Multipartite Secret Sharing by Bivariate Interpolation*

Tamir Tassa[†] Nira Dyn[‡]

Abstract

Given a set of participants that is partitioned into distinct compartments, a multipartite access structure is an access structure that does not distinguish between participants that belong to the same compartment. We examine here three types of such access structures: two that were studied before – compartmented access structures and hierarchical threshold access structures, and a new type of compartmented access structures that we present herein. We design ideal perfect secret sharing schemes for these types of access structures that are based on bivariate interpolation. The secret sharing schemes for the two types of compartmented access structures are based on bivariate Lagrange interpolation with data on parallel lines. The secret sharing scheme for the hierarchical threshold access structures is based on bivariate Lagrange interpolation with data on lines in general position. The main novelty of this paper is the introduction of bivariate Lagrange interpolation and its potential power in designing schemes for multipartite settings, as different compartments may be associated with different lines or curves in the plane. In particular, we show that the introduction of a second dimension may create the same hierarchical effect as polynomial derivatives and Birkhoff interpolation were shown to do in [17].

Keywords. Secret sharing, multipartite access structures, compartmented access structures, hierarchical threshold access structures, bivariate interpolation, monotone span programs.

AMS (2000) Subject Classification: Primary: 94A60 Secondary: 65D05

[*] A preliminary version of this paper appeared in The Proceedings of ICALP 2006

[†] Division of Computer Science, The Open University, Ra'anana, Israel.

[‡] Department of Applied Mathematics, Tel Aviv University, Tel Aviv, Israel.

1 Introduction

Secret sharing schemes have attracted a lot of attention over the past decade. A great deal of the ongoing research in this area is devoted to the properties of multipartite access structures and to secret sharing schemes (especially ideal ones) that realize them. Letting $\mathcal{U} = \{u_1, \ldots, u_n\}$ be the underlying set of participants and $\mathcal{P} = \{\mathcal{C}_1, \ldots, \mathcal{C}_m\}$ be a partition of $\mathcal{U}$ into m disjoint subsets, or *compartments*, an m-partite (or multipartite) access structure on $\mathcal{U}$ with respect to partition $\mathcal{P}$ is any access structure that does not distinguish between members of the same compartment. Weighted threshold access structures [15, 1], multilevel access structures [16, 3], hierarchical threshold access structures [17], compartmented access structures [3, 9], bipartite access structures [13], and tripartite access structures [1, 5, 9] are typical examples of such multipartite access structures.

There are several reasons why multipartite access structures were the focus of attention of so many studies in secret sharing, from the first years of secret sharing [15, 16, 3] till today, e.g. [6]. The first reason lies in their generality; in fact, every access structure may be viewed as a multipartite access structure with singleton compartments (though, usually, when speaking of multipartite access structures one thinks of settings in which m, the number of compartments, is significantly smaller than n, the number of participants). The second reason is that those are very natural and well-motivated access structures, from both theoretical and practical points of view. The practical motivation stems from the fact that we live in a world where everyone is equal, but some are more equal than others. The theoretical motivation is due to the fact that such access structures usually have a very concise description by a small set of conditions, and since they seem like a natural way of generalizing threshold access structures: Instead of imposing a threshold condition on the number of participants in a given subset, we impose a small set of conditions on the number of participants in the subset from each of the compartments.

Shamir's threshold secret sharing scheme [15] is based on polynomial interpolation. That scheme realizes the k-out-of-n threshold access structure, where any subset of $\mathcal{U}$ of size at least k is authorized to recover the secret S. Letting the secret S be an element of a finite field $\mathbb{F}$, the dealer selects a random polynomial $P(x)$ of degree $k-1$ over $\mathbb{F}$ where $P(0) = S$. Each participant $u_i \in \mathcal{U}$ is identified with some (public) identity in the field, $x_i \in \mathbb{F}$, and is given the private share $P(x_i)$. Clearly, any subset of $\mathcal{U}$ of size at least k has enough information to recover P, and, consequently, also the secret. It is easy to see that any subset of size less than k remains completely oblivious regarding the value of $S = P(0)$.

Polynomial interpolation served as the basis for secret sharing also in [17] for realizing hierarchical threshold access structures. Such access structures are multipartite where the partition represents a hierarchy on $\mathcal{U}$. In order to distinguish between the participants of different levels, the dealer uses polynomial derivatives. Participants of lesser ranks in the hierarchy receive private shares that correspond to higher derivatives of the polynomial, as such shares convey less information on the polynomial than shares that correspond to lower derivatives. By appropriately selecting the orders of the derivatives and the identities of the participants in the underlying field, one obtains a secret sharing scheme that realizes the hierarchical threshold access structure.

In this paper we show how to utilize bivariate interpolation in order to realize some multipartite access structures. Letting $\mathbb{F}$ be a finite field of size $q = |\mathbb{F}|$ sufficiently large so that the domain of all possible secrets may be embedded in $\mathbb{F}$, the secret $S \in \mathbb{F}$ is encoded by the coefficients of an unknown bivariate polynomial $P(x, y) \in \mathbb{F}[x, y]$. The dealer associates each participant $u_i \in \mathcal{U}$ with a unique point $(x_i, y_i) \in \mathbb{F}^2$ and gives that participant the private share $P(x_i, y_i)$. The idea is to select the participant identities and the secret value so that authorized subsets will be able to recover $P(x, y)$ and, consequently, the secret, while unauthorized subsets will not be able to learn any information about the secret. What makes bivariate interpolation suitable for multipartite settings is the ability to associate each compartment with a different line in the plane. Namely, participants from a given compartment are associated with points that lie on the same line, where each compartment is associated with a different line.

To the best of our knowledge, this is the first time in which bivariate interpolation is used in the context of secret sharing. Bivariate polynomials were used in conjunction with secret sharing in the past, e.g. [12]. However, those bivariate polynomials were no more than a sequence of univariate polynomials. Namely, the bivariate polynomial $P(x, y)$ was interpreted as a sequence of univariate polynomials $\{P(\cdot, y) : y \in \mathbb{F}\}$ and Shamir's threshold secret sharing scheme was utilized separately on each of those univariate polynomials.

The paper is organized as follows. In Section 2 we provide the necessary formal definitions and notation agreements regarding secret sharing (Subsection 2.1) and monotone span programs (Subsection 2.2). We also outline the main idea of our proof strategy (Subsection 2.3) and review some basic results in algebra that we shall use later on (Subsection 2.4). In Section 3 we deal with compartmented access structures. We distinguish between two types of such structures: one that agrees with the type that was presented and studied by Brickell in [3], and another that we present here for the first time. We design for those access structures ideal secret sharing schemes that are based on bivariate Lagrange interpolation with data on parallel lines. In Section 4 we deal with hierarchical threshold access structures and we realize them by bivariate Lagrange interpolation with data on lines in general position. In [17], those access structures were realized by introducing polynomial derivatives and Birkhoff interpolation in order to create the desired hierarchy between the different compartments (that are called *levels* in that context). Here, we show that we may achieve the same hierarchical effect by introducing a second dimension, in lieu of polynomial derivatives. All necessary background from bivariate interpolation theory is provided there. Finally, in Section 5, we contemplate on the possible advantages of using more involved interpolation settings.

2 Preliminaries

2.1 Secret Sharing

Hereinafter, we adopt the following notation convention: Vectors are denoted by bold-face letters while their components are denoted with the corresponding italic-type indexed letter. In addition, $\mathbb{N}$ stands for the nonnegative integers.

We begin by formal definitions of access structures and secret sharing schemes.

Definition 2.1 (Access Structure) *Let $\mathcal{U} = \{u_1, \ldots, u_n\}$. A collection $\Gamma \subseteq 2^{\mathcal{U}}$ is monotone if $\mathcal{V} \in \Gamma$ and $\mathcal{V} \subseteq \mathcal{W}$ imply that $\mathcal{W} \in \Gamma$. An access structure is a monotone collection $\Gamma \subseteq 2^{\mathcal{U}}$ of non-empty subsets of $\mathcal{U}$. Sets in Γ are called authorized, and sets not in Γ are called unauthorized. An authorized set $\mathcal{V} \in \Gamma$ is called a minterm if for every $\mathcal{W} \subsetneq \mathcal{V}$, the set $\mathcal{W}$ is unauthorized. An unauthorized set $\mathcal{V} \notin \Gamma$ is called a maxterm if for every $\mathcal{W} \supsetneq \mathcal{V}$, the set $\mathcal{W}$ is authorized.*

Definition 2.2 (Secret-Sharing Scheme) *Let $\mathcal{S}$ be a finite set of secrets, where $|\mathcal{S}| \geq 2$. A (perfect) secret-sharing scheme Π on $\mathcal{U} = \{u_1, \ldots, u_n\}$ with domain of secrets $\mathcal{S}$ is a randomized mapping from $\mathcal{S}$ to a set of n-tuples $\prod_{i=1}^{n} \mathcal{S}_i$, where $\mathcal{S}_i$ is called the share-domain of u_i. A dealer shares a secret $S \in \mathcal{S}$ among the n participants of $\mathcal{U}$ according to Π by first sampling a vector of shares $\Pi(S) = (S_1, \ldots, S_n) \in \prod_{i=1}^{n} \mathcal{S}_i$, and then privately communicating each share S_i to the participant u_i. We say that Π realizes an access structure $\Gamma \subseteq 2^{\mathcal{U}}$ if the following two requirements hold:*

Correctness. *The secret S can be reconstructed by any authorized set of participants. That is, for any authorized set $\mathcal{V} \in \Gamma$ (where $\mathcal{V} = \{u_{i_1}, \ldots, u_{i_{|\mathcal{V}|}}\}$), there exists a reconstruction function*[1] $\textsc{Recon}_{\mathcal{V}} : \mathcal{S}_{i_1} \times \cdots \times \mathcal{S}_{i_{|\mathcal{V}|}} \to \mathcal{S}$ *such that for every $S \in \mathcal{S}$ and for every possible value of the restriction of $\Pi(S)$ to its $\mathcal{V}$-entries, denoted $\Pi_{\mathcal{V}}(S)$, the following equality holds:*

$$\textsc{Recon}_{\mathcal{V}}(\Pi_{\mathcal{V}}(S)) = S.$$

Privacy. *Every unauthorized set can learn nothing about the secret (in the information theoretic sense) from their shares. Formally, for any unauthorized set $\mathcal{W} \notin \Gamma$, for every two secrets $S, S' \in \mathcal{S}$, and for every possible $|\mathcal{W}|$-tuple of shares $\langle S_i \rangle_{u_i \in \mathcal{W}}$:*

$$\Pr[\,\Pi_{\mathcal{W}}(S) = \langle S_i \rangle_{u_i \in \mathcal{W}}\,] \quad = \quad \Pr[\,\Pi_{\mathcal{W}}(S') = \langle S_i \rangle_{u_i \in \mathcal{W}}\,].$$

Viewing the secret S as a random variable that takes values in $\mathcal{S}$, and letting $H(\cdot)$ denote the entropy, the correctness and privacy requirements are equivalent to saying that for any value of the random mapping Π,

$$H(S|\Pi_{\mathcal{V}}(S)) = 0 \quad \forall \mathcal{V} \in \Gamma\,, \quad \text{while} \quad H(S|\Pi_{\mathcal{V}}(S)) = H(S) \quad \forall \mathcal{V} \notin \Gamma\,.$$

We proceed to define multipartite access structures.

[1] The reconstruction function $\textsc{Recon}_{\mathcal{V}}$ need not be efficiently implemented. However, this is the case for all the secret sharing schemes designed in this paper.

Definition 2.3 (Multipartite Access Structures) *Let $\mathcal{U}$ be a set of participants and assume that it is partitioned into m disjoint compartments,*

$$\mathcal{U} = \bigcup_{i=1}^{m} \mathcal{C}_i \ . \tag{1}$$

Let $\Gamma \in 2^{\mathcal{U}}$ be an access structure on $\mathcal{U}$ and assume that for all permutations $\pi : \mathcal{U} \to \mathcal{U}$ such that $\pi(\mathcal{C}_i) = \mathcal{C}_i$, $1 \le i \le m$, $\mathcal{V} \in \Gamma$ if and only if $\pi(\mathcal{V}) \in \Gamma$. Then Γ is called m-partite or multipartite with respect to partition (1).

Given any subset $\mathcal{W} \subseteq \mathcal{U}$, its *type* with respect to partition (1) is the vector $(t_1, \ldots, t_m) \in \mathbb{N}^m$ where $t_i = |\mathcal{W} \cap \mathcal{C}_i|$, $1 \le i \le m$. In view of Definition 2.3, the status of a given subset with respect to the multipartite access structure is solely determined by its type.

In every secret-sharing scheme, the size of the domain of shares of each participant is at least the size of the domain of the secrets [11], namely $|\mathcal{S}_i| \ge |\mathcal{S}|$ for all $1 \le i \le n$. This motivates the next definition.

Definition 2.4 (Ideality) *A secret-sharing scheme with domain of secrets $\mathcal{S}$ is ideal if the domain of shares of each user is $\mathcal{S}$. An access structure Γ is ideal if for some finite domain of secrets $\mathcal{S}$ there exists an ideal secret sharing scheme realizing it.*

In the Shamir k-out-of-n threshold secret sharing scheme that was described in the introduction, the domain of secrets is some finite field $\mathbb{F}$. That field serves also as the domain of possible private shares for each participant. Therefore, that scheme is ideal.

It is important to note that ideality is concerned only with the *private* data, and does not care about additional *public* data. For example, in the Shamir scheme, there are other pieces of information that are public, like k, n and the identities of all participants. The reason for this distinction between the private and public data is twofold: First, the security of any system tends to degrade when the amount of information that must be kept secret increases. Second, the size of the private shares influences the memory constraints for the participants as well as the efficiency of the distribution algorithm. Based on this distinction between private and public data, we present in this paper a novel framework in which the dealer publishes shares of some dummy participants, in addition to the private shares that are distributed to the real participants. Our schemes are still ideal, since the private shares are drawn from the same field $\mathbb{F}$ from which the secret is drawn. In fact, our proof techniques may be used to show that the dealer may always select the polynomial $P(x, y)$ so that the public shares of the dummy participants are all zero (whence, they need not be published). However, for convenience, we prefer to describe our ideal schemes in the more natural setting where we simply publish the shares of the dummy participants.

Most previously known secret sharing schemes are *linear*. The concept of linear secret sharing schemes was introduced by Brickell [3] in the ideal setting and was later generalized to non-ideal schemes. Linear schemes are equivalent to monotone span programs [10]. For simplicity we only define ideal linear schemes.

Definition 2.5 (Ideal Linear Secret Sharing Scheme) *Let $\mathbb{F}$ be a finite field. An ideal linear secret sharing scheme over $\mathbb{F}$ takes the following form: The domain of secrets and shares is $\mathcal{S} = \mathbb{F}$. The scheme is specified by $n+1$ vectors in $\mathbb{F}^d$ for some integer d: a vector $\mathbf{u}_i$ for each participant $u_i \in \mathcal{U}$, $1 \leq i \leq n$, and a so-called target vector $\mathbf{t}$. To share a secret $S \in \mathbb{F}$, the dealer chooses a random vector $\mathbf{w} \in \mathbb{F}^d$ such that $\mathbf{w} \cdot \mathbf{t} = S$ and then the share of participant u_i is $\mathbf{w} \cdot \mathbf{u}_i$.*

The next theorem characterizes the access structure that is realized by a linear secret sharing scheme.

Theorem 2.1 ([3, 10]) *A linear secret sharing scheme with vectors $\{\mathbf{u}_i\}_{1 \leq i \leq n}$ and $\mathbf{t}$ realizes the access structure $\Gamma = \{\mathcal{V} \subseteq \mathcal{U} : \mathbf{t} \in Span\{\mathbf{u}_i : u_i \in \mathcal{V}\}\}$.*

2.2 Monotone Span Programs

Karchmer and Wigderson [10] introduced monotone span programs as a linear algebraic model of computation for computing monotone functions. A monotone span program (MSP hereinafter) is a quintuple $\mathcal{M} = (\mathbb{F}, M, \mathcal{U}, \phi, \mathbf{t})$ 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 $\mathcal{U}$, and $\mathbf{t}$ 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 $\mathbf{t}$ 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 [8] it was shown that if $\mathcal{M} = (\mathbb{F}, M, \mathcal{U}, \phi, \mathbf{t})$ is an MSP that realizes a monotone access structure Γ, then there exists an MSP $\mathcal{M}^* = (\mathbb{F}, M^*, \mathcal{U}, \phi, \mathbf{t}^*)$ 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. An efficient construction of the MSP for the dual access structure was proposed in [7].

2.3 Our Strategy

All the secret sharing schemes that we shall present herein are ideal linear schemes. Namely, they are monotone span programs of size n (every participant has exactly one row in M with his label). In order to prove that a given scheme realizes perfectly some access structure Γ we shall prove two claims. Letting $\mathcal{V}$ be some subset of $\mathcal{U}$ and $M_{\mathcal{V}}$ be the sub-matrix of M that consists of all rows of M with labels in $\mathcal{V}$, we first show that if $\mathcal{V}$ is a minterm then, with high probability, $\mathbf{t} \in \text{row}(M_{\mathcal{V}})$. Namely, the vectors associated with the members of $\mathcal{V}$ span the target vector $\mathbf{t}$ with high probability, whence, $\mathcal{V}$ may reconstruct the secret S. Since the matrices $M_{\mathcal{V}}$, for a minterm $\mathcal{V}$, will always be square, we shall simply show that, with high probability, their determinant is nonzero. This will prove that, with almost certainty, $\mathcal{V}$ may reconstruct the secret. Then we proceed to show that if $\mathcal{V}$ is a maximal unauthorized subset then, with high probability, $\mathbf{t} \notin \text{row}(M_{\mathcal{V}})$. This is established by showing that if we augment $M_{\mathcal{V}}$ with the additional row $\mathbf{t}$, we get a matrix of full rank. Since the latter matrix will always be square, we shall show that, with high probability, it has a nonzero determinant. This will prove that, with almost certainty, $\mathcal{V}$ may not learn any information about the secret.

2.4 Some Algebra

Throughout this study we use the following basic lemma that provides an upper bound for the number of zeros of a multivariate polynomial over a finite field.

Lemma 2.2 (Schwartz-Zippel Lemma) *[14, 18] Let $G(z_1, \ldots, z_k)$ be a nonzero polynomial of k variables over a finite field $\mathbb{F}$ of size q. Assume that the highest degree of each of the variables z_j in G is no larger than d. Then the number of zeros of G in $\mathbb{F}^k$ is bounded from above by kdq^{k-1}.*

Proof. The claim is obviously true for $k = 1$. Proceeding by induction, we assume that it holds for $k - 1$ variables and prove the claim for k variables. The polynomial G may be written as follows:

$$G(z_1, \ldots, z_k) = \sum_{j=0}^{d} G_j(z_1, \ldots, z_{k-1}) z_k^j \ .$$

For every selection of $(z_1, \ldots, z_{k-1}) \in \mathbb{F}^{k-1}$ there are two possibilities: Either $G_j(z_1, \ldots, z_{k-1}) \neq 0$ for at least one $0 \leq j \leq d$, or $G_j(z_1, \ldots, z_{k-1}) = 0$ for all $0 \leq j \leq d$. In the first case, there are at most d values of z_k for which $G(z_1, \ldots, z_{k-1}, z_k) = 0$; in the second case, on the other hand, $G(z_1, \ldots, z_{k-1}, z_k) = 0$ for all $z_k \in \mathbb{F}$. By the induction assumption, the number of points $(z_1, \ldots, z_{k-1}) \in \mathbb{F}^{k-1}$ of the second kind, denoted herein ℓ, satisfies $\ell \leq (k-1)dq^{k-2}$. Hence, the number of points $(z_1, \ldots, z_k) \in \mathbb{F}^k$ in which $G(z_1, \ldots, z_k) = 0$ is bounded by

$$(q^{k-1} - \ell) \cdot d + \ell \cdot q = dq^{k-1} + \ell \cdot (q - d) < dq^{k-1} + (k-1)dq^{k-1} = kdq^{k-1} \ .$$

□

All the matrices that we shall consider in this study will consist of entries that are multivariate polynomials evaluated at a randomly selected point $(x_1, \ldots, x_t) \in \mathbb{F}^t$ for some t. The idea is to fix some of the components, say $x_1, \ldots, x_{t-k}$, and then view the determinant of the matrix as a polynomial in the last k variables $x_{t-k+1}, \ldots, x_t$. Denoting that polynomial by $G_{x_1,\ldots,x_{t-k}}(x_{t-k+1}, \ldots, x_t)$, we then prove two claims, using Lemma 2.2:

1. For almost all selections of the first $t-k$ variables, the resulting polynomial $G_{x_1,\ldots,x_{t-k}}$ is a nonzero polynomial.

2. When $G_{x_1,\ldots,x_{t-k}}$ is a nonzero polynomial, for almost all selections of $(x_{t-k+1}, \ldots, x_t)$, we have $G_{x_1,\ldots,x_{t-k}}(x_{t-k+1}, \ldots, x_t) \neq 0$.

As a final remark, we note that in some of our proofs we use the fact that a determinant of a matrix may be expressed as a linear combination of all minors that are contained within a selection of rows in that matrix. More specifically, let M be a $n \times n$ matrix and let k be an integer smaller than n. A minor of order k in M is a determinant of a sub-matrix of M of dimensions $k \times k$. There are $\binom{n}{k}$ such minors that are contained within the first k rows of M. It is easy to see that $\det M$ equals a linear combination of all those minors, where the coefficients of the linear combination depend only on the entries in the last $n-k$ rows of M. The proof for the case $k = n-1$ is immediate if we expand the determinant by the last row. The proof for other values of k now easily follows by induction.

3 Compartmented Access Structures

The original compartmented access structure that was presented in [3] is defined as follows. Let $t_i \in \mathbb{N}$, $1 \leq i \leq m$, and $t \in \mathbb{N}$ be thresholds such that $t \geq \sum_{i=1}^{m} t_i$. Then

$$\Gamma = \{\mathcal{V} \subseteq \mathcal{U} : \exists \mathcal{W} \subseteq \mathcal{V} \text{ such that } |\mathcal{W} \cap \mathcal{C}_i| \geq t_i, \ \ 1 \leq i \leq m, \text{ and } |\mathcal{W}| = t\} \ . \qquad (2)$$

Such access structures are suitable for situations in which the size of an authorized subset must be at least some threshold t, but, in addition, we wish to guarantee that every compartment is represented by at least some number of participants in the authorized subset. In other situations, however, an opposite demand may occur: while the size of an authorized subset must be at least some threshold, we would like to limit the number of participants that represent each of the compartments; namely,

$$\Delta = \{\mathcal{V} \subseteq \mathcal{U} : \exists \mathcal{W} \subseteq \mathcal{V} \text{ such that } |\mathcal{W} \cap \mathcal{C}_i| \leq s_i, \ \ 1 \leq i \leq m, \text{ and } |\mathcal{W}| = s\} \ , \qquad (3)$$

where $s_i, s \in \mathbb{N}$ and $s \leq \sum_{i=1}^{m} s_i$. Those two types of compartmented access structures protect democracy: While the first attempts to protect possibly weak compartments from being left out of a coalition that is capable of recovering the secret, the second prevents possibly strong compartments from dominating such a coalition. We refer to Γ as a *compartmented access structure with lower bounds*, while Δ is referred to hereinafter as a *compartmented access structure with upper bounds*.

When $m = 1$ both types of compartmented access structures coincide with the standard threshold access structures of Shamir [15]. When $m = 2$ the two types of access structures agree: a compartmented access structure with lower bounds t_1, t_2 and threshold t is a compartmented access structure with upper bounds $s_1 = t - t_2$, $s_2 = t - t_1$ and threshold $s = t$; conversely, an access structure of type (3) with bounds s_1, s_2 and s may be viewed as an access structure of type (2) with bounds $t_1 = s - s_2$, $t_2 = s - s_1$ and $t = s$. However, when $m \geq 3$, these two types of compartmented access structures differ. To exemplify this, we show an access structure of type (2) that does not fall within the framework (3), and another access structure of type (3) that does not fall within the framework (2).

The access structure Γ of type (2) with $m = 3$, $t_1 = 1$, $t_2 = 1$, $t_3 = 1$, and $t = 4$ has minterms $\mathcal{V}$ of types $(1,1,2)$ (namely, $|\mathcal{V} \cap \mathcal{C}_1| = 1$, $|\mathcal{V} \cap \mathcal{C}_2| = 1$, and $|\mathcal{V} \cap \mathcal{C}_3| = 2$), $(1,2,1)$, or $(2,1,1)$. This collection of minterms does not fall within the framework (3) for any choice of s_i and s. Indeed, if that collection of subsets was to fall under framework (3) then we should have had $s_1 = s_2 = s_3 = 2$, and $s = 4$; but then that collection should have also included subsets of type (0,2,2), which it doesn't. Hence, there is no way of fitting that compartmented access structure with lower bounds within the framework with upper bounds. An example that demonstrates the non-containment in the other direction is the access structure Δ of type (3) with $m = 3$, $s_1 = 1$, $s_2 = 1$, $s_3 = 1$, and $s = 2$. Its minterms are of types $(0,1,1)$, $(1,0,1)$, or $(1,1,0)$. To fit this collection into (2) we would need to have $t_1 = t_2 = t_3 = 0$ and $t = 2$, but such a choice of parameters allows also subsets of type $(0,0,2)$.

Compartmented access structures with lower bounds, (2), are already known to be ideal [3]. We design here ideal linear schemes for these access structures, as well as for the corresponding access structures with upper bounds, (3), that are based on bivariate interpolation.

3.1 Ideal Secret Sharing for Compartmented Access Structures with Upper Bounds

In this section we describe a linear secret sharing scheme for compartmented access structures with upper bounds, (3). Hereinafter, $S \in \mathbb{F}$ is the secret to be shared. Let x_i, $1 \le i \le m$, be m distinct random points in $\mathbb{F}$. Let $P_i(y) = \sum_{j=0}^{s_i-1} a_{i,j}\, y^j$, $1 \le i \le m$, be random polynomials over $\mathbb{F}$ such that $S = \sum_{i=1}^{m} \sum_{j=0}^{s_i-1} a_{i,j}$. Finally, we set

$$P(x,y) = \sum_{i=1}^{m} P_i(y) L_i(x) = \sum_{i=1}^{m} \sum_{j=0}^{s_i-1} a_{i,j}\, y^j\, L_i(x)\,, \tag{4}$$

where $L_i(x)$ are the Lagrange polynomials of degree $m-1$ over $\{x_i : 1 \le i \le m\}$, namely,

$$L_i(x) = \prod_{\substack{1 \le j \le m \\ j \ne i}} \frac{x - x_j}{x_i - x_j}\,, \quad 1 \le i \le m\ . \tag{5}$$

These polynomials have the property that $L_i(x_j) = \delta_{i,j}$ for all $1 \le i, j \le m$. Then the secret sharing scheme is as follows:

Secret Sharing Scheme 1:

1. *Each participant $u_{i,j}$ from compartment $\mathcal{C}_i$ is identified by a unique public point $(x_i, y_{i,j})$, where $y_{i,j} \ne 1$ is random, and his private is $P(x_i, y_{i,j})$.*
2. *In addition, we publish the value of P at $k := \sum_{i=1}^{m} s_i - s$ random points (x'_i, z_i), where $x'_i \notin \{x_1, \ldots, x_m\}$, $1 \le i \le k$.*

Figure 1 illustrates that scheme for the case of $m = 3$ compartments and $k = s_1 + s_2 + s_3 - s = 3$. The $k = 3$ public point values are denoted by full bullets. The point values that

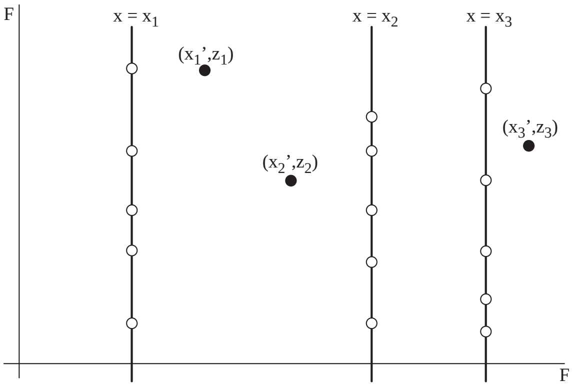

Figure 1: Secret Sharing Scheme 1

correspond to the participants are marked by empty circles along the three random parallel lines, $x = x_i$, $1 \leq i \leq 3$.

Clearly, this is an ideal scheme since the private shares of all users are taken from the domain of secrets $\mathbb{F}$. The number of unknowns in the polynomial P is $\sum_{i=1}^{m} s_i$ (the coefficients of all the univariate polynomials $P_i(y)$, $1 \leq i \leq m$). Since we are given for free $k := \sum_{i=1}^{m} s_i - s$ point values, we need additional s points for full recovery. Moreover, we cannot use more than s_i points from the line $x = x_i$, $1 \leq i \leq m$, because any s_i points from along that line already fully recover $P_i(y)$, but they do not contribute anything towards the recovery of $P_j(y)$ for $j \neq i$. In view of the above, this scheme agrees with the constraints in (3). We proceed to show that, with high probability (with respect to the random selection of points), the resulting scheme is perfect.

Lemma 3.1 *If $\mathcal{V} \in \Delta$ it may recover the secret S with probability $1 - Cq^{-1}$, where the constant C depends on m, s, and $s_1, \ldots, s_m$.*

Proof. Let $\mathcal{V}$ be a minimal set in Δ. Let us assume that $|\mathcal{V} \cap \mathcal{C}_i| = k_i \leq s_i$, $1 \leq i \leq m$. Then the system of equations in the unknown coefficients of $P(x, y)$, (4), namely $\{a_{i,j} : 1 \leq i \leq m, 0 \leq j \leq s_i - 1\}$ that $\mathcal{V}$ may construct has a matrix of coefficients of the following form:

$$M = \begin{pmatrix} M_1 & 0 & 0 & \cdots & 0 \\ 0 & M_2 & 0 & \cdots & 0 \\ 0 & 0 & M_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & M_m \\ H_1 & H_2 & H_3 & \cdots & H_m \end{pmatrix} \tag{6}$$

Here, M_i is a block of size $k_i \times s_i$ that represents the equations that are contributed by the

k_i participants from compartment $\mathcal{C}_i$. If $\mathcal{V} \cap \mathcal{C}_i = \{u_{i,1}, \ldots, u_{i,k_i}\}$ and $u_{i,j}$ is characterized by the point $(x_i, y_{i,j})$ then

$$M_i = \begin{pmatrix} 1 & y_{i,1} & y_{i,1}^2 & \cdots & y_{i,1}^{s_i-1} \\ 1 & y_{i,2} & y_{i,2}^2 & \cdots & y_{i,2}^{s_i-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & y_{i,k_i} & y_{i,k_i}^2 & \cdots & y_{i,k_i}^{s_i-1} \end{pmatrix} . \tag{7}$$

The last $k = \sum_{i=1}^{m} s_i - s$ rows in the matrix, denoted in (6) by the row of H-blocks, represent the additional k equations that result from the k public values of P that were published by the dealer. These k values are of the form $P(x'_j, z_j)$, $1 \leq j \leq k$. Then the jth row within the last row of blocks in M has the following form:

$$\begin{pmatrix} L_1(x'_j) & L_1(x'_j)z_j & \cdots & L_1(x'_j)z_j^{s_1-1} & \cdots & \cdots & L_m(x'_j) & L_m(x'_j)z_j & \cdots & L_m(x'_j)z_j^{s_m-1} \end{pmatrix}$$

We proceed to prove that, with high probability, the matrix M has a nonzero determinant, whence the minimal authorized set $\mathcal{V}$ may solve the corresponding system of linear equations and recover the entire polynomial, and consequently the secret, from their shares. To that end, we view the determinant of M as a k-variate polynomial $G(z_1, \ldots, z_k)$ whose coefficients depend on $L_i(x'_j)$, $1 \leq i \leq m$, $1 \leq j \leq k$, and on all $s \times s$ minors of M that are contained within its first s rows. There are two cases to consider: the case where that polynomial is identically zero, and the case that it is not.

Let us assume first that $G(z_1, \ldots, z_k)$ is not identically zero. Assuming, without loss of generality, that $s_1 \leq \cdots \leq s_m$. Then the degree of G with respect to each of its variables is no more than $s_m - 1$. Hence, Lemma 2.2 implies that the number of zeros of G in $\mathbb{F}^k$ is bounded by $k(s_m - 1)q^{k-1}$. Since z_j, $1 \leq j \leq k$, were randomly selected from $\mathbb{F}$, we infer that the probability of $(z_1, \ldots, z_k)$ being one of the zeros of G is bounded from above by $k(s_m - 1)q^{-1}$.

Regarding the case where $G(z_1, \ldots, z_k) \equiv 0$, we claim that the probability for such an event is also $O(q^{-1})$. Let us exemplify how such an event may occur. Assume, for example, that $m = 2$, $s_1 = s_2 = 3$ and $s = 5$, whence, $k = 1$. Then, if $\mathcal{V}$ is a minimal authorized set with $|\mathcal{V} \cap \mathcal{C}_1| = 3$ and $|\mathcal{V} \cap \mathcal{C}_2| = 2$, the corresponding matrix has the following form:

$$M = \begin{pmatrix} 1 & y_1 & y_1^2 & 0 & 0 & 0 \\ 1 & y_2 & y_2^2 & 0 & 0 & 0 \\ 1 & y_3 & y_3^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & y_4 & y_4^2 \\ 0 & 0 & 0 & 1 & y_5 & y_5^2 \\ L_1(x'_1) & L_1(x'_1)z_1 & L_1(x'_1)z_1^2 & L_2(x'_1) & L_2(x'_1)z_1 & L_2(x'_1)z_1^2 \end{pmatrix} .$$

Then $G(z_1) = a_0 + a_1 z_1 + a_2 z_1^2$ where the coefficients a_0, a_1, a_2 depend on $L_1(x'_1)$, $L_2(x'_1)$, and y_i, $1 \le i \le 5$. For example,

$$a_2 = L_2(x'_1) \cdot \begin{vmatrix} 1 & y_1 & y_1^2 & 0 & 0 \\ 1 & y_2 & y_2^2 & 0 & 0 \\ 1 & y_3 & y_3^2 & 0 & 0 \\ 0 & 0 & 0 & 1 & y_4 \\ 0 & 0 & 0 & 1 & y_5 \end{vmatrix} - L_1(x'_1) \cdot \begin{vmatrix} 1 & y_1 & 0 & 0 & 0 \\ 1 & y_2 & 0 & 0 & 0 \\ 1 & y_3 & 0 & 0 & 0 \\ 0 & 0 & 1 & y_4 & y_4^2 \\ 0 & 0 & 1 & y_5 & y_5^2 \end{vmatrix} .$$

Then $G \equiv 0$ if and only if $a_0 = a_1 = a_2 = 0$. In general, G is identically zero if and only if all of its coefficients are zero, where each of the coefficients is a polynomial in $\ell := \sum_{i=1}^m s_i$ variables (the s values of $y_{i,j}$ and $x'_1, \ldots, x'_k$) whose degree with respect to each of its variables is bounded by $d = \max\{s_m - 1, m - 1\}$. Hence, the number of selections of those ℓ variables that would make a single coefficient of G zero is bounded by $\ell d q^{\ell-1}$. The number of choices of the $y_{i,j}$'s and x'_j's, on the other hand, is $\Omega(q^\ell)$. Hence, we get that the probability of each of the coefficients to be zero is Cq^{-1}, where the constant C depends on m, s, and $s_1, \ldots, s_m$. This implies that the probability that $G \equiv 0$ is also Cq^{-1}. □

Lemma 3.2 *If $\mathcal{V} \notin \Delta$ then with probability $1 - Cq^{-1}$ it may not learn any information about the secret S, where the constant C depends on m, s, and $s_1, \ldots, s_m$.*

Proof. Assume that $\mathcal{V} \notin \Delta$. Without loss of generality we may assume that $|\mathcal{V} \cap \mathcal{C}_i| = k_i \le s_i$, $1 \le i \le m$, since if $|\mathcal{V} \cap \mathcal{C}_i| > s_i$ for some $1 \le i \le m$, we may discard the redundant participants from that compartment without reducing the row space of the corresponding matrix. Furthermore, we may assume that $|\mathcal{V}| = s - 1$, since if $|\mathcal{V}| < s - 1$ we may find a superset $\mathcal{V}' \supset \mathcal{V}$ such that $|\mathcal{V}' \cap \mathcal{C}_i| \le s_i$, $1 \le i \le m$, and $|\mathcal{V}'| = s - 1$ and prove that $\mathcal{V}'$ cannot learn a thing about the secret with probability $1 - O(q^{-1})$; since $\mathcal{V}'$ has more information than $\mathcal{V}$ does, that will settle our claim.

The matrix that corresponds to the information that $\mathcal{V}$ has regarding the coefficients of the polynomial is given by (6). As in the proof of Lemma 3.1, M_i is a Vandermonde block (7) of size $k_i \times s_i$ that represents the equations that are contributed by the k_i participants from compartment $\mathcal{C}_i$. The last $k = \sum_{i=1}^m s_i - s$ rows correspond to the public values of the polynomial. However, here M has only $\sum_{i=1}^m s_i - 1$ rows. We need to show that the vector $(1, \ldots, 1)$ is, most probably, not spanned by the rows of M. In order to show that, we augment M by adding to it that vector as a first row, and then show that the augmented M has a full rank of $\sum_{i=1}^m s_i$, with probability $1 - O(q^{-1})$. That part of the proof goes along the same line of argumentation as in the proof of Lemma 3.1. □

We are now ready to state and prove our main result regarding Secret Sharing Scheme 1.

Theorem 3.3 *The ideal Secret Sharing Scheme 1 is a perfect scheme that realizes the compartmented access structure with upper bounds (3) with probability $1 - \varepsilon$ where $\varepsilon = \binom{n+1}{s} Cq^{-1}$, and C is a constant that depends on m, s, and $s_1, \ldots, s_m$.*

Proof. Lemmas 3.1 and 3.2 provide an upper bound for the probability of a failure of the scheme for a given subset $\mathcal{V} \subseteq \mathcal{U}$. We may now use the union bound to upper bound the probability of having any failure at all. It is sufficient to consider only the minterms and maxterms. Namely, if we guarantee that the scheme is correct for all minterms $\mathcal{V} \in \Delta_0$, then it is also correct for all other authorized subsets in Δ. Similarly, if the scheme is private with respect to all maxterms $\mathcal{V} \notin \Delta$ it is certainly private with respect to any other unauthorized subset.

Since any minterm of Δ is of size s, the number of minterms is bounded from above by $\binom{n}{s}$. In view of the analysis in the proof of Lemma 3.2, it suffices to consider only maxterms of size $s-1$. The number of such maxterms is bounded from above by $\binom{n}{s-1}$. Therefore, as $\binom{n}{s} + \binom{n}{s-1} = \binom{n+1}{s}$, we may combine the probability estimates in Lemmas 3.1 and 3.2 to conclude that the scheme fails to be perfect with probability that does not exceed $\varepsilon = \binom{n+1}{s} C q^{-1}$, where C is a constant that depends on m, s, and $s_1, \ldots, s_m$. This completes the proof. □

We would like to stress that the probability here is with respect to the choices of the points in the plane. Once such a choice was made, the dealer may check that all minimal authorized subsets (minterms) may recover the secret while all maximal non-authorized subsets (maxterms) may not learn a thing about the secret. If all those subsets pass the test then the resulting scheme is perfectly secure. In the event that one of the subsets did not pass the test, the dealer has only to try another selection. Having said that, it should be noted that as, typically, n and s are small numbers while q is of cryptographic magnitudes, the probability of success in Theorem 3.3 is overwhelming and it renders the above described check unnecessary.

Most constructions of linear schemes, including the linear scheme of Brickell for compartmented access structures with lower bounds [3], suffer from a similar problem: there is a small probability that the allocation of vectors to participants might result in a minterm that cannot recover the secret, or a maxterm that can. However, as explained above, practically it is an insignificant problem, unless the underlying parameters (n, m, s, and $s_1, \ldots, s_m$ in our case) are exceptionally large. There are very few linear schemes in which there is an allocation of vectors that is provably secure (namely, an allocation that may be proven to always yield a perfect scheme). The Shamir scheme is such. Another example is the scheme due to Tassa in [17] for hierarchical threshold secret sharing, where, relying upon results from the theory of Birkhoff interpolation, it was possible to get a provably perfect scheme using the so-called *monotone allocation* of identities in the field (provided that the field is large enough).

Corollary 3.4 *The compartmented access structure with upper bounds (3) may be realized ideally by a linear secret sharing scheme over fields $\mathbb{F}$ of size $q = |\mathbb{F}| > C\binom{n+1}{s}$, where C is a constant that depends on m, s, and $s_1, \ldots, s_m$.*

3.2 Ideal Secret Sharing for Compartmented Access Structures with Lower Bounds

In this section we describe a linear secret sharing scheme for compartmented access structures with lower bounds, (2). To that end, we construct a scheme for the dual access structure Γ^*.

3.2.1 Realizing the dual access structure

The dual access structure of (2) is given by $\Gamma^* = \{\mathcal{V} : \mathcal{V}^c \notin \Gamma\}$. Hence, $\mathcal{V} \in \Gamma^*$ if and only if $|\mathcal{V}^c| < t$ or $|\mathcal{V}^c \cap \mathcal{C}_i| < t_i$ for some $1 \leq i \leq m$. Introducing the notations $n = |\mathcal{U}|$ and $n_i = |\mathcal{C}_i|$, $1 \leq i \leq m$, we infer that $\mathcal{V} \in \Gamma^*$ if and only if $|\mathcal{V}| \geq n-t+1$ or $|\mathcal{V} \cap \mathcal{C}_i| \geq n_i - t_i + 1$ for some $1 \leq i \leq m$. Namely,

$$\Gamma^* = \{\mathcal{V} \subseteq \mathcal{U} : |\mathcal{V}| \geq r \text{ or } |\mathcal{V} \cap \mathcal{C}_i| \geq r_i \text{ for some } 1 \leq i \leq m\} \ , \tag{8}$$

where

$$r = n - t + 1 \text{ and } r_i = n_i - t_i + 1 \ , \quad 1 \leq i \leq m \ . \tag{9}$$

Since $t \geq \sum_{i=1}^m t_i$ and $n = \sum_{i=1}^m n_i$, we see that

$$\sum_{i=1}^m r_i = \sum_{i=1}^m n_i - \sum_{i=1}^m t_i + m \geq n - t + m = r + m - 1 \ .$$

Therefore, the thresholds in the dual access structure (8) satisfy

$$\sum_{i=1}^m r_i \geq r + m - 1 \ . \tag{10}$$

We proceed to describe a linear ideal secret sharing scheme for realizing such access structures and then prove that, with high probability, it is perfect.

Let x_i, $1 \leq i \leq m$, be m distinct random points in $\mathbb{F}$ and let $P_i(y)$ be a polynomial of degree $r_i - 1$ over $\mathbb{F}$, such that

$$P_1(0) = \cdots = P_m(0) = S \,, \tag{11}$$

where S is the secret. Define

$$P(x,y) = \sum_{i=1}^m P_i(y) L_i(x) = \sum_{i=1}^m \sum_{j=0}^{r_i - 1} a_{i,j}\, y^j L_i(x) \ , \tag{12}$$

where $L_i(x)$, $1 \leq i \leq m$, are, as before, the Lagrange polynomials of degree $m-1$ over $\{x_i : 1 \leq i \leq m\}$, (5). Note that condition (11) implies that $a_{1,0} = \cdots = a_{m,0}$ and, consequently, the number of unknown coefficients in the representation of $P(x,y)$ with respect to the basis $L_i(x)y^j$, $1 \le i \le m$, $0 \le j \le r_i - 1$, is $g = \sum_{i=1}^{m} r_i - (m-1)$. Note that by (10), $g \ge r$.

Our secret sharing scheme for the realization of the dual access structure Γ^*, (8), is as follows:

Secret Sharing Scheme 2:

1. *Each participant $u_{i,j}$ from compartment $\mathcal{C}_i$ will be identified by a unique public point $(x_i, y_{i,j})$, where $y_{i,j} \neq 0$ is random, and his private share will be the value of P at that point.*

2. *In addition, we publish the value of P at $k = g - r$ random points (x'_i, z_i), where $x'_i \notin \{x_1, \ldots, x_m\}$, $1 \le i \le k$.*

Lemma 3.5 *If $\mathcal{V} \in \Gamma^*$ it may recover the secret S with probability $1 - Cq^{-1}$, where the constant C depends on m, r, and $r_1, \ldots, r_m$.*

Proof. Let $\mathcal{V}$ be an authorized set in Γ^*. Then either $|\mathcal{V} \cap \mathcal{C}_i| \ge r_i$ for some $1 \le i \le m$, or $|\mathcal{V}| \ge r$. In the first case the claim is straightforward. Indeed, if $|\mathcal{V} \cap \mathcal{C}_i| \ge r_i$ for some $1 \le i \le m$ then it may fully recover $P_i(y)$, and, consequently, it may learn the value of $S = P_i(0)$.

Hence, we assume hereinafter that $|\mathcal{V} \cap \mathcal{C}_i| = k_i < r_i$, $1 \le i \le m$, and that $\mathcal{V}$ is a minimal authorized subset, namely, $|\mathcal{V}| = r$. Then the system of equations in the $\sum_{i=1}^{m} r_i$ unknown coefficients of $P(x,y)$ that $\mathcal{V}$ may construct has a matrix of coefficients of the following form:

$$M = \begin{pmatrix} M_1 & G_{1,2} & 0 & 0 & \cdots & 0 \\ 0 & M_2 & G_{2,3} & 0 & \cdots & 0 \\ 0 & 0 & M_3 & G_{3,4} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & M_{m-1} & G_{m-1,m} \\ 0 & 0 & 0 & \cdots & 0 & M_m \\ H_1 & H_2 & H_3 & \cdots & H_{m-1} & H_m \end{pmatrix} \tag{13}$$

The pair of blocks M_i and $G_{i,i+1}$, $1 \le i \le m-1$, represents the equations that are contributed by the k_i participants from compartment $\mathcal{C}_i$, plus the additional equation $a_{i,0} = a_{i+1,0}$. If $\mathcal{V} \cap \mathcal{C}_i = \{u_{i,1}, \ldots, u_{i,k_i}\}$ and $u_{i,j}$ is characterized by the point $(x_i, y_{i,j})$ then this pair of blocks has the following form:

$$\begin{pmatrix} M_i & G_{i,i+1} \end{pmatrix} = \begin{pmatrix} 1 & y_{i,1} & y_{i,1}^2 & \cdots & y_{i,1}^{r_i-1} & 0 & 0 & \cdots & 0 \\ 1 & y_{i,2} & y_{i,2}^2 & \cdots & y_{i,2}^{r_i-1} & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ldots & \vdots \\ 1 & y_{i,k_i} & y_{i,k_i}^2 & \cdots & y_{i,k_i}^{r_i-1} & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 & -1 & 0 & \cdots & 0 \end{pmatrix} \tag{14}$$

Here, M_i is a block of size $(k_i+1)\times r_i$ and $G_{i,i+1}$ is a block of size $(k_i+1)\times r_{i+1}$.

M_m represents the equations that are contributed by the k_m participants from compartment $\mathcal{C}_m$. Assuming that they are identified by the points $(x_m, y_{m,j})$, $1 \le j \le k_m$,

$$M_m = \begin{pmatrix} 1 & y_{m,1} & y_{m,1}^2 & \cdots & y_{m,1}^{r_m-1} \\ 1 & y_{m,2} & y_{m,2}^2 & \cdots & y_{m,2}^{r_m-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & y_{m,k_m} & y_{m,k_m}^2 & \cdots & y_{m,k_m}^{r_m-1} \end{pmatrix} . \tag{15}$$

As for the last $k = g - r = \sum_{i=1}^m r_i - (m-1) - r$ rows in the matrix, denoted in (13) by the row of H-blocks, they represent the additional k equations that result from the k public values of P that were published by the dealer. These k values are of the form $P(x'_j, z_j)$, $1 \le j \le k$. Then, as in the previous section, the jth row within the last row of blocks in M has the following form:

$$\begin{pmatrix} L_1(x'_j) & L_1(x'_j)z_j & \cdots & L_1(x'_j)z_j^{r_1-1} & \cdots & \cdots & L_m(x'_j) & L_m(x'_j)z_j & \cdots & L_m(x'_j)z_j^{r_m-1} \end{pmatrix}$$

We claim that the first $\sum_{i=1}^m k_i + (m-1)$ rows in M are independent. This stems from the Vandermonde structure of the blocks, our assumption that $k_i < r_i$, and the fact that $y_{i,j} \ne 0$, for $1 \le i \le m$ and $1 \le j \le k_i$. Indeed, consider the rectangular block $(M_i\ G_{i,i+1})$ that is given in (14). Since $k_i \le r_i - 1$, the first k_i columns in this rectangular block form a square Vandermonde block of the form

$$\begin{pmatrix} 1 & y_{i,1} & y_{i,1}^2 & \cdots & y_{i,1}^{k_i} \\ 1 & y_{i,2} & y_{i,2}^2 & \cdots & y_{i,2}^{k_i} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & y_{i,k_i} & y_{i,k_i}^2 & \cdots & y_{i,k_i}^{k_i} \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Since $y_{i,j}$, $1 \le j \le k_i$, are distinct and nonzero, the above Vandermonde block is nonsingular. Hence, by applying a Gaussian elimination within that row of blocks we may arrive at a full-rank row-reduced echelon form for that row of blocks. Applying a Gaussian elimination within each of the first m block-rows in M, (13), we may arrive at a full-rank row-reduced echelon form for the first $\sum_{i=1}^m k_i + (m-1)$ rows in M. That settles our claim that the first $\sum_{i=1}^m k_i + (m-1)$ rows in M are independent.

Next, we aim at showing that all of the rows in M are linearly independent, with probability $1 - O(q^{-1})$. To that end, we may view the determinant of M as a k-variate polynomial $G(z_1, \ldots, z_k)$ whose coefficients depend on $L_i(x'_j)$, $1 \le i \le m$, $1 \le j \le k$, and on all $(\sum_{i=1}^m r_i - k) \times (\sum_{i=1}^m r_i - k)$ minors of M that are contained within its first $\sum_{i=1}^m r_i - k$ rows. Arguing along the same lines as in the proof of Lemma 3.1, we claim, omitting further details, that $G(z_1, \ldots, z_k)$ vanishes with probability Cq^{-1}, where the constant C depends on m, r, and $r_1, \ldots, r_m$. □

Lemma 3.6 *If $\mathcal{V} \notin \Gamma^*$ then with probability $1 - Cq^{-1}$ it may not learn any information about the secret S, where the constant C depends on m, r, and $r_1, \ldots, r_m$.*

Proof. Assume that $\mathcal{V} \notin \Gamma^*$. Then $|\mathcal{V} \cap \mathcal{C}_i| = k_i < r_i$, $1 \leq i \leq m$, and in addition $|\mathcal{V}| = r - 1 - \ell$ for some $\ell \geq 0$. Condition (10) on the thresholds imply that we may augment $\mathcal{V}$ with ℓ additional participants so that its size becomes exactly $r - 1$ while its number of participants in each compartment $\mathcal{C}_i$, $1 \leq i \leq m$, still does not reach the necessary threshold r_i. Indeed, the maximal number that the augmented $\mathcal{V}$ may have in compartment $\mathcal{C}_i$ so that it remains unauthorized is $r_i - 1$. As, by (10), $\sum_{i=1}^m (r_i - 1) \geq r - 1$, the above described procedure is possible.

We proceed to show that the augmented $\mathcal{V}$ cannot learn a thing about the secret S with probability $1 - O(q^{-1})$. The matrix that corresponds to $\mathcal{V}$ is given by (13), and its size is $(d-1) \times d$ where $d = \sum_{i=1}^m r_i$. Let $\mathbf{e}_i$ denote the standard basis vector in $\mathbb{F}^d$ whose ith component equals 1 while all the rest are zero. In addition, we introduce the notation $h_j = 1 + \sum_{i=1}^{j-1} r_i$, $1 \leq j \leq m$; h_j denotes the index of the free coefficient of $P_j(y)$ within the vector of unknown coefficients of $P(x, y)$ (hence, $h_1, \ldots, h_m$ correspond to the indices of the m unknown coefficients that equal the secret S). We need to show that none of the vectors $\mathbf{e}_{h_j}$ is in the row space of the matrix M. It is easy to see that it suffices to show that $\mathbf{e}_{h_m}$ is not in that row space.

To show that, we add $\mathbf{e}_{h_m}$ as a last row vector in the block-row $\begin{pmatrix} 0 & \cdots & 0 & M_m \end{pmatrix}$. Since $y_{i,j} \neq 0$ for all $1 \leq i \leq m$ and $1 \leq j \leq k_i$, we may argue along the same lines as in the proof of Lemma 3.5 to conclude that the first $\sum_{i=1}^m k_i + m$ rows in the augmented matrix M are linearly independent. Then, the remainder of the proof that the augmented M has, with probability $1 - O(q^{-1})$, a full rank of $\sum_{i=1}^m r_i$ is the same as in the proof of Lemma 3.5. □

Using Lemmas 3.5 and 3.6 and arguing along the same lines as in the proof of Theorem 3.3, we arrive at the following result:

Theorem 3.7 *The ideal Secret Sharing Scheme 2 is a perfect scheme that realizes the compartmented access structure (8) with probability $1 - \varepsilon$ where $\varepsilon = \binom{n+1}{r} Cq^{-1}$, and C is a constant that depends on m, r, and $r_1, \ldots, r_m$.*

3.2.2 A scheme for compartmented access structures with lower bounds

Using the results of Section 3.2.1 we may now easily construct an ideal secret sharing scheme for compartmented access structures with lower bounds, (2). Given such an access structure, Γ, we construct the ideal linear secret sharing scheme for its dual, (8)-(9). Then we translate that ideal scheme (equivalently, MSP) into an ideal scheme (MSP) for $\Gamma = (\Gamma^*)^*$, using the explicit construction that is described in [7]. We omit further details.

Our scheme differs from the scheme suggested by Brickell [3]. Both schemes require to check a large number of matrices for non-singularity. (There are no known schemes for compartmented access structures that circumvent that problem.) However, while in [3] it is only proven that a proper allocation of participant identities exist, in our scheme we may randomly select the participant identities, knowing that the resulting scheme is guaranteed to be perfect with probability of at least $1 - \binom{n+1}{r} C q^{-1}$, Theorem 3.7. As that probability is overwhelmingly close to certainty with typical values of q, n, m and the thresholds, the check of all matrices that correspond to the minterms and maxterms of the access structure may be avoided.

4 Hierarchical Threshold Access Structures

Here we present an ideal secret sharing scheme for the realization of hierarchical access structures. That scheme uses Lagrange interpolation of bivariate polynomials where the data is given on lines in general position in the plane. In Subsection 4.1 we review all necessary background regarding that type of interpolation. Then, in Subsection 4.2 we deal with the following question: Given the values of a bivariate polynomial in a set of points in the plane, what is the amount of information that those values reveal on the polynomial. Using those results, we proceed to Subsection 4.3 where we define hierarchical access structures and present a scheme that realizes them.

4.1 Lagrange Interpolation with Data on Lines in General Positions

Let

$$\{L_i\}_{1 \le i \le n} \ , \quad L_i = \{(x,y) \in \mathbb{F}^2 : L_i(x,y) := a_i x + b_i y + c_i = 0\} \ ,$$

be a collection of n lines in $\mathbb{F}^2$ in general position. Namely, for every pair $1 \le i < j \le n$, L_i and L_j intersect in a point $A_{i,j} = (x_{i,j}, y_{i,j})$ and $A_{i,j} \ne A_{k,\ell}$ whenever $\{i,j\} \ne \{k,\ell\}$ (Figure 2 illustrates the case $n = 4$). Let $f(x,y)$ be a function on $\mathbb{F}^2$. Then there exists a unique polynomial of degree $n-2$,

$$P(x,y) = \sum_{0 \le i+j \le n-2} a_{i,j} x^i y^j \in \mathbb{F}[x,y] \ , \tag{16}$$

that satisfies

$$P(x_{i,j}, y_{i,j}) = f(x_{i,j}, y_{i,j}) \quad 1 \le i < j \le n \ . \tag{17}$$

That polynomial is given by

$$P(x,y) = \sum_{1 \le i < j \le n} f(x_{i,j}, y_{i,j}) L_{i,j}(x,y) \tag{18}$$

where

$$L_{i,j}(x,y) = \prod_{\substack{1 \le k \le n \\ k \ne i,j}} \frac{L_k(x,y)}{L_k(x_{i,j}, y_{i,j})} \ . \tag{19}$$

The bivariate Lagrange polynomials $L_{i,j}(x,y)$ are of degree $n-2$, and $L_{i,j}(x_{i,j}, y_{i,j}) = 1$ while $L_{i,j}(x_{k,\ell}, y_{k,\ell}) = 0$ for all $\{k,\ell\} \ne \{i,j\}$ (because the point $(x_{k,\ell}, y_{k,\ell})$ lies on a line other than L_i or L_j, whence the numerator in (19) becomes zero). Note that the number

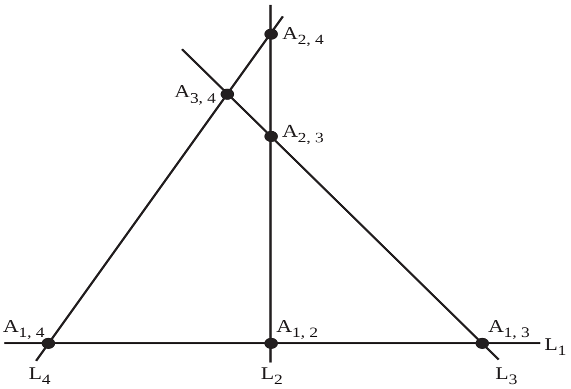

Figure 2: Four lines in general position and the corresponding interpolation points

of independent terms (monoms) in (16) agrees with the number of constraints in (17), i.e., $\binom{n}{2}$.

This type of bivariate interpolation was studied first in [4]. We shall be using this bivariate interpolation in a slightly different manner. As described above, in order to recover a polynomial $P(x, y)$ of degree k, we need its values at the intersection points of $k + 2$ lines in general position. Assume, however, that we have only $k + 1$ lines in general position, but we were able to fully recover the restriction of $P(x, y)$ to each of these lines (the restriction of a bivariate polynomial of degree k to a line is the univariate polynomial of degree k that is obtained by replacing x and y in $P(x, y)$ with their linear parameterization along that line). Then that information is also sufficient for the full recovery of $P(x, y)$ since we may add a $(k + 2)$th line that intersects all of the original $k + 1$ lines and then, as we know the value of P along each of those $k + 1$ lines, we know its value in all of the $\binom{k+2}{2}$ intersection points of the $k+2$ lines; this enables the full recovery of $P(x, y)$ through (18)-(19). For example, in order to recover a quadratic polynomial $P(x, y)$ ($k = 2$), we need its values in the 6 intersection points of $k + 2 = 4$ lines in general position (L_1, L_2, L_3 and L_4 in Figure 2); alternatively, we may compute its restriction to only $k + 1 = 3$ of those lines, say L_1, L_2, and L_3, and that is sufficient for finding the value of P in all 6 intersection points of L_1, L_2, L_3 and L_4. Hence, while in this section our setting included n lines and a polynomial $P(x, y)$ of degree $n - 2$, in the following sections our settings will include n lines and a polynomial $P(x, y)$ of degree $n - 1$.

4.2 Constructibility and Non-constructibility Results

Let:

- $\mathbb{F}$ be a finite field;
- $\{L_i\}_{1\le i\le n}$, $L_i = \{(x, y) \in \mathbb{F}^2 : L_i(x, y) := a_ix + b_iy + c_i = 0\}$, be a collection of n lines in $\mathbb{F}^2$ in general position;

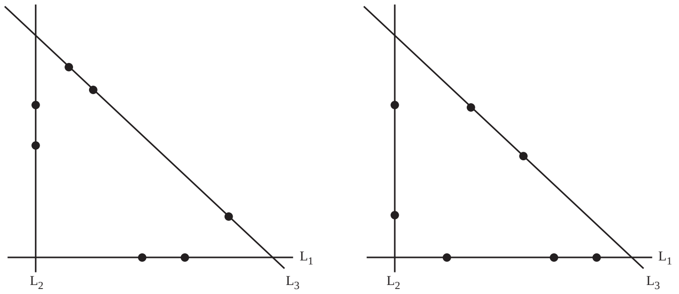

Figure 3: Two point sets of type $(2, 2, 3)$

- $P(x, y) = \sum_{0 \leq i+j \leq n-1} a_{i,j} x^i y^j$ be a polynomial of degree (at most) $n-1$ in $\mathbb{F}[x, y]$; and
- $\mathcal{V} \subset \bigcup_{i=1}^{n} L_i$ be a set of points on the given lines, none of which is an intersection point of two of those lines.

The question that we address here is the amount of information that $D := P|_{\mathcal{V}}$ reveals on the polynomial P.

In order to answer that question, we define the *type* of a set $\mathcal{V}$ (Definition 4.1) and an order on such types (Definition 4.2).

Definition 4.1 *Let $\{L_i\}_{1 \leq i \leq n}$ be n lines in general position in $\mathbb{F}^2$. A finite subset of points, none of which is an intersection point,*

$$\mathcal{V} \subset \left(\bigcup_{i=1}^{n} L_i \right) \setminus \left(\bigcup_{1 \leq i < j \leq n} L_i \cap L_j \right) ,$$

is said to be of type $\mathbf{v} \in \mathbb{N}^n$, where $\mathbf{v}$ is a monotone vector in the sense that $0 \leq v_1 \leq v_2 \leq \cdots \leq v_n$, if there exists a permutation π of $(1, \ldots, n)$ such that $|\mathcal{V} \cap L_{\pi(i)}| = v_i$ for all $1 \leq i \leq n$.

For example, the two subsets depicted in Figure 3 are of type $\mathbf{v} = (2, 2, 3)$.

Definition 4.2 *A vector $\mathbf{u} \in \mathbb{N}^n$ dominates the vector $\mathbf{v} \in \mathbb{N}^n$, denoted $\mathbf{u} \succeq \mathbf{v}$, if for all $1 \leq i \leq n$, $\sum_{j=1}^{i} u_j \geq \sum_{j=1}^{i} v_j$.*

For example, $(1, 3, 3, 3) \succeq (1, 2, 3, 4)$ while $(1, 1, 4, 5) \not\succeq (1, 2, 3, 4)$.

Theorem 4.1 *Let $\mathbb{F}$ be a finite field of size q and n be a natural number such that $q > C_n := \sum_{k=3}^{n} k^{k+2}$. Let:*

- *$\{L_i\}_{1 \leq i \leq n}$ be n lines in general position in $\mathbb{F}^2$, none of which goes through the origin $(0, 0)$;*

- *$\mathcal{V}$ be a randomly selected set of points on those lines, none of which is an intersection point, and let $\mathbf{v}$ be the type of that set;*

- *$P(x, y) = \sum_{0 \le i+j \le n-1} a_{i,j} x^i y^j$ be a polynomial of degree (at most) $n-1$ in $\mathbb{F}[x, y]$, and $P|_{\mathcal{V}}$ be the values of P in the points of $\mathcal{V}$.*

Then if $\mathbf{v} \succeq (1, 2, \ldots, n)$, the set of values $P|_{\mathcal{V}}$ determines the polynomial P with probability of $1 - C_n q^{-1}$ at least.

Theorem 4.2 *Let:*

- *$\{L_i\}_{1 \le i \le n}$ be n lines in general position in $\mathbb{F}^2$;*

- *$\mathcal{V}$ be a set of points on those lines, none of which is an intersection point, of type $\mathbf{v} \not\succeq (1, 2, \ldots, n)$;*

- *$P(x, y) = \sum_{0 \le i+j \le n-1} a_{i,j} x^i y^j$ be a polynomial of degree (at most) $n-1$ in $\mathbb{F}[x, y]$, and $P|_{\mathcal{V}}$ be the values of P in the points of $\mathcal{V}$.*

- *S be a random linear combination of the coefficients of P.*

Then $P|_{\mathcal{V}}$ does not yield any information on S with probability $1 - q^{-1}$ at least, where $q = |\mathbb{F}|$.

Remarks.

1. Note that the probability in Theorem 4.1 is with respect to the random selection of $\mathcal{V} \in \Omega$ where

$$\Omega := \left\{ \mathcal{V} \subseteq \left(\bigcup_{i=1}^{n} L_i \right) \setminus \left(\bigcup_{1 \le i < j \le n} L_i \cap L_j \right) \middle| \mathbf{v} := \text{type}(\mathcal{V}) \succeq (1, 2, \ldots, n) \right\}. \tag{20}$$

   In Theorem 4.2, the set $\mathcal{V}$ is fixed and the probability is with respect to the selection of the random coefficients in the linear combination S.

2. The value of the constant C_n may be reduced by applying tighter estimates. However, in practical applications of Theorem 4.1 for the secret sharing scheme that we present later on, the typical values of n and q are usually such that $C_n q^{-1}$ is a very small probability.

In the following, we use the notation $\sigma_n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Lemma 4.3 *Let $\mathbf{v}$ be a monotone vector such that $\mathbf{v} \succeq (1, 2, \ldots, n)$. Then there exists a monotone vector $\mathbf{u}$ such that $\mathbf{u} \le \mathbf{v}$ (namely, $u_i \le v_i$ for all $1 \le i \le n$), $\mathbf{u} \succeq (1, 2, \ldots, n)$, $\sum_{i=1}^{n} u_i = \sigma_n$, and $u_n \le n$.*

Proof. We prove the claim by induction. The claim clearly holds for $n = 1$. Assume it holds for vectors of length $n-1$ and let $\mathbf{v}$ be a monotone vector in $\mathbb{N}^n$ such that $\mathbf{v} \succeq (1, 2, \dots, n)$.

If $v_n \geq n$, we define $\mathbf{u} = (u_1, \dots, u_n)$ as follows: $u_n = n$ while $(u_1, \dots, u_{n-1})$ is a monotone vector such that $u_i \leq v_i$ for all $1 \leq i \leq n-1$, $(u_1, \dots, u_{n-1}) \succeq (1, 2, \dots, n-1)$, $\sum_{i=1}^{n-1} u_i = \sigma_{n-1}$, and $u_{n-1} \leq n-1$. The vector $(u_1, \dots, u_{n-1})$ exists by the induction hypothesis since if $\mathbf{v} \succeq (1, 2, \dots, n)$ then $(v_1, \dots, v_{n-1}) \succeq (1, 2, \dots, n-1)$. The vector $\mathbf{u} = (u_1, \dots, u_{n-1}, u_n)$ thus defined satisfies all of the requirements.

Assume next that $v_n < n$. If $\sum_{i=1}^{n} v_i = \sigma_n$, we are done, since we can take $\mathbf{u} = \mathbf{v}$. If, on the other hand, $\sum_{i=1}^{n} v_i > \sigma_n$, we proceed to find a vector $\mathbf{u} = (w_1, \dots, w_{n-1}, v_n)$ such that $w_i \leq v_i$, $1 \leq i \leq n-1$, $(w_1, \dots, w_{n-1})$ is a monotone vector that dominates $(1, 2, \dots, n-1)$, $\sum_{i=1}^{n-1} w_i = \sigma_{n-1} + (n - v_n)$ and $w_{n-1} \leq v_n$. Such a vector would satisfy all of the requirements. By the induction hypothesis there exists a monotone vector $(u_1, \dots, u_{n-1})$ such that $u_i \leq v_i$ for all $1 \leq i \leq n-1$, $(u_1, \dots, u_{n-1}) \succeq (1, 2, \dots, n-1)$, and $\sum_{i=1}^{n-1} u_i = \sigma_{n-1}$. Hence, since

$$\sum_{i=1}^{n-1} v_i - \sum_{i=1}^{n-1} u_i = \left(\sum_{i=1}^{n} v_i - \sum_{i=1}^{n-1} u_i \right) - v_n > (\sigma_n - \sigma_{n-1}) - v_n = n - v_n \ ,$$

there exists a monotone vector $(w_1, \dots, w_{n-1})$, such that $u_i \leq w_i \leq v_i$, $1 \leq i \leq n-1$, and $\sum_{i=1}^{n-1} w_i = \sigma_{n-1} + (n - v_n)$. Specifically, if j is the maximal index for which $d_j := \sum_{i=j}^{n-1} v_i - \sum_{i=j}^{n-1} u_i \geq n - v_n$, then

$$w_i = \begin{cases} u_i & 1 \leq i < j \\ v_j - (d_j - (n - v_n)) & i = j \\ v_i & j < i \leq n-1 \end{cases} .$$

Finally, as $(w_1, \dots, w_{n-1}) \succeq (u_1, \dots, u_{n-1}) \succeq (1, 2, \dots, n-1)$ and $w_{n-1} \leq v_{n-1} \leq v_n$, we are done. □

Proof of Theorem 4.1. Let $\mathcal{V}$ be a randomly selected set from Ω, (20). By Lemma 4.3, $\mathcal{V}$ has a subset of points $\mathcal{V}'$ of type $\mathbf{v}'$ such that $\mathbf{v}' \succeq (1, 2, \dots, n)$, $\sum_{i=1}^{n} v'_i = \sigma_n$, and $v'_n \leq n$. We proceed to show that $P|_{\mathcal{V}'}$ determines the polynomial P with probability of $1 - C_n q^{-1}$ at least. Since $P|_{\mathcal{V}}$ is a superset of $P|_{\mathcal{V}'}$, this will settle our claim. For simplicity of notation, we denote the subset $\mathcal{V}'$ and its type $\mathbf{v}'$ by $\mathcal{V}$ and $\mathbf{v}$, respectively.

The case $n = 1$ is trivial. Let us examine the case $n = 2$. In that case, the unknown polynomial is $P(x, y) = a + bx + cy$, there are two intersecting lines, L_1 and L_2, and we are given the value of P at three points: $(x_1, y_1) \in L_1$ and $(x_2, y_2), (x_3, y_3) \in L_2$ (none of which is $A_{1,2} := L_1 \cap L_2$), see Figure 4. First, we compute the restriction of P to L_2. That restriction is a linear univariate polynomial, and hence, we may compute it by standard univariate interpolation through the two points (x_2, y_2) and (x_3, y_3). As a result, we have the value of P in $A_{1,2}$. This, in turn, enables us to compute the restriction of P to L_1, again, by univariate interpolation, this time through $A_{1,2}$ and (x_1, y_1). Now, if L_3 is any

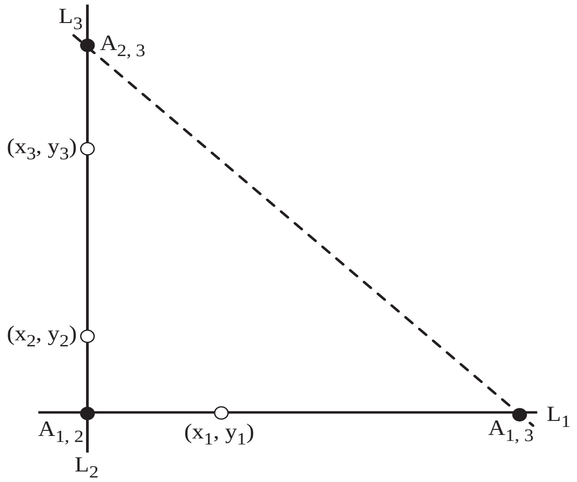

Figure 4: Interpolating a linear polynomial on two intersecting lines

line that lies in a general position with respect to L_1 and L_2, we have the value of P in the corresponding three intersection points, $A_{i,j} = L_i \cap L_j$, $1 \le i < j \le 3$. Using the techniques presented in Section 4.1, we may fully recover $P(x,y)$.

We proceed by induction. Without loss of generality we may assume that $|\mathcal{V} \cap L_i| = v_i$, $1 \le i \le n$ (namely, we assume that the permutation π in Definition 4.1 is the identity). Let us denote the points in $\mathcal{V}$ by $\{(x_i, y_i) : 1 \le i \le \sigma_n\}$. The values $P|_{\mathcal{V}}$ give rise to a linear system of σ_n equations in the σ_n unknown coefficients of $P(x,y) = \sum_{0 \le i+j \le n-1} a_{i,j} x^i y^j$. Denote by M the matrix of that linear system; then its ith row, $1 \le i \le \sigma_n$, is given by

$$M_{i,\cdot} = \left(\begin{array}{cccccccccccc} 1 & x_i & y_i & x_i^2 & x_i y_i & y_i^2 & \dots & x_i^{n-1} & x_i^{n-2} y_i & \dots & x_i y_i^{n-2} & y_i^{n-1} \end{array} \right) .$$

We aim at showing that M is singular with probability that does not exceed $C_n q^{-1}$.

To that end, we invoke Lemma 4.3 for the vector $(v_1, \dots, v_{n-1})$. Since that vector dominates the vector $(1, \dots, n-1)$ there exists a monotone vector $(u_1, \dots, u_{n-1})$ such that $u_i \le v_i$, $1 \le i \le n-1$, $u_{n-1} \le n-1$ and $\sum_{i=1}^{n-1} u_i = \sigma_{n-1}$. Let us rearrange the order of the rows in M so that the first σ_{n-1} rows correspond to a subset of points of type $(u_1, \dots, u_{n-1})$. Hence, by induction, the main σ_{n-1}-dimensional minor of M is singular with probability that does not exceed $C_{n-1} q^{-1}$.

Next, we consider the determinant

$$\det M = \det \left(\begin{array}{cccc|cccc} 1 & x_1 & y_1 & \dots & x_1^{n-1} & x_1^{n-2} y_1 & \dots & y_1^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{\sigma_{n-1}} & y_{\sigma_{n-1}} & \dots & x_{\sigma_{n-1}}^{n-1} & x_{\sigma_{n-1}}^{n-2} y_{\sigma_{n-1}} & \dots & y_{\sigma_{n-1}}^{n-1} \\ \hline 1 & x_{\sigma_{n-1}+1} & y_{\sigma_{n-1}+1} & \dots & x_{\sigma_{n-1}+1}^{n-1} & x_{\sigma_{n-1}+1}^{n-2} y_{\sigma_{n-1}+1} & \dots & y_{\sigma_{n-1}+1}^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{\sigma_n} & y_{\sigma_n} & \dots & x_{\sigma_n}^{n-1} & x_{\sigma_n}^{n-2} y_{\sigma_n} & \dots & y_{\sigma_n}^{n-1} \end{array} \right) .$$

We view the first σ_{n-1} points in the sequence as fixed, and the last n points as variables. In addition, for all $\sigma_{n-1}+1 \leq i \leq \sigma_n$, y_i depends on x_i linearly, $y_i = \hat{a}_i x_i + \hat{b}_i$. (The constants $\hat{a}_i$ and $\hat{b}_i$ are the parameters of the line on which the point (x_i, y_i) lies. We assume, without loss of generality, that none of the lines is of the form x=Const.) Therefore, we may view $\det M$ as a polynomial in the variables $(x_{\sigma_{n-1}+1}, \ldots, x_{\sigma_n})$. For the sake of simplicity, we denote the variables $(x_{\sigma_{n-1}+1}, \ldots, x_{\sigma_n})$ by $\xi_1, \ldots, \xi_n$ (and the corresponding y-coordinates by $\eta_1, \ldots, \eta_n$).

We claim, and prove later, that $\det M(\xi_1, \ldots, \xi_n)$ is a nonzero polynomial whenever the main σ_{n-1}-dimensional minor of M is nonzero. Since ξ_i are chosen randomly in $\mathbb{F}$, under the restriction that $\xi_i \neq \xi_j$ whenever they both correspond to points on the same line, the number of selections of $(\xi_1, \ldots, \xi_n)$ is at least $\binom{q}{n}$. Since the degree of the polynomial $\det M(\xi_1, \ldots, \xi_n)$ with respect to each of its variables is at most $n-1$, we infer, by Lemma 2.2, that $\det M(\xi_1, \ldots, \xi_n)$ has at most $n(n-1)q^{n-1}$ zeros. Therefore, the probability of selecting $(\xi_1, \ldots, \xi_n)$ as one of the zeros of $\det M$ is at most $\frac{n(n-1)q^{n-1}}{\binom{q}{n}} < c_n q^{-1}$ for $c_n = n^{n+2}$. Altogether, we conclude that $\det M$ vanishes with probability that does not exceed $C_{n-1}q^{-1} + c_n q^{-1} = C_n q^{-1}$. This implies that $P|_{\mathcal{V}}$ determines the polynomial with probability at least $1 - C_n q^{-1}$.

It remains to prove that if the main σ_{n-1}-dimensional minor of M is nonzero, then $\det M(\xi_1, \ldots, \xi_n)$ is a nonzero polynomial. Observe that

$$\det M(\xi_1, \ldots, \xi_n) = M_{\sigma_{n-1}} \cdot p(\xi_1, \ldots, \xi_n) + r(\xi_1, \ldots, \xi_n),$$

where $M_{\sigma_{n-1}}$ is the main σ_{n-1}-dimensional minor of M (which is assumed to be nonzero),

$$p(\xi_1, \ldots, \xi_n) := \det \begin{pmatrix} \xi_1^{n-1} & \xi_1^{n-2}\eta_1 & \cdots & \xi_1\eta_1^{n-2} & \eta_1^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \xi_n^{n-1} & \xi_n^{n-2}\eta_n & \cdots & \xi_n\eta_n^{n-2} & \eta_n^{n-1} \end{pmatrix} \tag{21}$$

is the determinant of the lower right block in M, and $r(\xi_1, \ldots, \xi_n)$ stands for the sum of all other terms in the determinant. We show that $\det M(\xi_1, \ldots, \xi_n)$ is a nonzero polynomial by proving the following two claims:

- **Claim 1.** $p(\xi_1, \ldots, \xi_n)$ is a nonzero polynomial.
- **Claim 2.** $\deg r(\xi_1, \ldots, \xi_n) < \deg p(\xi_1, \ldots, \xi_n)$.

Proof of Claim 1. By extracting ξ_i^{n-1} from the ith row in the determinant in (21), for all $1 \leq i \leq n$, we obtain a Vandermonde determinant. This brings us to the conclusion that

$$p(\xi_1, \ldots, \xi_n) = \prod_{i=1}^{n} \xi_i^{n-1} \cdot \prod_{1 \leq i < j \leq n} \left(\frac{\eta_j}{\xi_j} - \frac{\eta_i}{\xi_i} \right) = \prod_{1 \leq i < j \leq n} (\xi_i \eta_j - \xi_j \eta_i),$$

or, after substituting $\eta_i = \hat{a}_i\xi_i + \hat{b}_i$, that

$$p(\xi_1,\ldots,\xi_n) = \prod_{1\le i<j\le n} p_{i,j}(\xi_1,\ldots,\xi_n)\,, \tag{22}$$

where

$$p_{i,j}(\xi_1,\ldots,\xi_n) = (\hat{a}_j - \hat{a}_i)\xi_i\xi_j + \hat{b}_j\xi_i - \hat{b}_i\xi_j\,.$$

The polynomial $p_{i,j}(\xi_1,\ldots,\xi_n)$ is nonzero since $\hat{b}_i, \hat{b}_j \neq 0$ (as implied by our assumption that none of the lines goes through the origin). As it is a polynomial of degree 1 in each of the two variables ξ_i, ξ_j, it has no more than $2q$ zeros in $\mathbb{F}_{\xi_i} \times \mathbb{F}_{\xi_j}$. Consequently, viewed as a polynomial in $(\xi_1,\ldots,\xi_n)$, $p_{i,j}(\xi_1,\ldots,\xi_n)$ has no more than $2q^{n-1}$ zeros. Since, by (22), $p(\xi_1,\ldots,\xi_n)$ is a product of $\binom{n}{2}$ such polynomials, it has no more than $n(n-1)q^{n-1}$ zeros in $\mathbb{F}^n$. As $n(n-1) < q$, the number of zeros of $p(\xi_1,\ldots,\xi_n)$ is smaller than $|\mathbb{F}^n|$. This implies that $p(\xi_1,\ldots,\xi_n)$ is a nonzero polynomial.

Proof of Claim 2. det$M$ is a linear combination of all minors of size $n\times n$ that are contained within the last n rows of M. While $p(\xi_1,\ldots,\xi_n)$ is the $n\times n$ minor that corresponds to the n right-most columns, the remainder $r(\xi_1,\ldots,\xi_n)$ corresponds to all other minors that involve at least one of the first σ_{n-1} columns.

Let $\mu(\xi_1,\ldots,\xi_n)$ and $\mu'(\xi_1,\ldots,\xi_n)$ be two such $n\times n$ minors that differ in one column only: while the first column in $\mu(\xi_1,\ldots,\xi_n)$ consists of entries of the form $\xi_i^j\eta_i^k$, the first column in $\mu'(\xi_1,\ldots,\xi_n)$ consists of entries of the form $\xi_i^{j'}\eta_i^{k'}$. (All other $n-1$ columns in those two minors are the same.) We proceed to show that if $j'+k' < j+k$ then $\deg\mu'(\xi_1,\ldots,\xi_n) < \deg\mu(\xi_1,\ldots,\xi_n)$. As shown later, this will settle our claim.

Let $\mu(\xi_1,\ldots,\xi_n) = \sum_{i=1}^n \mu_i(\xi_1,\ldots,\xi_n)$ be the expansion of the determinant μ with respect to its first column. Then the corresponding expansion of μ' is given by $\mu'(\xi_1,\ldots,\xi_n) = \sum_{i=1}^n \mu_i'(\xi_1,\ldots,\xi_n)$ where $\mu_i' = \mu_i\cdot\xi_i^{j'-j}\eta_i^{k'-k}$. Assume that $\deg\mu(\xi_1,\ldots,\xi_n) = d$. Namely, the highest order terms in each of $\mu_i(\xi_1,\ldots,\xi_n)$, $1\le i\le n$, are of the form $\prod_{i=1}^n \xi_i^{h_i}$ where $\sum_{i=1}^n h_i \le d$. Hence, the highest order terms in all of $\mu_i'(\xi_1,\ldots,\xi_n)$, $1\le i\le n$, are of degree $d + (j'+k') - (j+k) < d$ at most. That settles our claim because every minor in $r(\xi_1,\ldots,\xi_n)$ may be obtained from the minor $p(\xi_1,\ldots,\xi_n)$ by a number of degree-decreasing column-switches of that sort, and, consequently, the degree of each such minor is strictly less than that of $p(\xi_1,\ldots,\xi_n)$.
□

Proof of Theorem 4.2. Assume that $\mathbf{v} \not\geq (1,2,\ldots,n)$. To prove this part of the theorem, it is more convenient to change the basis of the space of bivariate polynomials of degree $n-1$. Let L_0 be a line in $\mathbb{F}^2$ that intersects all of the lines $L_1,\ldots,L_n$ in n distinct points, none of which is in $\mathcal{V}$. Then, in view of our discussion in Section 4.1, any polynomial

$$P(x,y) = \sum_{0\le i+j\le n-1} a_{i,j}x^iy^j \in \mathbb{F}_{n-1}[x,y]$$

has an alternative representation

$$P(x,y) = \sum_{0\le i<j\le n} b_{i,j} L_{i,j}(x,y) \tag{23}$$

where

$$L_{i,j}(x,y) = \prod_{\substack{0\le k\le n\\ k\ne i,j}} L_k(x,y)\ , \tag{24}$$

and $L_k(x,y)=0$ is the equation that defines the line L_k, $0\le k\le n$.

As in the proof of Theorem 4.1, let us denote the points in $\mathcal{V}$ by $\{(x_i,y_i) : 1\le i\le |\mathbf{v}|\}$. The values $P|_{\mathcal{V}}$ give rise to a system of $|\mathbf{v}|$ equations in the σ_n unknown coefficients in (23). Letting M denote the matrix of coefficients in that system, the ith row of M, $1\le i\le|\mathbf{v}|$, is given by,

$$M_{i,\cdot} = \left(\ L_{0,1}(x_i,y_i)\quad L_{0,2}(x_i,y_i)\quad L_{1,2}(x_i,y_i)\quad \cdots\quad L_{0,n}(x_i,y_i)\quad \cdots\quad L_{n-1,n}(x_i,y_i)\ \right)\ . \tag{25}$$

We proceed to show that the rank of M is smaller than σ_n. This will imply that a random vector from $\mathbb{F}^{\sigma_n}$ is in the row space of M with probability q^{-1} at the most. Since S is a random linear combination of the σ_n coefficients of P, this will imply that $P|_{\mathcal{V}}$ does not yield any information on S with probability $1-q^{-1}$ at least.

The main observation towards this end is that if $(x_i,y_i)\in L_j$ then $L_{k,\ell}(x_i,y_i)=0$ if $j\notin\{k,\ell\}$. Consequently, in every row of the matrix M there are σ_{n-1} entries that are zero. For example, in rows that correspond to points $(x_i,y_i)\in L_n$, only the last n entries, $L_{j,n}(x_i,y_i)$, $0\le j\le n-1$, are nonzero.

As $\mathbf{v}\not\succeq(1,2,\ldots,n)$, there exists $1\le j\le n$ for which $\sum_{i=1}^{j} v_i<\sigma_j$. Assume that the rows of the matrix M are ordered so that the first v_1 rows correspond to the points on L_1, the next v_2 rows correspond to the points on L_2, and so forth. Then in all the rows after the first $\sum_{i=1}^{j} v_i$ rows, the first σ_j entries are zero. Indeed, the first σ_j entries in each row are

$$M_{i,1\,:\,\sigma_j} = \left(\ L_{0,1}(x_i,y_i)\quad L_{0,2}(x_i,y_i)\quad L_{1,2}(x_i,y_i)\quad \cdots\quad L_{0,j}(x_i,y_i)\quad \cdots\quad L_{j-1,j}(x_i,y_i)\ \right)\ .$$

Each row after the first $\sum_{i=1}^{j} v_i$ rows corresponds to a point (x_i,y_i) that lies on one of the lines $L_{j+1},\ldots,L_n$. For such points, $L_{k,\ell}(x_i,y_i)=0$ for all $0\le k<\ell\le j$. We arrive at the conclusion that the first σ_j columns of the matrix M are identically zero beyond the first $\sum_{i=1}^{j} v_i<\sigma_j$ rows. That means that the column rank of M is lacking. As the number of columns of M is σ_n, we infer that the rank of M is at most σ_n-1. $\Box$

4.3 Hierarchical Threshold Access Structures

Let $\mathcal{U}$ be a set of participants that is partitioned into m disjoint *levels*, (1), and let $k_1<k_2<\cdots<k_m$ be a sequence of thresholds. The corresponding hierarchical threshold access

structure is defined by

$$\Gamma = \left\{ \mathcal{V} \subset \mathcal{U} : \left| \mathcal{V} \cap \left(\bigcup_{j=1}^{i} \mathcal{C}_j \right) \right| \geq k_i \text{ for all } 1 \leq i \leq m \right\} . \tag{26}$$

Those access structures were presented and studied in [17]. They are realized there by an ideal secret sharing scheme that is based on Birkhoff interpolation, namely, interpolation in which the given values of the unknown polynomial, $P(x)$, include also derivative values. Specifically, participants from level $\mathcal{C}_i$, $1 \leq i \leq m$, receive the value of the (k_{i-1})th derivative of P at the point x that identifies them (where hereinafter $k_0 := 0$). As participants from higher levels (namely, $\mathcal{C}_i$ for lower values of i) have shares that equal derivatives of P of lower orders, those shares carry more information on the coefficients of P than shares of participants from lower levels.

Here we show how to realize such hierarchical access structures using bivariate Lagrange interpolation on lines in general position. The scheme that we present here does not use derivatives, as the Birkhoff interpolation-based scheme of [17] did, but instead it adds one more dimension in order to achieve the same hierarchical effect.

Let $\{L_j\}_{1 \leq j \leq n}$ be $n := k_m$ lines in general position in $\mathbb{F}^2$, none of which goes through the origin $(0,0)$. Let $\{w_{i,j}\}_{0 \leq i+j \leq n-1}$ be publicly known values that are selected randomly and independently from $\mathbb{F}$. Finally, let $P(x,y) = \sum_{0 \leq i+j \leq n-1} a_{i,j} x^i y^j$ be a random polynomial in $\mathbb{F}_{n-1}[x,y]$, whose coefficients are selected so that $S = \sum_{0 \leq i+j \leq n-1} a_{i,j} w_{i,j}$. Then the secret sharing scheme in this case is as follows.

Secret Sharing Scheme 3:

1. *Each participant from level $\mathcal{C}_i$ will be identified by a unique public point on $L_{k_i} \setminus \left(\bigcup_{\substack{1 \leq j \leq n \\ j \neq k_i}} L_j \right)$ and his private share will be the value of P at that point.*

2. *In addition, we publish the value of P at:*

   - *k_{i-1} additional points on L_{k_i}, $2 \leq i \leq m$; and*
   - *j points on L_j for all $j \in \{1, 2, \ldots, n\} \setminus \{k_i : 1 \leq i \leq m\}$.*

Example. Assume that there are $m = 3$ levels with thresholds $k_1 = 2$, $k_2 = 4$ and $k_3 = 5$ (namely, $\mathcal{V} \in \Gamma$ if and only if it has at least 2 participants from the highest level $\mathcal{C}_1$, at least 4 participants from the two highest levels $\mathcal{C}_1 \cup \mathcal{C}_2$, and at least 5 participants altogether). Then we select 5 random lines in general position: L_i, $1 \leq i \leq 5$. The allocation of private shares will be as follows:

1. Participants from $\mathcal{C}_1$ will be given polynomial shares on L_2 (since $k_1 = 2$).

2. Participants from $\mathcal{C}_2$ will be given polynomial shares on L_4 (since $k_2 = 4$).

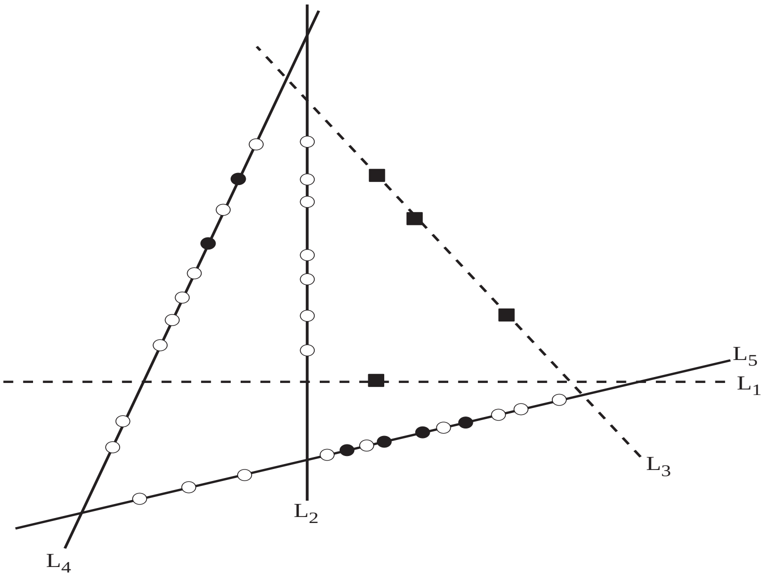

Figure 5: Secret Sharing Scheme 3

3. Participants from $\mathcal{C}_3$ will be given polynomial shares on L_5 (since $k_3 = 5$).

The corresponding points are marked in Figure 5 by empty circles. The public values will be:

1. 2 point values on L_4, and 4 point values on L_5 (those points are marked by full bullets in Figure 5).
2. 1 point value on L_1 and 3 point values on L_3 (those points are marked by full squares in Figure 5).

Theorem 4.4 *The ideal Secret Sharing Scheme 3 is a perfect scheme that realizes the hierarchical threshold access structure (26), with probability* $1 - C_n q^{-1}$ *at least, where* $C_n := \sum_{k=3}^{n} k^{k+2}$.

A direct consequence of Theorem 4.4 is that there exists an ideal secret sharing scheme for the hierarchical threshold access structure, (26), whenever

$$q = |\mathbb{F}| > C_n := \sum_{k=3}^{n} k^{k+2}\,, \tag{27}$$

where $n = k_m$ is the size of minimal authorized subsets. This lower bound on the size of the underlying field is a significant improvement with respect to the corresponding result in [17, Corollary 3.4] where the condition on the size of the field was

$$q > \binom{|\mathcal{U}|+1}{n} \cdot \frac{(n-2)(n-1)}{2} + n \, .$$

(The improvement is due to the fact that typically $|\mathcal{U}| >> n$.)

Proof of Theorem 4.4. Given $\mathcal{V} \subset \mathcal{U}$, let $x_i = |\mathcal{V} \cap \mathcal{C}_i|$, $1 \le i \le m$, denote the number of participants that $\mathcal{V}$ has from the ith level. Then $\mathcal{V}$ knows the value of P at v_j points along L_j, $1 \le j \le n$, where

$$v_j = \begin{cases} k_{i-1} + x_i & j = k_i \text{ for some } 1 \le i \le m \\ j & \text{otherwise} \end{cases} \, . \tag{28}$$

Let us denote $\mathbf{v} := (v_1, \ldots, v_n)$, and let $\mathbf{v}'$ denote the monotone non-decreasing ordering of $\mathbf{v}$; namely, $\mathbf{v}'$ is the *type* of the set of points in which $\mathcal{V}$ knows the value of P. In view of Theorems 4.1 and 4.2 we need only to show that $\mathbf{v}' \succeq (1, 2, \ldots, n)$ if and only if $\mathcal{V} \in \Gamma$.

Part 1: $\mathcal{V} \in \Gamma$ implies that $\mathbf{v}' \succeq (1, 2, \ldots, n)$.

Assume that $\mathcal{V} \in \Gamma$. Then, by (26),

$$\sum_{j=1}^{i} x_j \ge k_i \quad , \quad 1 \le i \le m \, . \tag{29}$$

The vectors $\mathbf{v}$ and $\mathbf{v}'$ include components of two kinds, as seen in (28): *level components*, that correspond to positions $\{k_1, \ldots, k_m\}$ in $\mathbf{v}$, and *separator components*, that are the remaining $n - m$ components. This induces a similar separation on the components of the vector $(1, 2, \ldots, n)$: we refer to the components in positions $\{k_1, \ldots, k_m\}$ as level components, and to the remaining ones as separator components. Let $\mathbf{w} = (v_{k_1}, v_{k_2}, \ldots, v_{k_m})$ be the sub-vector of all level components within $\mathbf{v}$, let $\mathbf{w}'$ be its monotone non-decreasing ordering, and let $(k_1, k_2, \ldots, k_m)$ be the sub-vector of all level components within $(1, 2, \ldots, n)$. We begin by proving that

$$\mathbf{w}' \succeq (k_1, k_2, \ldots, k_m) \, . \tag{30}$$

We will then use (30) in order to establish the full domination relation, i.e.,

$$\mathbf{v}' \succeq (1, 2, \ldots, n) \, . \tag{31}$$

- Step 1: Proving (30). In order to prove (30) we need to show that

$$\sum_{j=1}^{\ell} w'_j \ge \sum_{j=1}^{\ell} k_j \quad , \quad 1 \le \ell \le m \, . \tag{32}$$

Fix ℓ in the range $1 \leq \ell \leq m$. There are two cases to consider: If $\{w'_1, \ldots, w'_\ell\} = \{v_{k_1}, \ldots, v_{k_\ell}\}$ then

$$\sum_{j=1}^{\ell} w'_j = \sum_{j=1}^{\ell} v_{k_j} = \sum_{j=1}^{\ell} (k_{j-1} + x_j) = \sum_{j=1}^{\ell-1} k_j + \sum_{j=1}^{\ell} x_j \geq \sum_{j=1}^{\ell} k_j \ , \tag{33}$$

where the last inequality stems from (29). If, on the other hand, $\{w'_1, \ldots, w'_\ell\} \neq \{v_{k_1}, \ldots, v_{k_\ell}\}$ (this may happen only when $\ell < m$) then there exists a minimal index i, $1 \leq i \leq \ell$, such that $v_{k_i} \notin \{w'_1, \ldots, w'_\ell\}$. Hence,

$$\sum_{j=1}^{\ell} w'_j = \sum_{j=1}^{i-1} v_{k_j} + \sum_{j=i}^{\ell} v_{k_{r_j}} \ , \tag{34}$$

where

$$i < r_i < r_{i+1} < \cdots < r_\ell \ . \tag{35}$$

As argued in (33),

$$\sum_{j=1}^{i-1} v_{k_j} \geq \sum_{j=1}^{i-1} k_j \ . \tag{36}$$

On the other hand, (35) implies that $r_j \geq j+1$ for all $i \leq j \leq \ell$. Hence, as $k_1 \leq k_2 \leq \cdots \leq k_m$, we conclude that $k_{r_j} \geq k_{j+1}$. Therefore, by the definition of v_{k_j}, (28), we conclude that

$$v_{k_{r_j}} \geq k_{r_j - 1} \geq k_j \quad , \quad i \leq j \leq \ell \ . \tag{37}$$

Finally, (32) follows from (34), (36) and (37).

• Step 2: Proving (31). Having shown (30) we proceed to prove (31). To that end we need to show that if we add to the two vectors on both sides of the domination relation (30) the $n - m$ separator components $\{1, 2, \ldots, n\} \setminus \{k_1, \ldots, k_m\}$, the domination relation (31) still holds, i.e.,

$$\sum_{j=1}^{i} v'_j \geq \sum_{j=1}^{i} j \quad , \quad 1 \leq i \leq n \ . \tag{38}$$

Fix an i, let $1 \leq \ell \leq m$ be the maximal index such that $k_\ell \leq i$, and let t be the number of level components in $(v'_1, \ldots, v'_i)$. There are three cases to consider:

1. If $t = \ell$, then $(38)_i$ follows from $(32)_\ell$. Indeed, in that case the $t = \ell$ level components in $(v'_1, \ldots, v'_i)$ are exactly $(w'_1, \ldots, w'_\ell)$ and the additional separator components on the left hand side of $(38)_i$ are $\{1, 2, \ldots, i\} \setminus \{k_1, \ldots, k_\ell\}$. Hence, by adding the sum of $\{1, 2, \ldots, i\} \setminus \{k_1, \ldots, k_\ell\}$ to both sides of the inequality $(32)_\ell$, we arrive at $(38)_i$.

2. If $t > \ell$ then

$$\sum_{j=1}^{i} v'_j = \sum_{j=1}^{t} w'_j + g_{i-t} \tag{39}$$

where g_r stands for the sum of the smallest r separator values, namely, the r minimal numbers in $\{1, 2, \ldots, n\} \setminus \{k_1, \ldots, k_m\}$. In view of (32), equality (39) implies that

$$\sum_{j=1}^{i} v'_j \geq \sum_{j=1}^{t} k_j + g_{i-\ell} - (g_{i-\ell} - g_{i-t}) \ .$$

By the definition of the partial sums g_r, $\sum_{j=1}^{\ell} k_j + g_{i-\ell} = \sum_{j=1}^{i} j$. Hence, it remains to prove that

$$\sum_{j=\ell+1}^{t} k_j \geq (g_{i-\ell} - g_{i-t}) \tag{40}$$

in order to establish our claim (38) in this case. Indeed, as, by our assumption, the prefix $\{1, 2, \ldots, i\}$ includes exactly ℓ level components, $\{k_1, \ldots, k_\ell\}$, the difference $g_{i-\ell} - g_{i-t}$ is composed of the $t - \ell$ largest numbers in $\{1, 2, \ldots, i\} \setminus \{k_1, \ldots, k_\ell\}$, all of which are less than or equal to i. On the other hand,

$$\sum_{j=\ell+1}^{t} k_j \geq (t - \ell) \cdot k_{\ell+1} > (t - \ell) \cdot i \ .$$

Hence, (40) follows and our claim in this case is settled.

3. If $t < \ell$ then equality (39) still holds. In view of (32), equality (39) implies that

$$\sum_{j=1}^{i} v'_j \geq \sum_{j=1}^{t} k_j + g_{k_t - t} + (g_{i-t} - g_{k_t - t})$$

(note that in this case $k_t < k_\ell \leq i$). Since, by the definition of the partial sums g_r, $\sum_{j=1}^{t} k_j + g_{k_t - t} = \sum_{j=1}^{k_t} j$ we need only to prove that

$$g_{i-t} - g_{k_t - t} \geq \sum_{j=k_t+1}^{i} j \tag{41}$$

in order to establish our claim (38) in this case. Indeed, as the minimal separator value in $g_{i-t} - g_{k_t - t}$ is at least $k_t + 1$ and each separator value is strictly larger than its predecessor, inequality (41) holds. This settles our claim in this case as well, and thus the proof of (38) is complete.

Part 2: $\mathcal{V} \notin \Gamma$ implies that $\mathbf{v}' \not\geq (1, 2, \ldots, n)$.

Assume next that $\mathcal{V} \notin \Gamma$. Then there exists a minimal $i \geq 1$ such that

$$\sum_{j=1}^{\ell} x_j \geq k_\ell \quad \text{for all} \quad 1 \leq \ell < i \tag{42}$$

and

$$\sum_{j=1}^{i} x_j < k_i \ . \tag{43}$$

In that case, we claim that

$$\sum_{j=1}^{k_i} v_j < \sum_{j=1}^{k_i} j \ . \tag{44}$$

Indeed, by the definition of $\mathbf{v}$, (28),

$$\sum_{j=1}^{k_i} v_j = \sum_{\substack{1\le j\le k_i \\ j\notin\{k_1,\ldots,k_i\}}} v_j + \sum_{j=1}^{i} v_{k_j} = \sum_{\substack{1\le j\le k_i \\ j\notin\{k_1,\ldots,k_i\}}} j + \sum_{j=1}^{i}(k_{j-1}+x_j) = \sum_{j=1}^{k_i-1} j + \sum_{j=1}^{i} x_j < \sum_{j=1}^{k_i} j \ ,$$

where the last inequality is implied by (43). Since $\mathbf{v}'$ is the monotone non-decreasing ordering of $\mathbf{v}$, inequality (44) implies that $\sum_{j=1}^{k_i} v'_j < \sum_{j=1}^{k_i} j$, whence $\mathbf{v}' \not\geq (1, 2, \ldots, n)$. The proof is thus complete. □

5 Epilogue

The advantage of bivariate interpolation over the standard univariate one in designing linear secret sharing schemes for multipartite settings is in the ability to associate different compartments with different lines in the plane. Bivariate interpolation on lines was extended to multivariate interpolation on flats in several dimensions in [2]. By going to higher dimensions and by adequately choosing the flats that represent the compartments, it might be possible to design secret sharing schemes for a wide array of interesting access structures. (In several dimensions we have more flexibility in choosing the dimensions of the flats and their interrelation.) It would be also interesting to explore the possible advantages of using non-linear manifolds instead of flats.

We would like to note that after the completion of this work, we came across the new paper of Herranz and Sáez [9] where they introduce a new type of a multipartite access structure. In that access structure, each authorized subset must be of size at least t, and it must include representatives from at least k different compartments. Namely, if $\mathcal{U}$ is partitioned to m compartments, (1), then $\mathcal{V} \in \Gamma$ if and only if $|\mathcal{V}| \geq t$ for some $t > 0$ and $|\mathcal{V} \cap \mathcal{C}_i| > 0$ for at least k indices $1 \leq i \leq m$. (Clearly, $k \leq m, t$.) The linear scheme that was proposed in [9] for that access structure may be viewed as a scheme that is based on bivariate polynomial interpolation. With that interpretation, their scheme takes the following form:

Secret Sharing Scheme 4:

1. *The dealer generates a random polynomial* $P(x, y) = Q(x) + R(y)$ *over* $\mathbb{F}$, *where* $Q(x) = \sum_{i=0}^{k-1} a_i x^i$ *and* $R(y) = \sum_{j=1}^{t-k} b_i y^i$.

2. *The secret is* $S = P(0, 0)$.

3. *Each participant* $u_{i,j}$ *from compartment* $\mathcal{C}_i$ *will be identified by a unique public point* $(x_i, y_{i,j})$*, where* $x_i \neq 0$ *and* $y_{i,j} \neq 0$*, and his private share will be* $P(x_i, y_{i,j})$.

Here, x_i, $1 \leq i \leq m$, are m distinct values in the field $\mathbb{F}$. All participants of compartment $\mathcal{C}_i$ receive private shares on the vertical line $x = x_i$. It is shown in [9] that there exists an allocation of identities in $\mathbb{F}^2$ for which the resulting scheme is perfect. Utilizing the same techniques that we used here for the compartmented access structures, it is possible to prove that a random allocation of identities will result in a perfect scheme with probability of $1 - O(q^{-1})$.

References

[1] A. Beimel, T. Tassa and E. Weinreb, Characterizing ideal weighted threshold secret sharing, to appear in *SIAM Journal of Discrete Mathematics.* A preliminary version appeared in *The Proceedings of the Second Theory of Cryptography Conference, TCC 2005*, February 2005, MIT, pp. 600-619.

[2] C. de Boor, N. Dyn and A. Ron, Polynomial interpolation to data on flats in $\mathbb{R}^d$, *Journal of Approximation Theory*, 105 (2000), pp. 313-343.

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

[4] K.C. Chung and T.H. Yao, On lattices admitting unique Lagrange interpolation, *SIAM Journal on Numerical Analysis*, 14 (1977), pp. 735-743.

[5] M.J. Collins, A note on ideal tripartite access structures, available at http://eprint.iacr.org/2002/193/ (2002).

[6] O. Farràs, J. Martí-Farré and C. Padró, Ideal multipartite secret sharing schemes, *Advances in Cryptology - EUROCRYPT 2007*, LNCS 4515 (2007), pp. 448-465.

[7] S. Fehr Efficient construction of the dual span program, *Manuscript*, May 1999.

[8] A. Gál, *Combinatorial methods in Boolean function complexity*, Ph.D. thesis, University of Chicago, 1995.

[9] J. Herranz and G. Sáez, New results on multipartite access structures, *IEE Proc. Information Security*, 153 (2006), pp. 153-162.

[10] M. Karchmer and A. Wigderson, On span programs, in *The Proceedings of the 8th Structures in Complexity conference*, (1993), pp. 102-111.

[11] E. D. Karnin, J. W. Greene, and M. E. Hellman, On secret sharing systems, *IEEE Trans. on Information Theory*, 29 (1983), pp. 35 - 41.

[12] M. Naor and B. Pinkas, Secure and efficient metering, *Advances in Cryptology - EUROCRYPT 98*, LNCS 1403 (1998), pp. 576-590.

[13] C. Padró and G. Sáez, Secret sharing schemes with bipartite access structure, *IEEE Transactions on Information Theory*, 46 (2000), pp. 2596-2604.

[14] J. Schwartz, Fast probabilistic algorithms for verification of polynomial identities, *Journal of the ACM*, 27 (1980), pp. 701 - 717.

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

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

[17] T. Tassa, Hierarchical threshold secret sharing, *Journal of Cryptology*, 20 (2007), pp. 237-264. An earlier version appeared in *The Proceedings of the First Theory of Cryptography Conference, TCC 2004*, February 2004, MIT, Cambridge, pp. 473-490.

[18] R. Zippel, Probabilistic algorithms for spare polynomials, in *Proceedings of Symbolic and Algebraic Computation, EUROSAM 79*, Marseille, 1979, pp. 216-226.