Multipartite Secret Sharing by Bivariate Interpolation

Tamir Tassa[1] and Nira Dyn[2]

[1] Division of Computer Science, The Open University, Ra'anana, Israel.
[2] Department of Applied Mathematics, Tel Aviv University, Tel Aviv, Israel.

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 - compartmented access structures with lower bounds, compartmented access structures with upper bounds, and hierarchical threshold access structures. We realize those access structures by ideal perfect secret sharing schemes that are based on bivariate Lagrange interpolation. The main novelty of this paper is the introduction of bivariate interpolation and its potential power in designing schemes for multipartite settings, as different compartments may be associated with different lines 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 [13].

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

1 Introduction

Let $\mathcal{U}$ be a set of participants and assume that it is partitioned into m disjoint subsets,

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

to which we refer hereinafter as *compartments*. An m-partite access structure on $\mathcal{U}$ is any access structure that does not distinguish between members of the same compartment. More specifically, an access structure $\Gamma \in 2^{\mathcal{U}}$ is m-partite with respect to partition (1) if for all permutations $\pi : \mathcal{U} \to \mathcal{U}$ such that $\pi(\mathcal{C}_i) = \mathcal{C}_i$, $1 \le i \le m$, $\mathcal{A} \in \Gamma$ if and only if $\pi(\mathcal{A}) \in \Gamma$. Weighted threshold access structures [11, 1], multilevel access structures [12, 3], hierarchical threshold access structures [13], compartmented access structures [3, 8], bipartite access structure [10], and tripartite access structures [1, 5, 8] are typical examples of such multipartite access structures. (Of-course, every access structure may be viewed as a multipartite access structure with singleton compartments; however, that term is reserved to non-degenerate cases where the number of compartments is smaller than the number of participants.)

In this paper we show how to utilize bivariate interpolation in order to realize some multipartite access structures. 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.

In Section 2 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 3 we deal with hierarchical threshold access structures and we realize them by bivariate Lagrange interpolation with data on lines in general position. In [13], 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 herein. Finally, in Section 4, we contemplate on the possible advantages of using more involved interpolation settings.

Hereinafter, $\mathbb{F}$ is a finite field of size $q = |\mathbb{F}|$. The field size is large enough so that the domain of all possible secrets may be embedded in $\mathbb{F}$. The secret $S \in \mathbb{F}$ will be encoded by the coefficients of an unknown polynomial $P(x, y) \in \mathbb{F}[x, y]$. We also 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.

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 1. *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}.*

All proofs are given in the full version of this paper.

2 Compartmented Access Structures

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

Then

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

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 to that, 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 t, we would like to limit the number of participants that represent each of the compartments; namely,

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

where $s_i, s \in \mathbb{N}$ and $s \leq \sum_{i=1}^{m} s_i$. 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 [11]. When $m = 2$ the two types of access structures agree: a compartmented access structure with lower bounds t_1, t_2 and t is a compartmented access structure with upper bounds $s_1 = t - t_2$, $s_2 = t - t_1$ and $s = t$; 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. As an example, consider an access structure of type (2) where $m = 3$, $t_1 = 1$, $t_2 = 1$, $t_3 = 2$, and $t = 5$. Then the minimal subsets $\mathcal{V}$ are of types $(1, 1, 3)$ (namely, $|\mathcal{V} \cap \mathcal{C}_1| = 1$, $|\mathcal{V} \cap \mathcal{C}_2| = 1$, and $|\mathcal{V} \cap \mathcal{C}_3| = 3$), $(1, 2, 2)$, or $(2, 1, 2)$. This collection of minimal subsets 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 $s_1 = s_2 = 2, s_3 = 3$, and $s = 5$; but then that collection should have included also subsets of type (0,2,3), which it doesn't. Hence, there is no way of fitting that compartmented access structure with lower bounds within the framework with upper bounds.

Compartmented access structures with lower bounds, (2), are already known to be ideal. 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.

2.1 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). Let x_i, $1 \leq i \leq m$, be m distinct points in $\mathbb{F}$ and let $P_i(y)$ be a polynomial of degree $s_i - 1$ over $\mathbb{F}$. Define

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

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

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

These polynomials are orthogonal in the sense 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. *The secret is* $S = \sum_{i=1}^{m} \sum_{j=0}^{s_i - 1} a_{i,j}$.
2. *Each participant* $u_{i,j}$ *from compartment* $\mathcal{C}_i$ *will be identified by a unique public point* $(x_i, y_{i,j})$, *where* $y_{i,j} \ne 1$, *and his private share will be the value of* P *at that point.*
3. *In addition, we publish the value of* P *at* $k := \sum_{i=1}^{m} s_i - s$ *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 correspond to the participants are marked by empty circles along the three random parallel lines, $x = x_i$, $1 \le i \le 3$.

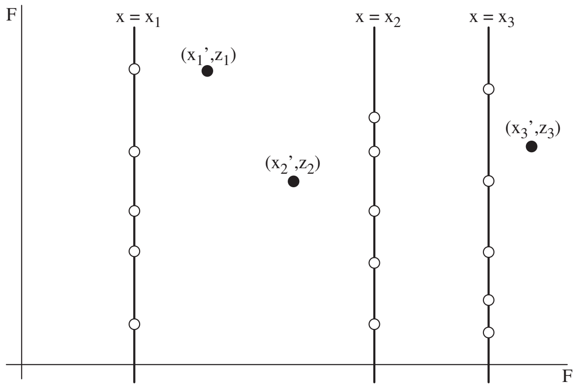

Fig. 1. Secret Sharing Scheme 1

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 each of the univariate polynomials $P_i(y)$, $1 \le i \le m$). 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 $x = x_i$, $1 \le i \le m$, 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, the resulting scheme is perfect.

Theorem 1. *With probability $1 - O(q^{-1})$, the ideal Secret Sharing Scheme 1 is a perfect scheme that realizes the compartmented access structure with upper bounds (3).*

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 authorized subsets may recover the secret while all non-authorized subsets may not learn a thing about the secret. If all subsets pass that test then the resulting scheme is perfectly secure. In the rare event (of probability $O(q^{-1})$) that one of the subsets did not pass the test, the dealer has only to try another selection.

2.2 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^*. Let us begin with a brief overview of what are dual access structures and recall the main result concerning duality that we need for the design of our scheme.

Karchmer and Wigderson [9] introduced monotone span programs as a linear algebraic model of computation for computing monotone functions. A monotone span program (MSP hereinafter) is a quintuple $\mathcal{M} = (\mathbb{F}, M, \mathcal{U}, \phi, \mathbf{e})$ where $\mathbb{F}$ is a field, M is a matrix of dimensions $a \times b$ over $\mathbb{F}$, $\mathcal{U} = \{u_1, \ldots, u_n\}$ is a finite set, ϕ is a surjective function from $\{1, \ldots, a\}$ to $\mathcal{U}$, and $\mathbf{e}$ is some target row vector from $\mathbb{F}^b$. The MSP $\mathcal{M}$ realizes the monotone access structure $\Gamma \subset 2^{\mathcal{U}}$ when $\mathcal{V} \in \Gamma$ if and only if $\mathbf{e}$ is spanned by the rows of the matrix M whose labels belong to $\mathcal{V}$. The size of $\mathcal{M}$ is a, the number of rows in M. Namely, in the terminology of secret sharing, the size of the MSP is the total number of shares that were distributed to all participants in $\mathcal{U}$. An MSP is ideal if $a = n$.

If Γ is a monotone access structure over $\mathcal{U}$, its dual is defined by $\Gamma^* = \{\mathcal{V} : \mathcal{V}^c \notin \Gamma\}$. It is easy to see that Γ^* is also monotone. In [7] it was shown that if $\mathcal{M} = (\mathbb{F}, M, \mathcal{U}, \phi, \mathbf{e})$ is an MSP that realizes a monotone access structure Γ, then there exists an MSP $\mathcal{M}^* = (\mathbb{F}, M^*, \mathcal{U}, \phi, \mathbf{e}^*)$ of the same size like $\mathcal{M}$ that realizes the dual access structure Γ^*. Hence, an access structure is ideal if and only if its dual is. An efficient construction of the MSP for the dual access structure was proposed in [6].

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 $1 \le i \le m$. Introducing the notations $n = |\mathcal{U}|$ and $n_i = |\mathcal{C}_i|$, $1 \le i \le m$, 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,

$$\Gamma^* = \{\mathcal{V} \subseteq \mathcal{U} : |\mathcal{V}| \geq r \text{ or } |\mathcal{V} \cap \mathcal{C}_i| \geq r_i \text{ for some } 1 \leq i \leq m\} \ , \tag{6}$$

where

$$r = n - t + 1 \text{ and } r_i = n_i - t_i + 1 \ , \quad 1 \leq i \leq m \ . \tag{7}$$

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 (6) satisfy

$$\sum_{i=1}^{m} r_i \geq r + m - 1 \ . \tag{8}$$

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 points in $\mathbb{F}$ and let $P_i(y)$ be a polynomial of degree $r_i - 1$ over $\mathbb{F}$, such that

$$P_1(0) = \cdots = P_m(0) \ . \tag{9}$$

Define

$$P(x, y) = \sum_{i=1}^{m} P_i(y) L_i(x) = \sum_{i=1}^{m} \sum_{j=0}^{r_i - 1} a_{i,j} \cdot y^j L_i(x) \ , \tag{10}$$

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 (9) implies that $a_{1,0} = \cdots = a_{m,0}$ and, consequently, that the number of unknown coefficients in the representation of $P(x, y)$ with respect to the basis $L_i(x)y^j$, $1 \leq i \leq m$, $0 \leq j \leq r_i - 1$, is $g = \sum_{i=1}^{m} r_i - (m - 1)$. Note that by (8), $g \geq r$.

Our secret sharing scheme for the realization of the dual access structure Γ^*, (6), is as follows:

Secret Sharing Scheme 2:

1. *The secret is* $S = a_{1,0} = \cdots = a_{m,0}$.
2. *Each participant* $u_{i,j}$ *from compartment* $\mathcal{C}_i$ *will be identified by a unique public point* $(x_i, y_{i,j})$*, where* $y_{i,j} \neq 0$*, and his private share will be the value of* P *at that point.*
3. *In addition, we publish the value of* P *at* $k = g - r$ *points* (x'_i, z_i)*, where* $x'_i \notin \{x_1, \ldots, x_m\}$*,* $1 \leq i \leq k$*.*

Theorem 2. *With probability* $1 - O(q^{-1})$*, the ideal Secret Sharing Scheme 2 is a perfect scheme that realizes the access structure (6).*

A scheme for compartmented access structures with lower bounds Using the results of Section 2.2 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, (6)-(7). Then we translate that ideal scheme (equivalently, MSP) into an ideal scheme (MSP) for $\Gamma = (\Gamma^*)^*$, using the explicit construction that is described in [6]. We omit further details.

3 Hierarchical Threshold Access Structures

3.1 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 $n - 2$,

$$P(x, y) = \sum_{0 \le i+j \le n-2} a_{i,j} x^i y^j \in \mathbb{F}[x, y] \ , \tag{11}$$

that satisfies

$$P(x_{i,j}, y_{i,j}) = f(x_{i,j}, y_{i,j}) \quad 1 \le i < j \le n \ . \tag{12}$$

That polynomial is given by

$$P(x, y) = \sum_{1 \le i < j \le n} f(x_{i,j}, y_{i,j}) L_{i,j}(x, y) \tag{13}$$

where

$$L_{i,j}(x, y) = \prod_{\substack{1 \le k \le n \\ k \ne i,j}} \frac{L_k(x, y)}{L_k(x_{i,j}, y_{i,j})} \ . \tag{14}$$

The bivariate Lagrange polynomials $L_{i,j}(x, y)$ are of degree $n-2$, and they form an orthogonal set in the sense that $L_{i,j}(x_{i,j}, y_{i,j}) = 1$ 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 (14) becomes zero). Note that the number of independent terms (monoms) in (11) agrees with the number of constraints in (12), 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 hereinafter. 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 (13)-(14). 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 $n-1$.

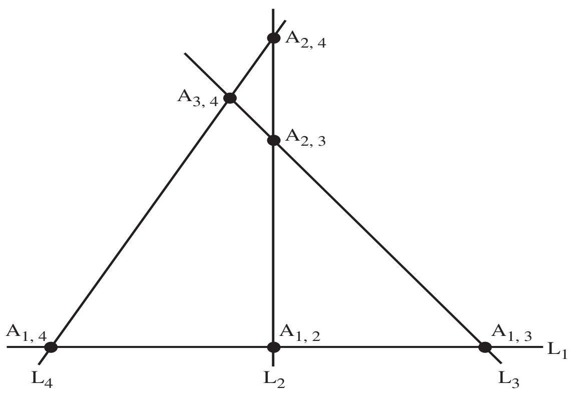

Fig. 2. Four lines in general position and the corresponding interpolation points

3.2 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;
- $P(x,y)=\sum_{0\le i+j\le n-1} a_{i,j}x^iy^j$ 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 $S := P(0,0)$. Since the underlying model is that of a monotone span program, it is clear that either the given data, D, uniquely determines the unknown, S, or the former does not reveal any information about the latter.

In order to answer that question, we define the *type* of a set $\mathcal{V}$ (Definition 1) and an order on such types (Definition 2).

Definition 1. *Let $\{L_i\}_{1\le i\le n}$ be n lines in general position in $\mathbb{F}^2$. A subset*

$$\mathcal{V} \subset \left(\bigcup_{i=1}^{n} L_i\right) \setminus \left(\bigcup_{1\le i<j\le n} L_i \cap L_j\right) \tag{15}$$

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

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

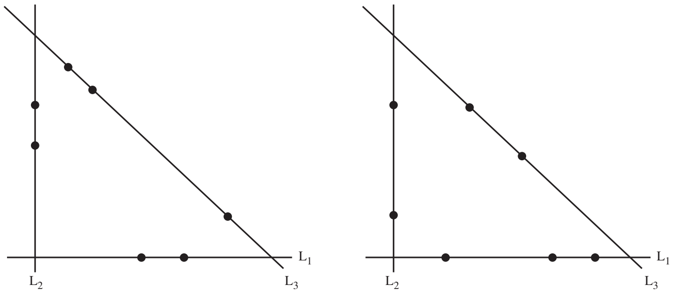

Fig. 3. Two point sets of the same type

Definition 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 $1 \le i \le n$, $\sum_{j=1}^{i} u_j \ge \sum_{j=1}^{i} v_j$.*

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

Definition 3. *Let $\{L_i\}_{1\le i\le n}$ be n lines in general position in $\mathbb{F}^2$, and let $\mathcal{V}$ be a set of points on those lines, (15). The vector set that corresponds to $\mathcal{V}$ is the set of vectors*

$$R_{\mathcal{V}} = \{\mathbf{r}_{(x,y),n} : (x,y) \in \mathcal{V}\} \tag{16}$$

where

$$\mathbf{r}_{(x,y),n} := (1, x, y, x^2, xy, y^2, \dots, x^{n-1}, x^{n-2}y, \dots, xy^{n-2}, y^{n-1}) \in \mathbb{F}^{n(n+1)/2} \tag{17}$$

Theorem 3. *Let $\{L_i\}_{1\le i\le n}$ be n lines in general position in $\mathbb{F}^2$, none of which goes through the origin $(0,0)$. Let $\mathcal{V}$ be a randomly selected set of points on those lines, (15), and let $\mathbf{v}$ be the type of that set. Then the following claim holds in probability $1 - O(q^{-1})$:*

1. *If $\mathbf{v} \succeq (1, 2, \dots, n)$ then $\mathbf{e}_1 \in Span\{R_{\mathcal{V}}\}$.*
2. *If $\mathbf{v} \not\succeq (1, 2, \dots, n)$ then $\mathbf{e}_1 \notin Span\{R_{\mathcal{V}}\}$.*

This theorem actually characterizes the sets of data points that allow the construction of a polynomial $P(x, y) \in \mathbb{F}_{n-1}[x, y]$. Given the values of the polynomial in the points of $\mathcal{V}$, $P|_{\mathcal{V}}$, it is possible (with almost certainty) to reconstruct the entire polynomial (and not just the free coefficient $P(0, 0)$ that corresponds to the vector $\mathbf{e}_1$) if the type of the data set, $\mathbf{v}$, dominates the vector $(1, 2, \dots, n)$. If, on the other hand, $\mathbf{v} \not\succeq (1, 2, \dots, n)$, then there is not enough data to reconstruct the polynomial, and this implies (with almost certainty) that we cannot learn any information about $P(0, 0)$.

3.3 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

$$\Gamma = \left\{ \mathcal{V} \subset \mathcal{U} : \left| \mathcal{V} \cap \left(\cup_{j=1}^{i} \mathcal{C}_j \right) \right| \ge k_i \text{ for all } 1 \le i \le m \right\} . \tag{18}$$

Those access structures were presented and studied in [13]. 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 $\mathcal{C}_i$, $1 \le i \le m$, 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 [13] did, but instead it adds one more dimension in order to achieve the same hierarchical effect.

Let $\{L_j\}_{1\le j\le n}$ be $n := k_m$ lines in general position in $\mathbb{F}^2$, none of which goes through the origin $(0, 0)$. Let

$$P(x, y) = \sum_{0 \le i+j \le n-1} a_{i,j} x^i y^j$$

be a random polynomial in $\mathbb{F}_{n-1}[x,y]$.

Secret Sharing Scheme 3:

1. *The secret is* $S = P(0,0)$.
2. *Each participant from level* $\mathcal{C}_i$ *will be identified by a unique public point on* $L_{k_i} \setminus \left(\bigcup_{\substack{1 \le j \le n \\ j \neq k_i}} L_j \right)$ *and his private share will be the value of* P *at that point.*
3. *In addition, we publish the value of* P *at:*
   - k_{i-1} *additional points on* L_{k_i}, $2 \le i \le m$; *and*
   - j *points on* L_j *for all* $j \in \{1, 2, \ldots, n\} \setminus \{k_i : 1 \le i \le m\}$.

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, $1 \le i \le 5$. 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 $k_2 = 4$).
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 4 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 4).
2. 1 point value on L_1 and 3 point values on L_3 (those points are marked by full squares in Figure 4).

Theorem 4. *With probability* $1 - O(q^{-1})$, *the ideal Secret Sharing Scheme 3 is a perfect scheme that realizes the hierarchical threshold access structure (18).*

4 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.

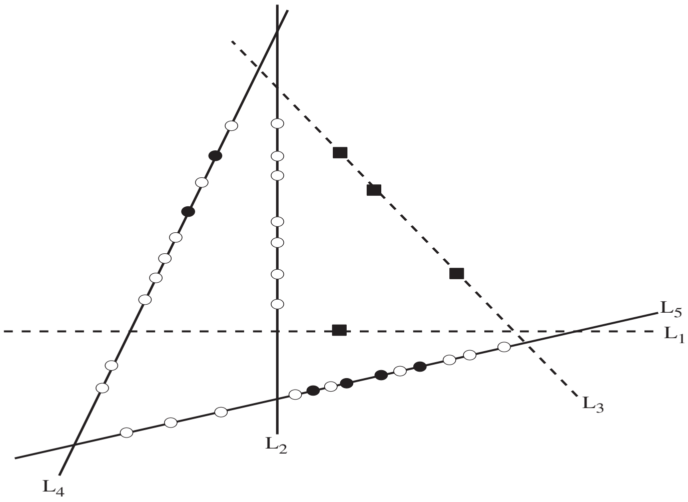

Fig. 4. Secret Sharing Scheme 3

References

1. A. Beimel, T. Tassa and E. Weinreb, Characterizing ideal weighted threshold secret sharing, *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 $\mathcal{R}^d$, *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. S. Fehr Efficient construction of the dual span program, *Manuscript*, May 1999.
7. A. Gál, *Combinatorial methods in Boolean function complexity*, Ph.D. thesis, University of Chicago, 1995.
8. J. Herranz and G. Sáez, New results on multipartite access structures, available at http://eprint.iacr.org/2006/048 (2006).
9. M. Karchmer and A. Wigderson, On span programs, in *The Proceedings of the 8th Structures in Complexity conference*, (1993), pp. 102-111.
10. C. Padró and G. Sáez, Secret sharing schemes with bipartite access structure, *IEEE Transactions on Information Theory*, 46 (2000), pp. 2596-2604.
11. A. Shamir, How to share a secret, *Communications of the ACM*, 22 (1979), pp. 612-613.
12. G.J. Simmons, How to (really) share a secret, *Advances in Cryptology - CRYPTO 88*, LNCS 403 (1990), pp. 390-448.
13. T. Tassa, Hierarchical threshold secret sharing, in *The Proceedings of the First Theory of Cryptography Conference, TCC 2004*, February 2004, MIT, Cambridge, pp. 473-490. (To appear in Journal of Cryptology).