Hierarchical Threshold Secret Sharing

Tamir Tassa

Division of Computer Science,
The Open University, Tel Aviv, Israel
and
Department of Computer Science,
Ben Gurion University, Beer Sheva, Israel
tamir_tassa@yahoo.com

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 the course of this discussion, we borrow some results from the theory of Birkhoff interpolation over $\mathbb{R}$ and import them to the context of finite fields.

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 [4, 15]. Generalized secret sharing refers to situations where the collection of permissible subsets of $\mathcal{U}$ is any collection $\Gamma \subset 2^{\mathcal{U}}$. Given such a collection, the corresponding generalized secret sharing 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; this makes sense, of-course, only if the access structure is monotone in the sense that if $B \in \Gamma$ then any superset of B also belongs to Γ.

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. *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 $0 \le i < j \le m$. 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 secret sharing problem is the problem of assigning each participant $u \in \mathcal{U}$ a share of a given secret S such that the access structure is*

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

In other words, if $\sigma(u)$ stands for the share assigned to $u \in \mathcal{U}$, and for any $\mathcal{V} \subset \mathcal{U}$, $\sigma(\mathcal{V}) = \{\sigma(u) : u \in \mathcal{V}\}$, then

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

while

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

The zero conditional entropy equality (2) should be understood in a constructive sense. Namely, if it holds then $\mathcal{V}$ may compute S.

There are few methods of solving this problem. The simplest way [18] is to generate m random and independent secrets S_i, $1 \le i \le m$, of the same size as S and define $S_0 = S \bigoplus S_1 \bigoplus \cdots \bigoplus S_m$. Then, for every $0 \le i \le m$, the secret S_i is distributed among all participants of $\cup_{j=0}^{i} \mathcal{U}_j$ using a $(k_i, \sum_{j=0}^{i} |\mathcal{U}_j|)$ threshold secret sharing scheme. The secret S may be recovered only if all S_i, $0 \le i \le m$, 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 solution. 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, its information rate is $1/(m+1)$ since all members of $\mathcal{U}_0$ are assigned $m+1$ shares.

Another method is the monotone circuit construction due to Benaloh and Leichter [2]. Assume a monotone access structure Γ over a set of n participants. Let $C(x_1, \ldots, x_n)$ be a monotone circuit that recognizes the access structure (namely, $C(x_1, \ldots, x_n) = 1$ if and only if the subset of the variables that have a 1 value belongs to Γ). They then show how to build a perfect secret sharing scheme from the description of that circuit. 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 circuit is of size $O(n \log n)$ [9], which implies an information rate of $O(1/\log n)$ for the corresponding secret sharing scheme.

Another construction is due to Brickell [5]. The main observation in his construction is the following: 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. Assume that there exists a function $\phi : \mathcal{U} \to \mathbb{F}^d$ with the property

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

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

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

This is indeed a perfect secret sharing scheme, (2)+(3), and, as opposed to the previous construction of Benaloh and Leichter, it is ideal since every participant receives a share that is of the same size as the secret. Alas, finding a mapping ϕ that satisfies condition (4) is not simple. Given a specific access structure, it is usually a matter of trial and error until such ϕ is found.

In this paper, we present a simple solution for the hierarchical secret sharing problem that is both perfect and ideal. Our construction is, in fact, a realization of the general vector space construction of Brickell 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 [15] 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 $P \in \mathbb{R}_k[x]$. 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 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, this allocation of shares dictates 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 the Birkhoff interpolation problems that are associated with the authorized subsets would be well posed.

Organization of the paper. In Section 2 we review the basic terminology and results from the theory of Birkhoff interpolation [12]. 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 later on 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 4.

Related work. The problem of secret sharing in hierarchical (or *multilevel*) structures, was studied before under different assumptions, e.g. [3, 5–7, 16, 17]. Already Shamir, in his seminal work [15], 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, 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 $w_0 > w_1 > \cdots > w_m$. 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 [16], and later Brickell [5], considered a similar, yet slightly more rigid 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 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,

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

His solution to that version is based on a geometric construction that was presented by Blakley [4]. 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 suggests 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 $\mathcal{W}_i \cap W_\mathcal{S} = \{S\}$ 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 $W_\mathcal{S}$ 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.

Shamir's version of the hierarchical setting is slightly more relaxed than Simmons'. 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 note that none of the above mentioned explicit secret sharing schemes that are suitable for hierarchical structures (i.e., the first solution of splitting the secret to $m+1$ sub-secrets, Benaloh and Leichter's monotone circuit construction, Shamir's scheme and Simmons' scheme) is ideal. The scheme introduced herein is.

Padró and Sáez [13] studied the information rate of secret sharing schemes with a bipartite access structure. A bipartite access structure is one in which there are two levels of participants, $\mathcal{U} = \mathcal{U}_0 \cup \mathcal{U}_1$, and all participants in the same level 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, are consistent with Brickell's construction [5]. 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 [13, Theorem 5]. They characterized four types of quasi-threshold access structures, denoted Ω_i, $1 \le i \le 4$. It may be shown that when there are two levels, i.e., $m = 1$, our *conjunctive* problem, (1), is consistent with type Ω_2 or Ω_3, while Simmons' *disjunctive* problem, (7), agrees with Ω_1. What we show in this paper is that in the multi-partite case, the conjunctive threshold access structures are vector access structures and that Birkhoff interpolation yields an explicit construction.

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, $I(E) = \{(i,j) : e_{i,j} = 1\}$, $d = |I(E)|$, and $C = \{c_{i,j} : (i,j) \in I(E)\}$ be a set of d real values (we assume hereinafter that the right-most column in E is nonzero). 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*.

Unlike Lagrange or Hermite interpolation that are unconditionally well-posed, the Birkhoff interpolation problem may not admit a unique solution. The pair $\langle X, E\rangle$ is called *regular* if the system (8) has a unique solution for any choice of C, and *singular* otherwise. 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 [14].

Lemma 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*

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

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. *A* 1*-sequence in the interpolation matrix E is a maximal run of consecutive* 1*s in a row of the matrix E. Namely, a triplet of the form (i, j_0, j_1) where $1 \le i \le k$, $0 \le j_0 \le j_1 \le \ell$, such that $e_{i,j} = 1$ for all $j_0 \le j \le j_1$ 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* 1*s 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 1. *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 1, being algebraic, is not restricted to the reals and applies over any field. Theorem 1, on the other hand, relies upon the existence of *order* in $\mathbb{R}$. Hence, as finite fields are not ordered, Theorem 1 does not apply to them. However, Theorem 1 may be of use over finite fields as well 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. Let $\mathbb{F}$ be a finite field of large size, say $\mathbb{F}_q$ where q is a prime number. The size of the field is determined by the size of the secret S (for example, if S is an AES key then q should be at least 128 bits long). Let $k = k_m$ be the overall number of participants that are required for recovery of the secret. Then the dealer selects a random polynomial $P(x) \in \mathbb{F}_{k-1}[x]$, where

$$P(x) = \sum_{i=0}^{k-1} a_i x^i \quad \text{and} \quad a_0 = S \ , \tag{10}$$

and then distributes shares to all participants $u \in \mathcal{U}$ in the following manner. First, each participant is identified with a field element, which we also denote by u (i.e., $\mathcal{U}$ may be viewed as a subset of the field $\mathbb{F}$). Then, each participant of the ith level in the hierarchy, $u \in \mathcal{U}_i$, $0 \le i \le m$, receives the share $P^{(k_{i-1})}(u)$, i.e., the (k_{i-1})th derivative of $P(x)$ at $x = u$, where $k_{-1} = 0$. This scheme is of-course ideal, as every participant receives a share that is a field element, just like the secret. Note that the Shamir secret sharing scheme [15] 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

$$\begin{array}{c} v_1, \ldots, v_{\ell_0} \in \mathcal{U}_0 \\ v_{\ell_0+1}, \ldots, v_{\ell_1} \in \mathcal{U}_1 \\ \vdots \\ v_{\ell_{m-1}+1}, \ldots, v_{\ell_m} \in \mathcal{U}_m \end{array} \quad \text{where} \quad 0 \le \ell_0 \le \cdots \le \ell_m = |\mathcal{V}| \ . \tag{11}$$

$\mathcal{V}$ 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 $\mathcal{V}$, (11), 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),

$$M_{\mathcal{V}} = \Big(\mathbf{r}(v_1), \ldots, \mathbf{r}(v_{\ell_0}) \ ; \ \mathbf{r}^{(k_0)}(v_{\ell_0+1}), \ldots, \mathbf{r}^{(k_0)}(v_{\ell_1}) \ ; \ \ldots \ ;$$

$$\mathbf{r}^{(k_{m-1})}(v_{\ell_{m-1}+1}), \ldots, \mathbf{r}^{(k_{m-1})}(v_{\ell_m})\Big) \ , \tag{12}$$

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 1. *The Birkhoff interpolation problem that needs to be solved by an authorized subset satisfies Pólya's condition (9).*

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 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 $M_{\mathcal{V}}$, (12), 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 (11). 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 $0 \le j \le m$; i.e., using the notations of (11),

$$\ell_i \ge k_i \quad 0 \le i \le j-1 \quad , \quad \ell_j = k_j - 1 \quad \text{and} \quad \ell_i \ge k_i - 1 \quad j+1 \le i \le m \ . \tag{13}$$

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 $M_{\mathcal{V}}$; let $\mathcal{V}_0 = \mathcal{V} \setminus \mathcal{W}$. By (13),

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

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. $\square$

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

$$\mathrm{Prob}(\mathcal{U} = \mathcal{W}) = \frac{1}{\binom{q-1}{n}} \qquad \forall\, \mathcal{W} \subset \mathbb{F} \setminus \{0\}\ ,\ |\mathcal{W}| = n\ . \tag{14}$$

Theorem 3. *Assume a random allocation of participant identities, (14). Let $\mathcal{V}$ be a randomly selected subset from $2^{\mathcal{U}}$. Then if $\mathcal{V} \in \Gamma$*

$$\mathit{Prob}\,(H(S|\sigma(\mathcal{V})) = 0) \geq 1 - \varepsilon\ , \tag{15}$$

while otherwise

$$\mathit{Prob}\,(H(S|\sigma(\mathcal{V})) = H(S)) \geq 1 - \varepsilon\ , \tag{16}$$

where

$$\varepsilon = \frac{(k-2)(k-1)}{2(q-k)}\ . \tag{17}$$

Proof. Let $\mathcal{V} \in \Gamma$ be an authorized subset, not necessarily minimal. In view of Theorem 2 there exists a minimal authorized subset $\mathcal{V}_0$ (i.e., $|\mathcal{V}_0| = k$) such that if $\det M_{\mathcal{V}_0} \neq 0$, $\mathcal{V}$ may recover S. On the other hand, we saw in Theorem 2 that if $0 \in \mathcal{U}_0$ and $\mathcal{V} \notin \Gamma$ is an unauthorized subset, 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, (15) and (16), 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, (11). We proceed to show that

$$\mathrm{Prob}\,(\det(M_{\mathcal{V}}) = 0) \leq \frac{(k-2)(k-1)}{2(q-k)}\ . \tag{18}$$

Noting that (18) 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 $\mathcal{V} \cap \mathcal{U}_m$).

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

$$\det(M_{\mathcal{V}}) = \sum_{i=0}^{k-2-h} c_i v_k^i + \frac{(k-1)!}{(k-1-h)!} \cdot \mu_{k-1} \cdot v_k^{k-1-h}\ , \tag{19}$$

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

$$\mathrm{Prob}(\det(M_{\mathcal{V}}) = 0) =$$

$$= \sum_{\mathbf{v} \in \mathbb{F}^{k-1} \setminus \Omega} \mathrm{Prob}(\det(M_{\mathcal{V}}) = 0 | \mathbf{v}) \cdot \mathrm{Prob}(\mathbf{v}) + \sum_{\mathbf{v} \in \Omega} \mathrm{Prob}(\det(M_{\mathcal{V}}) = 0 | \mathbf{v}) \cdot \mathrm{Prob}(\mathbf{v}) \ . \tag{20}$$

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, (19). Hence, there are at most $k-1-h$ values of v_k for which $\det(M_{\mathcal{V}}) = 0$. This implies that

$$\mathrm{Prob}(\det(M_{\mathcal{V}}) = 0 | \mathbf{v}) \leq \frac{k-1-h}{(q-1)-(k-1)} \qquad \forall \mathbf{v} \in \mathbb{F}^{k-1} \setminus \Omega \tag{21}$$

(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, $\mathrm{Prob}(\det(M_{\mathcal{V}}) = 0) = 0$. Therefore, the worst case in (21) is when $h = 1$. Hence, we rewrite (21) as follows:

$$\mathrm{Prob}(\det(M_{\mathcal{V}}) = 0 | \mathbf{v}) \leq \frac{k-2}{q-k} \qquad \forall \mathbf{v} \in \mathbb{F}^{k-1} \setminus \Omega \ . \tag{22}$$

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., (18) for $k-1$) and conclude that

$$\mathrm{Prob}(\mathbf{v} \in \Omega) \leq \frac{(k-3)(k-2)}{2(q-k+1)} \ . \tag{23}$$

Finally, combining (20), (22) and (23) we may prove (18) in this case:

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

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

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

The proof is thus complete. □

Theorem 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 $\Theta(1/q)$ and therefore negligible, as it is equivalent to the probability of simply guessing the secret.

Corollary 1. *Assume a random allocation of participant identities, (14). Then the probability that the resulting scheme has accessibility, (2), for all authorized subsets and and perfect security, (3), for all unauthorized subsets is at least* $1-\binom{n+1}{k}\cdot\varepsilon$*, where* ε *is as in (17).*

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.

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 size of the underling field, q, is sufficiently large.

For every $0 \le i \le m$ 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,

$$u \in \mathcal{U}_i \ , \ v \in \mathcal{U}_j \ , \ i < j \Rightarrow u < v \ , \tag{24}$$

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

In Lemma 2 and Theorem 4 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 2 we prove our basic lower bound on q that guarantees these two conditions. Then, in Theorem 4, we use the bound of Lemma 2 and carry out a more delicate analysis that yields a better bound.

Lemma 2. *Let* $(\mathbf{k}, n)$ *be a hierarchical secret sharing problem. Assume that the participants in* $\mathcal{U}$ *were assigned identities in* $\mathbb{F}$ *in a monotone manner, namely, in concert with condition (24), and let* $N = \max\mathcal{U}$*. Finally, assume that*

$$2^{-k} \cdot (k+1)^{(k+1)/2} \cdot N^{(k-1)k/2} < q = |\mathbb{F}| \ , \tag{25}$$

(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 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 $M_{\mathcal{V}}$, (12), is regular. Without loss of generality we assume that the participant identities in $\mathcal{V}$ are given by (11) (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

$$\det M_{\mathcal{V}} \neq 0 \qquad \text{in } \ \mathbb{R} \ . \tag{26}$$

Then, invoking (25), we shall prove that

$$|\det M_{\mathcal{V}}| < q \qquad \text{in } \mathbb{R} . \tag{27}$$

Combining (26) and (27) we conclude that $\det M_{\mathcal{V}} \neq 0$ in $\mathbb{F} = \mathbb{Z}_q$, as required.

In order to prove (26), 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. Recalling Proposition 1, we infer that the conditions of Theorem 1 are satisfied. Therefore, the corresponding Birkhoff interpolation problem is well-posed over $\mathbb{R}$, (26).

In order to bound the determinant of $M_{\mathcal{V}}$, we invoke Hadamard's maximal determinant theorem [8, problem 523]. According to that theorem, if A is a $k \times k$ real matrix, and

$$|A_{i,j}| \leq 1 \quad , \quad 0 \leq i, j \leq k-1 , \tag{28}$$

then

$$|\det(A)| \leq 2^{-k} \cdot (k+1)^{(k+1)/2} . \tag{29}$$

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 (28), we conclude, in view of (29) and (25), that $M_{\mathcal{V}}$ satisfies (27). That completes the proof. $\square$

Theorem 4. *Under the conditions of Lemma 2, the hierarchical secret sharing scheme satisfies conditions (2) and (3) provided that*

$$\alpha(k) N^{(k-1)(k-2)/2} < q = |\mathbb{F}| \quad \textit{where} \quad \alpha(k) := 2^{-k+2} \cdot (k-1)^{(k-1)/2} \cdot (k-1)! . \tag{30}$$

Proof. Assume that $\mathcal{V} \in \Gamma$ is as in (11), and assume that it has k participants whose identities are ordered in the usual sense in $\mathbb{R}$, $v_1 < v_2 < \cdots < v_k$. Let d_i, $1 \leq i \leq k$, be the order of derivative of the share that v_i got. Namely, in view of (11) and (12), $d_i = 0$ for $1 \leq i \leq \ell_0$, $d_i = k_0$ for $\ell_0 + 1 \leq i \leq \ell_1$, 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 $M_{\mathcal{V}}$, (12). Finally, let t be the largest integer such that $d_i = i - 1$ for all $1 \leq i \leq t$. We note that t is well defined and $t \geq 1$ 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 P from the shares of $\{v_i\}_{1 \leq i \leq k}$. 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, $t-1 \leq i \leq k-1$, see (10)) from the shares of v_i, $t \leq i \leq k$.

– Problem $\mathcal{P}_2$. Recovering a_{i-1} from the share of v_i, for $i = t-1, \dots, 1$.

Indeed, the equations that correspond to the $k-t+1$ last 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, $i = t-1, \dots, 1$, 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 1.)

The dimension of the interpolation problem $\mathcal{P}_1$ is $k-t+1$. Hence, since the left hand side in (30) 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 (10)):

$$P(x) = \sum_{j=0}^{k-1} c_j \prod_{i=1}^{j} (x - v_i) \; . \tag{31}$$

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,

$$\hat{M} = \begin{pmatrix} B_1 & 0 \\ B_2 & B_3 \end{pmatrix} \tag{32}$$

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

$$B_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 1 & v_2 - v_1 & 0 & 0 & \cdots & 0 \\ 1 & v_3 - v_1 & \prod_{i=1}^{2}(v_3 - v_i) & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & v_s - v_1 & \prod_{i=1}^{2}(v_s - v_i) & \prod_{i=1}^{3}(v_s - v_i) & \cdots & \prod_{i=1}^{s-1}(v_s - v_i) \end{pmatrix} \tag{33}$$

(we use the notation $\hat{M}$ in order to distinguish this matrix from $M = M_{\mathcal{V}}$, (12), that was the coefficient matrix in the linear system for the unknowns a_i in the standard representation of the interpolant $P(x)$, (10)). Invoking the same arguments as in Lemma 2, we conclude that

$$\det \hat{M} \neq 0 \qquad \text{in } \ \mathbb{R} \ . \tag{34}$$

We need to show that

$$\det \hat{M} \neq 0 \qquad \text{in } \ \mathbb{F} \ . \tag{35}$$

In order to prove (35), we first invoke (32) to conclude that

$$\det \hat{M} = \det B_1 \cdot \det B_3 \ . \tag{36}$$

As $N < q$, all terms on the diagonal of B_1, (33), are nonzero in $\mathbb{F}$, so that B_1 is invertible over $\mathbb{F}$. Therefore, by (36), we only need to show that

$$\det B_3 \neq 0 \qquad \text{in } \ \mathbb{F} \ , \tag{37}$$

in order to prove (35). Since $\det B_3 \neq 0$ in $\mathbb{R}$, as implied by (34) and (36), this amounts to showing that

$$|\det B_3| < q \qquad \text{in } \ \mathbb{R} \ . \tag{38}$$

In order to prove (38), we shall show that

$$|\hat{M}_{i,j}| \leq j \cdot N^{j-1} \quad \text{for all} \quad s+1 \leq i \leq k \ , \ s \leq j \leq k-1 \tag{39}$$

(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 (38) 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 (39), the normalized block A satisfies condition (28) of Hadamard's maximal determinant theorem. Hence, by (29),

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

Consequently, since $s \geq 2$,

$$|\det B_3| = |\det A| \cdot \left(\prod_{j=s}^{k-1} j \cdot N^{j-1} \right) \leq 2^{-k+2} \cdot (k-1)^{(k-1)/2} \cdot (k-1)! \cdot N^{(k-1)(k-2)/2} \ . \tag{40}$$

Inequalities (40) and (30) prove (38).

The only missing link is (39). In order to prove this inequality, we need to derive an expression for the derivatives of $P(x)$, (31). Let us introduce the notations

$$P_j(x) = \prod_{i=1}^{j} (x - v_i) \quad \text{and} \quad P_{j,h}(x) = \frac{d^h P_j(x)}{dx^h} \quad , \quad 0 \leq j \leq k-1 \ , \ h \geq 0 \ . \tag{41}$$

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

$$P^{(h)}(x) = \sum_{j=h}^{k-1} c_j P_{j,h}(x) \ . \tag{42}$$

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

$$P_{j,h}(x) = \sum \left\{ \Pi_{(g_1,\ldots,g_h)}(x) \ : \ (g_1, \ldots, g_h) \in G(j,h) \right\} \ , \tag{43}$$

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

$$\Pi_{(g_1,\ldots,g_h)}(x) = \prod \left\{ (x - v_i) \ : \ i \in \{1, \ldots, j\} \setminus \{g_1, \ldots, g_h\} \right\} \ . \tag{44}$$

Setting $x = v_\ell$, for some $s + 1 \leq \ell \leq k$, in (42), we see that the ℓth row in $\hat{M}$ takes the form

$$(\hat{M}_{\ell,j})_{0 \leq j \leq k-1} = \begin{pmatrix} 0 \cdots 0 \ P_{h,h}(v_\ell) \cdots P_{k-1,h}(v_\ell) \end{pmatrix} \ , \tag{45}$$

where $h = d_\ell$ is the order of derivative of the share of v_ℓ. From (43),

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

Since, by (44), $|\Pi_{(g_1,\ldots,g_h)}(v_\ell)| \leq N^{j-h}$, we conclude that

$$|P_{j,h}(v_\ell)| \leq \frac{j!}{(j-h)!} \cdot N^{j-h} \quad , \quad h \leq j \leq k-1 \ . \tag{46}$$

As the definition of s implies that $h \geq 1$ for all rows $s + 1 \leq \ell \leq k$, and since $j \leq k - 1 < N$, we infer by (46) and (45) that

$$|\hat{M}_{\ell,j}| \leq j \cdot N^{j-1} \quad , \quad h \leq j \leq k-1 \ . \tag{47}$$

Since, by (45), the inequality in (47) holds trivially for columns $0 \leq j \leq h - 1$ as well, that proves (39). The proof of the theorem is thus complete. $\square$

Condition (30) 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.

Table 1 includes for each value of k, $5 \leq k \leq 8$, the maximal value of N for which the original condition, (25), and the improved one, (30), 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 (30) 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.

k	Condition (25)	Condition (30)
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 (25) and (30)

4 An ideal scheme for the disjunctive hierarchical secret sharing problem

As described in the Introduction, Simmons [16] studied a closely related hierarchical secret sharing problem, where the conjunction of threshold conditions is replaced by a disjunction (compare (1) to (7)). His solution to the problem was not ideal. Using the ideal secret sharing scheme that we presented herein for the conjunctive version of the problem, we may get an ideal secret sharing scheme also for the disjunctive version.

Karchmer and Wigderson [11] 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 [10] it was shown that if $\mathcal{M} = (\mathbb{F}, M, \mathcal{U}, \phi, \mathbf{e})$ is a MSP that realizes a monotone access structure Γ, then there exists a 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 2. *Let* $\mathcal{U} = \bigcup_{i=0}^{m} \mathcal{U}_i$ *and* $\mathbf{k} = \{k_i\}_{i=0}^{m}$ *be as in Definition 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 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, at least over fields that are sufficiently large, we conclude the following.

Corollary 2. *The disjunctive access structure (7) is ideal.*

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

References

1. Atkinson, K., Sharma, A.: A partial characterization of poised Hermite-Birkhoff interpolation problems. Siam Journal on Numerical Analysis **6** (1969) 230-235
2. Benaloh, J., Leichter, J.: Generalized secret sharing and monotone functions. Advances in Cryptology - CRYPTO 88, LNCS **403** (1990) 27-35
3. Beutelspacjer, A., Vedder, K.: Geometric structures as threshold schemes. In Cryptography and Coding, Clarendon Press (1989) 255-268
4. Blakley, G.R.: Safeguarding cryptographic keys. In Proceedings of the National Computer Conference, AFIPS **48** (1979) 313-317
5. Brickell, E.F.: Some ideal secret sharing schemes. Journal of Combinatorial Mathematics and Combinatorial Computing **9** (1989) 105-113
6. Charnes, C., Martin, K., Pieprzyk, J., Safavi-Naini, R.: Sharing secret information in hierarchical groups. Information and Communications Security, LNCS **1334** (1997) 81-86
7. Dawson, E., Donovan, D.: The breadth of Shamir's secret sharing scheme. Computers and Security **13** (1994) 69-78
8. Faddeev, D.K., Sominskii, I.S.: Problems in Higher Algebra, San Francisco, W. H. Freeman, 1965
9. Friedman, J.: 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) 506-515
10. Gál, A.: Combinatorial Methods in Boolean Function Complexity. Ph.D. thesis, University of Chicago, 1995
11. Karchmer, M., Wigderson, A.: On span programs. In 8th Annual Conference on Structure in Complexity Theory (SCTC'93), IEEE Computer Society Press (1993) 102-111
12. Lorentz, G.G., Jetter, K., Riemenschneider, S.D.: Birkhoff Interpolation. In Encyclopedia of Mathematics and its Applications **19** (1983), Addison-Wesley, Reading, Mass.
13. Padró, C., Sáez, G.: Secret sharing schemes with bipartite access structure. Advances in Cryptology - EUROCRYPT 98, LNCS **1403** (1998) 500-511
14. Schoenberg, I.J.: On Hermite-Birkhoff interpolation. Journal of Mathematical Analysis and Applications **16** (1966) 538-543
15. Shamir, A.: How to share a secret. Communications of the ACM **22** (1979) 612-613
16. Simmons, G.J.: How to (really) share a secret. Advances in Cryptology - CRYPTO 88, LNCS **403** (1990) 390-448
17. Simmons, G.J.: An introduction to shared secret and/or shared control schemes and their applications. In Contemporary Cryptology, The Science of Information Integrity, IEEE Press (1991) 441-497
18. Wool, A.: Private communication