Designs, Codes and Cryptography (2021) 89:2067–2078
https://doi.org/10.1007/s10623-021-00900-9

Generalized threshold secret sharing and finite geometry

Peter Ligeti[1] · Peter Sziklai[2,3] · Marcella Takáts[2,4]

Received: 1 August 2020 / Revised: 23 May 2021 / Accepted: 31 May 2021 / Published online: 23 June 2021

Abstract
In the history of secret sharing schemes many constructions are based on geometric objects. In this paper we investigate generalizations of threshold schemes and related finite geometric structures. In particular, we analyse compartmented and hierarchical schemes, and deduce some more general results, especially bounds for special arcs and novel constructions for conjunctive 2-level and 3-level hierarchical schemes.

Keywords Secret sharing · Threshold schemes · Finite geometry · Projective space

Mathematics Subject Classification 94A62 · 05B25

1 Introduction

Secret sharing refers to methods for distributing some secret information amongst a group of participants $\mathcal{P}$, each of whom is allocated a partial information of the secret called *share*. The secret and the shares are generated by a special user, called *dealer*. The secret s can be reconstructed from the respective shares only when a sufficient number of shares are combined together. The collection of possible “reconstructers” (or authorized subsets) is described by the a set of subsets of the participants, the so-called access structure $\mathcal{A}$. We consider perfect secret sharing schemes only, which yields two security requirements for the scheme: on one hand, the “reconstructers” (i.e. the elements of $\mathcal{A}$) can recover the secret from its shares, while the unauthorized subsets (the subsets outside $\mathcal{A}$) can learn nothing. Note that the term “nothing” is considered in the information-theoretic sense, namely the unauthorized

Communicated by M. Paterson.

✉ Peter Ligeti
ligetipeter@inf.elte.hu

Peter Sziklai
peter.sziklai@ttk.elte.hu

Marcella Takáts
marcella.takats@ttk.elte.hu

[1] Department of Computer Algebra, Eötvös Loránd University, Budapest, Hungary

[2] Department of Computer Science, Eötvös Loránd University, Budapest, Hungary

[3] Rényi Institute of Mathematics, Budapest, Hungary

[4] MTA-ELTE Geometric and Algebraic Combinatorics Research Group, Budapest, Hungary

users can use infinite computational power. As a consequence of this, the efficiency of a scheme can be measured by the amount of information the participants have to maintain per secret bit, i.e. the size of the shares related to the size of the secret. It is easy to see, that in the most optimal setting, every share has the same size as the secret itself. These are the so-called *ideal* secret sharing schemes.

Secret sharing was first introduced independently by Blakley [3] and Shamir [14] in 1979. In both papers perfect t*-threshold schemes* were presented, when every t-element subset of n participants is qualified, but neither of the $t-1$-element subsets is. Let us recall the main ideas of the constructions:

Example 1 (Blakley [3]) Let V be a t-dimensional vector space over a finite field. Choose a point $R \in V$ uniformly at random and let the secret be the first coordinate of R. The shares are the hyperplanes of V containing R defined by their normal vectors. The normalvectors chosen for the participants must satisfy certain properties to make this a perfect secret sharing scheme.

Example 2 (Shamir [14]) Let the participants be indexed by the non-zero elements of a finite field $\mathbb{F}$ and let p be a polynomial of degree at most $t-1$ over $\mathbb{F}$ chosen uniformly at random. The share of participant i is $p(i)$ and the secret is the the constant term of $p(x)$, i.e. $p(0)$.

Note that the second example is a special case of the first, as the polynomials of degree at most $t-1$ form a vectorspace of dimension t and the polynomials p for which $p(i) = s_i$ for some fixed i and s_i form a hyperplane. On the other hand, all shares and the secret are vectors from the same vectorspace, hence the above constructions are ideal schemes as well.

In this work we are dealing with some generalizations of the t-threshold schemes called multilevel schemes, where the users are partitioned into subsets (i.e. the levels) such that within every level the users are equal from the scheme point of view. Simple examples are department members in a committee or different levels of hierarchy in a company. These generalizations have several applications, like sharing a key to a central vault in a bank, triggering mechanisms of nuclear weapons, key escrow or building blocks in sophisticated crypto-systems, e.g. advanced access control mechanisms, like attribute-based encryption or secure multiparty computation.

1.1 Preliminaries

Let $\mathcal{P}$ be a finite set of participants and let a special participant $D \notin \mathcal{P}$ be called the dealer. The access structure is a monotone subset of sets, more precisely:

Definition 1 *A set of subsets $\mathcal{A} \subseteq 2^{\mathcal{P}}$ is called access structure if it is monotone, i.e. if $A \in \mathcal{A}$ and $B \supset A$ then also $B \in \mathcal{A}$. The set of minimal elements of the access structure is denoted by $\mathcal{A}^*$*

Note that every access structure can be defined by its minimal elements only as a consequence of the monotonic property. If only $\mathcal{A}^*$ is specified, then the access structure is the set of all elements containing any minimal elements. The precise definition of secret sharing schemes uses random variables and independence:

Definition 2 *A perfect secret sharing scheme realizing $\mathcal{A}$ is a set of random variables ξ_i for every $i \in \mathcal{P}$ and furthermore ξ_D, with*

1. *Reconstruction: if $A \in \mathcal{A}$, then $\{\xi_i : i \in A\}$ determines ξ_D;*

2. *Perfectness: if $B \notin \mathcal{A}$, then $\{\xi_i : i \in B\}$ is independent of ξ_D.*

In this paper we use the constructive model of secret sharing introduced by Brickell and Stinson [6]. Let $\mathcal{S}$ be the set of possible secrets and let $\mathcal{S}_i$ be the set of possible shares of participant i for all $i \in \mathcal{P}$. We assume that the secret s and the shares s_i are chosen from finite sets $\mathcal{S}$ and $\mathcal{S}_i$, respectively, hence they can be represented as bit-strings of length $\log_2 |\mathcal{S}|$ and $\log_2 |\mathcal{S}_i|$. A perfect secret sharing scheme is ideal, if all the shares and the secret are chosen from domains of the same size, i.e. $\log_2 |\mathcal{S}| = \log_2 |\mathcal{S}_i|$ for every $i \in \mathcal{P}$.

Perfect secret sharing schemes can described by a collection of distribution methods describing the generation of the secrets and the respective shares.

Definition 3 *A function*

$$f : \{D\} \cup \mathcal{P} \to \mathcal{S} \cup \bigcup_{i \in \mathcal{P}} \mathcal{S}_i$$

is a distribution method if $f(D) = s \in \mathcal{S}$ and $f(i) = s_i \in \mathcal{S}_i$ for every $i \in \mathcal{P}$.

Let $\mathcal{F}$ denote the set of all possible distribution methods from $\{D\} \cup \mathcal{P}$ to $\mathcal{S} \cup \bigcup_{i \in \mathcal{P}} \mathcal{S}_i$ and $\mathcal{F}_s = \{f \in \mathcal{F} : f(D) = s\}$ for every $s \in \mathcal{S}$. As a first step of the generation process, the dealer chooses a secret $s \in \mathcal{S}$ uniformly at random. Next, the dealer chooses a distribution method $f \in \mathcal{F}_s$ uniformly at random as well and use this method for generating the shares. Apart from that, the dealer does not participate in any communication or computation.

Finally, let us recall the simplest case of the linear algebraic construction by Blakley and Kabatianskii [4]. Let us assume that the dealer and the participants are assigned vectors $d, v_i \in \mathbb{F}_q^k$ for $i \in \mathcal{P}$. In a (one-dimensional) linear secret sharing generated by $G = (d, v_1, \ldots, v_{|\mathcal{P}|})$ the dealer chooses $e \in \mathbb{F}_q^k$ uniformly at random and let the secret be the inner product of vectors e and d and the share of participant i be the inner product of vectors e and v_i. Note that however more general linear constructions are proposed in [4] and [20], we will use the following rather simple and useful result only:

Theorem 1 (Blakley and Kabatianskii [4]) *A linear secret sharing generated by $G = (d, v_1, \ldots, v_{|\mathcal{P}|})$ represents an ideal perfect secret sharing scheme realizing $\mathcal{A}$ if and only if the following conditions hold:*

1. *$\forall X \in \mathcal{A}$ the vector d is a linear combination of the vectors v_x, $x \in X$;*
2. *$\forall Y \notin \mathcal{A}$ the vector d is disjoint from the subspace generated by vectors v_y, $y \in Y$.*

1.2 Related work

Multilevel secret sharing is one straightforward generalization of t-threshold schemes, where, apart from some threshold value(s), the set of participants is partitioned into smaller disjoint subsets (called groups or levels) such that the users within any given level are equivalent from the secret sharing point of view. We are focusing on two special cases, namely on compartmented access structures with upper bounds and on hierarchical threshold access structures.

In the original presentation of compartmented access structures the goal is to guarantee some proportion of members from every department. More precisely, let $\mathcal{P} = \bigcup_{i=1}^{m} \mathcal{G}_i$, let t be the threshold and let $l_1, \ldots, l_m \in \mathbb{N}$ be the lower bounds with $t \geq \sum_{i=1}^{m} l_i$ and the minimal elements of the access structure are the following

$$\mathcal{A}^* = \{A \subseteq \mathcal{P} : |A| = t \text{ and } |A \cap \mathcal{G}_i| \geq l_i, \forall 1 \leq i \leq m\} \qquad (1)$$

This version called *compartmented access structures with lower bounds* was introduced by Brickell [5], see [9,18,21] for interpolation constructions.

In *compartmented access structures with upper bounds* the goal is to avoid a given percentage of members from all (disjoint) groups in qualified subsets. More precisely, let $\mathcal{P} = \bigcup_{i=1}^{m} \mathcal{G}_i$ and let $t \in \mathbb{N}, t_i \in \mathbb{N}, i = 1, \ldots, m$ be thresholds with $t \leq \sum_{i=1}^{m} t_i$. Then the minimal elements in access structure are the following:

$$\mathcal{A}^* = \{A \subseteq \mathcal{P} : |A| = t \text{ and } |A \cap \mathcal{G}_i| \leq t_i, \forall 1 \leq i \leq m\} \tag{2}$$

This problem seems to be a bit counter-intuitive for the first sight, such situation can occur if the size of a qualified subset has to exceed some threshold, but we would like to limit the number of participants representing each compartments. This problem was introduced by Tassa and Dyn [18] and the authors proposed a general solution based on bivariate interpolation techniques. Fuji-Hara and Miao [8] considered a special case of $t_1 = \cdots = t_m = t - 1$ (i.e. when there are no qualified subsets from one single group) in a slightly different interpretation (the authors refer to this case as *parallel model*) for a fixed small threshold (i.e. $t = 3$) only. We extend their result in Sect. 2 and show the limits of this method as well.

In *hierarchical* threshold access structures with m disjoint levels, let $\mathcal{P} = \bigcup_{i=1}^{m} \mathcal{L}_i$ and let $t_1 < t_2 < \cdots < t_m$ be a sequence of thresholds. There are two main variants of generalized threshold schemes based on the logical relation between the conditions.

In *conjunctive* $(t_1, \ldots, t_m)$*-hierarchical schemes* the access structure is the following:

$$\mathcal{A} = \Big\{A \subseteq \mathcal{P} : \big|A \cap \big(\bigcup_{j=1}^{i} \mathcal{L}_j\big)\big| \geq t_i, \text{ for all } 1 \leq i \leq m\Big\}. \tag{3}$$

In *disjunctive* $(t_1, \ldots, t_m)$*-hierarchical schemes* the access structure is the following:

$$\mathcal{A} = \Big\{A \subseteq \mathcal{P} : \big|A \cap \big(\bigcup_{j=1}^{i} \mathcal{L}_j\big)\big| \geq t_i, \text{ for some } 1 \leq i \leq m\Big\}. \tag{4}$$

In the conjunctive case there are only few general solutions based on interpolation by Tassa [17], Tassa and Dyn [18], Shima and Doi [15] and on MDS codes by Tentu et al. [19]. Furthermore, there are some constructions for special cases of two levels, like a (1, 3)-scheme by Fuji-Hara and Miao [8].

In the disjunctive case there are significantly more constructions, some of them are based on finite geometry arguments, see [2,11–13]. Farràs and Padrò [7] give a characterization of ideal hierarchical schemes using matroid theory.

Within this paper we give some constructions for special cases of compartmented access structures in Sect. 2. Note that the resulting geometric constructions are interesting on their own. Next, we suggest ideal construction for 2-level conjunctive $(1, n + 1)-$hierarchical scheme in Sect. 3.2. Furthermore, we present a novel 3-level conjunctive $(1, 2, n+1)$ scheme using finite geometry constructions in Sect. 3.3. Apart from the general constructions [15,17–19] on arbitrary levels , this is the first ideal conjunctive scheme on 3-levels. Note that neither of the above general methods yielding our geometry construction.

The proposed construction has no restrictions on the related finite field in contrast with the scheme of Tassa [17] working over fields of characteristic larger than 2, and the scheme of Shima and Doi [15] working only over fields of characteristic 2. Furthermore, the proposed constructions are unconditionally perfect in contrast with the solution of Tentu et al. [19] which is probabilistic in the sense that a non-qualified subset can compute the secret with negligible probability. The proposed scheme also improves the lower bound on the size of the underlying field in the case of 2 or 3 levels. Last, but not least, the constructions in Sects. 3.2 and 3.3 are the first for conjunctive hierarchical schemes based on finite geometry arguments.

2 Compartmented access structures

In this section we use the notion of *arc* in a projective space $\mathrm{PG}(n, q)$: it is a set of points with no subset of $(n + 1)$ points lying in a hyperplane. We will denote the maximum cardinality of an arc in $\mathrm{PG}(n, q)$ by $M(n, q)$. It is known that

(i) $M(2, q) = q + 1$ if q is odd and $M(2, q) = q + 2$ if q is even;
(ii) $M(n, q) = q + 1$ if $n \le 2p - 3$, where $q = p^h$, p prime;
(iii) $M(n, q) = q + 1$ if $n \le \frac{1}{4}\sqrt{q} + \frac{9}{4}$ and q odd;
(iv) it is generally conjectured that $M(n, q) = q + 1$ for $2 < n < q - 2$.

Note that (ii) and (iii) can be found in Ball and De Beule [1], while (iv) is the famous MDS-conjecture by B. Segre.

2.1 Bounds for pencil arcs—bounds for $|\mathcal{P}|$

Let $\mathrm{PG}(n, q)$ denote the projective space of dimension n over the finite field $\mathbb{F}_q$. Π_r will be the shorthand for a projective subspace of dimension r. A *pencil* in Π_r is the set of the $(q + 1)$ Π_{r-1} -s (in the fixed Π_r), each containing a common fixed Π_{r-2}. A set of t points $(1 \le t \le n + 1)$ in $\mathrm{PG}(n, q)$ is *independent* if no Π_{t-2} contain them. A set of k points in $\mathrm{PG}(n, q)$ is a *k-arc* if any subset of size $n + 1$ is independent. Note that if $n = 1$ it means that in $\mathrm{PG}(1, q)$ *any* set of points is an arc. The following configuration defined in [8] is the key to our constructions:

Definition 4 *Let $\Psi_0, \ldots, \Psi_q$ be a pencil through some Π_{n-2} in $\mathrm{PG}(n, q)$. A pencil arc (k-parc) $\mathcal{K}$ is a set of k points, in $\mathrm{PG}(n, q)$ satisfying the following conditions:*

1. *Each $\mathcal{K} \cap \Psi_i$ is a k_i-arc in Π_{n-1} for $0 \le i \le q$, where $k_i = |\mathcal{K} \cap \Psi_i|$;*
2. *$\mathcal{K} \cap \Psi_i \cap \Psi_j = \emptyset$ for $0 \le i \ne j \le q$;*
3. *Any $n + 1$ points of $\mathcal{K}$ not contained in any single Ψ_i are independent.*

We note that Fuji-Hara and Miao showed that if there is a k-parc in $\mathrm{PG}(t - 1, q)$ as above, with $k = k_0 + k_1 + \ldots + k_m$ points, $k_i \ge 1$ for $0 \le i \le m$ and $k_0 = \min\{k_i\}$, then there exists an ideal secret sharing scheme realizing compartmented access structure with upper bounds $t_1 = \cdots = t_m = t - 1$ on $|\mathcal{P}| = k - k_0$ participants, where m is the number of groups and $k_{m+1} = \cdots = k_q = 0$.

In [8] it was proved that in $\mathrm{PG}(2, q)$, a k-parc is of size at most $k \le 2q$. We extend this result to higher dimensions.

Theorem 2 *Let $\mathcal{K}$ be a k-parc in $\mathrm{PG}(n, q)$. Then*

(i) if $n = 2$ then $k \le 2q$, with equality if and only if $\mathcal{K}$ is the point set of two lines minus their intersection point;
(ii) if $n \ge 3$ then $k \le M(n - 1, q) + 1$, where $M(n, q)$ is the largest size of an arc in $\mathrm{PG}(n, q)$.

Proof (i) We recall that within a line $\mathrm{PG}(1, q)$, *any* point set is an arc (so a pencil line is allowed to contain any number of points). Let ℓ be any line of the pencil with

$|\ell \cap \mathcal{K}| = h$, $1 \le h \le q$. Then on any further line through a fixed $P \in \ell \cap \mathcal{K}$, there is at most one point of $\mathcal{K}$, hence $k \le h + q \le 2q$. In case of $k = 2q$, $|\ell \cap \mathcal{K}| = q$ for any pencil line containing at least one point of $\mathcal{K}$.

(ii) If $n \ge 3$ then choose a point $P \in \mathcal{K}$ from a pencil-hyperplane H_0 and project $\mathcal{K} \backslash \{P\}$ onto another pencil-hyperplane H_1. Note that the projection is one-to-one and so the image $\mathcal{K}'$ is a $(k-1)$-arc in H_1. □

Note that we have examples of size $k = M(n-1, q) + 1$:

- an arc of size $M(n-1, q)$ in the pencil-hyperplane H_1 plus an extra point P outside H_1;
- an arc of size $M(n-1, q)$ minus a deleted point Q in the pencil-hyperplane H_1, plus two extra points on a line through Q but not in H_1.

Though the above constructions are rather interesting from geometry point of view, there is a technical consequence for the resulting secret sharing scheme, namely a necessary condition for the size of the participants: for every ideal compartmented scheme with upper bounds $t_1 = \cdots = t_m = t-1$ arising from a parc $|\mathcal{P}| \le 2q - k_0$ if $t = 3$ and $|\mathcal{P}| \le M(n-1, q) + 1 - k_0$ if $t = n + 1 \ge 4$.

2.2 Generalization of the Baer construction

In their paper [8], Fuji-Hara and Miao gave a construction based on Baer subplanes for 2-dimensional pencil arcs. We extend their constructions in two ways.

2.2.1 Parcs from planar arcs

Consider a projective plane $\mathrm{PG}(2, q^h) = \mathrm{AG}(2, q^h) \cup (\ell_\infty)$. Then let's identify $\mathrm{AG}(2, q^h) \sim X \times Y$, where $X \sim \mathbb{F}_q^h$ and $Y \sim \mathbb{F}_q^h$ are the horizontal and the vertical axes. Let's call here the translates of the first factor (horizontal axis) "the horizontal lines" $\ell_0, \ldots, \ell_{q^h-1}$, which, together with ℓ_∞, form "the" pencil with center P.

Let L_1 be a $(h-1)$-dimensional q-subspace of the horizontal axis, i.e. $X = L_0 \times L_1$ for some 1-dimensional q-vectorspace $L_0 \subset X$, without loss of generality $L_0 = \mathbb{F}_q$. Let L_2 be a 1-dimensional q-subspace of the vertical axis Y, again without loss of generality $L_2 = \mathbb{F}_q$. Finally, suppose without loss of generality that $\ell_0, \ldots, \ell_{q-1}$ happen to be those pencil lines who intersect L_2.

We remark that in the original construction, based on Baer subplanes, we have $h = 2$, so L_0, L_1 and L_2 are all isomorphic to $\mathbb{F}_q$.

Let $A_0 = L_1 \times L_2$. Any horizontal translate of it is either disjoint from A_0 or identical with it, hence they form a partition $\cup_{\lambda \in \mathbb{F}_q}(A_0 + \lambda) = \ell_0 \cup \ldots \cup \ell_{q-1}$. Note that here, for any point $Q \in \ell_0 \cup \ldots \cup \ell_{q-1}$, it has coordinates $Q = (a + \lambda, y)$, where $a \in L_1$, $\lambda \in L_0$ and $y \in L_2$.

We remark that in the Baer suplane construction, i.e. when $h = 2$, we have $A_0 = \mathbb{F}_q \times \mathbb{F}_q$ an affine Baer subplane.

Consider the affine plane $\mathrm{AG}(2, q) \sim L_0 \times L_2$ and an arc S in it. Now define

$$K := \{(a + \lambda, y) : a \in L_1, (\lambda, y) \in S\}.$$

Observe that K consists of $|S|$ 'line segments', each contained in one of the pencil lines ℓ_i and of size $|L_1| = q^{h-1}$. We claim that K is a pencil arc (of size $|S|q^{h-1}$). To verify this we have to prove that no three distinct points $(a_j + \lambda_j, y_j)$, $j = 1, 2, 3$ can be collinear if they are not contained in the same pencil line, i.e. their second coordinates are not all equal. If already two of them has equal values y_i then we are done (either the third y_j is different and hence it is not on the same horizontal line $Y = y_i$ so not all the three are collinear, or the third y_i is the same and then they are on a pencil line). Finally, if their corresponding arc points are pairwise different:

$$\begin{vmatrix} a_1 + \lambda_1 & y_1 & 1 \\ a_2 + \lambda_2 & y_2 & 1 \\ a_3 + \lambda_3 & y_3 & 1 \end{vmatrix} = \begin{vmatrix} a_1 & y_1 & 1 \\ a_2 & y_2 & 1 \\ a_3 & y_3 & 1 \end{vmatrix} + \begin{vmatrix} \lambda_1 & y_1 & 1 \\ \lambda_2 & y_2 & 1 \\ \lambda_3 & y_3 & 1 \end{vmatrix}$$

Consider the last two terms: the first one takes value from L_1 while the second one from $L_0 = \mathbb{F}_q$. As $L_0 \cap L_1 = \{0\}$ and the last one is nonzero because of the arc property, this sum cannot be zero.

It is well known that there exist (many) arcs of size $q + 1$ in AG$(2, q)$ for q odd and arcs of size $q + 2$ in AG$(2, q)$ for q even. Hence we gain (many) k-parcs with $k = q^h + q^{h-1}$ in planes of odd order q^h; and k-parcs with $k = q^h + 2q^{h-1}$ in planes of even order q^h.

2.2.2 Parcs from caps

Let L_1 be a $(h - s)$-dimensional $\mathbb{F}_q$-subspace of the horizontal axis, i.e. $X = L_0 \times L_1$ for some s-dimensional $\mathbb{F}_q$-vectorspace $L_0 \subset X$. Let L_2 be a 1-dimensional $\mathbb{F}_q$-subspace of the vertical axis Y, without loss of generality we may assume $L_2 = \mathbb{F}_q$. Suppose without loss of generality that $\ell_0, \ldots, \ell_{q-1}$ happen to be the pencil lines who intersect L_2.

Let $A_0 = L_1 \times L_2$. Any horizontal translate of it is either disjoint from A_0 or identical with it, hence they form a partition $\cup_{v \in L_0}(A_0 + v) = \ell_0 \cup \ldots \cup \ell_{q-1}$. Note that here, for any point $Q \in \ell_0 \cup \ldots \cup \ell_{q-1}$, it has coordinates $Q = (a + v, y)$, where $a \in L_1$, $v \in L_0$ and $y \in L_2$.

Consider the affine space AG$(s + 1, q) \sim L_0 \times L_2$ and a **cap** S in it. (We recall that a cap is a pointset with no collinear triple of points.) Now define

$$K := \{(a + v, y) : a \in L_1, (v, y) \in S\}.$$

Observe that K consists of $|S|$ 'line segments', each contained in one of the pencil lines ℓ_i and of size $|L_1| = q^{h-s}$. We claim that K is a pencil arc (of size $|S|q^{h-s}$). To verify this we have to prove that no three distinct points $(a_j + v_j, y_j)$, $j = 1, 2, 3$ can be collinear if they are not contained in the same pencil line, i.e. their second coordinates are not all equal. We can repeat the earlier argument that if already two of them has equal values y_i then we are done (either the third y_j is different and hence it is not on the same horizontal line $Y = y_i$ so not all the three are collinear, or the third y_i is the same and then they are on a pencil line). Finally, if their corresponding cap points are pairwise different:

$$\begin{vmatrix} a_1 + v_1 & y_1 & 1 \\ a_2 + v_2 & y_2 & 1 \\ a_3 + v_3 & y_3 & 1 \end{vmatrix} = \begin{vmatrix} a_1 & y_1 & 1 \\ a_2 & y_2 & 1 \\ a_3 & y_3 & 1 \end{vmatrix} + \begin{vmatrix} v_1 & y_1 & 1 \\ v_2 & y_2 & 1 \\ v_3 & y_3 & 1 \end{vmatrix}$$

Consider the last two terms: the first one takes value from L_1 while the second one from L_0. As $L_0 \cap L_1 = \{0\}$ and the last one is nonzero because of the cap property, this sum cannot be zero and hence the three points cannot be collinear. There exist large caps in affine spaces but the constructions are not easy. Here, as an example we remark that e.g. when $h = 2$ then we may choose a cap (in different ways) in AG$(3, q)$ of size q^2, resulting in k-parcs with $k = q^3$.

3 Hierarchical access structures

3.1 Bounds for the size of hierarchical arcs—bounds for $|\mathcal{P}|$

Definition 5 *Let Ψ be a hyperplane of* $\mathrm{PG}(n,q)$*, $\mathcal{K}_1$ be a set of k_1 points in* $\mathrm{PG}(n,q)\backslash\Psi$*, and $\mathcal{K}_2$ be a set of k_2 points in Ψ. A hierarchical arc in* $\mathrm{PG}(n,q)$ *is a set $\mathcal{K}=\mathcal{K}_1\cup\mathcal{K}_2$ of k_1+k_2 points in* $\mathrm{PG}(n,q)$*, also called a (k_1,k_2)-harc, satisfying the following conditions:*

(1) $\mathcal{K}_1$ is a k_1-arc in $\mathrm{PG}(n,q)$*;*
(2) $\mathcal{K}_2$ is a k_2-arc in $\mathrm{PG}(n-1,q)$*;*
(3) Any $n+1$ points of $\mathcal{K}$ not contained in the hyperplane Ψ are independent.

Fuji-Hara and Miao [8] showed that if there is a (k_1,k_2)-harc in $\mathrm{PG}(t-1,q)$ with $k_1\geq 2$ and $k_2\geq 0$ then there exists an ideal conjunctive $(1,t)$-hierarchical scheme with $|\mathcal{P}|=k_1+k_2-1$. The authors also proved that in $\mathrm{PG}(2,q)$ for a (k_1,k_2)-harc its size is at most $k_1+k_2\leq q+2$. The following theorem extends this result to higher dimensions. We need the notion of *hyperfocused arc*s: an affine pointset $S\subset\mathrm{AG}(2,q)$ is called a hyperfocused arc if it is an arc and its secants determine $|S|-1$ directions (which is the least possible value). Note that

(i) if a hyperoval has 2 points at infinity then its q affine points (determining $q-1$ directions) form a hyperfocused arc;
(ii) a single affine point (determining zero directions) forms a hyperfocused arc.

The term *sharply focused set* was introduced by Simmons for a k-set such that its secants determine k directions [16]. He investigated only finite projective planes of odd order, where the secants of a k-arc cannot determine less directions. Holder studied planes of even order, where exist k-arcs such that the secants determine $(k-1)$ directions. Holder called them *super sharply focused sets*, and the term *very sharply focused sets* was also used in the literature. Later, Cherowitzo and Holder introduced the term *hyperfocused arc* for such arcs. There is a natural extension of the definition of hyperfocused arcs: a k-arc is called a *generalized hyperfocused arc* if there exist $(k-1)$ points (external to the arc) blocking each secant of the arc. For more details see [10].

Theorem 3 *Let $\mathcal{K}$ be a (k_1,k_2)-harc in* $\mathrm{PG}(n,q)$*, $|\mathcal{K}|=k_1+k_2=k$. Then*

(i) if $n=2$ then $k\leq q+2$, with equality if and only if $\mathcal{K}_1$ is a hyperfocused arc of the affine plane and $\mathcal{K}_2$ is the set of non-determined directions;
(ii) if $n\geq 3$ then $k\leq M(n-1,q)+1$, where $M(n,q)$ is the largest size of an arc in $\mathrm{PG}(n,q)$*.*

Proof (i) If $n=2$ then choose a point $P\in\mathcal{K}_1$. Then on any line through P, there is at most one further point of $\mathcal{K}$, hence $k\leq 1+(q+1)$. In case of equality, let's call the points of $\mathcal{K}_2$ (and the line containing them) the points at infinity. Now the pointset $\mathcal{K}_1$ does not determine the points ("directions") in $\mathcal{K}_2$ and so the number of directions determined by $\mathcal{K}_1$ is at most $q+1-k_2$ and at least k_1-1. As these two bounds are equal, $\mathcal{K}_1$ determines exactly k_1-1 directions. This is the definition of hyperfocused arcs.

(ii) If $n\geq 3$ then choose a point $P\in\mathcal{K}_1$ and project $\mathcal{K}\backslash\{P\}$ onto another hyperplane H_0. Note that the projection is one-to-one and so the image $\mathcal{K}_0$ is a $(k-1)$-arc in H_0. □

Similarly as above, this theorem can be rephrased as a secret sharing result, namely for every ideal 2-level conjunctive scheme arising from harc $|\mathcal{P}|\leq q+1$ for $(1,3)$ schemes and $|\mathcal{P}|\leq M(n-1,q)$ for $(1,n+1)$ schemes.

3.2 A conjunctive $(1, n+1)$-scheme ($n \geq 3$)

Within this section we propose a new construction for (k_1, k_2)-harc in $\mathrm{PG}(n, q)$. Though such a construction yields an ideal conjunctive $(1, n+1)$-hierarchical scheme based on [8], we prove it directly as well. More precisely, the set $\mathcal{P}$ consists of 2 levels $\mathcal{L}_1, \mathcal{L}_2$. A valid subset should contain at least $n+1$ elements from $\mathcal{L}_1 \cup \mathcal{L}_2$ and at least 1 element from $\mathcal{L}_1$.

In $\mathrm{PG}(n, q) = \mathrm{AG}(n, q) \cup H_\infty$ we will choose our sets as follows. Let

- $|\mathcal{L}_1| = k_1 = c_1 q^{1/n}$ be a subset of an arc (e.g. a so-called normal rational curve) in $\mathrm{AG}(n, q)$ and
- $|\mathcal{L}_2| = k_2 = c_2 q^{1/n}$ be a subset of an arc, e.g. a normal rational curve in H_∞);
- furthermore, a set $\mathcal{D} \subset \mathrm{AG}(n, q)$ of size cq will be determined below, such that the *dealer*, i.e. a point D will be chosen from $\mathcal{D}$.

We will calculate up to order of magnitude only.

First we choose $\mathcal{L}_1$. Then let L be the set of (at most $\binom{k_1}{n} = \frac{1}{n!} c_1^n q$) $(n-2)$-dimensional subspaces in H_∞ which are the intersection of H_∞ and the hyperplanes determined by the n-tuples of $\mathcal{L}_1$.

Now choose an arc C in H_∞ in such a way that $|C \cap (\bigcup L)|$ is at most $\frac{1}{n!} c_1^n q$ and let $C_0 = C \backslash (\bigcup L)$, then $|C_0| \geq (1 - \frac{1}{n!} c_1^n) q$. (It implies $c_1 < \sqrt[n]{n!}$.)

We would like to choose the points of $\mathcal{L}_2$ one-by-one from C_0. We start with an arbitrary subset $\{P_1\} \subset C_0$. Then, if we already have $\{P_1, \ldots, P_v\}$, for any n-tuple of $\mathcal{L}_1 \cup \mathcal{L}_2$ containing at least 1 point from $\mathcal{L}_1$ and at least 1 from $\{P_1, \ldots, P_v\}$, we remove the intersection points of the span of these n points with $C_0 \backslash \{P_1, \ldots, P_v\}$, so at most $(n-2)$ points. Let $d_2 = v/q^{1/n}$. This way we remove at most $\binom{k_1+v}{n}(n-2) = (n-2)\frac{(c_1+d_2)^n - c_1^n - d_2^n}{n!} q$ points, so if it is less than $|C_0| - v$ then we can choose the next point P_{v+1}. So we can go on until

$$\left(1 - \frac{1}{n!} c_1^n\right) q \geq (n-2) \frac{(c_1 + d_2)^n - c_1^n - d_2^n}{n!} q,$$

i.e. we may choose roughly

$$|\mathcal{L}_2| = v = d_2 q^{1/n} = c_2 q^{1/n} = \left(\sqrt[n]{\frac{n!}{n-2}} - c_1\right) q^{1/n}.$$

Finally we can choose a set $\mathcal{D} \subset \mathrm{AG}(n, q)$ in such a way, that it should contain no point from the union of hyperplanes spanned by n points of $\mathcal{L}_1 \cup \mathcal{L}_2$ but not all n from $\mathcal{L}_2$.

For this we have to remove from $\mathrm{AG}(n, q)$ at most $\frac{(c_1+c_2)^n - c_2^n}{n!} q^n$ points, so if it is significantly less than q^n then there remain enough points from which we can choose our set $\mathcal{D}$. It is more convenient to find an affine line intersecting this pointset in at least $(1 - \frac{(c_1+c_2)^n - c_2^n}{n!}) q$ points and choose from it our $\mathcal{D}$ of size cq.

Now one can check easily that

- any $n+1$ points of $\mathcal{L}_1 \cup \mathcal{L}_2$, at least 1 from $\mathcal{L}_1$ generate the space;
- any $n+1$ points from $\mathcal{L}_2$ does not generate the space.

We constructed $\mathcal{D}$ in such a way that (1) the minimal eligible sets generate the whole space hence adding a point $D \in \mathcal{D}$ to any eligible set does not increase its rank; while (2) the non-eligible sets from $\mathcal{L}_1 \cup \mathcal{L}_2$ span subspaces disjoint from $\mathcal{D}$.

These properties, together with Theorem 1 yield that the construction realizes a conjunctive $(1, n+1)$-scheme.

3.3 A conjunctive $(1, 2, n+1)$-scheme ($n \geq 3$)

As a generalization of the above ideas, we construct a geometric scheme composed of 3 levels $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3$. A valid subset should contain at least $n+1$ elements from $\mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3$, such that at least 2 elements are from $\mathcal{L}_1 \cup \mathcal{L}_2$ and at least 1 element from $\mathcal{L}_1$.

In $\mathrm{PG}(n, q) = \mathrm{AG}(n, q) \cup H_\infty$ we will choose our sets as follows. Let

- $|\mathcal{L}_1| = k_1 = c_1 q^{1/n}$ be a subset of an arc (e.g. a so-called normal rational curve) in $\mathrm{AG}(n, q)$;
- $|\mathcal{L}_2| = k_2 = c_2 q^{1/n}$ be a subset of an arc, e.g. a normal rational curve in H_∞) and
- $|\mathcal{L}_3| = k_3 = c_3 q^{1/n}$ be a subset of an arc, e.g. a normal rational curve in H, which is a $(n-2)$-dimensional subspace of H_∞;
- furthermore, a set $\mathcal{D} \subset \mathrm{AG}(n, q)$ of size $c_4 q$ will be determined below, such that the *dealer*, i.e. a point D will be chosen from $\mathcal{D}$.

Similarly as above, we will calculate up to order of magnitude only. First we choose $\mathcal{L}_1$. Then let B be the set of the at most $\binom{k_1}{2} = \frac{1}{2}c_1^2 q^{2/n}$ directions determined by the pairs from $\mathcal{L}_1$ and L be the set of (at most $\binom{k_1}{n} = \frac{1}{n!}c_1^n q$) $(n-2)$-dimensional subspaces in H_∞ which are the intersection of H_∞ and the hyperplanes determined by the n-tuples of $\mathcal{L}_1$.

Now choose an arc C in H_∞ in such a way that $|C \cap (B \cup \bigcup L)|$ is at most $\frac{1}{n!}c_1^n q$ and let $C_0 = C \setminus (B \cup \bigcup L)$, then $|C_0| \geq (1 - \frac{1}{n!}c_1^n)q$. (It implies $c_1 < \sqrt[n]{n!}$)

We would like to choose the points of $\mathcal{L}_2$ one-by-one from C_0. We start with an arbitrary subset $\{P_1\} \subset C_0$. Then, if we already have $\{P_1, \ldots, P_v\}$, for any n-tuple of $\mathcal{L}_1 \cup \mathcal{L}_2$ containing at least 2 points from $\mathcal{L}_1$ and at least 1 from $\{P_1, \ldots, P_v\}$, we remove the intersection points of the span of these n points with C_0. Let $d_2 = v/q^{1/n}$. This way we remove at most $\binom{k_1+v}{n}(n-2) = (n-2)\frac{(c_1+d_2)^n - c_1^n - nc_1 d_2^{n-1} - d_2^n}{n!}q$ points, so if it is less than $|C_0| - v$ then we can choose the next point P_{v+1}. So we can go on until

$$(1 - \frac{1}{n!}c_1^n)q \geq (n-2)\frac{(c_1 + d_2)^n - c_1^n - nc_1 d_2^{n-1} - d_2^n}{n!}q,$$

i.e. we may choose

$$|\mathcal{L}_2| = v = d_2 q^{1/n} = c_2 q^{1/n} = \left(\sqrt[n]{\frac{n!}{n-2}} - c_1\right)q^{1/n}.$$

Next, take an $(n-2)$-dimensional subspace $H \subset H_\infty$ which is disjoint from $B \cup \mathcal{L}_2$, and remove from H the points in the intersection with the hyperplanes spanned by n points of $\mathcal{L}_1 \cup \mathcal{L}_2$ but not all n from $\mathcal{L}_2$.

This way we remove at most $\frac{(c_1+c_2)^n - c_2^n}{n!}q^{n-2}$ points, so if it is significantly less than q^{n-2} then there exists a normal rational curve in H with at least $\frac{(c_1+c_2)^n - c_2^n}{n!}q$ non-deleted points and $\mathcal{L}_3$ can be chosen from it with cardinality $c_3 q^{1/n}$. (When $n = 3$ so H is a line then by the "normal rational curve" we mean just the complete line H.)

Here is the point when we can choose a set $\mathcal{D} \subset \mathrm{AG}(n, q)$ in such a way, that it should contain no point from the union of hyperplanes spanned by k points of $\mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3$ but not all n from $\mathcal{L}_2 \cup \mathcal{L}_3$.

This way we remove at most $\frac{(c_1+c_2+c_3)^n - (c_2+c_3)^n}{n!}q^n$ points, so if it is significantly less than q^n then there remain enough points from which we can choose our set $\mathcal{D}$. It is more convenient to find an affine line intersecting this point set in at least $(1 - \frac{(c_1+c_2+c_3)^n - (c_2+c_3)^n}{n!})q$ points and choose from it our $\mathcal{D}$ of size $c_4 q$.

Note that with the suitable choice of the constants we have e.g. for $c_1 = c_2 = c_3 = c_4$
$n = 3: \ c_1 = c_2 = c_3 = c_4 = 0.529$
$n = 4: \ c_1 = c_2 = c_3 = c_4 = 0.614$
etc.
Now one can check easily that

- any n points of $\mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3$, at least 1 from $\mathcal{L}_1$ and at least 2 from $\mathcal{L}_1 \cup \mathcal{L}_2$ generate the space;
- any 1 point from $\mathcal{L}_1$ and $n-1$ points from $\mathcal{L}_3$ does not generate the space;
- any n points from $\mathcal{L}_2 \cup \mathcal{L}_3$ does not generate the space.

We constructed $\mathcal{D}$ in such a way that (1) the minimal eligible sets generate the whole space hence adding a point $D \in \mathcal{D}$ to any eligible set does not increase its rank; while (2) the noneligible sets span subspaces disjoint from $\mathcal{D}$

These properties, together with Theorem 1 yield that the construction realizes a conjunctive $(1, 2, n+1)$-scheme.

Note that, this construction works if $q > cn^n$ yielding an $O(n^3)$ improvement in the size of the underlying field in contrast with the best known general result of Tassa and Dyn [18].

4 Summary

In this paper we have investigated various generalizations of threshold secret sharing schemes and related finite geometry constructions. In particular, we analysed compartmented and hierarchical models, and deduced some more general results. The proposed results are of two-fold interests. On one hand, we achieved geometric results by proving bounds for pencil and hierarchical arcs in higher dimensions and suggesting novel constructions for pencil arcs. On the other hand, we proposed novel secret sharing schemes by giving new constructions for a ideal conjunctive $(1, n+1)$ and $(1, 2, n+1)$-hierarchical schemes using a finite geometrical arguments over finite Galois fields.

Acknowledgements This research has been partially supported by Application Domain Specific Highly Reliable IT Solutions project which has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the Thematic Excellence Programme TKP2020-NKA-06 (National Challenges Subprogramme) funding scheme, by the European Union, co-financed by the European Social Fund (EFOP-3.6.2-16-2017-00013, Thematic Fundamental Research Collaborations Grounding Innovation in Informatics and Infocommunications) and by the Lendület programme of the HAS. The second author is grateful for the partial support of project K-120154 of the National Research, Development and Innovation Fund of Hungary and Momentum. The third author is grateful for the partial support of project 132625 of the National Research, Development and Innovation Fund of Hungary. The authors are grateful to the referees for their suggestions which helped to improve the quality of this paper and to Laci Csirmaz for the fruitful discussions on secret sharing.

Funding Open access funding provided by Eötvös Loránd University.

References

1. Ball S., De Beule J.: On sets of vectors of a finite vector space in which every subset of basis size is a basis II. Des. Codes Cryptogr. **65**, 5–14 (2012).
2. Beutelspacher A., Wettl F.: On 2-level secret sharing. Des. Codes Cryptogr. **3**, 127–134 (1993).
3. Blakley G.R.: Safeguarding cryptographic keys. Proc. Natl. Compd. Conf. **48**, 313–317 (1979).
4. Blakley E.F., Kabatianskii G.A.: Linear algebra approach to secret sharing schemes. Error Control, Cryptology, and Speech Compression LNCS **829**, 33–40 (1994).
5. Brickell E.F.: Some ideal secret sharing schemes. J. Comb. Math. Comb. Comp. **9**, 105–113 (1989).
6. Brickell E.F., Stinson D.R.: Some improved bounds on the information rate of perfect secret sharing schemes. J. Cryptol. **5**, 153–166 (1992).
7. Farràs O., Padrò C.: Ideal Hierarchical Secret Sharing Schemes, Theory of Cryptography, TCC 2010, LNCS 5978, 219–236 (2010).
8. Fuji-Hara R., Miao Y.: Ideal Secret Sharing Schemes, Yet Another Combinatorial Characterization, Certain Access Structures, and Related Geometric Problems (2008). https://infoshako.sk.tsukuba.ac.jp/~fujihara/ftp/sssOct.pdf.
9. Ghodosi H., Pieprzyk J., Safavi-Naini R.: Secret Sharing in Multilevel and Compartmented Groups, ACISP 1998: Information Security and Privacy. LNCS 1438, 367–378 (2006).
10. Giulietti M., Montanucci E.: On hyperfocused arcs in $PG(2, q)$. Discret. Math. **306**, 3307–3314 (2006).
11. Giulietti M., Vincenti R.: Three-level secret sharing schemes from the twisted cubic. Discret. Math. **310**, 3236–3240 (2010).
12. Jackson W.-A., Martin K.M., O'Keefe C.M.: Geometrical contributions to secret sharing theory. J. Geom. **79**, 102–133 (2004).
13. Korchmáros G., Lanzone V., Sonnino A.: Projective k-arcs and 2-level secret-sharing schemes. Des. Codes Cryptogr. **64**, 3–15 (2012).
14. Shamir A.: How to share a secret. Commun. ACM **22**, 612–613 (1979).
15. Shima K., Doi H.: A hierarchical secret sharing scheme over finite fields of characteristic 2. J. Inf. Process. **25**, 875–883 (2017).
16. Simmons G.: Sharply focused sets of lines on a conic in $PG(2, q)$. Congr. Numer. **73**, 181–204 (1989).
17. Tassa T.: Hierarchical Threshold Secret Sharing. Theory of Cryptography, TCC 2004. LNCS 2591, 473–490 (2004)
18. Tassa T., Dyn N.: Multipartite secret sharing by bivariate interpolation. J. Cryptol. **22**, 227–258 (2009).
19. Tentu A.N., Paul P., Vadlamudi C.V.: Conjunctive Hierarchical Secret Sharing Scheme Based on MDS Codes, IWOCA 2013: Combinatorial Algorithms. LNCS 8288, 463–467 (2013).
20. van Dijk M.: A linear construction of secret sharing schemes. Des. Codes Cryptogr. **12**, 161–201 (1997).
21. Wang X., Xiang C., Fu F.-W.: Secret sharing schemes for compartmented access structures. Cryptogr. Commun. **9**, 625–635 (2017).