On some generalizations of Shamir's secret sharing scheme

An extended abstract of PhD thesis

Aleksander Zabłocki

October 27, 2015

1 Secret sharing and our area of interest

Suppose that there is a confidential information (e.g. a piece of financial data) which we would like to make available for n persons $p_0, \ldots, p_{n-1}$ but only when a reasonably large group of them (say, a subset of size $\geqslant k$) decides to cooperate. A simple and efficient solution of Shamir [16] is to choose a prime power $q > n$ such that the secret can be encoded as an element S of the finite field $\mathbb{F}_q$, then randomly choose a polynomial $P(x)$ over $\mathbb{F}_q$ of degree $k-1$ such that $P(0) = S$, and finally equip each participant p_i with the value $P(x_i)$, where the *participants' identities* $x_i \in \mathbb{F}_q$ are pairwise distinct and non-zero. Then, each subset of k participants can recover S (by Lagrange interpolation), while any smaller set can obtain *no information* on S (in the sense of information theory).

More generally, *secret sharing* means distributing the knowledge of a *secret* among a set of *participants* by equipping them with pieces of partial information (called *shares*) in a way which realizes a given *access structure*, that is, allows to specify exactly which sets of participants shall be able to reconstruct the secret if they pool their shares together (such sets are called *authorized* in the access structure). In particular, Shamir's solution realizes the *k-threshold* access structure (authorized $\Leftrightarrow$ of size $\geqslant k$), which is very particular but most frequently needed in practice [9, Section 3.5]. Brickell [2] has proposed a more general construction, capable of handling a much broader range of access structures; the price paid for this is an increase of computational complexity, which, however, may be negligible in many applications.

Our research concentrates on an intermediate class between Shamir's and Brickell's schemes, proposed by Lai and Ding in [8], called *Lai-Ding's schemes* in [17]. Comparing to the Shamir's procedure described above, they introduce three modifications:

(i) dispersion of monomial degrees: P shall be now chosen among polynomials of the form $\sum_{j=0}^{k-1} a_j x^{c_j}$, where $\mathbf{c} = (c_0, \ldots, c_{k-1})$ is a fixed increasing sequence of non-negative integers, treated as a new (publicly known) parameter of the scheme;

(ii) shift of the secret: it shall be the coefficient a_i, where $0 \leqslant i \leqslant k-1$ is a new parameter of the scheme;

(iii) allowing that one of participants may have its identity x_j set to $0 \in \mathbb{F}_q$.

For further convenience, we will denote a concrete scheme of this form by $\Sigma_q^{LD}(\mathbf{c}, i)$. Note that Shamir's schemes correspond to the case $\mathbf{c} = (0, 1, \ldots, k-1)$ and $i = 0$ (with $x_j = 0$ forbidden).

Lai-Ding's schemes have been investigated in [8] and [17]; certain their special sub-cases are also studied in [7], [21], [13], [18] and [19]. Most of the prior research involves only a rather particular special subclass of Lai-Ding's schemes, called *Shamir's type schemes* in [19], in which $\mathbf{c} = (0, 1, \ldots, k-1)$ (that is, only modifications of type (ii) and (iii) are allowed).

2 Motivation and main goals

There are two main reasons for studying the intermediate classes described above. First, Shamir's type schemes can handle many examples of non-threshold access structures, as shown in [8] and [21], and Lai-Ding's schemes turn out to be even much more general, as we show in the thesis (see Section 6 below for more details). Second, even if we are not interested in sophisticated access structures, it might be valuable to design new schemes for realizing simpler ones; a potential value of such "duplicate" schemes is that some of them might turn out to satisfy additional desired properties, e.g. resistance to some kind of attacks. (For more examples of such "desired properties", see [20, Chapter 10] and [9, Section 3.4]). Since the field is still evolving, the list of such properties is likely to expand (particularly as non-standard applications of secret sharing are being proposed; see [1, p. 1]).

Within the above motivation, our primary objective is to answer several questions raised (and, sometimes partially, answered for Shamir's type schemes) in [17], [13], [18] and [19]. Some of these questions concern the range of possible access structures; however, most focus on quantitative analysis corresponding to the second aspect discussed above.

More precisely, the latter direction is focused on the notion of an *admissible* coalition of participants, which is understood in the simplest setting as a set C such that the restriction of the scheme to C (obtained by simply disregarding all other participants) is k-threshold. Following mainly [13] and [19], we focus on ensuring existence of sets of a given size n which satisfy (or do not satisfy) this condition, as well as providing asymptotic estimates for their total number.

In doing it, we will always consider the asymptotics with respect to q, for a fixed choice of $\mathbf{c}$, i, n (in the thesis, the potentially influential parameters are marked explicitly in the asymptotic notation). In particular, our existential criteria take the form of lower estimates for q (in terms of $\mathbf{c}$, i and n); here, we pay particular attention to their practical tractability. To enhance discussion, we distinguish three classes of such bounds:

- *sufficiently large* (*SL*) means any provably existing bound;

- *reasonably sufficiently large* (*RSL*) means any concrete bound which depends polynomially on n and c_{k-1} but possibly exponentially on k;
- *polynomially sufficiently large* (*PSL*) means that the dependence on k is also polynomial.

As already observed in [17], admissibility in Lai-Ding's schemes is algebraically described by *Schur polynomials*, best known from representation theory [5]. More precisely, admissibility of a set X is (usually) described by *non-vanishing* of a system of such polynomials on the elements of X; correspondingly, non-admissible sets correspond (indirectly) to their *zeroes*. This suggests that, in general, non-admissible sets are much harder to describe than the admissible ones. While this difference is not so evident for Shamir's type schemes (where all relevant Schur polynomials are *elementary symmetric polynomials*, for which describing zeroes is much simpler than in the general case), it becomes significant for general Lai-Ding's schemes. As a result, the connection between Lai-Ding's schemes and Schur polynomials ultimately leads to yet another, purely algebraic, branch of our research.

Below, we briefly describe our results in each of the main topics discussed above.

3 Admissible sets

Following [13], we study the behaviour of admissible sets of a given size $n \geqslant k-1$ in a given Lai-Ding's scheme over the field $\mathbb{F}_q$ having q elements, where q is an arbitrary prime power treated as a parameter of the scheme. We also denote the characteristic of $\mathbb{F}_q$ by p.

Given such input, the main problems considered in [13] are:

(A) For which q are there any admissible sets of size n?
(B) What is the asymptotics, with respect to q, of the number of such sets?
(C) Is there a procedure to build (almost) all such sets?

Also, assuming that the parameter $\mathbf{c}$ is fixed but i is varying, it has been asked:

(D) Can we answer the above questions for $\mathbf{c}$-*admissible* sets, i.e. sets which are simultaneously admissible for the given $\mathbf{c}$ and *every* $0 \leqslant i \leqslant k-1$?

For Shamir's type schemes, these questions have been answered in [13], as follows:

- Admissible sets of size n exist for q RSL, and their number is $\Theta(q^n)$;
- The same applies to $\mathbf{c}$-admissible sets (for fixed $\mathbf{c}$ and varying i).

In our results stated below, we show that both above claims generalize to all Lai-Ding's schemes. (To avoid technical details, we state them here in a simplified form).

Theorem 1. *Assume that $k \geqslant 2$, $0 \leqslant i < k$ and $n \geqslant k$. Then, the number of admissible sets in $\Sigma_q^{LD}(\mathbf{c}, i)$ of size n is $\Omega_{\mathbf{c},i}(q^n)$, and they exist whenever*

$$q > n - 1 + \tbinom{n-1}{k-1}\big(c_{k-1} - (k-1)\big) + \tbinom{n-1}{k-2}\big(c_{k-1} - (k-2)\big).$$

Theorem 2. *Assume that $k \geqslant 2$ and $n \geqslant k$. Then, the number of $\mathbf{c}$-admissible sets in $\Sigma_q^{LD}(\mathbf{c}, i)$ of size n is $\Omega_{\mathbf{c},i}(q^n)$, and they exist whenever*

$$q > n + \tbinom{n-1}{k-1}\big(c_{k-1} - c_0 - (k-1)\big) + k \cdot \tbinom{n-1}{k-2}\big(c_{k-1} - c_0 - (k-2)\big).$$

In fact, the proofs share the main idea with [13], which is ensuring existence of many simultaneous non-zeroes of a system of Schur polynomials. This part of the thesis, already published as a stand-alone paper [23], seems to be the simplest one.

4 Non-admissible sets

In [19] and [13], non-admissible sets in Shamir's type schemes are considered with regard to the above questions (A-C). We generalize this to Lai-Ding's schemes, although with restriction to the case $n = k - 1$. (As we explain in the thesis, this case seems to be the crucial starting point for understanding the situation for all $n \geqslant k - 1$; smaller values of n are probably much harder to handle).

The prior results for Shamir's type schemes show that, for arbitrary $n \geqslant k - 1$, the behaviour of the total number of non-admissible sets of size n (with respect to q) falls into one of two templates, depending on the value of i:

(T1) there are no non-admissible sets of size n with non-zero elements;
(T2) non-admissible sets of size n exist for q RSL, and their number is $\Theta(q^{n-1})$.

However, the situtation for general Lai-Ding's schemes is more complex, and involves at least two new templates. Actually, our results involve three scenarios:

(T2′) non-admissible sets of size n exist if q is RSL and in addition p is PSL;
under these assumptions, their number is $\Theta(q^{n-1})$;
(T2*) non-admissible sets of size n exist if q and p are SL;
under these assumptions, their number is $\Theta(q^{n-1})$;
(T3) the number of non-admissible sets of size n is either 0 or $\Theta(q^{n-1})$, depending on the residue of q modulo some positive integer, with both possibilities indeed taking place infinitely many times;
in particular, such sets exist if q is PSL *and in addition* yields a good residue.

The templates (T2′) and (T3) can be regarded as computationally tractable, unlike (T2*). On the other hand, while we can provide concrete examples for (T2′) and (T3) (showing in particular that (T2′) does not always reduce to (T2)); we do not know if there are any "really untractable" examples of (T2*), not satisfying (T2′) or some other reasonable strengthening. (See the Main Theorem below).

Recall that we restrict to the case $n = k - 1$. In this case, we classify *all* Lai-Ding's schemes into one of the above templates; moreover, with even more effort, we manage to rule out (T2*) in a broad range of cases by strengthening our knowledge to (T2′). For simplicity, we will present all these results in a unified statement; however, we need to precede it with several auxiliary definitions.

Definition. A sequence $\mathbf{c} = (c_0, \ldots, c_{k-1})$ is *step-coprime* if

$$\gcd(c_{i+1} - c_i,\, c_{i+2} - c_{i+1}) = 1 \qquad \text{for} \qquad 0 \leqslant i \leqslant k - 3.$$

Definition. A subset $A \subseteq \mathbb{N}$ is called *ultimately periodic* [10] if there exist $N \geqslant 0$, $k > 0$ and a set of residues $B \subseteq \{0, 1, \ldots, k-1\}$ such that

$$\forall_{n>N} \qquad \big(n \in A \quad \Leftrightarrow \quad n \bmod k \in B\big).$$

If in addition $0 < |B| < k$, we will call A *proper ultimately periodic*.

Denotation. For a sequence $\mathbf{c} = (c_0, \ldots, c_{k-1})$, we will denote

$$\hat{\mathbf{c}}_i = (c_0,\, c_1,\, \ldots,\, c_{i-1},\, c_{i+1},\, \ldots,\, c_{k-1}).$$

Main Theorem. *Let $k \geqslant 1$ and $0 \leqslant i < k$. Denote by $N_{\mathbf{c},i}(q)$ the number of non-admissible sets of size $k-1$ in $\Sigma_q^{LD}(\mathbf{c}, i)$, and by $B_{\mathbf{c},i}$ the set of all prime powers q for which $N_{\mathbf{c},i}(q) > 0$. Let $\widetilde{P}$ denote the set of all prime powers. Then, we have*

$$N_{\mathbf{c},i}(q) = \Theta(q^{k-2}) \qquad \textit{for} \quad q \in B_{\mathbf{c},i},$$

and moreover:

- ***(1)*** *If $k = 1$, then $B_{\mathbf{c},i} = \emptyset$;*
- ***(2)*** *If $c_i = 0$ and $k \geqslant 2$, then $B_{\mathbf{c},i}$ contains all prime powers greater than k;*
- ***(3)*** *If $c_i > 0$, $k \geqslant 2$, and $\hat{\mathbf{c}}_i$ is an arithmetic progression with common difference l, then, denoting by m the difference $c_i - c_j$ for an arbitrary $0 \leqslant j < k$ distinct from i, we have:*
  - ***(a)*** *If $l \mid m$, then $B_{\mathbf{c},i} = \emptyset$;*
  - ***(b)*** *If $2 \mid l$ and $2 \nmid m$, then $B_{\mathbf{c},i}$ contains all powers q of primes p such that*

    $$p > 2, \qquad\qquad q > k;$$

    on the other hand, there are infinitely many powers of 2 outside $B_{\mathbf{c},i}$;
  - ***(c)*** *In all other cases, $B_{\mathbf{c},i}$ is an intersection of $\widetilde{P}$ with a proper ultimately periodic set;*
- ***(4)*** *If $c_i > 0$, $k \geqslant 3$, $\hat{\mathbf{c}}_i$ is not arithmetic, and $\mathbf{c}$ is arithmetic with common difference λ, then $B_{\mathbf{c},i}$ contains powers q of primes p such that*

  $$p > 2, \qquad\qquad q > \max\big(10^{13}\big(\lambda \ln(2\lambda)\big)^5,\;\; 128\lambda^4 + \tfrac{1}{4}k^2\big);$$

- ***(5)*** *If $c_i > 0$, $k \geqslant 4$, $\hat{\mathbf{c}}_i$ is not arithmetic and it is step-coprime, then $B_{\mathbf{c},i}$ contains all powers q of primes p such that*

  $$p > c_{k-1} - c_0, \qquad\qquad q > 10^{10}k^3(D \ln D)^5, \qquad \textit{where} \quad D = \sum_{j=1}^{k-1}(c_j - c_0);$$

- ***(6)*** *In all other cases, $B_{\mathbf{c},i}$ contains all powers q of primes p such that p is sufficiently large.*

Note that the eight scenarios described above adhere, respectively, to

(T1), (T2), (T1), (T2′), (T3), (T2′), (T2′), (T2*).

In particular, (3b) and (3c) show that (T2′) and (T3) cannot be avoided in our classification. However, the question of necessity of (T2*) is left open.

Following some prior papers (e.g. [19]), we also analyze, though only within parts (1-4), the effect of restricting to non-zero participants' identities (i.e. revoking step (iii) of the definition of Lai-Ding's scheme). In this setting, (2) no longer holds; on the other hand, we show that the assumption $c_i > 0$ may be removed from (3) and (4).

The first two parts (1), (2) are simple, and follow respectively from Fact 2.18 and Corollary 4.3 in the thesis. The subsequent parts (3-6) require more effort, and appear in the thesis, respectively, as Theorems 4, 5, 8 and 6. As for (3), while its proof takes several pages, it is still elementary. For the three remaining parts, we use a deep theorem of Weil [22], in a flavour provided by Schmidt ([15], [14]):

Weil's Theorem ([22], [15], [14])**.** *Let q be a prime power, and $A \in \mathbb{F}_q[\mathbf{x}]$ be an absolutely irreducible polynomial of total degree $d > 0$. Denote by n the length of $\mathbf{x}$, and by $N_A(q)$ the number of zeroes of A in $\mathbb{F}_q^n$. Then, we have,*

$$N_A(q) = q^{n-1} + \Theta_d(q^{n-\frac{3}{2}}),$$

and moreover, the following concrete estimate from below holds:

$$N_A(q) \geqslant q^{n-1} - (d-1)(d-2)q^{n-\frac{3}{2}} - 6d^2q^{n-2} \qquad \text{for} \quad q > 10^{10}n^3(d\ln d)^5.$$

(Recall that a polynomial $A \in K[\mathbf{x}]$ is *absolutely irreducible* if it is irreducible as an element of $\overline{K}[\mathbf{x}]$, where $\overline{K}$ is the algebraic closure).

Proving part (4) of our Main Theorem requires applying Weil's Theorem in a very particular and relatively simple case. For (5) and (6), we use it in its full strength, which results in a reduction of the initial problem to verifying absolute irreducibility (and some coprimality properties) of Schur polynomials over finite fields. However, this verification turns out to require a laborous excursion into pure algebra, described below.

5 Irreducibility of Schur polynomials

To complete the proof of parts (5-6) of the Main Theorem, we need to understand how the corresponding Schur polynomials factor over the algebraic closure $\overline{\mathbb{F}_q}$. For our purposes, it is convenient to diverge from the standard notation of [4] or [5] and define Schur polynomials by the formula

$$S_{\mathbf{c}}(\mathbf{x}) = \frac{\det\left[x_i^{c_j}\right]_{0\leqslant i,j<k}}{\det\left[x_i^{j}\right]_{0\leqslant i,j<k}},$$

where $\mathbf{c} = (c_0, \ldots, c_{k-1})$ is an increasing sequence of non-negative integers, and $\mathbf{x} = (x_0, \ldots, x_{k-1})$ is a sequence of indeterminates of the same length. With this notation, properties of the scheme

$\Sigma_q^{LD}(\mathbf{c}, i)$ reduce to the properties of $S_{\mathbf{c}}$ and $S_{\hat{\mathbf{c}}_j}$ for $0 \leqslant j < k$. On the other hand, note that our $S_{\mathbf{c}}$ coincides with s_λ of [4] and S_λ of [5] provided that

$$\lambda = \big(c_{k-1} - (k-1),\, c_{k-2} - (k-2),\, \ldots,\, c_1 - 1,\, c_0\big).$$

Our primary goal is to find sufficient conditions for absolute irreducibility of these polynomials. If this fails, we also allow some non-absolutely-irreducible cases, in which we need to verify an additional coprimality property.

Although Schur polynomials are classical and widely studied, surprisingly little has been known on them in this regard. Even over the field $\mathbb{C}$ of complex numbers, the question of their irreducibility has been solved only recently, in [3] and independently in [12]. This knowledge can be projected to fields of finite (but rather huge) characteristics by standard means of elimination theory, which suffices to prove (6). However, the resulting bounds for q (and even for p) are far from being RSL, so (5) requires another approach.

In this direction, we obtain two results. First, we show that a theorem of [11] regarding the case $k = 3$ can be combined with an adjustment of fragments of the proof for the $\mathbb{C}$-based case from [12], leading to the following statement:

Theorem 7 (essentially by Monge [11] and Rajan [12])**.** *Let $k \geqslant 3$ and $\mathbf{c} = (c_0, \ldots, c_{k-1})$ be an increasing sequence of non-negative integers. Assume that $c_0 = 0$ and that $\mathbf{c}$ is step-coprime. Let p be a prime such that*

$$p \nmid c_{j+1} - c_j \quad \text{for } \ 0 \leqslant j \leqslant k-2, \qquad\qquad p \nmid c_{j+2} - c_j \quad \text{for } \ 0 \leqslant j \leqslant k-3$$

and let K be any field of characteristic p. Then, the Schur polynomial $S_{\mathbf{c}}(\mathbf{x}) \in K[\mathbf{x}]$ is either constant (if $\mathbf{c} = (0, 1, \ldots, k-1)$) or irreducible in $K[\mathbf{x}]$ (in the other case).

This result is new, but the proof uses known techniques. (However, it takes us some pages to use them properly and explain the details). Since the conditions on p stated above are satisfied for $p > c_{k-1} - c_0$, which is a bound of the PSL type, Theorem 7 leads to part (5) of our Main Theorem, though still not immediately.

As a second result, we show that, in the proof of Theorem 7, the (adjusted) arguments of [12] can be replaced with another, somewhat simpler reasoning, which enables proving irreducibility for a broad class of perturbations of Schur polynomials. This result is digressive, in that it does not tell anything new about Lai-Ding's schemes; nevertheless, it seems to be interesting from a purely algebraic viewpoint. Below, we state in a simplified form; even for this, we need a number of definitions.

Definition. Let $\mathbf{x} = (x_0, \ldots, x_{k-1})$ and $P(\mathbf{x}) = \sum_{\mathbf{s} \in \mathbb{Z}^k} a_{\mathbf{s}} \cdot \mathbf{x}^{\mathbf{s}}$, where $\mathbf{x}^{\mathbf{s}}$ denotes $\prod_{i=0}^{k-1} x_i^{s_i}$. Then, we define:

- the *Newton polytope* [6] of P as the convex hull (in $\mathbb{R}^k$) of the set $\{\mathbf{s} \in \mathbb{Z}^k \,|\, a_{\mathbf{s}} \neq 0\}$;
- the *maximal* (resp. *minimal*) *i-face* of P as the sum of all non-zero monomials $a_{\mathbf{s}} \cdot \mathbf{x}^{\mathbf{s}}$ appearing in P with the maximal (resp. minimal) possible value of s_i;

- an *iterated standard face of order l* as any polynomial F_l such that there are sequences

$$P = F_0, F_1, \ldots, F_l, \qquad i_1, i_2, \ldots, i_l$$

such that, for every $1 \leqslant j \leqslant l$, F_{j+1} is either maximal or minimal i_j-face of F_j, and moreover, the indices i_j are all pairwise distinct.

We note that these notions have a clear "geometric" interpretation (not to be confused with algebraic geometry) in the context of Newton polytopes.

Now, we are ready to our result, again, in a simplified version.

Theorem 7'. *Let* $\mathbf{c}$*,* i*,* p *and* K *satisfy all the assumptions of Theorem 7, and assume in addition that*

$$c_{j+1} - c_j > 1 \quad \text{for} \quad 1 \leqslant j \leqslant k-3. \tag{1}$$

Let P *be any polynomial in* $K[\mathbf{x}]$ *which agrees with* $S_{\mathbf{c}}$ *upon Newton polytope and all iterated standard faces of order* $k-3$*. Then,* P *is either constant (if* $\mathbf{c} = (0, 1, \ldots, k-1)$*) or irreducible in* $K[\mathbf{x}]$ *(in the other case).*

In the full statement given in the thesis, we consider all cases which can be handled by interchanging the proof of Theorem 7 and our new proof of the above claim. (This makes sense since both reasonings are inductive on k). As a result, a "trade" on the assumptions becomes possible: one can omit (1) for certain values of j, in exchange for requiring additionally that P agrees with $S_{\mathbf{c}}$ upon certain iterated standard faces of orders smaller than $k-3$. In particular, Theorem 7 can be obtained as another extreme case of this general picture (lift the whole (1) in exchange for decreasing the order from $k-3$ to 0).

6 Access structures

Apart from investigating (non-)admissible sets, the prior papers, particularly [18], provide some insight into the possible range of access structures realized by Shamir's type schemes. However, their results are far from giving a complete picture of such structures, which reflects the general difficulty of the problem. For general Lai-Ding's schemes, the task seems even more complex (due to the transition from elementary symmetric to general Schur polynomials), and we have only obtained preliminary results in two directions.

First, we prove that the class of *all* Lai-Ding's schemes is *almost* as general (with respect to realizable access structures) as that of Brickell's schemes. The precise meaning of *almost* depends on whether we allow *repeated identities* in Lai-Ding's schemes; while the prior defintions of [8] and [17] both forbid that, it seems potentially acceptable to consider such schemes as well, particularly as repeated identities are allowed by Brickell [2] in his class.

Theorem 9. *Let* Γ *be a Brickell access structure. Then:*

- *If the empty set* $\emptyset$ *is not authorized in* Γ*, then it can be realized by a Lai-Ding's scheme, possibly with repeated identities;*

- Γ *can be realized by a Lai-Ding's scheme without repeated identities if the following holds:* $\emptyset$ *is not authorized, and moreover, whenever two distinct participants* p_1, p_2 *are equipotent (i.e.* $C \cup \{p_1\}$ *is authorized if and only* $C \cup \{p_2\}$ *is, for every set* C*), then they must be nilpotent (i.e.* $C \cup \{p_1\}$ *is authorized if and only if* C *is).*

The assumptions of the second part, while complicated, seem to be fairly weak from a practical viewpoint; in typical applications, equipotent pairs of participants are likely either not to exist or to admit a simple unification.

Altogether, Theorem 9 might look appealing; however, from the practical viewpoint, it is rather an advertisement of Lai-Ding's schemes than a truly usable result, since our proof of Theorem 9 tends to produce Lai-Ding's schemes with exponentially growing sequences $\mathbf{c}$ even if the initial Brickell's scheme is fairly simple. Nevertheless, Theorem 9 seems to be valuable as a demonstration of diversity of Lai-Ding's access structures; in particular, by comparing with the results of [18], it follows that they are substantially more general than the Shamir's type access structures.

As a second direction, we investigate the access structures which may arise in the relatively simple cases considered in parts (3) and (4) of the Main Theorem, i.e. $\mathbf{c}$ or $\hat{\mathbf{c}}_i$ arithmetic. The first of these cases is similar to Shamir's type schemes, and we show that the results from [18] and [19] generalize there, with appropriate subtle modifications. Since the precise statement is rather lengthy, we refer the reader to Theorem 10 in the thesis.

The case of $\hat{\mathbf{c}}_i$ arithmetic is significantly different: unlike in Shamir's type schemes, there may exist authorized sets of size 2. On the other hand, at least for non-zero identities, all minimal authorized sets must be of size 2 or k, which substantially limits the range of access structures realizable by this class of schemes.

To achieve better understanding of those access structures, we model their "priviledged layers" by graphs, in which edges represent authorized sets of size 2. Then, it turns out that the graphs which can arise in this way can be exactly described:

Theorem. *Let* $\mathbf{c}$ *be an increasing sequence of non-negative integers of length* k *and* $0 \leqslant i < k$*. Assume that* $\hat{\mathbf{c}}_i$ *is arithmetic, and let* q *be a prime power. Let* $G_{\mathbf{c},i,q}$ *be the graph whose vertices are the participants of the Lai-Ding's scheme* $\Sigma_q^{LD}(\mathbf{c}, i)$*, and edges connect pairs of participants which form authorized sets of size* 2*. Then:*

- *(Lemma 6.17b) for every* $\mathbf{c}$*,* i*,* q *as above,* $G_{\mathbf{c},i,q}$ *is a difference of two graphs (sharing common vertex sets), each of which is a disjoint union of cliques;*
- *(Theorem 11, weakened) for every graph* G *as above, there exist some* $\mathbf{c}, i, q$ *as above such that* $G_{\mathbf{c},i,q}$ *is isomorphic to* G*.*

While this result has a much narrower scope than Theorem 9, it is valuable in that it provides a concrete and efficient construction of certain Lai-Ding's schemes which realize access structures not realizable by any Shamir's type scheme, including some of the *graphic structures* defined by [20].

References

[1] A. Beimel. Secret-sharing schemes: A survey. In YeowMeng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang, Huaxiong Wang, and Chaoping Xing, editors, *Coding and Cryptology*, volume 6639 of *Lecture Notes in Computer Science*, pages 11–46. Springer Berlin Heidelberg, 2011.

[2] E. F. Brickell. Some ideal secret sharing schemes. In Jean-Jacques Quisquater and Joos Vandewalle, editors, *Advances in Cryptology — EUROCRYPT '89*, volume 434 of *Lecture Notes in Computer Science*, pages 468–475. Springer Berlin Heidelberg, 1990.

[3] R. Dvornicich and U. Zannier. Newton functions generating symmetric fields and irreducibility of schur polynomials. *Advances in Mathematics*, 222(6):1982 – 2003, 2009.

[4] W. Fulton. *Young tableaux : with applications to representation theory and geometry.* London Mathematical Society student texts. Cambridge University Press, Cambridge, New York, 1997. Autres tirages : 1999.

[5] W. Fulton and J. Harris. *Representation Theory: A First Course.* Graduate Texts in Mathematics. Springer-Verlag, 1991.

[6] Sh. Gao. Absolute irreducibility of polynomials via Newton polytopes. *Journal of Algebra*, 237(2):501 – 520, 2001.

[7] N. Kogan and T. Tassa. Improved efficiency for revocation schemes via Newton interpolation. *ACM Transactions on Information and System Security*, 9(4):461–486, 2006.

[8] C.-P. Lai and C. Ding. Several generalizations of Shamir's secret sharing scheme. *International Journal of Foundations of Computer Science*, 15(2):445–458, 2004.

[9] K. M. Martin. *Discrete structures in the theory of secret sharing.* PhD thesis, University of London, 1991.

[10] A. B. Matos. Periodic sets of integers. *Theoretical Computer Science*, 127(2):287 – 312, 1994.

[11] M. Monge. Generation of the symmetric field by Newton polynomials in prime characteristic. *Rocky Mountain Journal of Mathematics*, 42(2):729–749, 2012.

[12] C. S. Rajan. On the irreducibility of irreducible characters of simple Lie algebras. *Transactions of the American Mathematical Society*, 366(12):6443–6481, 2014.

[13] A. Schinzel, S. Spież, and J. Urbanowicz. Admissible tracks in Shamir's scheme. *Finite Fields and Their Applications*, 16(6):449–462, 2010.

[14] W. M. Schmidt. A lower bound for the number of solutions of equations over finite fields. *Journal of Number Theory*, 6(6):448 – 480, 1974.

[15] W. M. Schmidt. *Equations Over Finite Fields: An Elementary Approach.* Springer Berlin Heidelberg, 1976.

[16] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[17] S. Spież, M. Srebrny, and J. Urbanowicz. Remarks on the classical threshold secret sharing schemes. *Fundamenta Informaticae*, 114(3-4):345–357, 2012.

[18] S. Spież, A. Timofeev, and J. Urbanowicz. Non-admissible tracks in Shamir's scheme. *Finite Fields and Their Applications*, 17(4):329 – 342, 2011.

[19] S. Spież, J. Urbanowicz, and A. Zabłocki. On constructing privileged coalitions in Shamir's type scheme. *Finite Fields and Their Applications*, 19(1):73–85, 2013.

[20] D. R. Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography*, 2:357–390, 1992.

[21] T. Tassa and J. L. Villar. On proper secrets, (t, k)-bases and linear codes. *Designs, Codes and Cryptography*, 52(2):129–154, 2009.

[22] A. Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent.* Actualités scientifiques et industrielles. 1041. Hermann & Cie, 1948.

[23] A. Zabłocki. Admissible tracks in Lai–Ding's secret sharing scheme. *Finite Fields and Their Applications*, 27:72 – 87, 2014.