Hierarchical Threshold Secret Sharing

Tamir Tassa*

December 6, 2006

Abstract

We consider the problem of threshold secret sharing in groups with hierarchical structure. In such settings, the secret is shared among a group of participants that is partitioned into levels. The access structure is then determined by a sequence of threshold requirements: a subset of participants is authorized if it has at least k_0 members from the highest level, as well as at least $k_1 > k_0$ members from the two highest levels and so forth. Such problems may occur in settings where the participants differ in their authority or level of confidence and the presence of higher level participants is imperative to allow the recovery of the common secret. Even though secret sharing in hierarchical groups has been studied extensively in the past, none of the existing solutions addresses the simple setting where, say, a bank transfer should be signed by three employees, at least one of whom *must* be a department manager. We present a perfect secret sharing scheme for this problem that, unlike most secret sharing schemes that are suitable for hierarchical structures, is ideal. As in Shamir's scheme, the secret is represented as the free coefficient of some polynomial. The novelty of our scheme is the usage of polynomial derivatives in order to generate lesser shares for participants of lower levels. Consequently, our scheme uses Birkhoff interpolation, i.e., the construction of a polynomial according to an unstructured set of point and derivative values. A substantial part of our discussion is dedicated to the question of how to assign identities to the participants from the underlying finite field so that the resulting Birkhoff interpolation problem will be well posed. In addition, we devise an ideal and efficient secret sharing scheme for the closely related hierarchical threshold access structures that were studied by Simmons and Brickell.

Keywords. Secret sharing schemes, threshold schemes, hierarchical/multilevel access structures, ideal schemes, Birkhoff interpolation.

*Division of Computer Science, The Open University, Ra'anana, Israel. E-mail: tamirta@openu.ac.il

1 Introduction

A (k, n)-threshold secret sharing is a method of sharing a secret among a given set of n participants, $\mathcal{U}$, such that every k of those participants ($k \leq n$) could recover the secret by pooling their shares together, while no subset of less than k participants can do so [5, 17]. Generalized secret sharing refers to situations where the collection of permissible subsets of $\mathcal{U}$ may be any collection $\Gamma \subseteq 2^{\mathcal{U}}$ having the monotonicity property, i.e., if $A \in \Gamma$ and $A \subset B \subseteq \mathcal{U}$ then $B \in \Gamma$. Given such a collection, the corresponding secret sharing scheme is a method of sharing a secret among the participants of $\mathcal{U}$ such that only subsets in Γ (that is referred to as *the access structure*) may recover the secret, while all other subsets cannot.

There are many real-life examples of threshold secret sharing. Typical examples include sharing a key to the central vault in a bank, the triggering mechanism for nuclear weapons, or key escrow. We would like to consider here a special kind of generalized secret sharing scenarios that is a natural extension of threshold secret sharing. In all of the above mentioned examples, it is natural to expect that the participants are not equal in their privileges or authorities. For example, in the bank scenario, the shares of the vault key may be distributed among bank employees, some of whom are tellers and some are department managers. The bank policy could require the presence of, say, 3 employees in opening the vault, but at least one of them must be a department manager. Or in key escrow, the dealer might demand that some escrow agents (say, family members) must be involved in any emergency access to his private files. Such settings call for special methods of secret sharing. To this end, we define hierarchical secret sharing as follows:

Definition 1.1 *Let $\mathcal{U}$ be a set of n participants and assume that $\mathcal{U}$ is composed of levels, i.e., $\mathcal{U} = \bigcup_{i=0}^{m} \mathcal{U}_i$ where $\mathcal{U}_i \cap \mathcal{U}_j = \emptyset$ for all $0 \leq i < j \leq m$. Let $\mathbf{k} = \{k_i\}_{i=0}^{m}$ be a monotonically increasing sequence of integers, $0 < k_0 < \cdots < k_m$. Then the $(\mathbf{k}, n)$–hierarchical threshold access structure is*

$$\Gamma = \left\{ \mathcal{V} \subset \mathcal{U} : \left| \mathcal{V} \cap \left(\cup_{j=0}^{i} \mathcal{U}_j \right) \right| \geq k_i \quad \forall i \in \{0, 1, \ldots, m\} \right\} \ . \tag{1}$$

A corresponding $(\mathbf{k}, n)$–hierarchical threshold secret sharing scheme is a scheme that realizes this access structure; namely, a method of assigning each participant $u \in \mathcal{U}$ a share $\sigma(u)$ of a given secret S such that authorized subsets $\mathcal{V} \in \Gamma$ may recover the secret from the shares possessed by their participants, $\sigma(\mathcal{V}) = \{\sigma(u) : u \in \mathcal{V}\}$, while the shares of unauthorized subsets $\mathcal{V} \notin \Gamma$ do not reveal any information about the value of the secret. Viewing the secret S as a random variable that takes values in a finite domain $\mathcal{S}$, these two requirements may be stated as follows:

$$H(S|\sigma(\mathcal{V})) = 0 \quad \forall \mathcal{V} \in \Gamma \qquad \textit{(accessibility)} \tag{2}$$

and

$$H(S|\sigma(\mathcal{V})) = H(S) \quad \forall \mathcal{V} \notin \Gamma \ . \qquad \textit{(perfect security)} \tag{3}$$

Letting Σ_u denote the set of possible shares for participant $u \in \mathcal{U}$, the information rate of the scheme is

$$\rho = \min_{u \in \mathcal{U}} \frac{\log_2 |\mathcal{S}|}{\log_2 |\Sigma_u|} \ .$$

If $\rho = 1$, the scheme is called ideal.

The zero conditional entropy equality (2) should be understood in a constructive sense. Namely, if it holds then $\mathcal{V}$ may compute S. Also note that conditions (2)+(3) imply that the information

rate is bounded from above by 1; hence, $\rho = 1$ represents the ideal situation (all shares are of the minimal possible size, namely, the size of the secret).

Ito, Saito and Nishizeki [12] were the first to study secret sharing for general access structures. They provided constructions illustrating that any monotone access structure can be realized by a perfect secret sharing scheme. Their construction was simplified and extended by Benaloh and Leichter [3]. Those constructions are based on monotone formulas that realize the characteristic function of the access structure (namely, the function $f : \{0,1\}^n \to \{0,1\}$ such that $f(x_1, \ldots, x_n) = 1$ if and only if the subset $\mathcal{V} \subseteq \mathcal{U}$ that corresponds to $\{1 \leq i \leq n : x_i = 1\}$ is in Γ). However, for threshold access structures the resulting schemes are far from being ideal. Even for the simplest threshold problem of only one level (i.e., all participants are equal), an optimal formula is of size $O(n \log n)$ [10], which implies an information rate of $O(1/\log n)$ for the corresponding secret sharing scheme.

Using the monotone formula construction with threshold gates, where each threshold gate is realized by Shamir's threshold secret sharing scheme, we arrive at the following solution to the problem [22]: The secret is an element of a finite field, $S \in \mathbb{F}$; the dealer generates m random and independent secrets $S_i \in \mathbb{F}$, $1 \leq i \leq m$, and defines $S_0 = S - \sum_{i=1}^{m} S_i$. Then, for every $0 \leq i \leq m$, the dealer distributes the secret S_i among all participants of $\cup_{j=0}^{i} \mathcal{U}_j$ using Shamir's $(k_i, \sum_{j=0}^{i} |\mathcal{U}_j|)$-threshold secret sharing scheme. The secret S may be recovered only if all S_i, $0 \leq i \leq m$, are recovered. As the recovery of S_i requires the presence of at least k_i participants from $\cup_{j=0}^{i} \mathcal{U}_j$, the access requirements are met by this scheme. This scheme is perfect since if $\mathcal{V} \notin \Gamma$, it fails to satisfy at least one of the threshold conditions in (1) and, consequently, it is unable to learn a thing about the corresponding share S_i; such a deficiency implies (3). However, this scheme is not ideal: its information rate is $1/(m+1)$ since the shares of participants from $\mathcal{U}_0$ are composed of $m+1$ field elements.

In this paper, we present a simple solution for the hierarchical secret sharing problem that is both perfect and ideal. Our construction is a realization of the general vector space construction of Brickell [6]. The idea of Brickell was as follows: Let $\mathbb{F}$ be a finite field such that $S \in \mathbb{F}$ and let $\mathbb{F}^d$ be the d-dimensional vector space over that field, for some integer d. Assume that there exists a function $\phi : \mathcal{U} \to \mathbb{F}^d$ with the property

$$(1, 0, \ldots, 0) \in \text{Span}\{\phi(u) : u \in \mathcal{V}\} \Leftrightarrow \mathcal{V} \in \Gamma \ . \tag{4}$$

Then the dealer selects random and independent values $a_i \in \mathbb{F}$, $2 \leq i \leq d$, and then

$$\sigma(u) = \phi(u) \cdot \mathbf{a} \quad \text{where} \quad \mathbf{a} = (S, a_2, \ldots, a_d) \ . \tag{5}$$

This scheme is perfect and ideal (in general linear secret sharing schemes, or monotone span programs [13], ϕ may assign more than one vector to each participant). The main problem is of-course finding a mapping ϕ that satisfies condition (4). We find herein a proper mapping ϕ for the case of hierarchical threshold secret sharing. Our idea is based on *Birkhoff interpolation* (also known as *Hermite-Birkhoff* or *lacunary interpolation*). The basic threshold secret sharing of Shamir [17] was based upon Lagrange interpolation, namely, the construction of a polynomial of degree less than or equal to k from its values in $k+1$ distinct points. There are two other types of interpolation that are encountered in numerical analysis. In such problems, one is given data of the form

$$\frac{d^j P}{dx^j}(x_i) := P^{(j)}(x_i) = c_{i,j} \qquad (k+1 \text{ equations}) \tag{6}$$

and seeks a polynomial of degree less than or equal to k that agrees with the given data (6). If for each i (namely, at each interpolation point) the sequence of the derivative orders j that are given by (6) is an unbroken sequence that starts at zero, $j = 0, \ldots, j_i$, then the problem falls under the framework of *Hermite interpolation*. In that case the problem always admits a unique solution P. The more general case is when the data is lacunary in the sense that, at some sample points, the sequence of orders of derivatives is either broken or does not start from $j = 0$. This case is referred to as *Birkhoff interpolation* and it differs radically from the more standard Hermite or Lagrange interpolation. In particular, Birkhoff interpolation problems may be ill posed in the sense that a solution may not exist or may not be unique.

In our method, like in Shamir's, the secret is the free coefficient of some polynomial $P(x) \in \mathbb{F}_{k-1}[x]$, where $\mathbb{F}$ is a large finite field and $k = k_m$ is the maximal threshold, i.e., the total number of participants that need to collaborate in order to reconstruct the secret. Each participant $u \in \mathcal{U}$ is given an identity in the field, denoted also by u, and a share that equals $P^{(j)}(u)$ for some derivative order j that depends on the position of u in the hierarchy. The idea is that the more important participants (namely, participants who belong to levels with lower index) will get shares with lower derivative orders, since lower derivatives carry more information than higher derivatives. By choosing the derivative orders properly, we are able to meet the threshold access requirements (1). As a consequence, when an authorized subset collaborates and attempts to recover the secret, they need to solve a Birkhoff interpolation problem. Hence, a great part of our analysis is devoted to the question of how to assign participants with identities in the field so that, on one hand, the Birkhoff interpolation problems that are associated with the authorized subsets would be well posed, and, on the other hand, the Birkhoff interpolation problems that are associated with unauthorized subsets do not leak any information on the secret.

1.1 Related work

The problem of secret sharing in hierarchical (or *multilevel*) structures, was studied before under different assumptions, e.g. [4, 6, 7, 8, 18, 19]. Already Shamir, in his seminal work [17], has recognized that in some settings it would be desired to grant different capabilities to different participants according to their level of authority. He suggested to accomplish that by giving the participants of the more capable levels a greater number of shares. More precisely, if $\mathcal{U}$ has an hierarchical structure as in Definition 1.1, the participants in $\mathcal{U}_i$, $0 \leq i \leq m$, get w_i shares of the form $(u, P(u))$, $u \in \mathbb{F}$, where $w_0 > w_1 > \cdots > w_m$, whence the information rate of the scheme is $1/w_0$. This way, the number of participants from a higher level that would be required in order to reconstruct the secret would be smaller than the number of participants from a lower level that would need to cooperate towards that end.

Simmons [18], and later Brickell [6], considered another hierarchical setting. Assume a scenario where an electronic fund transfer (up to some maximum amount) may be authorized by any two vice presidents of a bank, or, alternatively, by any three senior tellers. A natural requirement in such a scenario is that also a mixed group of one vice president and two senior tellers could recover the private key that is necessary to sign and authorize such a transfer. Motivated by this example, Simmons studied a general hierarchical threshold secret sharing problem that agrees with the problem in Definition 1.1 with one difference: while we require in (1) a *conjunction* of threshold conditions, Simmons studied the problem with a *disjunction* of the threshold conditions. Namely,

in his version of the problem,

$$\Gamma = \left\{ \mathcal{V} \subset \mathcal{U} : \exists i \in \{0, 1, \ldots, m\} \text{ for which } \left| \mathcal{V} \cap \left(\cup_{j=0}^{i} \mathcal{U}_j \right) \right| \geq k_i \right\} \ . \tag{7}$$

His solution to that version is based on a geometric construction that was presented by Blakley [5]. Assume that the secret S is d-dimensional (typically $d = 1$; however, Simmon's construction may easily deal with the simultaneous sharing of $d > 1$ secrets as well). Then the construction is embedded in $\mathbb{F}^r$, where $\mathbb{F}$ is a large finite field and $r = k_m + d - 1$. Simmons suggested to construct a chain of affine subspaces $\mathcal{W}_0 \subset \mathcal{W}_1 \subset \cdots \subset \mathcal{W}_m$ of dimensions $k_i - 1$, $0 \leq i \leq m$, together with a publicly known affine subspace $\mathcal{W}_{\mathcal{S}}$ of dimension d, with the property that $\mathcal{W}_i \cap \mathcal{W}_{\mathcal{S}} = \{S\}$ for all $0 \leq i \leq m$ (i.e., each $\mathcal{W}_i$ intersects $\mathcal{W}_{\mathcal{S}}$ in a single point whose d coordinates in $\mathcal{W}_{\mathcal{S}}$ are the d components of the secret S). Then, each participant from level $\mathcal{U}_i$ gets a point in $\mathcal{W}_i \setminus \mathcal{W}_{i-1}$, $0 \leq i \leq m$ ($\mathcal{W}_{-1} = \emptyset$), such that every k_i points from $\cup_{j=0}^{i} \mathcal{U}_j$ span the entire subspace $\mathcal{W}_i$. Hence, if a subset of participants $\mathcal{V}$ satisfies at least *one* of the threshold conditions, say, $\left| \mathcal{V} \cap \left(\cup_{j=0}^{i} \mathcal{U}_j \right) \right| \geq k_i$ for some i, $0 \leq i \leq m$, then the corresponding $\mathcal{W}_i$ may be constructed and intersected with $\mathcal{W}_{\mathcal{S}}$ to yield the secret S. The information rate of the scheme, assuming the typical setting in which $d = 1$, is $1/k_m$ since the shares of the participants from $\mathcal{U}_m$ are points in $\mathbb{F}^{k_m}$. It should be also noted that the selected points must be in general position, and the verification of that may have an exponential cost.

Brickell [6] offered two schemes for the same problem, both ideal. The first one suffers from the same problem as Simmons', in the sense that the dealer is required to check (possibly exponentially) many matrices for non-singularity. In the second scheme this difficulty is replaced by the need to find an algebraic number of some degree over a prime order field. More specifically, if q is a prime number such that $q > \max_{0 \leq i \leq m} |\mathcal{U}_i|$ the dealer has to find $\alpha \in \mathbb{F}_q$ that satisfies an irreducible polynomial over $\mathbb{F}_q$ of degree $m \cdot k_m^2$.

Shamir's version of the hierarchical setting is slightly more relaxed than Simmons' and Brickell's. In the former, the number of participants that are required for recovery is determined by a *weighted average* of the thresholds that are associated with each of the levels that are represented in the subset of participants. In the latter, the necessary number of participants is the *highest* of the thresholds that are associated with the levels that are represented. However, it is natural to expect that more rigid conditions will be imposed in some scenarios. Namely, even though higher level (i.e., important) participants could be replaced by lower level ones, a minimal number of higher level participants would still need to be involved in any recovery of the secret. For example, the common practice of authorizing electronic fund transfers does call for the presence of at least one vice president or manager department. The above described solutions of Shamir and Simmons are incapable of imposing such restrictions since they allow the recovery of the secret for any subset of lower-level participants that is sufficiently large. This difference in the definition of the problem is manifested by the replacement of the existential quantifier $\exists$ in (7) with the universal quantifier $\forall$ in (1).

We proceed to examine the interrelation between the three above mentioned types of access structures. Fixing $\mathcal{U}$, the set of participants, we let $WTAS$ denote the class of all weighted threshold access structures of Shamir's type on $\mathcal{U}$, $HTAS_{\exists}$ denote the class of all hierarchical threshold access structures of the type that Simmons and Brickell studied, and $HTAS_{\forall}$ denote the class of all hierarchical threshold access structures of the type that we introduce and study herein. We note that

$$WTAS, HTAS_{\exists}, HTAS_{\forall} \subset 2^{2^{\mathcal{U}}} \ .$$

The intersection of those three classes is the class of basic threshold access structures (namely, $WTAS$ with equal weights, or $HTAS$ of either kind with only one level in the hierarchy). Since all minimal subsets of a $HTAS_\forall$ access structure are of the same size while this is not true for a $HTAS_\exists$ access structure (of more than one level), we deduce that there is no inclusion between those two classes. The results of this paper and of [2] imply that there is also no inclusion between $WTAS$ and the two hierarchical threshold classes (the fact that $WTAS \setminus HTAS_\exists \neq \emptyset$ and $WTAS \setminus HTAS_\forall \neq \emptyset$ stems from the fact that there are $WTAS$ access structures that are not ideal, while, as shown herein, all access structures of either $HTAS_\exists$ or $HTAS_\forall$ are ideal; the fact that $HTAS_\exists$ and $HTAS_\forall$ are not sub-classes of $WTAS$ stems from the characterization of all ideal $WTAS$ access structures that is given in [2]).

If Γ is a monotone access structure over $\mathcal{U}$, its dual is defined by $\Gamma^* = \{\mathcal{V} : \mathcal{V}^c \notin \Gamma\}$. It is easy to see that the two types of hierarchical threshold access structures, $HTAS_\exists$ and $HTAS_\forall$, are dual in that sense. In view of a result due to Gal [11], if an access structure Γ may be realized by an ideal secret sharing scheme, so can its dual Γ^*. Therefore, the ideality of the access structures that we study herein, (1), follows from the ideality of the access structures (7), as established in [6], combined with the above mentioned duality result. The schemes that we offer herein for realizing (1) are different from the schemes that one would get from combining the techniques presented in [6] and [11], and they rely upon different ideas. Moreover, they have an explicit and simple closed form (as opposed to the schemes that are implied by [6, 11]), they do not present some of the difficulties that appear in Brickell's schemes (namely, needing to check possibly exponentially many matrices for non-singularity or to find algebraic numbers of certain degrees over a finite field), and, in typical settings, they require slightly smaller field sizes (see the concluding remark of Section 4 for a detailed discussion of this issue).

Padró and Sáez [15] studied the information rate of secret sharing schemes with a bipartite access structure. A bipartite access structure is one in which there are two subsets of participants, $\mathcal{U} = \mathcal{U}_0 \cup \mathcal{U}_1$, and all participants in the same subset play an equivalent role in the structure. They showed that the ideal bipartite access structures are exactly those that are vector space access structures, namely, those which are consistent with Brickell's construction [6]. Furthermore, they showed that all such ideal access structures are quasi-threshold in the sense that a subset $\mathcal{V} \subset \mathcal{U}$ is authorized if $|\mathcal{V}|$, $|\mathcal{V} \cap \mathcal{U}_0|$ and $|\mathcal{V} \cap \mathcal{U}_1|$ satisfy some threshold conditions [15, Theorem 5]. They characterized four types of quasi-threshold access structures, denoted Ω_i, $1 \leq i \leq 4$. It may be shown that when there are two levels, i.e., $m = 1$, our *conjunctive* threshold access structures, (1), fall under types Ω_2, Ω_3 and Ω_4, while Simmons' *disjunctive* threshold access structures, (7), fall under type Ω_1. What we show in this paper is that in the multipartite case, the conjunctive threshold access structures, as well as their disjunctive counterpart, are vector space access structures and that Birkhoff interpolation yields an explicit construction.

We conclude this survey with a recent paper by Tassa and Dyn [21]. That paper studies three types of multipartite access structures and introduces ideal perfect secret sharing schemes for these types of access structures that are based on bivariate interpolation. One of these families is the family of hierarchical threshold access structures that are the subject of the present paper, and they are realized there by bivariate Lagrange interpolation with data on lines in general position. Hence, while in the present study the desired hierarchy between the different levels is achieved by using polynomial derivatives and Birkhoff interpolation, the schemes in [21] show that the same hierarchical effect may be obtained by introducing a second dimension.

1.2 Organization of the paper

In Section 2 we review the basic terminology and results from the theory of Birkhoff interpolation [14]. We present those results in the context of the reals, $\mathbb{R}$, which is the natural context in numerical analysis. However, as $\mathbb{R}$ is not the field of choice in cryptography, one should be very careful when borrowing results from such a theory and migrating them to the context of finite fields. The algebraic statements usually travel well and survive the migration; the analytic ones, however, might not. Part of our analysis will be dedicated to those issues. Section 3 is devoted to our scheme. After presenting the scheme, we discuss in Section 3.1 conditions for accessibility, (2), and perfect security, (3). Then, we proceed to examine strategies for allocating participant identities in the underlying finite field so that accessibility and perfect security are achieved. In Section 3.2 we consider the strategy of random allocation of participant identities and prove that such a strategy guarantees that both (2) and (3) hold with almost certainty. In Section 3.3 we consider a simple monotone allocation of participant identities. Borrowing an interesting result from the theory of Birkhoff interpolation, we prove that such an allocation is guaranteed to provide both accessibility and perfect security, (2)+(3), provided that the prime order of the field is sufficiently large with respect to n (number of participants) and k_m (minimal number of participants in an authorized subset), Theorem 3.6. In order to illustrate the discussion in Section 3.3, we list in Appendix A all possible scenarios when $k_m \leq 4$. In Section 4 we turn our attention to the closely related hierarchical threshold access structures that were studied by Simmons [18] and Brickell [6]. Relying on a duality result from the theory of monotone span programs, we show how the ideality of those access structures follows from the ideality of the conjunctive threshold access structures. We then show how the schemes that we proposed for the conjunctive hierarchical threshold access structures may be modified in order to be suitable for hierarchical threshold access structures of the disjunctive type. Finally, in Section 5 we describe two closely related open problems.

A preliminary version of this paper appeared in [20].

2 Birkhoff interpolation

Let

- $X = \{x_1, \ldots, x_k\}$ be a given set of points in $\mathbb{R}$, where $x_1 < x_2 < \cdots < x_k$;
- $E = (e_{i,j})_{i=1}^{k}{}_{j=0}^{\ell}$ be a matrix with binary entries, $I(E) = \{(i,j) : e_{i,j} = 1\}$ and $d = |I(E)|$ (we assume hereinafter that the right-most column in E is nonzero);
- $C = \{c_{i,j} : (i,j) \in I(E)\}$ be a set of d real values.

Then the Birkhoff interpolation problem that corresponds to the triplet $\langle X, E, C \rangle$ is the problem of finding a polynomial $P(x) \in \mathbb{R}_{d-1}[x]$ that satisfies the d equalities

$$P^{(j)}(x_i) = c_{i,j} \quad , \quad (i,j) \in I(E) \ . \tag{8}$$

The matrix E is called the *interpolation matrix*.

Lagrange and Hermite interpolations may be viewed as special cases of Birkhoff interpolation: the interpolation matrix in Lagrange interpolation has only one column (since all data corresponds to the zeroth order derivative), while Hermite interpolation matrices are those in which each row

(that stands for an interpolation point x_i) begins with 1s, followed by 0s (namely, the sequence of given values at that point is of the form $P^{(j)}(x)$, $0 \leq j \leq j_i$, for some $j_i \geq 0$). Unlike Lagrange or Hermite interpolation that are unconditionally well-posed, the Birkhoff interpolation problem may not admit a unique solution. The system of equations (8) translates into a square linear system of equations $A\vec{x} = \vec{b}$ where the vector of unknowns $\vec{x}$ consists of the coefficients of the requested polynomial P, the matrix A is determined by X and E, and the right hand side $\vec{b}$ consists of the data in C. The pair $\langle X, E\rangle$ is called *regular* if the resulting matrix A is regular, so that the system (8) has a unique solution for any choice of C, while otherwise it is called *singular*. The matrix E is called *regular* or *poised* if $\langle X, E\rangle$ is regular for all $X = \{x_1 < x_2 < \cdots < x_k\} \subset \mathbb{R}$.

The following lemma provides a simple necessary condition that E must satisfy, lest $\langle X, E\rangle$ would be singular for *all* X [16].

Lemma 2.1 *(Pólya's condition) A necessary condition that the interpolation matrix E must satisfy in order for the corresponding Birkhoff interpolation problem to be well posed is that for each $0 \leq t \leq \ell$, ℓ being the highest derivative order in the data, there are given at least $t+1$ values of derivatives of P of order less than or equal to t; i.e.,*

$$|\{(i,j) \in I(E) \ : \ j \leq t\}| \geq t+1 \quad , \quad 0 \leq t \leq \ell \ . \tag{9}$$

Proof. Let $P(x) = \sum_{s=0}^{d-1} a_s x^s$ be the unknown interpolant. Assume that condition (9) fails to hold for some $0 \leq t \leq \ell$. Concentrating on the equations in (8) that correspond to the pairs $(i,j) \in I(E)$ where $j \leq t$, we note that these are the only equations in (8) that involve one of the first $t+1$ unknowns, a_s, $0 \leq s \leq t$ (indeed, all other equations in (8) correspond to derivative orders that are higher than t and, consequently, they do not involve those unknowns). Hence, the restriction of the linear system in $(a_0, \ldots, a_{d-1})$ to a system in $(a_0, \ldots, a_t)$ yields a system where the number of equations is smaller than the number of unknowns. Such systems are singular. □

Pólya's is a necessary condition. *Sufficient* conditions, on the other hand, are scarce. We continue to describe one such condition that will serve us later on in our application to secret sharing. To this end we define the following.

Definition 2.1 *A 1-sequence in the interpolation matrix E is a maximal run of consecutive 1s in a row of the matrix E; namely, it is a triplet of the form (i, j_0, j_1) where $1 \leq i \leq k$, $0 \leq j_0 \leq j_1 \leq \ell$, such that $e_{i,j} = 1$ for all $j_0 \leq j \leq j_1$ while $e_{i,j_0-1} = e_{i,j_1+1} = 0$ (letting $e_{i,-1} = e_{i,\ell+1} = 0$). A 1-sequence (i, j_0, j_1) is called supported if E has 1s both to the northwest and southwest of the leading entry in the sequence; i.e., there exist $i_{nw} < i$, $i_{sw} > i$ and $j_{nw}, j_{sw} < j_0$ such that $e_{i_{nw},j_{nw}} = e_{i_{sw},j_{sw}} = 1$.*

The following theorem was first proved by K. Atkinson and A. Sharma [1].

Theorem 2.2 *Assume that $x_1 < x_2 < \cdots < x_k$. Then the interpolation problem (8) has a unique solution if the interpolation matrix E satisfies Pólya's condition and contains no supported 1-sequences of odd length.*

Lemma 2.1, being algebraic, is not restricted to the reals and applies over any field. Theorem 2.2, on the other hand, is more problematic. It relies upon the existence of *order* in $\mathbb{R}$ (that theorem is, in fact, a consequence of Rolle's theorem). Hence, as finite fields are not ordered and have no equivalent to Rolle's theorem, Theorem 2.2 does not apply to them. As a counter example, consider

the interpolation problem with $X = \{1, 2, 4\}$ and

$$E = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} . \tag{10}$$

Namely, we seek a polynomial $P(x) = a_2x^2 + a_1x + a_0$ that satisfies

$$P(1) = c_{1,0} \quad , \quad P(2) = c_{2,0} \quad , \quad P'(4) = c_{3,1} .$$

The corresponding system of linear equations in the unknowns (a_0, a_1, a_2) has the following matrix of coefficients:

$$A_{\langle X,E\rangle} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 0 & 1 & 8 \end{pmatrix} . \tag{11}$$

It is easy to see that E, (10), satisfies the conditions of Theorem 2.2 and, indeed, $\det(A_{\langle X,E\rangle}) = 5 \neq 0$. However, if we consider the same problem over the field $\mathbb{F}_5$, (11) becomes singular.

Despite this problem, Theorem 2.2 will be of use if we impose further restrictions on the set of points in X. This will be dealt with in Section 3.3.

3 An ideal hierarchical secret sharing scheme

Consider the hierarchical secret sharing problem $(\mathbf{k}, n)$, $\mathbf{k} = \{k_i\}_{i=0}^{m}$, as defined in Definition 1.1. Let $\mathbb{F}$ be a finite field of size q which is at least as large as the number of possible secrets. Let $k = k_m$ be the overall number of participants that are required for recovery of the secret. Then:

1. The dealer selects a random polynomial $P(x) \in \mathbb{F}_{k-1}[x]$, where

$$P(x) = \sum_{i=0}^{k-1} a_i x^i \quad \text{and} \quad a_0 = S . \tag{12}$$

2. The dealer identifies each participant $u \in \mathcal{U}$ with a field element. For simplicity, the field element that corresponds to $u \in \mathcal{U}$ will be also denoted by u (whence $\mathcal{U}$ may be viewed as a subset of $\mathbb{F}$).

3. The dealer distributes shares to all participants in the following manner: Each participant of the ith level in the hierarchy, $u \in \mathcal{U}_i$, $0 \leq i \leq m$, receives the share $P^{(k_{i-1})}(u)$, i.e., the (k_{i-1})th derivative of $P(x)$ at $x = u$, where $k_{-1} = 0$. (A reminder: given a polynomial $P(x) = \sum_{i=0}^{k-1} a_i x^i$ over any field $\mathbb{F}$, its derivative is defined formally as $P'(x) = \sum_{i=0}^{k-1} i a_i x^{i-1}$.)

For example, assume that there are three levels in the hierarchy, $\mathcal{U} = \mathcal{U}_0 \cup \mathcal{U}_1 \cup \mathcal{U}_2$, and that the thresholds are $\mathbf{k} = (k_0, k_1, k_2) = (2, 4, 7)$; namely, $\mathcal{V} \subset \mathcal{U}$ is authorized if and only if it has at least 7 participants, of whom at least 4 are from $\mathcal{U}_0 \cup \mathcal{U}_1$, of whom at least 2 are from $\mathcal{U}_0$. Then, as $k = k_2 = 7$ in this example, the dealer selects a random polynomial of degree 6, $P(x) = \sum_{i=0}^{6} a_i x^i$, where $a_0 = S$. He then distributes the shares as follows: participants $u \in \mathcal{U}_0$ will get the share $P(u)$ (namely, the value of P at the field element that identifies the corresponding participant);

participants $u \in \mathcal{U}_1$ will get the share $P''(u)$, since $k_0 = 2$; and those of the lowest level, $\mathcal{U}_2$, will get $P^{(4)}(u)$, since $k_1 = 4$.

This scheme is of-course ideal, as every participant receives a share that is a field element, just like the secret. Note that Shamir's secret sharing scheme [17] is a special case of our scheme since in that case all users belong to the same level (i.e., $\mathcal{U} = \mathcal{U}_0$) and, consequently, there are no derivatives and all users get shares of the form $P(u)$.

3.1 Conditions for accessibility and perfect security

The main questions that arise with regard to the scheme are whether it complies with conditions (2) and (3). Let $\mathcal{V} = \{v_1, \ldots, v_{|\mathcal{V}|}\} \subset \mathcal{U}$ and assume that

$$\begin{array}{c} v_1, \ldots, v_{\ell_0} \in \mathcal{U}_0 \\ v_{\ell_0+1}, \ldots, v_{\ell_1} \in \mathcal{U}_1 \\ \vdots \\ v_{\ell_{m-1}+1}, \ldots, v_{\ell_m} \in \mathcal{U}_m \end{array} \qquad \text{where} \quad 0 \le \ell_0 \le \cdots \le \ell_m = |\mathcal{V}| \ . \tag{13}$$

$\mathcal{V}$ is authorized if and only if $\ell_i \ge k_i$ for all $0 \le i \le m$. Let $\mathbf{r} : \mathbb{F} \to \mathbb{F}^k$ be defined as $\mathbf{r}(x) = (1, x, x^2, \ldots, x^{k-1})$ and, for all $i \ge 0$, let $\mathbf{r}^{(i)}(x)$ denote the ith derivative of that vector. Using this notation, we observe that the share that is distributed to participants $u \in \mathcal{U}_i$ is $\sigma(u) = \mathbf{r}^{(k_{i-1})}(u) \cdot \mathbf{a}$ where $\mathbf{a} = (a_0 = S, a_1, \ldots, a_{k-1})$ is the vector of coefficients of $P(x)$. Hence, when all participants of $\mathcal{V}$, (13), pool together their shares, the system that they need to solve in the unknown vector $\mathbf{a}$ is $M_{\mathcal{V}}\mathbf{a} = \boldsymbol{\sigma}$, where the coefficient matrix is (written by its rows),

$$M_{\mathcal{V}} = \Big(\mathbf{r}(v_1), \ldots, \mathbf{r}(v_{\ell_0}) \ ; \ \mathbf{r}^{(k_0)}(v_{\ell_0+1}), \ldots, \mathbf{r}^{(k_0)}(v_{\ell_1}) \ ; \ \ldots \ ; \ \mathbf{r}^{(k_{m-1})}(v_{\ell_{m-1}+1}), \ldots, \mathbf{r}^{(k_{m-1})}(v_{\ell_m})\Big) \ , \tag{14}$$

while

$$\boldsymbol{\sigma} = (\sigma(v_1), \sigma(v_2), \ldots, \sigma(v_{\ell_m}))^T \ .$$

In view of the discussion in Section 2, the matrix $M_{\mathcal{V}}$ is not always solvable, even if $\mathcal{V} \in \Gamma$. Our first observation is as follows.

Proposition 3.1 *The Birkhoff interpolation problem that needs to be solved by an authorized subset satisfies Pólya's condition (9). Conversely, the Birkhoff interpolation problem that needs to be solved by an unauthorized subset does not satisfy Pólya's condition.*

Proof. Let $\mathcal{V}$ be an authorized subset and let t be any derivative order in the range $0 \le t \le k_{m-1}$. As the thresholds are strictly increasing, $k_{-1} = 0 < k_0 < k_1 < \cdots < k_m$, there exists $0 \le i \le m$ for which $k_{i-1} \le t < k_i$. Hence, $\mathcal{V}$ has the values of P and its derivatives up to and including $P^{(t)}$ in $\left|\mathcal{V} \cap \left(\cup_{j=0}^{i}\mathcal{U}_j\right)\right|$ points. But since $\mathcal{V} \in \Gamma$, $\left|\mathcal{V} \cap \left(\cup_{j=0}^{i}\mathcal{U}_j\right)\right| \ge k_i \ge t+1$, as required by Pólya's condition. Next, assume that $\mathcal{V}$ is an unauthorized subset. Then there exists $0 \le i \le m$ for which $\left|\mathcal{V} \cap \left(\cup_{j=0}^{i}\mathcal{U}_j\right)\right| < k_i$. Then Pólya's condition fails to hold for $t = k_i - 1$, since the shares of participants in $\mathcal{V}$ from levels $\mathcal{U}_j$, $j \ge i+1$, correspond to derivatives of order k_i and up. □

Next, assume that $0 \in \mathcal{U}$ is a special phantom participant and that it belongs to the highest level $\mathcal{U}_0$. This assumption enables us to answer both questions of accessibility and perfect security by examining the regularity of certain matrices.

Theorem 3.2 *Assume that* $0 \in \mathcal{U}_0$ *and that for any minimal authorized subset* $\mathcal{V} \in \Gamma$ *(namely,* $|\mathcal{V}| = k$*), the corresponding square matrix* $M_{\mathcal{V}}$*, (14), is regular, i.e.,* $\det M_{\mathcal{V}} \neq 0$ *in* $\mathbb{F}$*. Then conditions (2) (accessibility) and (3) (perfect security) hold.*

Proof. Let $\mathcal{V}$ be a "genuine" authorized subset, namely $\mathcal{V} \in \Gamma$ and $0 \notin \mathcal{V}$. If $\mathcal{V}$ is minimal, $|\mathcal{V}| = k$, then $M_{\mathcal{V}}$ is square and regular; therefore, $\mathcal{V}$ may recover the polynomial $P(x)$ and, consequently, the secret S. If $\mathcal{V}$ is not minimal, $|\mathcal{V}| > k$, there exists a subset $\mathcal{V}_0 \subset \mathcal{V}$ of size $|\mathcal{V}_0| = k$ that is authorized. Since all $|\mathcal{V}|$ equations in the linear system of equations $M_{\mathcal{V}}\mathbf{a} = \boldsymbol{\sigma}$ are consistent and since, by assumption, the sub-matrix $M_{\mathcal{V}_0}$ is regular, then $M_{\mathcal{V}}\mathbf{a} = \boldsymbol{\sigma}$ has a unique solution $\mathbf{a}$, the first component of which is the secret S. Therefore, the assumptions of the theorem imply accessibility.

Next, we prove that those assumptions also imply the perfect security of the scheme. Let $\mathcal{V} \in 2^{\mathcal{U}\setminus\{0\}} \setminus \Gamma$ be an unauthorized subset and assume that $\mathcal{V}$ is as in (13). We aim at showing that even if all participants in $\mathcal{V}$ pool their shares together, they cannot reveal a thing about the secret S. Every unauthorized subset may be completed into an authorized subset (though not necessarily minimal) by adding to it at most k participants. Without loss of generality, we may assume that $\mathcal{V}$ is missing only one participant in order to become authorized. Therefore, if we add to $\mathcal{V}$ the phantom participant 0 we get an authorized subset, $\mathcal{V}_1 = \{0\} \cup \mathcal{V} \in \Gamma$, since 0 belongs to the highest level $\mathcal{U}_0$.

Let us assume first that $|\mathcal{V}| = k - 1$. Then $|\mathcal{V}_1| = k$ and, consequently, $M_{\mathcal{V}_1}$ is square and regular. Therefore, the row in $M_{\mathcal{V}_1}$ that corresponds to the user 0 is independent of the rows that correspond to the original $k-1$ members of $\mathcal{V}$, i.e.,

$$\mathbf{r}(0) = (1, 0, \ldots, 0) \notin \text{row-space}(M_{\mathcal{V}}) \ .$$

Hence, the value of the secret S is completely independent of the shares of $\mathcal{V}$.

Next, assume that $|\mathcal{V}| > k-1$. Assume that the single participant that $\mathcal{V}$ is missing in order to become authorized is missing at the jth level for some $0 \leq j \leq m$; i.e., using the notations of (13),

$$\ell_i \geq k_i \quad 0 \leq i \leq j-1 \quad , \quad \ell_j = k_j - 1 \quad \text{and} \quad \ell_i \geq k_i - 1 \quad j+1 \leq i \leq m \ . \tag{15}$$

Since $|\mathcal{V}| = \ell_m > k-1$, we conclude that $\ell_m - \ell_j > k - k_j$. All $\ell_m - \ell_j$ rows in $M_{\mathcal{V}}$ that correspond to the participants of $\mathcal{V}$ from levels $\mathcal{U}_{j+1}$ through $\mathcal{U}_m$ have at least k_j leading zeros, since they all correspond to derivatives of order k_j or higher. Therefore, those rows belong to a subspace of $\mathbb{F}^k$ of dimension $k - k_j$. Hence, we may extract from among them $k - k_j$ rows that still span the same subspace as the original $\ell_m - \ell_j$ rows. Let $\mathcal{W}$ denote the subset of $\mathcal{V}$ that corresponds to the $(\ell_m - \ell_j) - (k - k_j)$ redundant rows from among the last $\ell_m - \ell_j$ rows in $M_{\mathcal{V}}$ and let $\mathcal{V}_0 = \mathcal{V} \setminus \mathcal{W}$. By (15),

$$|\mathcal{V}_0| = |\mathcal{V}| - |\mathcal{W}| = \ell_m - [(\ell_m - \ell_j) - (k - k_j)] = \ell_j + k - k_j = k - 1 \ .$$

Clearly, the removal from $\mathcal{V}$ of the participants in $\mathcal{W}$ cannot create new deficiencies, whence, $\mathcal{V}_0$, like $\mathcal{V}$, also lacks only a single participant at the jth level in order to become authorized. Hence, we may apply to it our previous arguments and conclude that

$$\mathbf{r}(0) = (1, 0, \ldots, 0) \notin \text{row-space}(M_{\mathcal{V}_0}) \ .$$

But since

$$\text{row-space}(M_{\mathcal{V}_0}) = \text{row-space}(M_{\mathcal{V}}) \ ,$$

we arrive at the sought-after conclusion that

$$\mathbf{r}(0) = (1, 0, \ldots, 0) \notin \text{row-space}(M_{\mathcal{V}}) \ ,$$

which implies perfect security. □

3.2 Random allocation of participant identities

The first strategy of allocating participant identities that we consider is the random one. Namely, recalling that $|\mathcal{U}| = n$ and $|\mathbb{F}| = q$, the random strategy is such that

$$\text{Prob}(\mathcal{U} = \mathcal{W}) = \frac{1}{\binom{q-1}{n}} \qquad \forall\ \mathcal{W} \subset \mathbb{F} \setminus \{0\}\ ,\ |\mathcal{W}| = n\ . \tag{16}$$

Theorem 3.3 *Assume a random allocation of participant identities, (16). Let $\mathcal{V}$ be a randomly selected subset from $2^{\mathcal{U}}$. Then if $\mathcal{V} \in \Gamma$*

$$\mathit{Prob}\,(H(S|\sigma(\mathcal{V})) = 0) \geq 1 - \varepsilon\ , \tag{17}$$

while otherwise

$$\mathit{Prob}\,(H(S|\sigma(\mathcal{V})) = H(S)) \geq 1 - \varepsilon\ , \tag{18}$$

where

$$\varepsilon = \frac{(k-2)(k-1)}{2(q-k)}\ . \tag{19}$$

Proof. If $\mathcal{V} \in \Gamma$ there exists a minimal authorized subset $\mathcal{V}_0 \subseteq \mathcal{V}$, $|\mathcal{V}_0| = k$, such that if $\det M_{\mathcal{V}_0} \neq 0$ $\mathcal{V}$ may recover S. If, on the other hand, $\mathcal{V} \notin \Gamma$, we saw in Theorem 3.2 that if $0 \in \mathcal{U}_0$ there exists a minimal authorized subset $\mathcal{V}_0$ such that $\det M_{\mathcal{V}_0} \neq 0$ implies that $\mathcal{V}$ cannot learn any information about S. Hence, in order to prove both statements of the theorem, (17) and (18), it suffices to assume that $0 \in \mathcal{U}_0$ and then show that if $\mathcal{V} \in \Gamma$ is a *minimal* authorized subset, $M_{\mathcal{V}}$ has a nonzero determinant in probability at least $1 - \varepsilon$.

To that end, let $\mathcal{V}$ be such a subset and assume that its participants are ordered according to their position in the hierarchy, (13). We proceed to show that

$$\text{Prob}\,(\det(M_{\mathcal{V}}) = 0) \leq \frac{(k-2)(k-1)}{2(q-k)}\ . \tag{20}$$

Noting that (20) clearly holds when $k = 1, 2$, we continue by induction on k. There are two cases to consider:

1. The last row in $M_{\mathcal{V}}$ is $\mathbf{r}^{(h)}(v_k)$ where $h < k-1$ (this happens if $k_{m-1} < k_m - 1$ or if $\mathcal{V} \cap \mathcal{U}_m = \emptyset$).
2. The last row in $M_{\mathcal{V}}$ is $\mathbf{r}^{(k-1)}(v_k)$ (this happens when $k_{m-1} = k_m - 1$ and $\mathcal{V} \cap \mathcal{U}_m \neq \emptyset$; in that case v_k is the only participant in $\mathcal{V} \cap \mathcal{U}_m$, since $\mathcal{V}$ is minimal).

We begin by handling the first case. Let $\mathbf{v} = (v_1, \ldots, v_{k-1})$ and $(\mathbf{v}, v_k) = (v_1, \ldots, v_k)$. Let $\mu_{k-1} = \mu_{k-1}(\mathbf{v})$ denote the determinant of the $(k-1) \times (k-1)$ minor of $M_{\mathcal{V}}$ that is obtained

by removing the last row and last column in $M_{\mathcal{V}}$. Then, expanding the determinant by the last row, we may write it as a polynomial in v_k,

$$\det(M_{\mathcal{V}}) = \sum_{i=0}^{k-2-h} c_i v_k^i + \frac{(k-1)!}{(k-1-h)!} \cdot \mu_{k-1} \cdot v_k^{k-1-h} \ , \tag{21}$$

for some constants c_i that depend on $\mathbf{v}$. Let Ω denote the collection of all $\mathbf{v} \in \mathbb{F}^{k-1}$ for which $\mu_{k-1} = \mu_{k-1}(\mathbf{v}) = 0$. Then

$$\begin{aligned} &\text{Prob}(\det(M_{\mathcal{V}}) = 0) = \\ &= \sum_{\mathbf{v} \in \mathbb{F}^{k-1} \setminus \Omega} \text{Prob}(\det(M_{\mathcal{V}}) = 0 | \mathbf{v}) \cdot \text{Prob}(\mathbf{v}) + \sum_{\mathbf{v} \in \Omega} \text{Prob}(\det(M_{\mathcal{V}}) = 0 | \mathbf{v}) \cdot \text{Prob}(\mathbf{v}) \ . \end{aligned} \tag{22}$$

If $\mathbf{v} \in \mathbb{F}^{k-1} \setminus \Omega$ then $\det(M_{\mathcal{V}})$ is a polynomial of degree $k-1-h$ in v_k, (21). Hence, there are at most $k-1-h$ values of v_k for which $\det(M_{\mathcal{V}}) = 0$. This implies that

$$\text{Prob}(\det(M_{\mathcal{V}}) = 0 | \mathbf{v}) \leq \frac{k-1-h}{(q-1)-(k-1)} \qquad \forall \mathbf{v} \in \mathbb{F}^{k-1} \setminus \Omega \tag{23}$$

(recall that the participant identities are distinct and are randomly selected from $\mathbb{F} \setminus \{0\}$). Note that h could take any value between 0 and $k-2$. However, if $h = 0$ it means that all participants in $\mathcal{V}$ belong to the highest level, so that $M_{\mathcal{V}}$ is a Vandermonde matrix. In that case, the matrix is invertible and, consequently, $\text{Prob}(\det(M_{\mathcal{V}}) = 0) = 0$. Therefore, the worst case in (23) is when $h = 1$. Hence, we rewrite (23) as follows:

$$\text{Prob}(\det(M_{\mathcal{V}}) = 0 | \mathbf{v}) \leq \frac{k-2}{q-k} \qquad \forall \mathbf{v} \in \mathbb{F}^{k-1} \setminus \Omega \ . \tag{24}$$

If $\mathbf{v} \in \Omega$ then the degree of $\det(M_{\mathcal{V}})$ as a polynomial in v_k is less than $k-1-h$. The problem is that it may completely vanish and then $\det(M_{\mathcal{V}})$ would be zero for all values of v_k. However, as $\mathbf{v}$ is a vector of dimension $k-1$, we may invoke the induction assumption (i.e., (20) for $k-1$) and conclude that

$$\text{Prob}(\mathbf{v} \in \Omega) \leq \frac{(k-3)(k-2)}{2(q-k+1)} \ . \tag{25}$$

Finally, combining (22), (24) and (25) we may prove (20) in this case:

$$\text{Prob}(\det(M_{\mathcal{V}}) = 0) \leq \frac{k-2}{q-k} + \frac{(k-3)(k-2)}{2(q-k+1)} \leq \frac{(k-2)(k-1)}{2(q-k)} \ .$$

In the second case, $\det(M_{\mathcal{V}})$ does not depend on v_k as the last row in the matrix in this case is $(0, \ldots, 0, (k-1)!)$. Hence, we may solve for a_{k-1} and reduce the system to a system in only $(k-1)$ unknowns, $\{a_i\}_{i=0}^{k-2}$. Consequently, we may apply induction in order to conclude that

$$\text{Prob}\left(\det(M_{\mathcal{V}}) = 0\right) \leq \frac{(k-3)(k-2)}{2(q-k+1)} < \frac{(k-2)(k-1)}{2(q-k)} \ .$$

The proof is thus complete. □

Examples.

1. Consider a secret sharing problem with $\mathbf{k} = (k_0 = 3, k_1 = 4, k_2 = 6)$. Let $\mathcal{V}$ be an authorized subset that has $\ell_0 = 3$ participants from $\mathcal{U}_0$, $\ell_1 = 5$ participants from $\mathcal{U}_0 \cup \mathcal{U}_1$ and $\ell_2 = 6$ participants overall. Then $\mathcal{V}$ needs to solve a linear system for the polynomial coefficients $\mathbf{a} = (a_0, \ldots, a_5)$ where the corresponding matrix is

$$M_{\mathcal{V}} = \begin{pmatrix} 1 & v_1 & v_1^2 & v_1^3 & v_1^4 & v_1^5 \\ 1 & v_2 & v_2^2 & v_2^3 & v_2^4 & v_2^5 \\ 1 & v_3 & v_3^2 & v_3^3 & v_3^4 & v_3^5 \\ 0 & 0 & 0 & 6 & 24v_4 & 60v_4^2 \\ 0 & 0 & 0 & 6 & 24v_5 & 60v_5^2 \\ 0 & 0 & 0 & 0 & 24 & 120v_6 \end{pmatrix} . \tag{26}$$

Here, $\det(M_{\mathcal{V}}) = 120\mu_5 v_6 + c_0$, where μ_5 and c_0 depend on $\{v_i\}_{i=1}^5$ (see (21)). If

$$\mu_5 = \det \begin{pmatrix} 1 & v_1 & v_1^2 & v_1^3 & v_1^4 \\ 1 & v_2 & v_2^2 & v_2^3 & v_2^4 \\ 1 & v_3 & v_3^2 & v_3^3 & v_3^4 \\ 0 & 0 & 0 & 6 & 24v_4 \\ 0 & 0 & 0 & 6 & 24v_5 \end{pmatrix} \neq 0$$

then $\det(M_{\mathcal{V}})$ will vanish for only one value of v_6. If, on the other hand, $\mu_5 = 0$, there are two scenarios: either $c_0 \neq 0$, in which case the matrix is non-singular independently of v_6, or $c_0 = 0$, in which case the matrix is singular for all values of v_6. The proof of the theorem took into account the latter scenario which is worse. Therefore, $M_{\mathcal{V}}$ is singular in probability $\frac{(6-2)(6-1)}{2(q-6)} = \frac{10}{q-6}$ at most.

2. Assume now that $\mathbf{k} = (k_0 = 3, k_1 = 5, k_2 = 6)$ and $\mathcal{V}$ has the same structure as in the previous example. Then,

$$M_{\mathcal{V}} = \begin{pmatrix} 1 & v_1 & v_1^2 & v_1^3 & v_1^4 & v_1^5 \\ 1 & v_2 & v_2^2 & v_2^3 & v_2^4 & v_2^5 \\ 1 & v_3 & v_3^2 & v_3^3 & v_3^4 & v_3^5 \\ 0 & 0 & 0 & 6 & 24v_4 & 60v_4^2 \\ 0 & 0 & 0 & 6 & 24v_5 & 60v_5^2 \\ 0 & 0 & 0 & 0 & 0 & 120 \end{pmatrix} . \tag{27}$$

Here, a_5 may be found and then we are left with the first 5 equations in $(a_0, \ldots, a_4)$. Then, we conclude that $M_{\mathcal{V}}$ is singular in probability $\frac{(5-2)(5-1)}{2(q-5)} = \frac{6}{q-5}$ at most. In fact, in this particular example we can see that the matrix $M_{\mathcal{V}}$ is invertible for all values $v_1 < v_2 < \cdots < v_6$. Namely, concentrating on secret sharing settings with $\mathbf{k}$ as above, all authorized subsets of this type (i.e., with the same values of ℓ_0, ℓ_1, ℓ_2) are at no risk of being unable to recover the secret.

Theorem 3.3 implies that if k, the number of overall participants that are required in an authorized subset, is a small number, the failure probability is $\Theta(1/q)$. Since q should be at least as large as the number of possible secrets (and, hence, is usually very large), the failure probability is not much larger than the probability of simply guessing the secret.

As the number of minimal authorized subsets in $\mathcal{U} \cup \{0\}$ is $\binom{n+1}{k}$, Theorems 3.2 and 3.3 imply the following.

Corollary 3.4 *Assume a random allocation of participant identities, (16). Then the probability that the resulting scheme has accessibility, (2), for all authorized subsets and perfect security, (3), for all unauthorized subsets is at least* $1-\binom{n+1}{k}\cdot\varepsilon$*, where* ε *is as in (19). Consequently, hierarchical threshold access structures with* n *participants and minimal authorized subsets of size* k *may be realized ideally by a linear secret sharing scheme over fields* $\mathbb{F}$ *of size*

$$q = |\mathbb{F}| > \binom{n+1}{k} \cdot \frac{(k-2)(k-1)}{2} + k \ .$$

The random allocation is therefore a safe bet. Since usually n and k are not too large, the dealer may adopt this strategy and be certain in a high probability that both requirements – accessibility, and perfect security – will be satisfied.

If the number of minimal authorized subsets in $\mathcal{U} \cup \{0\}$, $\binom{n+1}{k}$, is manageable, the dealer could use the random allocation as a basis for finding a full-proof allocation of identities: The dealer will assign the identities to participants one at a time. For each newly generated participant identity, the dealer will scan all minimal authorized subsets that involve only participants from those that were assigned an identity thus far (including the phantom participant $u = 0$). If one of those subsets $\mathcal{V}$ happen to have a singular matrix $M_{\mathcal{V}}$ – an event of probability $\Theta(1/q)$ – the dealer will select a new random identity for the new participant. After finding a successful identity for that participant, the dealer will proceed to the next one until all participants are associated with some identity $u \in \mathbb{F}$.

Such a verification is feasible with modest values of n, say $n \leq 30$ and all values of $1 \leq k \leq n$. By carrying out a more careful scanning of all minimal authorized subsets, one can skip subsets that give rise to matrices that are unconditionally invertible and therefore significantly reduce the running time of the allocation process. One simple observation along those lines is the following: let $\ell_i = |\mathcal{V} \cap \bigcup_{j=0}^{i} \mathcal{U}_j|$, $0 \leq i \leq m$, be as in (13). Then if for each i there exists $j(i)$ such that $\ell_i = k_{j(i)}$, the matrix $M_{\mathcal{V}}$ is unconditionally invertible since it is block-triangular and the square blocks on the diagonal are generalized Vandermonde blocks (the number of blocks equals the size of the set $\{j(i)\}_{0 \leq i \leq m}$).

A verification process of that sort is not feasible for large values of n. In such cases, the dealer must perform an oblivious random allocation and rely on the negligible probability for a failure, as provided by Theorem 3.3 and Corollary 3.4.

3.3 Monotone allocation of participant identities

Here, we present a simple allocation method that guarantees both accessibility, (2), and perfect security, (3), if the field $\mathbb{F}$ is of a sufficiently large prime order q.

For every $0 \leq i \leq m$ we define $n_i = |\bigcup_{j=0}^{i} \mathcal{U}_i|$ and let $n_{-1} = 0$. The simpler version of our method associates all $n_i - n_{i-1}$ members of $\mathcal{U}_i$ with the identities $[n_{i-1}+1, n_i] \subset \mathbb{F}$. The more flexible version of this method leaves gaps between the $m+1$ intervals of identities, in order to allow new participants to be added to any level while still maintaining the monotonic principle,

$$u \in \mathcal{U}_i \ , \ v \in \mathcal{U}_j \ , \ i < j \Rightarrow u < v \ , \tag{28}$$

where the inequality is in the usual sense between integers in the interval $[0, q-1]$.

In Lemma 3.5 and Theorem 3.6 we prove that this method guarantees accessibility and perfect security, (2)+(3), provided that the size of the underlying field, q, is sufficiently large with respect to the parameters of the problem. In Lemma 3.5 we prove our basic lower bound on q that guarantees these two conditions. Then, in Theorem 3.6, we use the bound of Lemma 3.5 and carry out a more delicate analysis that yields a better bound.

Lemma 3.5 *Let $(\mathbf{k}, n)$ be a hierarchical threshold secret sharing problem. Assume that the participants in $\mathcal{U}$ were assigned identities in $\mathbb{F} = \mathbb{F}_q$, q being a prime, in a monotone manner, namely, in concert with condition (28), and let $N = \max \mathcal{U}$. Finally, assume that*

$$2^{-k} \cdot (k+1)^{(k+1)/2} \cdot N^{(k-1)k/2} < q = |\mathbb{F}| \ , \tag{29}$$

(where $k = k_m$ is the minimal size of an authorized subset). Then our hierarchical secret sharing scheme satisfies conditions (2) and (3).

Proof. In view of Theorem 3.2, it suffices to prove that if $\mathcal{V} \in \Gamma$ is a minimal authorized subset, that may include the phantom participant $u = 0$, then the corresponding square matrix $M_{\mathcal{V}}$, (14), is regular. Without loss of generality we assume that the participant identities in $\mathcal{V}$ are given by (13) (with $\ell_m = k$) and that they are ordered in the usual sense in $\mathbb{R}$, $v_1 < v_2 < \cdots < v_k$. First, we prove that

$$\det M_{\mathcal{V}} \neq 0 \qquad \text{in} \ \ \mathbb{R} \ . \tag{30}$$

Then, invoking (29), we shall prove that

$$|\det M_{\mathcal{V}}| < q \qquad \text{in} \ \ \mathbb{R} \ . \tag{31}$$

Combining (30) and (31) we conclude that

$$\det M_{\mathcal{V}} \neq 0 \qquad \text{in} \ \ \mathbb{F} = \mathbb{F}_q \ . \tag{32}$$

In order to prove (30), we observe that the interpolation matrix E that corresponds to the Birkhoff interpolation problem with which the participants in $\mathcal{V}$ are faced, has an echelon form. Indeed, all rows have exactly one entry that equals 1, and the position of the 1 is monotonically non-decreasing as we go down the rows of E: in the first ℓ_0 rows we encounter the 1 in column $j = 0$, in the next $\ell_1 - \ell_0$ rows the 1 appears in column $j = \ell_0$ and so forth. Hence, the matrix E has no supported 1-sequences in the sense of Definition 2.1. Recalling Proposition 3.1, we infer that the conditions of Theorem 2.2 are satisfied. Therefore, the corresponding Birkhoff interpolation problem is well-posed over $\mathbb{R}$, (30).

In order to bound the determinant of $M_{\mathcal{V}}$, we invoke Hadamard's maximal determinant theorem [9, problem 523]. According to that theorem, if A is a $k \times k$ real matrix, and

$$|A_{i,j}| \leq 1 \quad , \quad 0 \leq i, j \leq k-1 \ , \tag{33}$$

then

$$|\det(A)| \leq 2^{-k} \cdot (k+1)^{(k+1)/2} \ . \tag{34}$$

Let A be the matrix that is obtained from $M_{\mathcal{V}}$ if we divide its jth column by N^j, $0 \leq j \leq k-1$. Since that matrix A satisfies condition (33), we conclude, in view of (34) and (29), that $M_{\mathcal{V}}$ satisfies (31). That completes the proof. $\square$

Theorem 3.6 *Under the conditions of Lemma 3.5, the hierarchical threshold secret sharing scheme satisfies conditions (2) and (3) provided that*

$$\alpha(k)N^{(k-1)(k-2)/2} < q = |\mathbb{F}| \quad \textit{where} \quad \alpha(k) := 2^{-k+2} \cdot (k-1)^{(k-1)/2} \cdot (k-1)! \ . \tag{35}$$

Proof. Assume that $\mathcal{V}$ in (13) is a minimal authorized subset and that the participant identities are ordered in the usual sense in $\mathbb{R}$, $v_1 < v_2 < \cdots < v_k$. Let d_i, $1 \le i \le k$, be the order of derivative of the share that v_i got. Namely, in view of (13) and (14), $d_i = 0$ for $1 \le i \le \ell_0$, $d_i = k_0$ for $\ell_0 + 1 \le i \le \ell_1$, and so forth. We refer to $\mathbf{d} = (d_1, \ldots, d_k)$ as the *type* of the interpolation problem that needs to be solved by the participants of $\mathcal{V}$ since it characterizes the form of the coefficient matrix $M_{\mathcal{V}}$, (14). Finally, let t be the largest integer such that $d_i = i - 1$ for all $1 \le i \le t$. We note that t is well defined and $t \ge 1$ since always $d_1 = 0$ (i.e., $\mathcal{V}$ must always include at least one participant of the highest level $\mathcal{U}_0$).

Let $\mathcal{P}$ denote the problem of recovering the polynomial P from the shares of $\{v_i\}_{1 \le i \le k}$. We claim that $\mathcal{P}$ may be decomposed into two independent problems that may be solved in succession:

- Problem $\mathcal{P}_1$. Recovering $P^{(t-1)}$ (namely, the coefficients a_i, $t-1 \le i \le k-1$, see (12)) from the shares of v_i, $t \le i \le k$.
- Problem $\mathcal{P}_2$. Recovering a_{i-1} from the share of v_i, $t - 1 \ge i \ge 1$.

Indeed, the equations that correspond to the last $k - t + 1$ participants – $\{v_i\}_{t \le i \le k}$ – involve only the $k-t+1$ coefficients $\{a_i\}_{t-1 \le i \le k-1}$ (note that if $t = 1$, $\mathcal{P}_1$ coincides with the original problem $\mathcal{P}$ and then $\mathcal{P}_2$ is rendered void). Hence, we may first concentrate on solving the (possibly reduced) interpolation problem $\mathcal{P}_1$. If that problem is solvable, we may proceed to problem $\mathcal{P}_2$. That problem is always solvable by the following simple procedure: for every i, $i = t-1, \ldots, 1$, we perform one integration and then, using the share of v_i, we recover the coefficient a_{i-1} of P. Hence, we may concentrate on determining a sufficient condition for the solvability of $\mathcal{P}_1$. That condition will guarantee also the solvability of $\mathcal{P}$. (Note that $\mathcal{P}_1$ still satisfies Pólya's condition, Lemma 2.1.)

The dimension of the interpolation problem $\mathcal{P}_1$ is $k - t + 1$. Hence, since the left hand side in (35) is monotonically increasing in k, we may concentrate here on the worst case where $t = 1$ and the dimension of $\mathcal{P}_1$ is k (namely, $\mathcal{P}_1 = \mathcal{P}$). The main observation, that justifies this preliminary discussion and the decomposition of $\mathcal{P}$ into two sub-problems, is that in the type $\mathbf{d}$ of $\mathcal{P}_1$, $d_1 = d_2 = 0$. Indeed, $d_1 = 0$ and $d_2 \le 1$ as enforced by Pólya's condition; moreover, $d_2 \ne 1$ for otherwise $t \ge 2$, as opposed to our assumption that $t = 1$. With this in mind, we define $s \ge 2$ to be the maximal integer for which $d_i = 0$ for all $1 \le i \le s$.

Next, we write down the system of linear equations that characterizes the interpolation problem $\mathcal{P}_1$. To that end, we prefer to look for the polynomial P in its Newton form with respect to $\{v_i\}_{1 \le i \le k}$ (as opposed to its standard representation (12)):

$$P(x) = \sum_{j=0}^{k-1} c_j \prod_{i=1}^{j} (x - v_i) \ . \tag{36}$$

Writing down the system of linear equations in the unknowns $\{c_j\}_{0 \le j \le k-1}$, we see that the corresponding coefficient matrix, $\hat{M} = \hat{M}_{\mathcal{V}}$, has a block triangular form,

$$\hat{M} = \begin{pmatrix} B_1 & 0 \\ B_2 & B_3 \end{pmatrix} \tag{37}$$

where the upper-left $s \times s$ block is given by

$$B_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 1 & v_2 - v_1 & 0 & 0 & \cdots & 0 \\ 1 & v_3 - v_1 & \prod_{i=1}^{2}(v_3 - v_i) & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & v_s - v_1 & \prod_{i=1}^{2}(v_s - v_i) & \prod_{i=1}^{3}(v_s - v_i) & \cdots & \prod_{i=1}^{s-1}(v_s - v_i) \end{pmatrix} \tag{38}$$

(we use the notation $\hat{M}$ in order to distinguish this matrix from $M = M_{\mathcal{V}}$, (14), that was the coefficient matrix in the linear system for the unknowns a_i in the standard representation of the interpolant $P(x)$, (12)). Invoking the same arguments as in Lemma 3.5, we conclude that

$$\det \hat{M} \neq 0 \qquad \text{in } \mathbb{R} \, . \tag{39}$$

We need to show that

$$\det \hat{M} \neq 0 \qquad \text{in } \mathbb{F} \, . \tag{40}$$

In order to prove (40), we first invoke (37) to conclude that

$$\det \hat{M} = \det B_1 \cdot \det B_3 \, . \tag{41}$$

As $N < q$, all terms on the diagonal of B_1, (38), are nonzero in $\mathbb{F}$, so that B_1 is invertible over $\mathbb{F}$. Therefore, by (41), we only need to show that

$$\det B_3 \neq 0 \qquad \text{in } \mathbb{F} \, , \tag{42}$$

in order to prove (40). Since $\det B_3 \neq 0$ in $\mathbb{R}$, as implied by (39) and (41), this amounts to showing that

$$|\det B_3| < q \qquad \text{in } \mathbb{R} \, . \tag{43}$$

In order to prove (43), we shall show that

$$|\hat{M}_{i,j}| \leq j \cdot N^{j-1} \quad \text{for all} \quad s+1 \leq i \leq k \, , \; s \leq j \leq k-1 \tag{44}$$

(note that the rows of $\hat{M}$ correspond to v_i, $1 \leq i \leq k$, while the columns of $\hat{M}$ correspond to the unknown coefficient c_j, $0 \leq j \leq k-1$). Then, we may proceed to prove (43) using Hadamard's inequality: let A be the matrix that is obtained from B_3 after dividing its jth column, $s \leq j \leq k-1$, by $j \cdot N^{j-1}$. Then according to (44), the normalized block A satisfies condition (33) of Hadamard's maximal determinant theorem. Hence, by (34),

$$|\det A| \leq 2^{-k+s} \cdot (k-s+1)^{(k-s+1)/2} \, .$$

Consequently, since $s \geq 2$,

$$|\det B_3| = |\det A| \cdot \left(\prod_{j=s}^{k-1} j \cdot N^{j-1} \right) \leq 2^{-k+2} \cdot (k-1)^{(k-1)/2} \cdot (k-1)! \cdot N^{(k-1)(k-2)/2} \, . \tag{45}$$

Inequalities (45) and (35) prove (43).

The only missing link is (44). In order to prove this inequality, we need to derive an expression for the derivatives of $P(x)$, (36). Let us introduce the notations

$$P_j(x) = \prod_{i=1}^{j}(x - v_i) \quad \text{and} \quad P_{j,h}(x) = \frac{d^h P_j(x)}{dx^h} \quad , \quad 0 \le j \le k-1 \ , \ h \ge 0 \ . \tag{46}$$

Then, since $P_{j,h} = 0$ for all $j < h$,

$$P^{(h)}(x) = \sum_{j=h}^{k-1} c_j P_{j,h}(x) \ . \tag{47}$$

The expression for $P_{j,h}(x)$ is given by

$$P_{j,h}(x) = \sum \left\{ \Pi_{(g_1,\ldots,g_h)}(x) \ : \ (g_1,\ldots,g_h) \in G(j,h) \right\} \ , \tag{48}$$

where $G(j,h)$ is the set of all $\frac{j!}{(j-h)!}$ ordered selections of h elements from $\{1,\ldots,j\}$ and

$$\Pi_{(g_1,\ldots,g_h)}(x) = \prod \{ (x - v_i) \ : \ i \in \{1,\ldots,j\} \setminus \{g_1,\ldots,g_h\} \} \ . \tag{49}$$

Setting $x = v_\ell$, for some $s+1 \le \ell \le k$, in (47), we see that the ℓth row in $\hat{M}$ takes the form

$$(\hat{M}_{\ell,j})_{0 \le j \le k-1} = \Big(\ 0 \ \ \cdots \ \ 0 \ \ P_{h,h}(v_\ell) \ \ \cdots \ \ P_{k-1,h}(v_\ell) \ \Big) \ , \tag{50}$$

where $h = d_\ell$ is the order of derivative of the share of v_ℓ. From (48),

$$|P_{j,h}(v_\ell)| \le |G(j,h)| \cdot \max_{(g_1,\ldots,g_h)} |\Pi_{(g_1,\ldots,g_h)}(v_\ell)| \ .$$

Since, by (49), $|\Pi_{(g_1,\ldots,g_h)}(v_\ell)| \le N^{j-h}$, we conclude that

$$|P_{j,h}(v_\ell)| \le \frac{j!}{(j-h)!} \cdot N^{j-h} \quad , \quad h \le j \le k-1 \ . \tag{51}$$

As the definition of s implies that $h \ge 1$ for all rows $s+1 \le \ell \le k$, and since $j \le k-1 < N$, we infer by (51) and (50) that

$$|\hat{M}_{\ell,j}| \le j \cdot N^{j-1} \quad , \quad h \le j \le k-1 \ . \tag{52}$$

Since, by (50), the inequality in (52) holds trivially for columns $0 \le j \le h-1$ as well, that proves (44). The proof of the theorem is thus complete. □

Condition (35) is pretty sharp. It may be seen that the worst scenario is that in which $\mathbf{d} = (0,0,1,\ldots,1)$ – namely, $k_0 = 1$ (the number of participants from $\mathcal{U}_0$ must be at least 1) and there are two participants from $\mathcal{U}_0$ while all the rest are from $\mathcal{U}_1$. In such cases, the (real) determinant of the block B_3 in the matrix of coefficients $\hat{M}$ is $\Theta(N^{(k-1)(k-2)/2})$, though the constant $\alpha(k)$ may be somewhat improved. In the Appendix we list all possible cases where $k \le 4$. From that study one sees that (35) is sharp for $k = 2$, when it reads $1 < q$ (i.e., there is no restriction), and $k = 3$, when

k	Condition (29)	Condition (35)
5	$N \leq 5497$	$N \leq 1234795$
6	$N \leq 296$	$N \leq 3637$
7	$N \leq 56$	$N \leq 200$
8	$N \leq 19$	$N \leq 38$

Table 1: Values of k and N that satisfy conditions (29) and (35)

it reads $2N < q$. However, when $k = 4$, (35) demands that $3^{2.5}N/2 \approx 7.8N < q$, while a careful examination of all cases where $k = 4$ reveals that $6N < q$ suffices.

The improvement offered by (35) over (29) may be appreciated by comparing the logarithms to the base 2 of the two lower bounds on q. The difference between the logarithm to the base 2 of the lower bound in (29) and that of the lower bound in (35) is given by

$$(k-1) \cdot \log N + \frac{1}{2} \log \frac{(k+1)^{k+1}}{(k-1)^{k-1}} - \log((k-1)!) - 2 \ .$$

This difference shows the number of additional bits that estimate (35) allows for the prime number q comparing to the size in bits that is allowed by estimate (29).

Table 1 includes for each value of k, $5 \leq k \leq 8$, the maximal value of N for which the original condition, (29), and the improved one, (35), still holds when the secret to be shared is an AES key (namely, q is of size 128 bits). The figures in the table demonstrate the exponential drop in the capacity of the scheme, N, when k increases. However, this should not be worrisome because n and k in any plausible real-life application are usually small. In the unlikely scenario of k and N so large that condition (35) fails to hold for any prime q of the size of the secret to be shared, we may always go back to the random allocation strategy that was described in the previous section.

4 An ideal scheme for the disjunctive hierarchical secret sharing problem

As described in the Introduction, Simmons [18] studied a closely related hierarchical secret sharing problem, where the conjunction of threshold conditions is replaced by a disjunction (compare (1) to (7)). His scheme is not ideal and it requires (possibly exponentially) many checks to be made when assigning identities and shares to the participants. Brickell [6] offered two schemes for the same problem, both ideal. The first one suffers from the same problem as Simmons', in the sense that the dealer is required to check (possibly exponentially) many matrices for non-singularity. In the second scheme this difficulty is replaced by the need to find an algebraic number of some degree over a prime order field. Here we show how the ideality of the disjunctive hierarchical access structures follows immediately from the ideality of their conjunctive counterpart. We then proceed to describe an ideal scheme for their realization that does not involve any of the above mentioned difficulties of Simmons' and Brickell's schemes.

Karchmer and Wigderson [13] introduced monotone span programs as a linear algebraic model of computation for computing monotone functions. A monotone span program (MSP hereinafter) is a quintuple $\mathcal{M} = (\mathbb{F}, M, \mathcal{U}, \phi, \mathbf{e})$ where $\mathbb{F}$ is a field, M is a matrix of dimensions $a \times b$ over $\mathbb{F}$,

$\mathcal{U} = \{u_1, \ldots, u_n\}$ is a finite set, ϕ is a surjective function from $\{1, \ldots, a\}$ to $\mathcal{U}$, which is thought of as *labeling* of the rows of M, and $\mathbf{e}$ is some target row vector from $\mathbb{F}^b$. The MSP $\mathcal{M}$ realizes the monotone access structure $\Gamma \subset 2^{\mathcal{U}}$ when $\mathcal{V} \in \Gamma$ if and only if $\mathbf{e}$ is spanned by the rows of the matrix M whose labels belong to $\mathcal{V}$. The size of $\mathcal{M}$ is a, the number of rows in M. Namely, in the terminology of secret sharing, the size of the MSP is the total number of shares that were distributed to all participants in $\mathcal{U}$. An MSP is ideal if $a = n$.

If Γ is a monotone access structure over $\mathcal{U}$, its dual is defined by $\Gamma^* = \{\mathcal{V} : \mathcal{V}^c \notin \Gamma\}$. It is easy to see that Γ^* is also monotone. In [11] it was shown that if $\mathcal{M} = (\mathbb{F}, M, \mathcal{U}, \phi, \mathbf{e})$ is an MSP that realizes a monotone access structure Γ, then there exists an MSP $\mathcal{M}^* = (\mathbb{F}, M^*, \mathcal{U}, \phi, \mathbf{e}^*)$ of the same size like $\mathcal{M}$ that realizes the dual access structure Γ^*. Hence, an access structure is ideal if and only if its dual is.

Returning to the disjunctive hierarchial access structure that was studied by Simmons, (7), we claim the following straightforward proposition.

Proposition 4.1 *Let $\mathcal{U} = \bigcup_{i=0}^{m} \mathcal{U}_i$ and $\mathbf{k} = \{k_i\}_{i=0}^{m}$ be as in Definition 1.1. Let Γ be the corresponding disjunctive access structure as defined in (7). Then Γ^* is the conjunctive access structure that is defined in Definition 1.1 with thresholds $\mathbf{k}^* = \{k_i^*\}_{i=0}^{m}$ where $k_i^* = |\bigcup_{j=0}^{i} \mathcal{U}_j| - k_i + 1$, $0 \leq i \leq m$.*

Since the conjunctive hierarchial access structure is ideal in the sense that there exists an ideal secret sharing scheme that realizes it (over sufficiently large fields), we conclude the following.

Corollary 4.2 *The disjunctive access structure (7) is ideal.*

Finally, we describe how to modify our scheme for $(\mathbf{k}, n)$-conjunctive threshold access structures, (1), in order to be suitable for $(\mathbf{k}, n)$-disjunctive ones, (7). There are two small modifications that need to be made, both reflecting the duality of the two types of problems. As before, we let $k = k_m$ be the highest threshold, and the scheme is based on a secret polynomial $P(x) \in \mathbb{F}_{k-1}[x]$. But while in the original scheme the secret was a_0, in the new scheme it is going to be a_{k-1}, the coefficient of the highest power. Another modification is that the more important levels will now get lower order derivatives, as opposed to the original scheme. The scheme is therefore as follows:

1. The dealer selects a random polynomial $P(x) \in \mathbb{F}_{k-1}[x]$, where
$$P(x) = \sum_{i=0}^{k-1} a_i x^i \quad \text{and} \quad a_{k-1} = S \ . \tag{53}$$
2. The dealer identifies each participant $u \in \mathcal{U}$ with a field element, denoted by u.
3. The dealer distributes shares to all participants in the following manner: Each participant of the ith level in the hierarchy, $u \in \mathcal{U}_i$, $0 \leq i \leq m$, receives the share $P^{(k-k_i)}(u)$ (instead of $P^{(k_{i-1})}(u)$ in the original scheme).

For example, assume that there are three levels in the hierarchy, $\mathcal{U} = \mathcal{U}_0 \cup \mathcal{U}_1 \cup \mathcal{U}_2$, and that the thresholds are $\mathbf{k} = (k_0, k_1, k_2) = (2, 4, 7)$; namely, $\mathcal{V} \subset \mathcal{U}$ is authorized if and only if it has at least 7 participants, or at least 4 participants from $\mathcal{U}_0 \cup \mathcal{U}_1$, or at least 2 participants from $\mathcal{U}_0$. Then, as $k = k_2 = 7$, the dealer selects a random polynomial $P(x) = \sum_{i=0}^{6} a_i x^i$ where $a_6 = S$. He then distributes the shares as follows: participants $u \in \mathcal{U}_0$ will get the share $P^{(5)}(u)$, as $k - k_0 = 7 - 2 = 5$; participants $u \in \mathcal{U}_1$ will get the share $P^{(3)}(u)$, since $k - k_1 = 3$; and those of the lowest level, $\mathcal{U}_2$, will get $P(u)$.

The idea behind this allocation is simple: given $\mathcal{V} \subset \mathcal{U}$, its relevant threshold is determined by its lowest participant. If the lowest participant in $\mathcal{V}$ is from $\mathcal{U}_i$ (namely, $\mathcal{V} \subset \bigcup_{j=0}^{i} \mathcal{U}_j$) then all participants in $\mathcal{V}$ have shares with derivatives of order $k - k_i$ or higher. Hence, all linear equations that correspond to those shares involve only the $k - (k - k_i) = k_i$ highest coefficients of $P(x)$ as unknowns. Therefore, it is necessary to have at least k_i participants in order to have a sufficient number of equations. As before, the main concern is how to allocate the participant identities so that we achieve both accessibility (2) and perfect security (3). The random and monotone allocations that we described in Sections 3.2 and 3.3, and all of the results that we proved therein, apply equally to this modified scheme.

A concluding remark. In Corollary 3.4 we showed that hierarchical threshold access structures with n participants and minimal authorized subsets of size k may be realized ideally by a linear secret sharing scheme over fields $\mathbb{F}$ of size

$$|\mathbb{F}| > \binom{n+1}{k} \cdot \frac{(k-2)(k-1)}{2} + k \ . \tag{54}$$

A similar result was proven by Brickell [6] regarding disjunctive threshold access structures, (7). He proved that those access structures may be realized ideally by a linear secret sharing scheme over fields $\mathbb{F}$ of size

$$|\mathbb{F}| > \binom{n}{k-1} \cdot (k-1) \ , \tag{55}$$

where also here $k = k_m$ is the highest threshold. This may be translated into another lower bound for the conjunctive case, independent of ours, (54), using duality arguments. Since in the dual access structure $k \mapsto n - k + 1$, see Proposition 4.1, we infer from Brickell's estimate (55) and duality that conjunctive hierarchical threshold access structures may be realized ideally over fields of size

$$|\mathbb{F}| > \binom{n}{k} \cdot (n-k) \ . \tag{56}$$

The ratio between the two lower bounds (54) and (56) is given by

$$\frac{\binom{n+1}{k} \cdot \frac{(k-2)(k-1)}{2} + k}{\binom{n}{k} \cdot (n-k)} \approx \frac{n+1}{n+1-k} \cdot \frac{(k-2)(k-1)}{2(n-k)} \ . \tag{57}$$

This ratio is less than 1 whenever

$$k < \frac{-1 + \sqrt{8n+9}}{2} \ . \tag{58}$$

Namely, for those values of k, estimate (54) is better than (56); for greater values of k the latter estimate is better. Note that usually k is expected to be significantly smaller than n (namely, it is expected to satisfy (58)). In any case, the ratio in (57) shows that the difference between the two lower bounds is quite insignificant since, when comparing the number of bits that are required for representing field elements, it translates into a small additive term.

5 Open problems

The classes $HTAS_\forall$ and $HTAS_\exists$ may be viewed as the two extreme cases in a sequence of classes:

Definition 5.1 *Let $\mathcal{U}$ be a set of n participants and assume that $\mathcal{U}$ is composed of levels, i.e., $\mathcal{U} = \bigcup_{i=0}^{m} \mathcal{U}_i$ where $\mathcal{U}_i \cap \mathcal{U}_j = \emptyset$ for all $0 \leq i < j \leq m$. Let $\mathbf{k} = \{k_i\}_{i=0}^{m}$ be a monotonically increasing sequence of integers, $0 < k_0 < \cdots < k_m$. Then, for $1 \leq \ell \leq m+1$, the $(\mathbf{k}, n)$–hierarchical threshold access structure of type $(\ell, m+1)$ is*

$$\Gamma = \left\{ \mathcal{V} \subset \mathcal{U} : \left| \mathcal{V} \cap \left(\cup_{j=0}^{i} \mathcal{U}_j \right) \right| \geq k_i \quad \text{for at least } \ell \text{ values of } i \in \{0, 1, \ldots, m\} \right\} . \tag{59}$$

We see that $HTAS_\exists$ and $HTAS_\forall$ are the classes of all hierarchical threshold access structures of types $(1, m+1)$ and $(m+1, m+1)$, respectively, for some value of m. It may be easily verified that the access structures of types $(\ell, m+1)$ and $(m+2-\ell, m+1)$ are dual. The question is whether the access structures of types $(\ell, m+1)$ where $1 < \ell < m+1$ are ideal, and if so, how can they be realized ideally and efficiently by a secret sharing scheme.

Closely related threshold access structures that were studied by Simmons [18] and Brickell [6] are *comparmented access structures*.

Definition 5.2 *Let $\mathcal{U}$ be a set of n participants and assume that $\mathcal{U}$ is composed of compartments, i.e., $\mathcal{U} = \bigcup_{i=1}^{m} \mathcal{U}_i$ where $\mathcal{U}_i \cap \mathcal{U}_j = \emptyset$ for all $1 \leq i < j \leq m$. Let $\mathbf{k} = \{k_i\}_{i=0}^{m}$ be a sequence of integers such that $k_0 \geq \sum_{i=1}^{m} k_i$. Then the $(\mathbf{k}, n)$–compartmented access structure is*

$$\Gamma = \{ \mathcal{V} \subset \mathcal{U} : |\mathcal{V} \cap \mathcal{U}_i| \geq k_i \ \ \forall i \in \{1, \ldots, m\} \text{ and } |\mathcal{V}| \geq k_0 \} . \tag{60}$$

Brickell proved that those access structures are ideal, but the secret sharing scheme that he proposed suffered from the same problem of inefficiency as some previously mentioned schemes did (namely, the dealer must perform possibly exponentially many checks when assigning identities and shares the participants). The question is whether there exists an efficient ideal secret sharing scheme for such access structures.

A Appendix: Monotone allocation of identities – study cases

The goal of this study is to illustrate the analysis that we carried out in Section 3.3 and to demonstrate its sharpness. We deal here with problems of low dimension $k \leq 4$. As the case $k = 2$ is trivially solvable for all given data (this may be seen also by condition (35)), we concentrate on dimensions $k = 3$ and $k = 4$. In each of those cases we list all possible types of Birkhoff interpolation that may occur in such a dimension, where the word type is in the same sense as in the proof of Theorem 3.6. In doing so, we speak of the *order* of a given type, which means the order of the highest derivative that appears in the interpolation.

A.1 $k = 3$

There are five different types of Birkhoff interpolation that might occur when $k = 3$: $\mathbf{d} = (0, 0, 0)$, $(0, 0, 1)$, $(0, 1, 1)$, $(0, 0, 2)$ and $(0, 1, 2)$. Recall that the notation $\mathbf{d}$ was introduced in the proof of Theorem 3.6 and it indicates the order of the derivative of the share of each of the participants in the subset that attempts to recover the common secret. For example, $\mathbf{d} = (0, 1, 1)$ refers to

the scenario where the first participant is from $\mathcal{U}_0$ and his share is $P(v_1)$, while the other two participants are from $\mathcal{U}_1$ and their contribution is $P'(v_i)$, $i = 2, 3$; i.e., the system of equations that needs to be solved has the following matrix of coefficients,

$$M_{\mathcal{V}} = \begin{pmatrix} 1 & v_1 & v_1^2 \\ 0 & 1 & 2v_2 \\ 0 & 1 & 2v_3 \end{pmatrix} .$$

The solvability of each of the five types of interpolation is as follows:

- (0,0,0) is solvable, since it represents standard interpolation.
- (0,1,1) is solvable by first recovering P' and then P.
- (0,0,2) is solvable by first recovering P'' and then P.
- (0,1,2) is solvable by recovering P'', then P' and then P.
- (0,0,1) is the only interesting case in dimension $k = 3$. Let

  $$0 \le v_1 < v_2 < v_3 \le N \tag{61}$$

  be the identities of the three participants, where v_1 and v_2 are the two values in which $P(x)$ is known. Looking for the polynomial in its Newton form,

  $$P(x) = c_0 + c_1(x - v_1) + c_2(x - v_1)(x - v_2) , \tag{62}$$

  the linear system that we have is characterized by the matrix

  $$\hat{M}_{\mathcal{V}} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & v_2 - v_1 & 0 \\ 0 & 1 & (v_3 - v_1) + (v_3 - v_2) \end{pmatrix} ,$$

  (compare to (37), (38) and (48)–(50)). Hence, the problem is well posed if and only if

  $$(v_3 - v_1) + (v_3 - v_2) \neq 0 \quad \text{in } \mathbb{F} = \mathbb{F}_q . \tag{63}$$

  In view of (61), a sufficient condition that guarantees the inequality in (63) is

  $$2N < q . \tag{64}$$

  Note that this condition agrees with (35) when $k = 3$.

A.2 $k = 4$

We claim that all interpolation types in dimension 4 are well posed, provided that

$$6N^3 < q . \tag{65}$$

This is a somewhat milder condition than (35) when $k = 4$: the power of N is the same in both estimates but the constant in (35) is approximately 7.8 as opposed to 6 in (65). We proceed to examine all of those types according to their order.

Interpolation types of order 3 may involve in dimension 4 only one datum of the third order, $P^{(3)}(v)$, otherwise they fail to comply with Pólya's condition, Lemma 2.1. We may use that datum in order to recover a_3 and then we are left with a problem of dimension 3 and order 2 at the most, as discussed in Section A.1. Hence, all types of order 3 are well posed provided that condition (64) holds. Since (65) is stronger than (64), we conclude that it is a sufficient condition for the solvability of all types of order 3.

Next, we concentrate on types of order 2. There are five such types that comply with Pólya's condition: $\mathbf{d} = (0,0,0,2), (0,0,1,2), (0,1,1,2), (0,0,2,2)$ and $(0,1,2,2)$. Types $(0,0,2,2)$ and $(0,1,2,2)$ are solvable by first recovering P'' and then P. Type $(0,1,1,2)$ is solvable under assumption (65). Indeed, if (65) holds, we may use the data in v_2, v_3 and v_4 in order to recover P' (the type of interpolation problem that needs to be solved to that end is $(0,0,1)$, as discussed in Section A.1) and then use $P(v_0)$ in order to determine a_0.

In order to deal with the remaining two types, $(0,0,0,2)$ and $(0,0,1,2)$, we rewrite the interpolant in Newton form,

$$P(x) = c_0 + c_1(x - v_1) + c_2(x - v_1)(x - v_2) + c_3(x - v_1)(x - v_2)(x - v_3) \ , \tag{66}$$

where

$$0 \leq v_1 < v_2 < v_3 < v_4 \leq N \ . \tag{67}$$

The matrix of coefficients for type $(0,0,0,2)$ is:

$$\hat{M}_{\mathcal{V}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & v_2 - v_1 & 0 & 0 \\ 1 & v_3 - v_1 & (v_3 - v_1)(v_3 - v_2) & 0 \\ 0 & 0 & 2 & 2\sum_{i=1}^{3}(v_4 - v_i) \end{pmatrix} ,$$

(see (37), (38) and (48)–(50)). Indeed, this system is solvable since (67)+(65) guarantee that $\sum_{i=1}^{3}(v_4 - v_i) \neq 0$ in $\mathbb{F} = \mathbb{F}_q$. As for the type $(0,0,1,2)$, the matrix of coefficients is

$$\hat{M}_{\mathcal{V}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & v_2 - v_1 & 0 & 0 \\ 0 & 1 & \sum_{i=1}^{2}(v_3 - v_i) & (v_3 - v_1)(v_3 - v_2) \\ 0 & 0 & 2 & 2\sum_{i=1}^{3}(v_4 - v_i) \end{pmatrix} , \tag{68}$$

and this matrix is non-singular provided that

$$\Delta = \sum_{i=1}^{2}(v_3 - v_i) \cdot \sum_{i=1}^{3}(v_4 - v_i) - (v_3 - v_1)(v_3 - v_2) \neq 0 \quad \text{in } \mathbb{F} = \mathbb{F}_q \ . \tag{69}$$

It is not hard to see that, as a real number, $\Delta > 0$ in the domain in $\mathbb{R}^4$ defined by (67). On the other hand, (67) implies that $\Delta < 2N \cdot 3N = 6N^2$. Therefore, $0 < \Delta < 6N^2$ which, by (65), implies (69).

Finally, we deal with types of order 1. Here, there are three types to consider: $(0,0,0,1)$, $(0,0,1,1)$ and $(0,1,1,1)$. The third one, $(0,1,1,1)$, is unconditionally solvable since we may recover P' and then, using $P(v_1)$, determine P. As for $(0,0,1,1)$, the polynomial coefficients in the Newton

form, (66), satisfy a linear system with the following matrix of coefficients

$$\hat{M}_{\mathcal{V}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & v_2 - v_1 & 0 & 0 \\ 0 & 1 & \sum_{i=1}^{2}(v_3 - v_i) & (v_3 - v_1)(v_3 - v_2) \\ 0 & 1 & \sum_{i=1}^{2}(v_4 - v_i) & \sum_{1 \le i < j \le 3}(v_4 - v_i)(v_4 - v_j) \end{pmatrix} . \tag{70}$$

Therefore, the solvability condition is

$$\Delta = \det \begin{pmatrix} \sum_{i=1}^{2}(v_3 - v_i) & (v_3 - v_1)(v_3 - v_2) \\ \sum_{i=1}^{2}(v_4 - v_i) & \sum_{1 \le i < j \le 3}(v_4 - v_i)(v_4 - v_j) \end{pmatrix} \neq 0 \quad \text{in } \mathbb{F} = \mathbb{F}_q \tag{71}$$

(67) implies that $0 < \Delta < 2N \cdot 3N^2$. Together with (65), we arrive at the conclusion that $\Delta \neq 0$ in $\mathbb{F}_q$. Finally, the type $(0, 0, 0, 1)$ gives rise to the matrix

$$\hat{M}_{\mathcal{V}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & v_2 - v_1 & 0 & 0 \\ 1 & v_3 - v_1 & (v_3 - v_1)(v_3 - v_2) & 0 \\ 0 & 1 & \sum_{i=1}^{2}(v_4 - v_i) & \sum_{1 \le i < j \le 3}(v_4 - v_i)(v_4 - v_j) \end{pmatrix} , \tag{72}$$

which is solvable since

$$\sum_{1 \le i < j \le 3} (v_4 - v_i)(v_4 - v_j) \neq 0 \quad \text{in } \mathbb{F} = \mathbb{F}_q \ , \tag{73}$$

as guaranteed by (65).

Acknowledgement. The author thanks the anonymous referees for insightful comments on the manuscript.

References

[1] K. Atkinson and A. Sharma, A partial characterization of poised Hermite-Birkhoff interpolation problems, *Siam Journal on Numerical Analysis*, 6 (1969), pp. 230-235.

[2] A. Beimel, T. Tassa and E. Weinreb, Characterizing ideal weighted threshold secret sharing, *The Second Theory of Cryptography Conference, TCC 2005*, LNCS 3378 (2005), MIT, Cambridge, pp. 600-619.

[3] J. Benaloh and J. Leichter, Generalized secret sharing and monotone functions, *Advances in Cryptology - CRYPTO 88*, LNCS 403 (1990) pp. 27-35.

[4] A. Beutelspacjer and K. Vedder, Geometric structures as threshold schemes, in *Cryptography and Coding*, Clarendon Press (1989), pp. 255-268.

[5] G.R. Blakley, Safeguarding cryptographic keys, *The National Computer Conference 1979*, AFIPS 48 (1979), pp. 313-317.

[6] E.F. Brickell, Some ideal secret sharing schemes, *Journal of Combinatorial Mathematics and Combinatorial Computing*, 9 (1989), pp. 105-113.

[7] C. Charnes, K. Martin, J. Pieprzyk and R. Safavi-Naini, Sharing secret information in hierarchical groups, *Information and Communications Security*, LNCS 1334 (1997) pp. 81-86.

[8] E. Dawson and D. Donovan, The breadth of Shamir's secret sharing scheme, *Computers and Security*, 13 (1994), pp. 69-78.

[9] D.K. Faddeev and I.S. Sominskii, *Problems in Higher Algebra*, San Francisco: W. H. Freeman, 1965.

[10] J. Friedman, Constructing $O(n \log n)$ size monotone formulae for the k-th elementary symmetric polynomial of n Boolean variables, *IEEE Symposium on Foundations of Computer Science*, (1984), pp. 506-515.

[11] A. Gál, *Combinatorial Methods in Boolean Function Complexity*, Ph.D. thesis, University of Chicago, 1995.

[12] M. Ito, A. Saito and T. Nishizeki, Secret sharing scheme realizing general access structure, *IEEE Global Telecommunications Conference*, (1987), pp. 99-102.

[13] M. Karchmer and A. Wigderson, On Span Programs, in *The 8th Structures in Complexity conference*, (1993), pp. 102-111.

[14] G.G. Lorentz, K. Jetter and S.D. Riemenschneider, *Birkhoff Interpolation*, In Encyclopedia of Mathematics and its Applications, Vol. 19 (1983), Addison-Wesley, Reading, Mass.

[15] C. Padró and G. Sáez, Secret sharing schemes with bipartite access structure, *Advances in Cryptology - EUROCRYPT 98*, LNCS 1403 (1998), pp. 500-511.

[16] Schoenberg, I.J., On Hermite-Birkhoff interpolation, J. Math. Anal. Appl., 16 (1966), pp. 538-543.

[17] A. Shamir, How to share a secret, *Communications of the ACM*, 22 (1979), pp. 612-613.

[18] G.J. Simmons, How to (really) share a secret, *Advances in Cryptology - CRYPTO 88*, LNCS 403 (1990), pp. 390-448.

[19] G.J. Simmons, An introduction to shared secret and/or shared control schemes and their applications, in *Contemporary Cryptology, The Science of Information Integrity*, IEEE Press (1991), pp. 441-497.

[20] T. Tassa, Hierarchical threshold secret sharing, in *The First Theory of Cryptography Conference, TCC 2004*, LNCS 2951 (2004), MIT, Cambridge, pp. 473-490.

[21] T. Tassa and N. Dyn, Multipartite Secret Sharing by Bivariate Interpolation, *The 33rd International Colloquium on Automata, Languages and Programming, ICALP 2006*, Part II, LNCS 4052 (2006), Venice, pp. 288-299.

[22] A. Wool, Private communication.