} .$$

The columns of the second matrix occur in both parts of the first matrix. Hence one set of these columns has to be omitted such that they do not occur twice. The columns of the submatrices $\begin{pmatrix} * \\ *'' \end{pmatrix}$ and $(*''')$ are all possible vectors in $\mathbb{Z}_2^{t-v}$ and $\mathbb{Z}_2^{t-w-v}$, respectively. The columns of the submatrix $(*')$ are all vectors in $\mathbb{Z}_2^{t-w}$ except for the zero vector. We have to omit the zero vector because $\varepsilon_{\overline{\Gamma}}$ does not contain the zero column. We have $u = 2^{t-w} + 2^{t-v} - 2^{t-w-v} - 1$ unauthorized sets. Now we determine the weight distribution $w_{\overline{\Gamma}}$ of the rows of $\varepsilon_{\overline{\Gamma}}$. Again we use Remark 5.15.

linear combinations of rows belonging to ...	number	weight
N	$2^w - 1$	2^{t-v-1}
V	$2^{v-1} - 1$ 2^{v-1}	2^{t-w-1} $2^{t-w-1} + 2^{t-v} - 2^{t-w-v}$
$\mathcal{T} \setminus (N \cup V)$	$2^{t-w-v} - 1$	$2^{t-w-1} + 2^{t-v-1} - 2^{t-w-v-1}$
N, V	$(2^w - 1)(2^{v-1} - 1)$ $(2^w - 1) \cdot 2^{v-1}$	$2^{t-w-1} + 2^{t-v-1}$ $2^{t-w-1} + 2^{t-v-1} - 2^{t-w-v}$
N, $\mathcal{T} \setminus (N \cup V)$	$(2^w - 1)(2^{t-w-v} - 1)$	$2^{t-w-1} + 2^{t-v-1} - 2^{t-w-v-1}$
V, $\mathcal{T} \setminus (N \cup V)$	$(2^v - 1)(2^{t-w-v} - 1)$	$2^{t-w-1} + 2^{t-v-1} - 2^{t-w-v-1}$
N, V, $\mathcal{T} \setminus (N \cup V)$	$(2^w - 1)(2^v - 1)(2^{t-w-v} - 1)$	$2^{t-w-1} + 2^{t-v-1} - 2^{t-w-v-1}$

(As in the study of $\Gamma_{sn,sv}(N,V)$ there are cases where we have to distinguish between even and odd numbers of summands.)

This yields the following row weight of $\varepsilon_{\overline{\Gamma}}$:

$$\begin{array}{rl}
2^{t-v-1} & 2^w - 1 \text{ times,} \\
2^{t-w-1} & 2^{v-1} - 1 \text{ times,} \\
2^{t-w-1} + 2^{t-v} - 2^{t-w-v} & 2^{v-1} \text{ times,} \\
2^{t-w-1} + 2^{t-v-1} & 2^{w+v-1} - 2^w - 2^{v-1} + 1 \text{ times,} \\
2^{t-w-1} + 2^{t-v-1} - 2^{t-w-v} & 2^{w+v-1} - 2^{v-1} \text{ times,} \\
2^{t-w-1} + 2^{t-v-1} - 2^{t-w-v-1} & 2^t - 2^{w+v} \text{ times.}
\end{array}$$

If there is an elementary solution $(a_2, a_3, \ldots, a_{2^{t+1}})$ for (Γ, b_1, g, k), it has to fulfill the following equations:

$$\begin{aligned}
& a_{2i} - a_{2i-1} \\
&= \tfrac{1}{2^{t-1}}(b_1 - k + (\underbrace{2^{t-w} + 2^{t-v} - 2^{t-w-v} - 1}_{u} - 2 \cdot \underbrace{2^{t-v-1}}_{d_i})(g-k)) \\
&= \tfrac{1}{2^{t-1}}(b_1 - k + (2^{t-w} - 2^{t-w-v} - 1)(g-k)) && 2^w - 1 \text{ times,}
\end{aligned}$$

$$\begin{aligned}
& a_{2i} - a_{2i-1} \\
&= \tfrac{1}{2^{t-1}}(b_1 - k + (u - 2 \cdot 2^{t-w-1})(g-k)) \\
&= \tfrac{1}{2^{t-1}}(b_1 - k + (2^{t-v} - 2^{t-w-v} - 1)(g-k)) && 2^{v-1} - 1 \text{ times,}
\end{aligned}$$

$$\begin{aligned}
& a_{2i} - a_{2i-1} \\
&= \tfrac{1}{2^{t-1}}(b_1 - k + (u - 2 \cdot (2^{t-w-1} + 2^{t-v} - 2^{t-w-v}))(g-k)) \\
&= \tfrac{1}{2^{t-1}}(b_1 - k - (2^{t-v} - 2^{t-w-v} + 1)(g-k)) && 2^{v-1} \text{ times,}
\end{aligned}$$

$$\begin{aligned}
& a_{2i} - a_{2i-1} \\
&= \tfrac{1}{2^{t-1}}(b_1 - k + (u - 2 \cdot (2^{t-w-1} + 2^{t-v-1}))(g-k)) \\
&= \tfrac{1}{2^{t-1}}(b_1 - k - (2^{t-w-v} + 1)(g-k)) && 2^{w+v-1} - 2^w - 2^{v-1} + 1 \text{ times,}
\end{aligned}$$

$$\begin{aligned}
& a_{2i} - a_{2i-1} \\
&= \tfrac{1}{2^{t-1}}(b_1 - k + (u - 2 \cdot (2^{t-w-1} + 2^{t-v-1} - 2^{t-w-v}))(g-k)) \\
&= \tfrac{1}{2^{t-1}}(b_1 - k + (2^{t-w-v} - 1)(g-k)) && 2^{w+v-1} - 2^{v-1} \text{ times,}
\end{aligned}$$

$$\begin{aligned}
& a_{2i} - a_{2i-1} \\
&= \tfrac{1}{2^{t-1}}(b_1 - k + (u - 2 \cdot (2^{t-w-1} + 2^{t-v-1} - 2^{t-w-v-1}))(g-k)) \\
&= \tfrac{1}{2^{t-1}}(b_1 - k - (g-k)) && 2^t - 2^{w+v} \text{ times.}
\end{aligned}$$

Unfortunately, an elementary realization with $b_1 = g$ is only possible for $w = 1$ or $v = 1$. In this case we have

$$\begin{aligned}
\sum_{i=2}^{2^t} a_{2i} &= \frac{1}{2^{t-1}}\big((2^w-1)(2^{t-w}-2^{t-w-v})+(2^{v-1}-1)(2^{t-v}-2^{t-w-v}) \\
&\quad +(2^{w+v-1}-2^{v-1})\cdot 2^{t-w-v}\big)(g-k) \\
&= \frac{1}{2^{t-1}}(2^{t+1}-2^{t-w+1}-2^{t-v+1}+2^{t-w-v+1})(g-k) \\
&= 4\cdot\left(1-\frac{1}{2^w}\right)\left(1-\frac{1}{2^v}\right)(g-k) \\
&= \left(2-\frac{1}{2^{\max\{w,v\}-1}}\right)(g-k) \quad \text{as } w=1 \text{ or } v=1.
\end{aligned}$$

Let $\frac{g}{2} > k \geq \frac{g}{2} - \frac{g}{2^{\max\{w,v\}+1}-2}$. Then

$$\sum_{i=2}^{2^t} a_{2i} \leq \left(2-\frac{1}{2^{\max\{w,v\}-1}}\right)\left(\frac{g}{2}+\frac{g}{2^{\max\{w,v\}+1}-2}\right) = g = b_1.$$

That means there is actually an elementary solution $(a_2, a_3, \ldots, a_{2^{t+1}})$ for (Γ, b_1, b_1, k) with $w = 1$ or $v = 1$, if

Parameters for $\Gamma_{wn,wv}(N, V)$ for $w = 1$ or $v = 1$

- $b_1 = g$
- $\frac{g}{2} > k \geq \left(\frac{1}{2} - \frac{1}{2^{\max\{w,v\}+1}-2}\right) g$
- $2^{w+v-1} | g - k$

In this case Lemma 5.26 (b) says that for all $e \geq t + \max\{w, v\}$ the code $RM(1, e+1)$ is suitable for $(\Gamma_{wn,wv}(N, V), 2^e, 2^e, 2^{e-1} - 2^{t-1})$ for all codewords $s \in RM(1, e+1) \setminus \{(0, \ldots, 0), (1, \ldots, 1)\}$.

For larger necessary sets or veto sets there is no elementary realization with $b_1 = g$, since $v, w \geq 2$ yields

$$\begin{aligned}
\sum_{i=2}^{2^t} a_{2i} &= 4\cdot\left(1-\frac{1}{2^w}\right)\left(1-\frac{1}{2^v}\right)(g-k) \\
&\geq 4\cdot\left(\frac{3}{4}\right)^2 (g-k) > \frac{9}{8}\, g > g = b_1.
\end{aligned}$$

We show that in this case the following parameters are suitable:

Parameters for $\Gamma_{wn,wv}(N,V)$ for $w,v \geq 2$

- $b_1 \geq 2^{2t}$
- $g = b_1\left(\frac{1}{2} + \frac{1}{2^{t+2-v}}\right)$
- $k = \frac{b_1}{2} - 2^{t-1}$
- $2^{2t+1-v} | b_1$

For those parameters all right hand sides of the equations 2 up to 2^t of 4.2 are positive since for all $i = 2, \ldots, 2^t$

$$\begin{aligned} a_{2i} - a_{2i-1} &\geq \frac{1}{2^{t-1}}\Big(\underbrace{b_1 - k}_{\frac{b_1}{2}+2^{t-1}} -(2^{t-v} - 2^{t-w-v} + 1)\underbrace{(g-k)}_{\frac{b_1}{2^{t+2-v}}+2^{t-1}}\Big) \\ &= \frac{1}{2^{t-1}}\underbrace{b_1}_{\geq 2^{2t}}\Big(\frac{1}{4} + \underbrace{\frac{1}{2^{w+2}} - \frac{1}{2^{t-v+2}}}_{>0}\Big) - 2^{t-v} + 2^{t-w-v} \\ &\geq \underbrace{2^{t-1} - 2^{t-v}}_{\geq 0} + 2^{t-w-v} \;\geq\; 0. \end{aligned}$$

Hence we can apply Lemma 4.12(d) and obtain

$$\begin{aligned} \sum_{i=2}^{2^t} a_{2i} &= \frac{1}{2^{t-1}}\big((2^t-1)(b_1-k) - u(g-k)\big) \\ &= \frac{1}{2^{t-1}}\left((2^t-1)\left(\frac{b_1}{2} + 2^{t-1}\right) - (2^{t-w} + 2^{t-v} - 2^{t-w-v} - 1)\left(\frac{b_1}{2^{t+2-v}} + 2^{t-1}\right)\right) \\ &= \frac{b_1}{2^{t-1}}\left(2^{t-1} - \frac{3}{4} - 2^{v-w-2} + 2^{-w-2} + 2^{v-t-2}\right) + 2^t\left(1 - \frac{1}{2^w}\right)\left(1 - \frac{1}{2^v}\right) \\ &= b_1 - \left(\frac{3}{4} + 2^{v-w-2} - 2^{-w-2} - 2^{v-t-2}\right)\underbrace{\frac{b_1}{2^{t-1}}}_{\geq 2^{t+1}} + 2^t\left(1 - \frac{1}{2^w}\right)\left(1 - \frac{1}{2^v}\right) \\ &\leq b_1 - 2^t\Big(\frac{1}{2} + \underbrace{2^{v-w-1} - 2^{-w-1}}_{\geq 0}\underbrace{-2^{v-t-1} + 2^{-w}}_{\geq 0} + \underbrace{2^{-v} - 2^{-w-v}}_{\geq 0}\Big) \;\leq\; b_1. \end{aligned}$$

This show that there is an elementary solution for $(\Gamma_{wn,wv}(N,V), b_1, g, k)$ with the restrictions stated above. It has the property that all odd numbered components are zero. This is also the case in Theorem 4.22 (a) and it can be shown as in the proof of Theorem 4.22 (b), that each binary (not necessary linear) code $\mathcal{C}$ with minimum distance $d(\mathcal{C}) = b_1$, which contains the zero word, is suitable for $(s, \Gamma_{wn,wv}(N,V), b_1, g, k)$ for all codewords $s \in \mathcal{C}$ with weight b_1. For example $RM(1, e+1)$, $e \geq 2t+1$, is suitable for $(s, \Gamma_{wn,wv}(N,V), 2^e, 2^{e-1} + 2^{e-t-2+v}, 2^{e-1} - 2^{t-1})$ for all $s \in RM(1, e+1) \setminus$

$\{(0,\dots,0),(1,\dots,1)\}$ (see Corollary 4.24).

We end this chapter with a detailed example for the realization of the access structure $\Gamma_{sn,wv}(N,V)$ on an arbitrary number $t \geq 5$ of participants, where the disjoint subsets N, V both contain two elements. Compared to the universal solution provided by Theorem 4.22 this realization is far superior with regard to efficiency and security. Instead of a code length $n \geq b_1 \geq 2^{2t} - 2^t$ the code length $n = 128$ is sufficient for all $t \geq 5$. Furthermore we have the security distance $g = b_1$ instead of $g \leq b_1\left(\frac{1}{2} + \frac{1}{2^t}\right) - 2^{t-1}$.

Example 7.26. Let $\mathcal{T} = \{T_1,\dots,T_t\}$, $t \geq 5$, $N = \{T_1, T_2\}$ and $V = \{T_3, T_4\}$. Consider the access structure $\Gamma = \Gamma_{sn,wv}(N,V)$ which consists of all subsets of $\mathcal{T}$ which contain T_1 and T_2 and at most one of the participants T_3 and T_4. For $t = 5$ there are $u = 2^t - 2^{t-2} + 2^{t-2-2} - 1 = 25$ unauthorized subsets. The resulting matrix $\varepsilon_{\overline{\Gamma}}$ can be seen at the the end of the example. The weights of the rows are written in the additional column.

We choose the parameters $b_1 = g = 64$, $k = 24$ and the binary code $\mathcal{C} = RM(1,7)$. Let $s = (\underbrace{1,\dots,1}_{32}, \underbrace{0,\dots,0}_{32}, \underbrace{1,\dots,1}_{32}, \underbrace{0,\dots,0}_{32}) \sim 1 + x_6$ be the secret to be shared.
The row weights of $\varepsilon_{\overline{\Gamma}}$ yield the following system of linear equations:

$$\begin{array}{rcll}
a_{2i} - a_{2i-1} & = & \frac{1}{16}\left(b_1 - k + (u - 2\cdot 10)(g-k)\right) = 15 & \text{for } i = 2,3 \\
a_{2i} - a_{2i-1} & = & \frac{1}{16}\left(b_1 - k + (u - 2\cdot 12)(g-k)\right) = 5 & \text{for } i = 6,7,10,11,13,16 \\
a_{2i} - a_{2i-1} & = & \frac{1}{16}\left(b_1 - k + (u - 2\cdot 13)(g-k)\right) = 0 & \text{for } i = 17,18,19,\dots,32 \\
a_{2i} - a_{2i-1} & = & \frac{1}{16}\left(b_1 - k + (u - 2\cdot 14)(g-k)\right) = -5 & \text{for } i = 5,8,9,12,14,15 \\
a_{2i} - a_{2i-1} & = & \frac{1}{16}\left(b_1 - k + (u - 2\cdot 16)(g-k)\right) = -15 & \text{for } i = 4
\end{array}$$

In order to find an elementary solution we choose

$$\begin{array}{lll}
a_{2i} = 15, & a_{2i-1} = 0 & \text{for } i = 2,3 \\
a_{2i} = 5, & a_{2i-1} = 0 & \text{for } i = 6,7,10,11,13,16 \\
a_{2i} = 0, & a_{2i-1} = 0 & \text{for } i = 17,18,19,\dots,32 \\
a_{2i} = 0, & a_{2i-1} = 5 & \text{for } i = 5,8,9,12,14,15 \\
a_{2i} = 0, & a_{2i-1} = 15 & \text{for } i = 4.
\end{array}$$

Then we calculate

$$a_2 = b_1 - \sum_{i=2}^{2^t} a_{2i} = 64 - 2\cdot 15 - 6\cdot 5 = 4$$

and

$$a_1 = n - b_1 - \sum_{i=2}^{2^t} a_{2i-1} = 128 - 64 - 6\cdot 5 - 15 = 19.$$

$a_{2i} = a_{2i-1} = 0$ for all $i \geq 17$ means that $|\mathrm{supp}(k_5)| = 0$, hence k_5 is the zero word and we can exclude it from the further observations. We define the other shares by deciding which positions should be determined by the single a_j, $j = 1,2,\dots,32$:

j	s	k_1	k_2	k_3	k_4	a_j	positions
1	0	0	0	0	0	19	$33-51$
2	1	0	0	0	0	4	$1-4$
4	1	1	0	0	0	16	$67-81$
6	1	0	1	0	0	16	$10-24$
7	0	1	1	0	0	16	$104-119$
9	0	0	0	1	0	5	$57-61$
12	1	1	0	1	0	5	$87-91$
14	1	0	1	1	0	5	$30-32, 65, 66$
15	0	1	1	1	0	5	$124-128$
17	0	0	0	0	1	5	$52-56$
20	1	1	0	0	1	5	$82-86$
22	1	0	1	0	1	5	$25-29$
23	0	1	1	0	1	5	$119-123$
26	1	0	0	1	1	5	$5-9$
27	0	1	0	1	1	5	$99-103$
29	0	0	1	1	1	5	$62-64, 97, 98$
32	1	1	1	1	1	6	$92-96$

This yields the shares

$$\begin{aligned} k_1 = {} & 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000 \\ & 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000 \\ & 0011\ 1111\ 1111\ 1111\ 1111\ 1111\ 1111\ 1111 \\ & 0011\ 1111\ 1111\ 1111\ 1111\ 1111\ 1111\ 1111, \end{aligned}$$

$$\begin{aligned} k_2 = {} & 0000\ 0000\ 0111\ 1111\ 1111\ 1111\ 1111\ 1111 \\ & 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0111 \\ & 1100\ 0000\ 0000\ 0000\ 0000\ 0000\ 0001\ 1111 \\ & 1100\ 0001\ 1111\ 1111\ 1111\ 1111\ 1111\ 1111, \end{aligned}$$

$$\begin{aligned} k_3 = {} & 0000\ 1111\ 1000\ 0000\ 0000\ 0000\ 0000\ 0111 \\ & 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 1111\ 1111 \\ & 1100\ 0000\ 0000\ 0000\ 0000\ 0011\ 1111\ 1111 \\ & 1111\ 1110\ 0000\ 0000\ 0000\ 0000\ 0001\ 1111 \end{aligned}$$

and

$$\begin{aligned} k_4 = {} & 0000\ 1111\ 1000\ 0000\ 0000\ 0000\ 1111\ 1000 \\ & 0000\ 0000\ 0000\ 0000\ 0001\ 1111\ 0000\ 0111 \\ & 0000\ 0000\ 0000\ 0000\ 0111\ 1100\ 0001\ 1111 \\ & 1111\ 1110\ 0000\ 0000\ 0000\ 0011\ 1110\ 0000. \end{aligned}$$

When a subset of participants is authorized, the sum of their shares differs from the secret in 24 positions. Since $24 < \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor = \left\lfloor \frac{63}{2} \right\rfloor$, Hamming decoding yields the secret.

Otherwise, when the subset is unauthorized, the following table shows that Hamming decoding yields always the wrong codeword. Even the next non-zero codeword is not the secret. Furthermore, there are various codewords which have the same distance from the sum as the secret.

unauthorized sum S	nearest codeword(s) $c \neq 0$	# codewords c with $d(S,c) = 64$
k_1	$c \sim x_7$, $d(S,c) = 4$	192
k_2	$c \sim 1 + x_6 + x_7$, $d(S,c) = 24$	68
k_3	$c \sim 1 + x_4 + x_5$, $d(S,c) = 30$	80
$k_1 + k_3$	$c \sim 1 + x_4 + x_5 + x_7$, $d(S,c) = 34$	74
$k_2 + k_3$	$c \sim 1 + x_6 + x_7$, $d(S,c) = 24$	138
$k_1 + k_2 + k_3$	$c \sim 1 + x_6$, $d(S,c) = 24$	138
k_4	$c \sim 1 + x_5 + x_6 + x_7$, $d(S,c) = 44$	64
$k_1 + k_4$	$c \sim x_7$, $d(S,c) = 40$	64
$k_2 + k_4$	$c \sim 1 + x_6 + x_7$, $d(S,c) = 28$	60
$k_1 + k_2 + k_4$	$c \sim 1 + x_6$, $d(S,c) = 24$	70
$k_3 + k_4$	$c \sim x_5$, $d(S,c) = 28$	70
$k_1 + k_3 + k_4$	$c \sim x_5 + x_7$, $d(S,c) = 28$	70
$k_2 + k_3 + k_4$	$c \sim 1 + x_5 + x_6 + x_7$, $d(S,c) = 32$	70
$k_1 + k_2 + k_3 + k_4$	$c \sim x_4 + x_5 + x_6$, $d(S,c) = 30$	72
k_j, $j \geq 5$	all $c \in \mathcal{C} \setminus \{(0,\ldots,0)(1,\ldots,1)\}$, $d(S,c) = 64$	254

In the case $t > 5$ all participants k_j with $j \geq 6$ receive the zero word as share. The shares of $T_1, \ldots, T_5$ remain the same.

$$\varepsilon_{\overline{\Gamma}} = \begin{array}{cc} \left(\begin{array}{ccccccccccccccccccccccccc}
1&0&0&1&0&0&1&0&0&1&0&1&0&1&0&0&1&0&0&1&0&0&1&0&1\\
0&1&0&0&1&0&0&1&0&0&1&1&0&0&1&0&0&1&0&0&1&0&0&1&1\\
1&1&0&1&1&0&1&1&0&1&1&0&0&1&1&0&1&1&0&1&1&0&1&1&0\\
0&0&1&1&1&0&0&0&1&1&1&1&0&0&0&1&1&1&0&0&0&1&1&1&1\\
1&0&1&0&1&0&1&0&1&0&1&0&0&1&0&1&0&1&0&1&0&1&0&1&0\\
0&1&1&1&0&0&0&1&1&1&0&0&0&0&1&1&1&0&0&0&1&1&1&0&0\\
1&1&1&0&0&0&1&1&1&0&0&1&0&1&1&1&0&0&0&1&1&1&0&0&1\\
0&0&0&0&0&1&1&1&1&1&1&1&0&0&0&0&0&0&1&1&1&1&1&1&1\\
1&0&0&1&0&1&0&1&1&0&1&0&0&1&0&0&1&0&1&0&1&1&0&1&0\\
0&1&0&0&1&1&1&0&1&1&0&0&0&0&1&0&0&1&1&1&0&1&1&0&0\\
1&1&0&1&1&1&0&0&1&0&0&1&0&1&1&0&1&1&1&0&0&1&0&0&1\\
0&0&1&1&1&1&1&1&0&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0&0\\
1&0&1&0&1&1&0&1&0&1&0&1&0&1&0&1&0&1&1&0&1&0&1&0&1\\
0&1&1&1&0&1&1&0&0&0&1&1&0&0&1&1&1&0&1&1&0&0&0&1&1\\
1&1&1&0&0&1&0&0&0&1&1&0&0&1&1&1&0&0&1&0&0&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&0&0&1&0&0&1&0&0&1&0&1&1&0&1&1&0&1&1&0&1&1&0&1&0\\
0&1&0&0&1&0&0&1&0&0&1&1&1&1&0&1&1&0&1&1&0&1&1&0&0\\
1&1&0&1&1&0&1&1&0&1&1&0&1&0&0&1&0&0&1&0&0&1&0&0&1\\
0&0&1&1&1&0&0&0&1&1&1&1&1&1&1&0&0&0&1&1&1&0&0&0&0\\
1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\
0&1&1&1&0&0&0&1&1&1&0&0&1&1&0&0&0&1&1&1&0&0&0&1&1\\
1&1&1&0&0&0&1&1&1&0&0&1&1&0&0&0&1&1&1&0&0&0&1&1&0\\
0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0\\
1&0&0&1&0&1&0&1&1&0&1&0&1&0&1&1&0&1&0&1&0&0&1&0&1\\
0&1&0&0&1&1&1&0&1&1&0&0&1&1&0&1&1&0&0&0&1&0&0&1&1\\
1&1&0&1&1&1&0&0&1&0&0&1&1&0&0&1&0&0&0&1&1&0&1&1&0\\
0&0&1&1&1&1&1&1&0&0&0&0&1&1&1&0&0&0&0&0&0&1&1&1&1\\
1&0&1&0&1&1&0&1&0&1&0&1&1&0&1&0&1&0&0&1&0&1&0&1&0\\
0&1&1&1&0&1&1&0&0&0&1&1&1&1&0&0&0&1&0&0&1&1&1&0&0\\
1&1&1&0&0&1&0&0&0&1&1&0&1&0&0&0&1&1&0&1&1&1&0&0&1
\end{array}\right) & \begin{array}{c}
10\\ 10\\ 16\\ 14\\ 12\\ 12\\ 14\\ 14\\ 12\\ 12\\ 14\\ 12\\ 14\\ 14\\ 12\\ 13\\ 13\\ 13\\ 13\\ 13\\ 13\\ 13\\ 13\\ 13\\ 13\\ 13\\ 13\\ 13\\ 13\\ 13\\ 13
\end{array} \end{array} .$$

Chapter 8

Conclusion

In this thesis we introduced a new approach towards secret sharing using error-correcting codes. We developed a method which enables us to realize arbitrary access structures. It turned out that the price for this generality is a limitation regarding the security and the efficiency of the scheme.

The secret is a codeword in a binary error-correcting code and the shares are binary words of the same length. They have the property that Hamming decoding applied to the sum of the shares of a set of participants yields the secret iff the set is authorized.

The following restrictions were made: We studied the case that there is only one large distance g from the share sums of the unauthorized sets to the secret and only one small distance k from the share sums of the authorized sets to the secret. This enabled us to describe each set of suitable shares in terms of non-negative integer solutions of the linear system 4.2:

$$\begin{aligned}
\sum_{i=1}^{2^t} a_{2i} &= b_1 \\
a_4 - a_3 &= \frac{1}{2^{t-1}} E_2 \cdot b \\
&\vdots \\
a_{2i} - a_{2i-1} &= \frac{1}{2^{t-1}} E_i \cdot b \\
&\vdots \\
a_{2^{t+1}} - a_{2^{t+1}-1} &= \frac{1}{2^{t-1}} E_{2^t} \cdot b,
\end{aligned}$$

where we considered only elementary solutions with $a_{2i} = 0$ or a_{2i-1} for all $i = 2, \ldots, 2^t$.

Based on these considerations Theorem 4.22 provides parameters b_1, g, k depending only on the number t of the involved participants, which can be used to realize *all* access structures. b_1 is the weight of the secret to be shared.

- $b_1 \in \mathbb{N}$, $b_1 \geq 2^{2t} - 2^t$ such that $2^t \mid b_1$
- $k = \frac{b_1}{2} - 2^{t-1}$

- $g \in \mathbb{N}$, $\frac{b_1}{2} < g \leq b_1 \left(\frac{1}{2} + \frac{1}{2^t}\right) - 2^{t-1}$ such that $2^{t-1} \mid g$

Furthermore, Theorem 4.22 says that each binary (not necessarily linear) code $\mathcal{C}$ with minimum distance $d(\mathcal{C}) = b_1$ which contains the zero word is suitable for sharing all codewords in $\mathcal{C}$ with weight b_1.

Using the parameters provided by Theorem 4.22, the security distance g is rather small and large code length $n \geq b_1 \geq 2^{2t} - 2^t$ are required. The problem of the small distances g can be overcome by the use of a combiner, but the large code lengths remain problematic. So, it must be said that our realization for arbitrary access structures is unsuitable in practice.

In order to find special access structures which allow better parameters, we classified all access structures, such that all access structures lying in the same class allow the same parameters. Furthermore we studied the impact of changes in the access structure on the elementary realizations. As a result, we have been able to identify special classes which are far superior with regard to efficiency and security.

On the one hand these are access structures related to Boolean polynomials of degree one with the constant summand 1. In these access structures a set is authorized iff it contains an odd number of participants of an arbitrary fixed subset of the participant set. Here the security distance $g = b_1$ is possible and the weight b_1 of the secret can be chosen arbitrarily with $2^{t-1}|b_1$. Furthermore $\mathbb{Z}_2^n$ is a suitable code for all $n \geq b_1$ and all words with weight b_1. On the other hand, some access structures defined by necessary sets and veto sets allow larger security distances and smaller code lengths:

-
$$\Gamma_{sn}(N) = \{A : N \subseteq A\}$$
defined by a strongly necessary set N allow the parameters $b_1 = g$, $k = 0$ where b_1 has to be divisible by 2^{t-1}. $\mathcal{C} = \mathbb{Z}_2^n$ is suitable for all $n \geq b_1 \left(2 - \frac{1}{2^{|V|-1}}\right)$.

-
$$\Gamma_{wn}(N) = \{A : N \cap A \neq \varnothing\}$$
defined by a weakly necessary set N allows $g = b_1$ and $\mathcal{C} = RM(1, |N| + 2 + h)$ for all $h \geq |N| - 1$.

-
$$\Gamma_{sv}(V) = \{A \neq \varnothing : V \cap A = \varnothing\}$$
defined by a strong veto set V allows $g = b_1$ and $\mathcal{C} = RM(1, |V| + 2 + h)$ for all $h \geq |V| - 1$.

-
$$\Gamma_{sn,sv}(N, V) = \{A : N \subseteq A \text{ and } V \cap A = \varnothing\}$$
defined by a strongly necessary set N and a strong veto set V, allow $g = b_1$ with $2^{|V|-1}|b_1$, $k = 0$ and $\mathcal{C} = \mathbb{Z}_2^n$ for all $n \geq b_1 + \frac{b_1}{2^{|V|-1}}$.

- $$\Gamma_{wn,sv}(N,V) = \{A : N \cap A \neq \varnothing \text{ and } V \cap A = \varnothing\}$$

  defined by a weakly necessary set N and a strong veto set V, allow $g = b_1$ and $\mathcal{C} = RM(1, e+1)$ for all $e \geq t + |N|$.

- $$\Gamma_{sn,wv}(N,V) = \{A : N \subseteq A \text{ and } V \nsubseteq A\}$$

  defined by a strongly necessary set N and a weak veto set V, allow $g = b_1$ and $\mathcal{C} = RM(1, e+1)$ for all $e \geq t + |V|$.

- $$\Gamma_{wn,wv}(N,V) = \{A : N \cap A \neq \varnothing \text{ and } V \nsubseteq A\}$$

  defined by a weakly necessary set N and a weak veto set V, allow $g = b_1$ and $\mathcal{C} = RM(1, e+1)$ for all $e \geq t + \max\{|N|, |V|\}$.

Besides the results of this thesis, there are still many open questions and ideas for further research, which are not followed yet.

Firstly the question arise, whether there are further classes of access structures, which have efficient and secure realizations using our approach. For this purpose it might be helpful to develop more techniques for changing access structures and to study their influence on the realizations.

Another question is, what kinds of realizations can be found when different large and different small distances are allowed, or when we do not consider *elementary* solutions.

Furthermore a change in the methods for finding integer solutions for the linear system 4.1 might bring interesting results. For example, methods from linear optimization could be used .

Bibliography

[1] A. E. Ashikhmin and A. Barg, *Minimal Vectors in Linear Codes*, IEEE Transactions on Information Theory, 44 (1998), pp. 2010–2017.

[2] C. Asmuth and J. Bloom, *A modular approach to key safeguarding*, IEEE Transactions on Information Theory, 29 (1983), pp. 208–210.

[3] A. Beimel, *Secret-Sharing Schemes: A Survey*, in Coding and Cryptology, vol. 6639 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2011, pp. 11–46.

[4] M. Beiter, *Secret Sharing Schemes on General Access Structures*, PhD thesis, Universität Tübingen, 2008.

[5] E. R. Berlekamp, *Algebraic Coding Theory*, Aegean Park Press, 1984.

[6] M. Bertilsson and I. Ingemarsson, *A Construction of Practical Secret Sharing Schemes using Linear Block Codes*, in Advances in Cryptology - AUSCRYPT '92, vol. 718, 1992, pp. 67–79.

[7] G. R. Blakely, *Safeguarding Cryptographic Keys*, in Proceedings AFIPS 1979, vol. 48, National Computer Conference, 1979, pp. 313–317.

[8] C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro, *Secret sharing schemes with veto capabilities*, in Algebraic Coding, vol. 781 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 1994, pp. 82–89.

[9] E. F. Brickell, *Some Ideal Secret Sharing Schemes*, in Advances in Cryptology EUROCRYPT 89, vol. 434 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 1990, pp. 468–475.

[10] C. Carlet, C. Ding, and J. Yuan, *Linear codes from perfect nonlinear mappings and their secret sharing schemes*, IEEE Transactions on Information Theory, 51 (2005), pp. 2089–2102.

[11] H. Chen, *Linear Secret Sharing from Algebraic-Geometric Codes*, Computing Research Repository, (2006). http://arxiv.org/abs/cs/0603008.

[12] H. Chen and R. Cramer, *Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computations over Small Fields*, in Advances in Cryptology - CRYPTO 2006, vol. 4117 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2006, pp. 521–536.

[13] H. Chen, R. Cramer, S. Goldwasser, R. D. Haan, and V. Vaikuntanathan, *Secure computation from random error correcting codes*, in In EUROCRYPT, 2007, pp. 291–310.

[14] H. Chen, S. Ling, and C. Xing, *Access Structures of Elliptic Secret Sharing Schemes*, IEEE Transactions on Information Theory, 54 (2008), pp. 850–852.

[15] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*, North Holland, Amsterdam, 1997.

[16] R. Cramer, I. B. Damgrd, N. Döttling, S. Fehr, and G. Spini, *Linear Secret Sharing Schemes from Error Correcting Codes and Universal Hash Functions*, in Advances in Cryptology - EUROCRYPT 2015, vol. 9057 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2015, pp. 313–336.

[17] C. Ding, D. R. Kohel, and S. Ling, *Secret-sharing with a class of ternary codes*, Theoretical Computer Science, 246 (2000), pp. 285–298.

[18] C. Ding, T. Laihonen, and A. Renvall, *Linear Multisecret-Sharing Schemes and Error-Correcting Codes*, Journal of Universal Computer Science, 3 (1997), pp. 1023–1036.

[19] C. Ding and A. Salomaa, *Secret Sharing Schemes with Nice Access Structures*, Fundamenta Informaticae, 73 (2006), pp. 51–63.

[20] C. Ding and J. Yuan, *Covering and Secret Sharing with Linear Codes*, in Discrete Mathematics & Theoretical Computer Science, vol. 2731 of Lecture Notes in Computer Science, Springer, 2003, pp. 11–25.

[21] P. Hauck, *Codierungstheorie Skript zur Vorlesung im WS 2005/06.* http://dm.inf.uni-tuebingen.de/lehre, 2005.

[22] E. D. Karnin, J. W. Greene, and M. E. Hellman, *On secret sharing systems*, IEEE Transactions on Information Theory, 29 (1983), pp. 35–41.

[23] J. Kurihara, T. Uyematsu, and R. Matsumoto, *Secret Sharing Schemes Based on Linear Codes Can Be Precisely Characterized by the Relative Generalized Hamming Weight*, IEICE Transactions, 95-A (2012), pp. 2067–2075.

[24] L. Li and S. Yang, *On the Access Structures of Hyperelliptic Secret Sharing*, IACR Cryptology ePrint Archive, 2011 (2011), p. 415.

[25] Z. Li, T. Xue, and H. Lai, *Secret sharing schemes from binary linear codes*, Information Sciences, 180 (2010), pp. 4412 – 4419.

[26] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*, North Holland, 1983.

[27] K. M. Martin, G. J. Simmons, and W.-A. Jackson, *The Geometry of Shared Secret Schemes*, Bulletin of the ICA, 1 (1991), pp. 71–88.

[28] J. L. Massey, *Minimal Codewords and Secret Sharing*, in Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory, 1993, pp. 276–279.

[29] ——, *Some Applications of Coding Theory in Cryptography*, in Codes and Ciphers: Cryptography and Coding IV, 1995, pp. 33–47.

[30] R. J. McEliece and D. V. Sarwate, *On Sharing Secrets and Reed-Solomon Codes*, Communications of the ACM, 24 (1981), pp. 583–584.

[31] M. B. Paterson and D. R. Stinson, *A simple combinatorial treatment of constructions and threshold gaps of ramp schemes*, Cryptography and Communications, 5 (2013), pp. 229–240.

[32] I. S. Reed and G. Solomon, *Polynomial Codes Over Certain Finite Fields*, Journal of the Society for Industrial and Applied Mathematics, 8 (1960), pp. 300–304.

[33] A. Renvall and C. Ding, *The Access Structure of Some Secret-sharing Schemes*, in Proceedings of the First Australasian Conference on Information Security and Privacy, ACISP '96, Springer, 1996, pp. 67–78.

[34] C. Schulze, *Multifunktionale Secret Sharing Schemes*, in Mitteilungen aus dem Mathematischen Seminar Giessen, vol. 222, Giessen University, 1995, pp. 1–63.

[35] A. Shamir, *How to Share a Secret*, Communications of the ACM, 22 (1979), pp. 612–613.

[36] G. Simmons, *An Introduction to Shared Secret and/or Shared Control Schemes and Their Application*, Wiley-IEEE Press, 1992, pp. 441–497.

[37] D. Stinson, *An explication of secret sharing schemes*, Designs, Codes and Cryptography, 2 (1992), pp. 357–390.

[38] M. Sudan, *Algorithmic introduction to coding theory. Lecture 21.* `http://people.csail.mit.edu/madhu/FT01/scribe/lect21.ps`, 2001.

[39] X. Tan and Z. Wang, *New secret sharing scheme based on linear code*, Applied Mathematics-A Journal of Chinese Universities, 19 (2004), pp. 160–166.

[40] C. Tang, S. Gao, and C. Zhang, *The Optimal Linear Secret Sharing Scheme for Any Given Access Structure*, IACR Cryptology ePrint Archive, 2011 (2011), p. 147.

[41] A. N. Tentu, P. Paul, and V. C. Venkaiah, *Ideal and Perfect Hierarchical Secret Sharing Schemes based on MDS codes*, IACR Cryptology ePrint Archive, 2013 (2013), p. 189.

[42] M. van Dijk, *A linear construction of perfect secret sharing schemes*, in Advances in Cryptology EUROCRYPT'94, vol. 950 of Lecture Notes in Computer Science, Springer, 1995, pp. 23–34.

[43] J. van Lint, *Introduction to Coding Theory*, Springer, 1999.

[44] J. Yuan and C. Ding, *Secret Sharing Schemes from Three Classes of Linear Codes*, IEEE Transactions on Information Theory, 52 (2006), pp. 206–212.