New Monotone Span Programs from Old

Ventzislav Nikov[1] and Svetla Nikova[2]

[1] Department of Mathematics and Computing Science,
Eindhoven University of Technology
P.O. Box 513, 5600 MB, Eindhoven, the Netherlands
v.nikov@tue.nl
[2] Department Electrical Engineering, ESAT/COSIC,
Katholieke Universiteit Leuven, Kasteelpark Arenberg 10,
B-3001 Heverlee-Leuven, Belgium
svetla.nikova@esat.kuleuven.ac.be

Abstract. In this paper we provide several known and one new constructions of new linear secret sharing schemes (LSSS) from existing ones. This constructions are well-suited for didactic purposes, which is a main goal of this paper. It is well known that LSSS are in one-to-one correspondence with monotone span programs (MSPs). MSPs introduced by Karchmer and Wigderson, can be viewed as a linear algebra model for computing a monotone function (access structure). Thus the focus is in obtaining a MSP computing the new access structure starting from the MSPs that compute the existing ones, in the way that the size of the MSP after the transformation is well defined. Next we define certain new operations on access structures and prove certain related properties.

1 Introduction

A *secret sharing scheme* (SSS) is a system designed to share a secret among a group of participants in such a way that the secret can be reconstruct only by specified groups of participants. It was pointed out by Brickell [4] how the linear algebra view leads naturally to a wider class of secret sharing schemes. This have later been generalized to all possible so-called monotone access structures by Karchmer and Wigdreson [13] based on a linear algebra model of computation called *monotone span program* (MSP). An SSS is linear if the dealer and the participants use only linear operations to compute the shares and the secret. Each *linear SSS* (LSSS) can be viewed as derived from a monotone span program computing its access structure. On the other hand, each monotone span program gives rise to an LSSS. Hence, one can identify an LSSS with its underlying monotone span program. Such an MSP always exists, because MSPs can compute any monotone access structure. An important parameter of the MSP is its size, which is also the size of the corresponding LSSS. We will speak of the MSP *underlying* an LSSS and of the LSSS *induced* by an MSP.

A wide range of general approaches for designing secret sharing schemes are known, e.g., Shamir [21], Benaloh-Leicher [2], Ito *et al.* [10], Bertilsson and

Ingemarsson [3], Brickell [4], Massey [14], Blakley and Kabatyanskii [1], Simonis and Ashikhmin [22] and van Dijk [8]. All these techniques result in LSSSs and therefore are equivalent to MSP based secret sharing, but only few of them are suitable for building Verifiable SSS (VSS) and none of them for Multi-Party Computation (MPC).

It turns out to be convenient to describe the protocols in terms of MSPs. The results of Cramer *et al.* [6, 7] and Nikov *et al.* [16–19] show that distributed commitments (DC), verifiable secret sharing (VSS), proactive VSS, and multi-party computation (MPC) can be efficiently based on any LSSS induced by an MSP, provided that the access structure computed by the MSP allows DC, VSS, proactive VSS or MPC.

A general question for multi-parti protocols is to find a "good measure", so that "often" the protocols are polynomially efficient in the number of players. Let complexity mean the total number of rounds, bits exchanged, local computations done, etc. The best measure known for a protocol efficiency is the Monotone Span Program Complexity [6], which coincides with complexity in terms of linear secret sharing schemes over finite fields. On the other hand the MSP complexity is its size.

Shortly before the MSPs were introduced, Martin in [15] presented methods for producing new access structures and new LSSSs from existing ones. He uses general linear matrix presentation of an access structure, introduced by Brickell and Davenport in [5], which allows to distinguish between complete and incomplete access structures. While this approach provably extends the class of access structures that can be handled, from a practical point of view MSPs represent the most powerful known general technique for constructing DC, SSS, VSS and MPC protocols. That is why, in this paper we focus on MSP based approach for building LSSS.

In this paper we provide several known and one new constructions of new LSSSs from existing ones. The focus is in obtaining the MSP computing the new access structure starting from the MSPs that compute the existing ones. As a result the size of the MSP after the transformation is well defined. Next we define certain new operations on access structures and prove related properties.

The paper is organized as follows. In the next Section 2 we give some preliminaries. In Section 3 constructions for building new MSPs mfrom old are presented. In the last Section 4 of the paper we define certain new operations on access structures and prove certain properties, which are of independent interest.

2 Preliminaries

Let us denote the players in a Secret Sharing Scheme by $P_i,\ 1 \leq i \leq n$, the set of all players by $\mathcal{P} = \{P_1, \dots, P_n\}$ and the set of all subsets of $\mathcal{P}$ (i.e., the power set of $\mathcal{P}$) by $P(\mathcal{P})$. We call the groups who are allowed to reconstruct the secret *qualified* and the groups who should not be able to obtain any information about the secret *forbidden*. The set of qualified groups is denoted by Γ ($\Gamma \subseteq P(\mathcal{P})$) and the set of forbidden groups by Δ ($\Delta \subseteq P(\mathcal{P})$). The set Γ is called *monotone* *increasing* if for any set A in Γ any set containing A is also in Γ. Similarly, Δ is called *monotone decreasing*, if for each set B in Δ each subset of B is also in Δ. A monotone increasing set Γ can be efficiently described by the set Γ^- consisting of the *minimal elements* in Γ, i.e., the elements in Γ for which no proper subset is also in Γ. Similarly, the set Δ^+ consists of the *maximal elements* (sets) in Δ, i.e., the elements in Δ for which no proper superset is also in Δ. The tuple (Γ, Δ) is called an *access structure* if $\Gamma \cap \Delta = \emptyset$. It is obvious that (Γ^-, Δ^+) generates (Γ, Δ). If the union of Γ and Δ is equal to $P(\mathcal{P})$ (so Γ is equal to Δ^c, the complement of Δ), then we say that the access structure (Γ, Δ) is *complete* and we denote it just by Γ. Throughout the paper we will consider *connected access structures*, i.e., the access structures in which every player is in at least one minimal set. Also we will consider complete general monotone access structure Γ, which describes subsets of participants that are qualified to recover the secret $s \in \mathbb{F}$ ($\mathbb{F}$ - finite field) and therefore set $\Delta = \Gamma^c$.

Definition 1. *The* dual access structure $\Gamma^\perp$ *of an access structure* Γ*, defined on* $\mathcal{P}$*, is the collection of sets* $A \subseteq \mathcal{P}$ *such that* $\mathcal{P} \setminus A = A^c \notin \Gamma$ *(i.e.* $A^c \in \Delta$*).*

An $m \times d$ matrix M over a field $\mathbb{F}$ defines a map from $\mathbb{F}^d$ to $\mathbb{F}^m$ by taking a vector $\boldsymbol{v} \in \mathbb{F}^d$ to the vector $M\boldsymbol{v} \in \mathbb{F}^m$. Associated with $m \times d$ matrix M (or a linear map) are two natural subspaces, one in $\mathbb{F}^m$ and the other in $\mathbb{F}^d$. They are defined as follows. The *kernel* of M (denoted by $\ker(M)$) is the set of vectors $\boldsymbol{u} \in \mathbb{F}^d$, such that $M\boldsymbol{u} = \mathbf{0}$. The *image* of M (denoted by $\mathrm{im}(M)$) is the set of vectors $\boldsymbol{v} \in \mathbb{F}^m$ such that $\boldsymbol{v} = M\boldsymbol{u}$ for some $\boldsymbol{u} \in \mathbb{F}^d$.

For an arbitrary matrix M over $\mathbb{F}$, with m rows and for an arbitrary non-empty subset A of $\{1, \ldots, m\}$, let M_A denote the restriction of M to the rows i with $i \in A$. If $A = \{i\}$ we write M_i. Similarly for any vector $\mathbf{k} \in \mathbb{F}^m$ an arbitrary non-empty subset A of $\{1, \ldots, m\}$, let $\mathbf{k}_A \in \mathbb{F}^{|A|}$ denote the restriction of $\mathbf{k}$ to the coordinates $i \in A$. If $A = \{i\}$ we write $\mathbf{k}_i$. Let $M_{(i)} \in \mathbb{F}^m$, for $i = 1, \ldots, d$, denote the i-th column in $m \times d$ matrix M. Sometimes we will denote the matrix M by $[M_{(1)}, \ldots, M_{(d)}]$ too. In the sequel $\mathbf{v^i}$ will denote a vector but $\mathbf{v}_i$ stands for the i-th coordinate of vector $\mathbf{v}$.

With the standard inner product $\langle \mathbf{v}, \mathbf{w} \rangle = \sum \mathbf{v}_i \mathbf{w}_i$, we write $\mathbf{v} \perp \mathbf{w}$, when $\langle \mathbf{v}, \mathbf{w} \rangle = 0$. For an $\mathbb{F}$-linear subspace $\mathcal{V}$ of $\mathbb{F}^d$, $\mathcal{V}^\perp$ denotes the collection of elements of $\mathbb{F}^d$, that are orthogonal to all of $\mathcal{V}$ (the orthogonal complement). It is again an $\mathbb{F}$-linear subspace. For all subspaces $\mathcal{V}$ of $\mathbb{F}^d$ we have $\mathcal{V} = (\mathcal{V}^\perp)^\perp$. Other standard relations are $(\mathrm{im}(M^T))^\perp = \ker(M)$, and $\mathrm{im}(M^T) = (\ker(M))^\perp$, as well as $\langle \mathbf{v}, M^T\mathbf{w} \rangle = \langle M\mathbf{v}, \mathbf{w} \rangle$.

Let $\mathbf{v} = (\mathbf{v}_1, \ldots, \mathbf{v}_{d_1}) \in \mathbb{F}^{d_1}$ and $\mathbf{w} = (\mathbf{w}_1, \ldots, \mathbf{w}_{d_2}) \in \mathbb{F}^{d_2}$ be two vectors. The *tensor vector product* $\mathbf{v} \otimes \mathbf{w}$ is defined as a vector in $\mathbb{F}^{d_1 d_2}$ that the j-coordinate in $\mathbf{v}$ is replaced by $\mathbf{v}_j\mathbf{w}$, i.e., $\mathbf{v} \otimes \mathbf{w} = (\mathbf{v}_1\mathbf{w}, \ldots, \mathbf{v}_{d_1}\mathbf{w}) \in \mathbb{F}^{d_1 d_2}$. Let M be an $m_1 \times d_1$ matrix, and N be an $m_2 \times d_2$ matrix. The Kronecker (or tensor, direct, outer) product $M \otimes N$ is defined as an $m_1 m_2 \times d_1 d_2$ matrix with rows $M_i \otimes N_j$ for $1 \le i \le m_1$ and $1 \le j \le m_2$. Next we will give some properties of the tensor product.

Lemma 1. *Let $\mathbf{x}, \mathbf{a} \in \mathbb{F}^{m_1}$, $\mathbf{y}, \mathbf{b} \in \mathbb{F}^{m_2}$, $\mathbf{c} \in \mathbb{F}^{d_1}$ and $\mathbf{d} \in \mathbb{F}^{d_2}$ be arbitrary vectors. Let A be an $m_1 \times d_1$ matrix, B be an $m_2 \times d_2$ matrix, C be an $d_1 \times n_1$ matrix and D be an $d_2 \times n_2$ matrix. Then the following equations hold*

$$\begin{aligned}
\langle \mathbf{x} \otimes \mathbf{y}, \mathbf{a} \otimes \mathbf{b} \rangle &= \langle \mathbf{x}, \mathbf{a} \rangle \langle \mathbf{y}, \mathbf{b} \rangle \\
(A \otimes \mathbf{a})\mathbf{c} &= (A\mathbf{c}) \otimes \mathbf{a} \\
(A \otimes B)^T &= A^T \otimes B^T \\
(A \otimes B)(\mathbf{c} \otimes \mathbf{d}) &= (A\mathbf{c}) \otimes (B\mathbf{d}) \\
(A\ C) \otimes (B\ D) &= (A \otimes B)(C \otimes D).
\end{aligned}$$

Now we give a formal definition of a Monotone Span Program.

Definition 2. *[13] A* Monotone Span Program *(MSP) $\mathcal{M}$ is a quadruple $(\mathbb{F}, M, \boldsymbol{\varepsilon}, \psi)$, where $\mathbb{F}$ is a finite field, M is a matrix (with m rows and $d \leq m$ columns) over $\mathbb{F}$, $\psi : \{1, \ldots, m\} \to \{1, \ldots, n\}$ is a surjective function and $\boldsymbol{\varepsilon} = (1, 0, \ldots, 0)^T \in \mathbb{F}^d$ is called* target vector. *The size of $\mathcal{M}$ is the number m of rows and is denoted as size$(\mathcal{M})$.*

As ψ labels each row with a number i from $[1, \ldots, m]$ that corresponds to player $P_{\psi(i)}$, we can think of each player as being the "owner" of one or more rows. Also consider a "function" φ from $[P_1, \ldots, P_n]$ to $[1, \ldots, m]$ which gives for every player P_i the set of rows owned by him (denoted by $\varphi(P_i)$). In some sense φ is "inverse" of ψ. For any set of players $B \subseteq \mathcal{P}$ consider the matrix consisting of rows these players own in M, i.e. $M_{\varphi(B)}$. As is common, we shall shorten the notation $M_{\varphi(B)}$ to just M_B. The reader should stay aware of the difference between M_B for $B \subseteq \mathcal{P}$ and for $B \subseteq \{1, \ldots, m\}$.

An MSP is said *to compute* a (complete) access structure Γ when $\boldsymbol{\varepsilon} \in \mathrm{im}(M_A^T)$ if and only if A is a member of Γ. We say that A is *accepted* by $\mathcal{M}$ if and only if $A \in \Gamma$, otherwise we say A is *rejected* by $\mathcal{M}$. In other words, the players in A can reconstruct the secret precisely if the rows they own contain in their linear span the target vector of $\mathcal{M}$, and otherwise they get no information about the secret. Hence when a set A is accepted by $\mathcal{M}$ there exists a so-called *recombination vector* (column) $\boldsymbol{\lambda}$ such that $M_A^T \boldsymbol{\lambda} = \boldsymbol{\varepsilon}$. Notice that the vector $\boldsymbol{\varepsilon} \notin \mathrm{im}(M_B^T)$ if and only if there exists a vector $\boldsymbol{k} \in \mathbb{F}^d$ such that $M_B \boldsymbol{k} = \mathbf{0}$ and $\boldsymbol{k}_1 = 1$.

Let the dealer of the scheme shares a secret s, so in the sharing phase he chooses a random vector $\boldsymbol{\rho}$ and gives to player P_i $(1 \leq i \leq n)$ a share $M_i(s, \boldsymbol{\rho})^T$. In the reconstruction phase using the recombination vector $\boldsymbol{\lambda}$ any qualified group can reconstruct the secret as follows: $\langle \boldsymbol{\lambda}, M_A(s, \boldsymbol{\rho})^T \rangle = \langle M_A^T \boldsymbol{\lambda}, (s, \boldsymbol{\rho})^T \rangle = \langle \boldsymbol{\varepsilon}, (s, \boldsymbol{\rho})^T \rangle = s$. Regarding privacy, let B be forbidden group of players, and consider the joint information held by the players in B, i.e. $M_B \mathbf{x} = \mathbf{s}_B$, where $\mathbf{x} = (s, \boldsymbol{\rho})^T$. Let $s' \in \mathbb{F}$ be arbitrary, and let $\mathbf{k}$ be such that $M_B \mathbf{k} = \mathbf{0}$ and $\mathbf{k}_1 = 1$. Then $\mathbf{s}_B = M_B(\mathbf{x} + \mathbf{k}(s' - s))$ where the first coordinate of argument $\mathbf{x} + \mathbf{k}(s' - s)$ is now equal to s'. This means that, from the point of view of the players in B, their shares $\mathbf{s}_B$ are equally likely consistent with any secret $s' \in \mathbb{F}$.

3 Compositions of MSPs

In this section we shall consider the following problem:
Given some access structures, the MSPs computing them and a new access structure obtained from the given ones after certain operations, how can we construct an MSP that computes the new access structure?

3.1 Restrictions and Contractions

In this section we study the structure of monotone span programs which are produced within an existing secret sharing scheme, using certain constructions.

Definition 3. *[15] Let Γ be a monotone access structure defined on set $\mathcal{P}$ and let $Q \subseteq \mathcal{P}$. The* restriction *of Γ at Q, $\Gamma_{|Q}$, and the* contraction *of Γ at Q, $\Gamma_{.Q}$, are monotone access structures defined on $\mathcal{P} \setminus Q$ such that for each $A \subseteq \mathcal{P} \setminus Q$,*

$$A \in \Gamma_{|Q} \iff A \in \Gamma, \qquad A \in \Gamma_{.Q} \iff A \cup Q \in \Gamma.$$

Thus the members of $(\Gamma_{|Q})^-$ are precisely the members of Γ^- that do not contain any member of Q. If $Q \in \Gamma$ then the members of $(\Gamma_{.Q})^-$ are all the single participants of $\mathcal{P} \setminus Q$. If $Q \notin \Gamma$ then $(\Gamma_{.Q})^-$ comprises of all the minimal non empty sets of the form $A \cap (\mathcal{P} \setminus Q)$, where $A \in \Gamma^-$.

Theorem 1. *[15] Let $\mathcal{M}$ be an MSP computing Γ and $Q \subset \mathcal{P}$. Then there exists an MSP $\mathcal{M}_{|Q}$, computing the restriction of Γ at Q (i.e., $\Gamma_{|Q}$). The size of $\mathcal{M}_{|Q}$ is equal to $|\varphi(\mathcal{P} \setminus Q)|$ (smaller than the size of $\mathcal{M}$).*

Proof. Let $Q \subset \mathcal{P}$ and $A \subseteq Q^c$. Define $\Delta = \Gamma^c$, $\Delta_{|Q} = (\Gamma_{|Q})^c$ and take $\overline{M} = M_{|Q}$. Form the matrix $\overline{M}$ by removing the rows in M, which correspond to the members of Q, i.e., we set $\overline{M} = M_{Q^c}$. The functions ψ and φ are not changed. The proof that the MSP $\mathcal{M}_{|Q}$ with matrix $\overline{M}$ computes the access structure $\Gamma_{|Q}$ is now straightforward and left to the reader. □

Now we will consider contractions of a monotone access structure only in the non-trivial case, i.e., when $Q \notin \Gamma$.

Theorem 2. *[15] Let $\mathcal{M}$ be an MSP computing Γ and let $Q \subset \mathcal{P}$, $Q \notin \Gamma$. Then there exists an MSP $\mathcal{M}_{.Q}$, which computes the contraction of Γ at Q (i.e., $\Gamma_{.Q}$), with size equal to the size of $\mathcal{M}$.*

Proof. Now we will consider contractions of a monotone access structure in the non-trivial case, i.e., when $Q \notin \Gamma$. Let $Q \subset \mathcal{P}$, $Q \notin \Gamma$ and $A \subseteq Q^c$. Define $\Delta = \Gamma^c$, $\Delta_{.Q} = (\Gamma_{.Q})^c$ and take $\overline{M} = M_{.Q}$. The new matrix $\overline{M}$ is the same as M, but the rows which belong to the members of Q, become rows of all the members of Q^c, i.e., $\overline{\varphi}(P_i) = \varphi(P_i) \cup \varphi(Q)$, for $P_i \in Q^c$. Observe now that the MSP $\mathcal{M}_{.Q}$ with matrix $\overline{M}$ computes $\Gamma_{.Q}$. Indeed from ($A \in \Gamma_{.Q} \iff A \cup Q \in \Gamma$), it follows that ($B \in \Delta_{.Q} \iff B \cup Q \in \Delta$).

We will leave the proof that MSP $\mathcal{M}_{.Q}$ with matrix $\overline{M}$ computes the access structure $\Gamma_{.Q}$ again to the reader. □

3.2 Insertions

In this section we investigate a useful general construction, introduced by Martin [15], which allows to begin with "small" schemes with a few participants and build them up to "large" schemes with higher number of participants.

Definition 4. *[15] Let Γ_1 and Γ_2 be two monotone access structures defined on participant sets $\mathcal{P}_1$ and $\mathcal{P}_2$ respectively, and let $P_z \in \mathcal{P}_1$. Define the* insertion *of Γ_2 at player P_z in Γ_1, $\Gamma_1(P_z \to \Gamma_2)$, to be the monotone access structure defined on the set $(\mathcal{P}_1 \setminus P_z) \cup \mathcal{P}_2$ such that for $A \subseteq (\mathcal{P}_1 \setminus P_z) \cup \mathcal{P}_2$ we have*

$$A \in \Gamma_1(P_z \to \Gamma_2) \iff \begin{cases} A \cap \mathcal{P}_1 \in \Gamma_1, \quad or \\ ((A \cap \mathcal{P}_1) \cup P_z \in \Gamma_1 \quad and \quad A \cap \mathcal{P}_2 \in \Gamma_2) . \end{cases}$$

In other words $\Gamma_1(P_z \to \Gamma_2)$ is the monotone access structure Γ_1 with participant P_z "replaced" by the sets of Γ_2. Notice that this insertion is an operation *on a monotone increasing set*. Later we will define insertion on monotone decreasing set.

Theorem 3. *Let Γ_1 and Γ_2 be monotone access structures defined on the set of participants $\mathcal{P}_1$ and $\mathcal{P}_2$ and with MSPs $\mathcal{M}_1$ and $\mathcal{M}_2$ respectively, and let $P_z \in \mathcal{P}_1$. Let the size of $\mathcal{M}_1$ be m_1 and the size of $\mathcal{M}_2$ be m_2. Then there exists an MSP $\mathcal{M}$ computing the access structure $\Gamma_1(P_z \to \Gamma_2)$ of size equal to $m_1 + (m_2 - 1)|\varphi_1(P_z)|$.*

Proof. We will give here first the construction of MSP $\mathcal{M}$, then we prove that it computes $\Gamma_1(P_z \to \Gamma_2)$. Let $M^{(1)}$ and $M^{(2)}$ be corresponding matrices to MSPs $\mathcal{M}_1$ and $\mathcal{M}_2$. Let the matrix $M^{(2)} = (\mathbf{u}\ \widetilde{M}^{(2)})$, where $\mathbf{u}$ is its first column. Let $\overline{M}^{(1)} = M^{(1)}_{\mathcal{P}_1 \setminus \{P_z\}}$, i.e., all rows in $M^{(1)}$ except those owned by P_z and assume that the rows of P_z are the first rows in $M^{(1)}$. Consider the rows owned by P_z, i.e., $M^{(1)}_{P_z}$. Denote $q = |\varphi_1(P_z)|$ and let $\mathbf{u^i} = (0, \ldots, 0, 1, 0, \ldots, 0)^T \in \mathbb{F}^q$ be the column vector with 1 in the i-th position. Let matrix $\widetilde{M}$, consists of diagonal blocks sub-matrices $\mathbf{u^i} \otimes \widetilde{M}^{(2)}$ for $i = 1, \ldots, q$, i.e., $\widetilde{M} = \begin{pmatrix} \widetilde{M}^{(2)} & \cdot & 0 & \cdot & 0 \\ 0 & \cdot & \widetilde{M}^{(2)} & \cdot & 0 \\ 0 & \cdot & 0 & \cdot & \widetilde{M}^{(2)} \end{pmatrix}$ and denote by $\widehat{M}$ the matrix $M^{(1)}_{P_z} \otimes \mathbf{u}$. Then the MSP $M = \begin{pmatrix} \widehat{M} & \widetilde{M} \\ \overline{M}^{(1)} & 0 \end{pmatrix}$ computes $\Gamma_1(P_z \to \Gamma_2)$.

More specific define $\Gamma = \Gamma_1(P_z \to \Gamma_2)$, $\Delta = \Gamma^c$, and set $\Delta_1 = (\Gamma_1)^c$ and $\Delta_2 = (\Gamma_2)^c$. Let $\mathcal{M}_1$ be an MSP with $m_1 \times d_1$ matrix $M^{(1)}$, and functions ψ_1 and φ_1. Similarly let $\mathcal{M}_2$ be an MSP with $m_2 \times d_2$ matrix $M^{(2)}$, and functions ψ_2 and φ_2. Let $\overline{M}^{(1)} = M^{(1)}_{\mathcal{P}_1 \setminus \{P_z\}}$, i.e., all rows in $M^{(1)}$ except those owned by P_z and assume that the rows of P_z are the first rows in $M^{(1)}$. Consider the rows owned by P_z, i.e., $M^{(1)}_{P_z}$. Denote the columns in the matrix $M^{(1)}_{P_z}$ by $\mathbf{z^k}$ for $k = 1, \ldots, d_1$. Thus, this matrix is denoted by $[\mathbf{z^1}, \ldots, \mathbf{z^{d_1}}]$. Finally, let by $M^{(2)}_{(\ell)}$

denote the columns in $M^{(2)}$ for $\ell = 1, \dots, d_2$, i.e., $M^{(2)} = [M^{(2)}_{(1)}, \dots, M^{(2)}_{(d_2)}]$ and take $\widetilde{M}^{(2)} = [M^{(2)}_{(2)}, \dots, M^{(2)}_{(d_2)}]$ the matrix $M^{(2)}$ without its first column. Let $\mathbf{u^i} = (0, \dots, 0, 1, 0, \dots, 0)^T \in \mathbb{F}^{|\varphi_1(P_z)|}$ be the column vector with 1 in the i-th position.

Now we construct the MSP $\mathcal{M}$ for $\Gamma_1(P_z \to \Gamma_2)$ by its matrix M in the following way:
A) Take $M^{(1)}$ and replace every column $\mathbf{z^k}$ with $\mathbf{z^k} \otimes M^{(2)}_{(1)}$, for $k = 1, \dots, d_1$, i.e., $[\mathbf{z^1}, \dots, \mathbf{z^{d_1}}] \otimes M^{(2)}_{(1)}$. The rest of the matrix (i.e., $\overline{M}^{(1)}$) is not changed in this step. Thus this matrix now has size $(m_1 + (m_2 - 1)|\varphi_1(z)|) \times d_1$.
B) For the first $m_2|\varphi_1(P_z)|$ rows, add additional columns $\mathbf{u^i} \otimes M^{(2)}_{(\ell)}$, for $\ell = 2, \dots, d_2$, (i.e., $\mathbf{u^i} \otimes [M^{(2)}_{(2)}, \dots, M^{(2)}_{(d_2)}] = \mathbf{u_i} \otimes \widetilde{M}^{(2)}$) and repeat this operation for $i = 1, \dots, |\varphi_1(P_z)|$. For the remaining $m_1 - |\varphi_1(P_z)|$ rows add additional zero columns. The matrix now has size $(m_1 + (m_2 - 1)|\varphi_1(P_z)|) \times (d_1 + (d_2 - 1)|\varphi_1(P_z)|)$.

The obtained matrix M consists of four sub-matrices and has the form $M = \begin{pmatrix} \widehat{M} & \widetilde{M} \\ \overline{M}^{(1)} & 0 \end{pmatrix}$, where the sub-matrices are as follows. The first one in the upper left corner is $[\mathbf{z^1}, \dots, \mathbf{z^{d_1}}] \otimes M^{(2)}_{(1)}$ - will be denoted by $\widehat{M}$; the second one, in the upper right corner denoted by $\widetilde{M}$, consists of diagonal blocks sub-matrices $\mathbf{u^i} \otimes \widetilde{M}^{(2)}$, i.e., $\widetilde{M} = \begin{pmatrix} \widetilde{M}^{(2)} \cdot & 0 & \cdot & 0 \\ 0 & \cdot\, \widetilde{M}^{(2)} \cdot & & 0 \\ 0 & \cdot & 0 & \cdot\, \widetilde{M}^{(2)} \end{pmatrix}$. The third one, in the lower left corner is $\overline{M}^{(1)}$; and the last one in the lower right corner is the null matrix.

Now the rows owned by participant $P_i \in \mathcal{P}_1 \setminus \{P_z\}$ correspond to his previous rows in $\overline{M}^{(1)}$. But the rows owned by participant $P_j \in \mathcal{P}_2$ are repeated $|\varphi_1(P_z)|$ times, because $M^{(2)}$ is multiplied so many times.

We will prove that this MSP $\mathcal{M}$ computes access structure $\Gamma_1(P_z \to \Gamma_2)$. Rewriting Definition 4 in terms of Δ instead of Γ we have:

$$B \in \Delta \iff \left(B \cap \mathcal{P}_1 \in \Delta_1 \ \text{ and } \ \begin{cases} (B \cap \mathcal{P}_1) \cup \{P_z\} \in \Delta_1, & \text{or} \\ B \cap \mathcal{P}_2 \in \Delta_2. \end{cases} \right).$$

This can be rewritten as

$$B \in \Delta \iff \begin{cases} (B \cap \mathcal{P}_1) \cup \{P_z\} \in \Delta_1 \ \text{ or,} \\ (B \cap \mathcal{P}_1 \in \Delta_1, \ \text{ and } \ B \cap \mathcal{P}_2 \in \Delta_2). \end{cases}$$

The latest means that, in order to prove that MSP $\mathcal{M}$ computes access structure $\Gamma_1(P_z \to \Gamma_2)$ we need to prove the following three cases:
Case 1. If $(B \cap \mathcal{P}_1) \cup \{P_z\} \in \Delta_1$ we will prove that $B \in \Delta$ holds. Let $(B \cap \mathcal{P}_1) \cup \{P_z\} \in \Delta_1$. There exists a column vector $(1, \widehat{\mathbf{k}}) \in \mathbb{F}^{d_1}$ such that $M^{(1)}_{(B \cap \mathcal{P}_1) \cup \{P_z\}}$ $(1, \widehat{\mathbf{k}}) = \mathbf{0}$. Define a new column vector $(1, \mathbf{k}) \in \mathbb{F}^{d_1 + d_2 - 1}$ by $(1, \mathbf{k}) = (1, \widehat{\mathbf{k}}, \mathbf{0})$.

We have $M_B(1,\mathbf{k}) = \mathbf{0}$, since

$$
\begin{aligned}
M_{B\cap\mathcal{P}_1}(1,\mathbf{k}) &= \overline{M}^{(1)}_{B\cap\mathcal{P}_1}(1,\widehat{\mathbf{k}}) = \mathbf{0} \ \text{ and,}\\
M_{B\cap\mathcal{P}_2}(1,\mathbf{k}) &= \widehat{M}_{B\cap\mathcal{P}_2}(1,\widehat{\mathbf{k}}) = [[\mathbf{z^1},\dots,\mathbf{z^{d_1}}]\otimes M^{(2)}_{(1)}]_{B\cap\mathcal{P}_2}(1,\widehat{\mathbf{k}})\\
&= [[\mathbf{z^1},\dots,\mathbf{z^{d_1}}](1,\widehat{\mathbf{k}})]\otimes[M^{(2)}_{(1)}]_{B\cap\mathcal{P}_2} = \mathbf{0}\otimes[M^{(2)}_{(1)}]_{B\cap\mathcal{P}_2} = \mathbf{0}.
\end{aligned}
$$

Here $[M^{(2)}_{(1)}]_{B\cap\mathcal{P}_2}$ denotes the first column in matrix $M^{(2)}$ restricted to the rows owned by $B\cap\mathcal{P}_2$. Hence we proved that $(1,\mathbf{k})\in\ker(M_B)$ and thus it follows that $B\in\Delta$.

Case 2. If $B\cap\mathcal{P}_1\in\Delta_1$ and $B\cap\mathcal{P}_2\in\Delta_2$ we will prove that $B\in\Delta$ holds. Let $q=|\varphi_1(P_z)|$ denote the number of rows that player P_z possesses in $M^{(1)}$. Let $B\cap\mathcal{P}_1\in\Delta_1$ and $B\cap\mathcal{P}_2\in\Delta_2$. Then there exist column vectors $(1,\widehat{\mathbf{k}})\in\mathbb{F}^{d_1}$ and $(1,\widetilde{\mathbf{k}})\in\mathbb{F}^{d_2}$ such that $M^{(1)}_{B\cap\mathcal{P}_1}(1,\widehat{\mathbf{k}})=\mathbf{0}$ and $M^{(2)}_{B\cap\mathbf{P}_2}(1,\widetilde{\mathbf{k}})=\mathbf{0}$. Notice that now $(B\cap\mathcal{P}_1)\cup\{P_z\}\notin\Delta_1$ implies that $M^{(1)}_{P_z}(1,\widehat{\mathbf{k}})=[\mathbf{z^1},\dots,\mathbf{z^{d_1}}](1,\widehat{\mathbf{k}})=\boldsymbol{\alpha}\neq\mathbf{0}$, where $\boldsymbol{\alpha}\in\mathbb{F}^{|\varphi_1(P_z)|}=\mathbb{F}^q$. Construct a new column vector $(1,\mathbf{k})\in\mathbb{F}^{d_1+(d_2-1)|\varphi_1(P_z)|}$ by taking $(1,\mathbf{k})=(1,\widehat{\mathbf{k}},\boldsymbol{\alpha}_1\widetilde{\mathbf{k}},\dots,\boldsymbol{\alpha}_q\widetilde{\mathbf{k}})=(1,\widehat{\mathbf{k}},\boldsymbol{\alpha}\otimes\widetilde{\mathbf{k}})$. Now we check that $M_B(1,\mathbf{k})=\mathbf{0}$. Indeed

$$
\begin{aligned}
M_{B\cap\mathcal{P}_1}(1,\mathbf{k}) &= \overline{M}^{(1)}_{B\cap\mathcal{P}_1}(1,\widehat{\mathbf{k}}) = \mathbf{0} \ \text{ and,}\\
M_{B\cap\mathcal{P}_2}(1,\mathbf{k}) &= \widehat{M}_{B\cap\mathcal{P}_2}(1,\widehat{\mathbf{k}}) + \widetilde{M}_{B\cap\mathcal{P}_2}(\boldsymbol{\alpha}\otimes\widetilde{\mathbf{k}})\\
&= [\mathbf{z^1}\otimes M^{(2)}_{(1)},\dots,\mathbf{z^{d_1}}\otimes M^{(2)}_{(1)}]_{B\cap\mathcal{P}_2}(1,\widehat{\mathbf{k}})\\
&+ [\mathbf{u^i}\otimes M^{(2)}_{(2)},\dots,\mathbf{u^i}\otimes M^{(2)}_{(d_2)}]_{B\cap\mathcal{P}_2}(\boldsymbol{\alpha}_i\widetilde{\mathbf{k}})\\
&= [[\mathbf{z^1},\dots,\mathbf{z^{d_1}}](1,\widehat{\mathbf{k}})]\otimes[M^{(2)}_{(1)}]_{B\cap\mathcal{P}_2}\\
&+ \mathbf{u^i}\otimes[[M^{(2)}_{(2)},\dots,M^{(2)}_{(d_2)}](\boldsymbol{\alpha}_i\widetilde{\mathbf{k}})]_{B\cap\mathcal{P}_2}\\
&= \boldsymbol{\alpha}_i[M^{(2)}_{(1)}]_{B\cap\mathcal{P}_2} + \boldsymbol{\alpha}_i[[M^{(2)}_{(2)},\dots,M^{(2)}_{(d_2)}](\widetilde{\mathbf{k}})]_{B\cap\mathcal{P}_2}\\
&= \boldsymbol{\alpha}_i\{[[M^{(2)}_{(2)},\dots,M^{(2)}_{(d_2)}](\widetilde{\mathbf{k}})]_{B\cap\mathcal{P}_2} + [M^{(2)}_{(1)}]_{B\cap\mathcal{P}_2}\}\\
&= \boldsymbol{\alpha}_i\{[[M^{(2)}_{(1)},M^{(2)}_{(2)},\dots,M^{(2)}_{(d_2)}](1,\widetilde{\mathbf{k}})]_{B\cap\mathcal{P}_2}\}\\
&= \boldsymbol{\alpha}_i M^{(2)}_{B\cap\mathcal{P}_2}(1,\widetilde{\mathbf{k}}) = \mathbf{0}.
\end{aligned}
$$

Here starting from the second equality we consider $M^{(1)}_{P_z}$ row by row. It follows that $(1,\mathbf{k})\in\ker(M_B)$ and $B\in\Delta$.

Case 3. (Reverse) If $B\in\Delta$ we will prove that either $(B\cap\mathcal{P}_1)\cup\{P_z\}\in\Delta_1$ or $(B\cap\mathcal{P}_1\in\Delta_1$ and $B\cap\mathcal{P}_2\in\Delta_2)$ holds. Let $B\in\Delta$. Then there exists a column vector $(1,\mathbf{k})\in\mathbb{F}^{d_1+(d_2-1)|\varphi_1(P_z)|}$ such that $M_B(1,\mathbf{k})=\mathbf{0}$. We can rewrite $(1,\mathbf{k})$ as $(1,\widehat{\mathbf{k}},\widetilde{\mathbf{k^1}},\dots,\widetilde{\mathbf{k^q}})$, where $\widehat{\mathbf{k}}\in\mathbb{F}^{d_1-1}$, $\widetilde{\mathbf{k^i}}\in\mathbb{F}^{d_2-1}$ are column vectors. First, let us consider $(1,\widehat{\mathbf{k}})$:

From $M_B(1,\mathbf{k})=\mathbf{0}$ we conclude that $\overline{M}^{(1)}_{B\cap\mathcal{P}_1}(1,\widehat{\mathbf{k}})=\mathbf{0}$. If it is also true that $M^{(1)}_{P_z}(1,\widehat{\mathbf{k}})=\mathbf{0}$ it will follow that $(B\cap\mathbf{P}_1)\cup\{P_z\}\in\Delta_1$, so we are done.

But if $M^{(1)}_{P_z}(1,\widehat{\mathbf{k}}) = \boldsymbol{\alpha} \neq \mathbf{0}$ then from $M_B(1,\mathbf{k}) = \mathbf{0}$ we will have that $\widehat{M}_{B\cap\mathcal{P}_2}(1,\widehat{\mathbf{k}})+\widetilde{M}_{B\cap\mathcal{P}_2}(\widetilde{\mathbf{k^1}},\dots,\widetilde{\mathbf{k^q}}) = \mathbf{0}$. Rewriting the last equation, as in case 2), we obtain $\boldsymbol{\alpha}_i[M^{(2)}_{(1)}]_{B\cap\mathcal{P}_2} + [[\widetilde{M^{(2)}}](\widetilde{\mathbf{k^i}})]_{B\cap P_2} = \mathbf{0}$, for $i = 1,\dots,q$. Since at least one $\boldsymbol{\alpha}_j \neq 0$, we can construct a new vector $(1,\mathbf{k}) \in \mathbb{F}^{d_1+(d_2-1)|\varphi_1(P_z)|}$ such that $M_B(1,\mathbf{k}) = \mathbf{0}$, as follows: $(1,\mathbf{k}) = (1,\widehat{\mathbf{k}}, \frac{\boldsymbol{\alpha}_1}{\boldsymbol{\alpha}_j}\widetilde{\mathbf{k^j}},\dots,\frac{\boldsymbol{\alpha}_q}{\boldsymbol{\alpha}_j}\widetilde{\mathbf{k^j}})$. Now consider column vector $(1,\widetilde{\mathbf{k^j}}/\boldsymbol{\alpha}_j)$. It satisfies $M^{(2)}_{B\cap\mathcal{P}_2}(1,\widetilde{\mathbf{k^j}}/\boldsymbol{\alpha}_j) = \mathbf{0}$. Therefore we have both $B\cap\mathcal{P}_1 \in \Delta_1$ and $B\cap\mathcal{P}_2 \in \Delta_2$ which proves the case 3. □

3.3 Composite

In this section we will follow the settings given in [12]. Recall that $\mathcal{P}$ is the set of participants and let $\mathcal{P} = \mathcal{P}_1\cup\dots\cup\mathcal{P}_\ell$ be a partition of $\mathcal{P}$ (that is $\emptyset \neq \mathcal{P}_i \neq \mathcal{P}$, $\mathcal{P}_i\cap\mathcal{P}_j = \emptyset$, if $i\neq j$ and $\cup_{i=1}^{\ell}\mathcal{P}_i = \mathcal{P}$). Let us write $|\mathcal{P}_i| = n_i$ and $n = \sum_{i=1}^{\ell} n_i$. For a set $A\subseteq\mathcal{P}$ we denote $A_i = A\cap\mathcal{P}_i$. Obviously $A = A_1\cup\dots\cup A_\ell$. For $i = 1,\dots,\ell$, let Γ_i be an access structure on $\mathcal{P}_i$ and let Γ_0 be an access structure on the participants set $\mathcal{P}_0 = \{\mathcal{P}_1,\dots,\mathcal{P}_\ell\}$.

Definition 5. *[12] With the notion as above the* composite access structure *of $\Gamma_1,\dots,\Gamma_\ell$, following Γ_0, denoted by $\Gamma_0[\Gamma_1,\dots,\Gamma_\ell]$, is defined as follows*

$$\begin{aligned}\Gamma_0[\Gamma_1,\dots,\Gamma_\ell] &= \{A\subseteq\mathcal{P} \mid \exists B\in\Gamma_0 \;\; \textit{such that} \;\; A_i\in\Gamma_i \;\; \textit{for all} \;\; \mathcal{P}_i\in B\}\\ &= \bigcup_{B\in\Gamma_0}\{A_i\in\Gamma_i \;\; \textit{for all} \;\; \mathcal{P}_i\in B\}.\end{aligned}$$

That is, each of the sets $\mathcal{P}_i$ plays the role of a participant for Γ_0. A coalition $A\subseteq\mathcal{P}$ is qualified if and only if it includes, as subsets, qualified coalitions in enough of the components $\Gamma_1,\Gamma_2,\dots,\Gamma_\ell$ to constitute an qualified subset for Γ_0. Note that the access structures Γ_i could be defined over $\mathcal{P}$, not only over $\mathcal{P}_i$.

A composite SSS can be useful for secret sharing when the set of participants is divided into several groups, each of them with its own family of qualified coalitions. The relation among these groups is given by the structure Γ_0.

The following relations are known given a partition $\mathcal{P} = \mathcal{P}_1\cup\dots\cup\mathcal{P}_\ell$ and access structures $\Gamma_1,\dots,\Gamma_\ell$:

- the sum of $\Gamma_1,\dots,\Gamma_\ell$ is $\Gamma_1+\dots+\Gamma_\ell = \{A\subseteq\mathcal{P} \mid A_i\in\Gamma_i$ for some $i\}$, hence $\Gamma_1+\dots+\Gamma_\ell = T_{0,\ell}[\Gamma_1,\dots,\Gamma_\ell]$;
- the product of $\Gamma_1,\dots,\Gamma_\ell$ is $\Gamma_1\times\dots\times\Gamma_\ell = \{A\subseteq\mathcal{P} \mid A_i\in\Gamma_i$ for all $i\}$, hence $\Gamma_1\times\dots\times\Gamma_\ell = T_{\ell-1,\ell}[\Gamma_1,\dots,\Gamma_\ell]$;
- let Γ_1,Γ_2 be two structures defined on the sets $\mathcal{P}_1$ and $\mathcal{P}_2$ and let P_z is a participant from $\mathcal{P}_1$. Then the operation insertion can be presented also as $\Gamma_1(P_z\to\Gamma_2) = \Gamma_1[\Gamma_2,T_{0,1},\dots,T_{0,1}]$.
- Composite access structures can be obtained by applying insertion several times as follows $\Gamma_0[\Gamma_1,\dots,\Gamma_r] = \Gamma_0(\mathcal{P}_1\to\Gamma_1)(\mathcal{P}_2\to\Gamma_2)\dots(\mathcal{P}_r\to\Gamma_r)$.

Thus the composite access structures are equivalent to insertion (see Definition 4) applied multiple times.

Theorem 4. *[20] Let $\Gamma_0[\Gamma_1,\dots,\Gamma_\ell]$ be a composite access structure. Denote by $\mathcal{M}_j$ the MSP computing Γ_j for $j=0,\dots,\ell$ and by m_j the size of $\mathcal{M}_j$. Let $\mathcal{P}_i$ be the "owner" of m_i^0 rows in the MSP $\mathcal{M}_0$. Then there exists an MSP $\mathcal{M}$ computing $\Gamma_0[\Gamma_1,\dots,\Gamma_\ell]$ of size $m=\sum_{i=1}^{\ell} m_i^0\, m_i$.*

Proof. We will give first the construction of MSP $\mathcal{M}$ from [20], then we prove that it computes $\Gamma_0[\Gamma_1,\dots,\Gamma_\ell]$. Suppose that access structures $\Gamma_0,\Gamma_1,\dots,\Gamma_\ell$ are computed by MSPs $\mathcal{M}_0,\mathcal{M}_1,\dots,\mathcal{M}_\ell$. Let $M^{(j)}$ be the corresponding matrices. Then the MSP $M=\begin{pmatrix} M^{(0)} & I^{(1)} & I^{(2)} & \dots \\ 0 & M^{(1)} & 0 & \\ 0 & 0 & M^{(2)} & \\ \vdots & & & \ddots \end{pmatrix}$ computes $\Gamma_0[\Gamma_1,\dots,\Gamma_\ell]$, where $I^{(j)}$ is the matrix which has a single 1 in the j-th row and 1-st column, all other entries are 0. But the size of $\mathcal{M}$ is bigger than $\sum_{i=1}^{\ell} m_i^0\, m_i$.

On the other hand since the composite access structure $\Gamma_0[\Gamma_1,\dots,\Gamma_\ell]$ can be constructed by applying several times the operation insertion. By applying Theorem 3 we obtain the MSP that computes $\Gamma_0[\Gamma_1,\dots,\Gamma_\ell]$. The size of the MSP is $m=m_0+\sum_{i=1}^{\ell} m_i^0(m_i-1)$. To complete the proof we only need to recall that $m_0=\sum_{i=1}^{\ell} m_i^0$. $\square$

Corollary 1. *If access structures $\Gamma_0,\Gamma_1,\dots,\Gamma_\ell$ are ideal, then the composite access structure $\Gamma_0[\Gamma_1,\dots,\Gamma_\ell]$ is also ideal.*

Proof. Since Γ_0 is ideal it follows that $m_i^0=1$ and $m_0=\ell$. From the fact that Γ_i is ideal for $i=1,\dots,\ell$ it follows that $m_i=n_i$, where n_i is the number of players in $\mathcal{P}_i$. Applying Theorem 4 we obtain that $m=\sum_{i=1}^{\ell} n_i=n$, i.e. the scheme is ideal. $\square$

3.4 Sums and Products

As Martin pointed out in [15] there are many special cases of the use of insertion. He considered two of them.

Definition 6. *[15] If Γ_1 and Γ_2 are defined on $\mathcal{P}_1$ and $\mathcal{P}_2$ respectively, then one can define the* sum *$\Gamma_1+\Gamma_2$ and the* product *$\Gamma_1\times\Gamma_2$ as the monotone access structures defined on $\mathcal{P}_1\cup\mathcal{P}_2$ such that for $A\subseteq\mathcal{P}_1\cup\mathcal{P}_2$,*

$$\begin{aligned} A\in\Gamma_1+\Gamma_2 &\iff (A\cap\mathcal{P}_1\in\Gamma_1 \quad \textit{or} \quad A\cap\mathcal{P}_2\in\Gamma_2)\,,\\ A\in\Gamma_1\times\Gamma_2 &\iff (A\cap\mathcal{P}_1\in\Gamma_1 \quad \textit{and} \quad A\cap\mathcal{P}_2\in\Gamma_2)\,. \end{aligned}$$

Van Dijk [8] showed some relations between insertion, product, sum of the access structures and the dual access structures.

$$\begin{aligned} (\Gamma_1(P_z\to\Gamma_2))^\perp &= \Gamma_1^\perp(P_z\to\Gamma_2^\perp), \\ (\Gamma_1\times\Gamma_2)^\perp &= \Gamma_1^\perp+\Gamma_2^\perp, \\ (\Gamma_1+\Gamma_2)^\perp &= \Gamma_1^\perp\times\Gamma_2^\perp. \end{aligned} \tag{1}$$

Theorem 5. *[20, 6] Let Γ_1 and Γ_2 be monotone access structures defined on $\mathcal{P}_1$ and $\mathcal{P}_2$ with MSPs $\mathcal{M}_1$ of size m_1 and $\mathcal{M}_2$ of size m_2 respectively. Then there exists an MSP $\mathcal{M}$ of size $m_1 + m_2$ computing the sum $\Gamma_1 + \Gamma_2$.*

Proof. We will give first the construction of MSP $\mathcal{M}$, then we prove that it computes $\Gamma_1 + \Gamma_2$. Martin proves in [15] that using the access structure $\overline{\Gamma} = \{P_a, P_b, P_a P_b\}$ defined on the set $\{P_a, P_b\}$, where the players P_a, and P_b are not in $\mathcal{P}_1 \cup \mathcal{P}_2$ we have $\Gamma_1 + \Gamma_2 = \overline{\Gamma}(P_a \to \Gamma_1)(P_b \to \Gamma_2)$. Thus it is possible to construct $\mathcal{M}$ starting from $\overline{\mathcal{M}}$ applying twice Theorem 3. The MSP $\overline{\mathcal{M}}$ computes $\overline{\Gamma}$ and has matrix $\overline{M} = \binom{1}{1}$.

Suppose that access structures Γ_1 and Γ_2 are computed by MSPs $\mathcal{M}_1, \mathcal{M}_2$. Let $M^{(1)}$ and $M^{(2)}$ be the corresponding matrices. Let the matrices $M^{(1)} = (\mathbf{u}\ \overline{M}^{(1)})$ and $M^{(2)} = (\mathbf{v}\ \overline{M}^{(2)})$, where $\mathbf{u}, \mathbf{v}$ are their first columns. Then the MSP $M = \begin{pmatrix} \mathbf{u}\ \overline{M}^{(1)} & 0 \\ \mathbf{v} \quad 0 & \overline{M}^{(2)} \end{pmatrix}$ computes the sum $\Gamma_1 + \Gamma_2$. Thus M is a $(m_1 + m_2) \times (d_1 + d_2 - 1)$ matrix. The labelling of M is carried over in a natural way from $\mathcal{M}_1$ and $\mathcal{M}_2$.

Now we will show that this MSP computes the access structure $\Gamma_1 + \Gamma_2$. As usual let $\Gamma = \Gamma_1 + \Gamma_2$ and $\Delta = \Gamma^c$, correspondingly $\Delta_1 = (\Gamma_1)^c$ and $\Delta_2 = (\Gamma_2)^c$. Rewriting Definition 6 in terms of Δ instead of Γ we have:

$$B \in \Delta \iff (B \cap \mathcal{P}_1 \in \Delta_1 \ \text{ and } \ B \cap \mathcal{P}_2 \in \Delta_2)\,.$$

Thus we will check that both directions hold. If $B \cap \mathcal{P}_1 \in \Delta_1$ and $B \cap \mathcal{P}_2 \in \Delta_2$ there exist column vectors $(1, \widehat{\mathbf{k}}) \in \mathbb{F}^{d_1}$ and $(1, \widetilde{\mathbf{k}}) \in \mathbb{F}^{d_2}$ such that $M^{(1)}_{B \cap \mathcal{P}_1}(1, \widehat{\mathbf{k}}) = \mathbf{0}$ and $M^{(2)}_{B \cap \mathcal{P}_2}(1, \widetilde{\mathbf{k}}) = \mathbf{0}$. Construct the column vector $(1, \mathbf{k}) = (1, \widehat{\mathbf{k}}, \widetilde{\mathbf{k}}) \in \mathbb{F}^{d_1 + d_2 - 1}$. It is easy to check that $M_B(1, \mathbf{k}) = \mathbf{0}$, using the fact that $B = (B \cap \mathcal{P}_1) \cup (B \cap \mathcal{P}_2)$ and hence $B \in \Delta$.

On the other hand, if $B \in \Delta$ then there exists a column vector $(1, \mathbf{k}) \in \mathbb{F}^{d_1 + d_2 - 1}$ such that $M_B(1, \mathbf{k}) = \mathbf{0}$. Rewrite it in the form $(1, \mathbf{k}) = (1, \widehat{\mathbf{k}}, \widetilde{\mathbf{k}})$, where $\widehat{\mathbf{k}} \in \mathbb{F}^{d_1 - 1}$ and $\widetilde{\mathbf{k}} \in \mathbb{F}^{d_2 - 1}$ are column vectors. Then it is easy to check that $M^{(1)}_{B \cap \mathcal{P}_1}(1, \widehat{\mathbf{k}}) = \mathbf{0}$ and $M^{(2)}_{B \cap \mathcal{P}_2}(1, \widetilde{\mathbf{k}}) = \mathbf{0}$. Thus we have $B \cap \mathcal{P}_1 \in \Delta_1$ and $B \cap \mathcal{P}_2 \in \Delta_2$. Thus M computes Γ. □

Theorem 6. *[20] Let Γ_1 and Γ_2 be monotone access structures defined on $\mathcal{P}_1$ and $\mathcal{P}_2$ with MSPs $\mathcal{M}_1$ of size m_1 and $\mathcal{M}_2$ of size m_2 respectively. Then there exists an MSP $\mathcal{M}$ of size $m_1 + m_2$ computing the product $\Gamma_1 \times \Gamma_2$.*

Proof. We will give first the construction of MSP $\mathcal{M}$, then we will show that it computes $\Gamma_1 \times \Gamma_2$. Martin proves in [15] that using the access structure $\overline{\Gamma} = \{P_a P_b\}$ defined on the set $\{P_a, P_b\}$, where the players P_a, and P_b are not in $\mathcal{P}_1 \cup \mathcal{P}_2$ we have $\Gamma_1 \times \Gamma_2 = \overline{\Gamma}(P_a \to \Gamma_1)(P_b \to \Gamma_2)$. Thus it is possible to construct $\mathcal{M}$ starting from $\overline{\mathcal{M}}$ applying twice Theorem 3. The MSP $\overline{\mathcal{M}}$ computes $\overline{\Gamma}$ and has the matrix $\overline{M} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$.

In order to compute the size($\mathcal{M}$) we need a direct construction instead of the method proposed by Martin. Thus, another way to construct the same MSP is to use the construction from Theorem 5, taking into account the relation between product and sum (see (1)) and applying three times the construction of Cramer and Fehr for constructing a dual MSP [7]. Although this construction allows us to compute the size of $\mathcal{M}$ it does not give information about the properties of $\mathcal{M}$. For this purpose we build the matrix M as follows:

Suppose that access structures Γ_1 and Γ_2 are computed by MSPs $\mathcal{M}_1, \mathcal{M}_2$. Let $M^{(1)}$ and $M^{(2)}$ be the corresponding matrices. Let the matrices $M^{(1)} = (\mathbf{u}\ \overline{M}^{(1)})$ and $M^{(2)} = (\mathbf{v}\ \overline{M}^{(2)})$, where $\mathbf{u}, \mathbf{v}$ are their first columns. Then the MSP $M = \begin{pmatrix} \mathbf{u} & -\mathbf{u} & \overline{M}^{(1)} & 0 \\ 0 & \mathbf{v} & 0 & \overline{M}^{(2)} \end{pmatrix}$ computes the product $\Gamma_1 \times \Gamma_2$. Thus M is a $(m_1 + m_2) \times (d_1 + d_2)$ matrix. The labelling of M is carried over in the natural way from $\mathcal{M}_1$ and $\mathcal{M}_2$.

We will show that this MSP computes the access structure $\Gamma_1 \times \Gamma_2$. As usual write $\Gamma = \Gamma_1 \times \Gamma_2$, $\Delta = \Gamma^c$, $\Delta_1 = (\Gamma_1)^c$ and $\Delta_2 = (\Gamma_2)^c$. Rewriting Definition 6 in terms of Δ instead of Γ we have:

$$B \in \Delta \iff (B \cap \mathcal{P}_1 \in \Delta_1 \text{ or } B \cap \mathcal{P}_2 \in \Delta_2)\,.$$

Thus we will check that both directions hold. Now, if $B \cap \mathcal{P}_1 \in \Delta_1$ or $B \cap \mathcal{P}_2 \in \Delta_2$ then there exists a column vector $(1, \widehat{\mathbf{k}}) \in \mathbb{F}^{d_1}$ or $(1, \widetilde{\mathbf{k}}) \in \mathbb{F}^{d_2}$ such that $M^{(1)}_{B\cap\mathcal{P}_1}(1, \widehat{\mathbf{k}}) = \mathbf{0}$ or $M^{(2)}_{B\cap\mathcal{P}_2}(1, \widetilde{\mathbf{k}}) = \mathbf{0}$. Construct a column vector $(1, \mathbf{k}) = (1, \alpha, (1-\alpha)\widehat{\mathbf{k}}, \alpha\widetilde{\mathbf{k}}) \in K^{d_1+d_2}$, for $\alpha = 0$ or $\alpha = 1$. It is easy to check that $M_B(1, \mathbf{k}) = 0$ and hence $B \in \Delta$.

Conversely, if $B \in \Delta$ then there exists a column vector $(1, \mathbf{k}) \in \mathbb{F}^{d_1+d_2}$ such that $M_B(1, \mathbf{k}) = \mathbf{0}$. Rewrite it in the form $(1, \mathbf{k}) = (1, \alpha, \widehat{\mathbf{k}}, \widetilde{\mathbf{k}})$, where $\widehat{\mathbf{k}} \in \mathbb{F}^{d_1-1}$ and $\widetilde{\mathbf{k}} \in \mathbb{F}^{d_2-1}$ are column vectors too. Then it is easy to check that $M^{(1)}_{B\cap\mathcal{P}_1}(1, \widehat{\mathbf{k}}/(1-\alpha)) = \mathbf{0}$, when $1-\alpha \neq 0$ or $M^{(2)}_{B\cap\mathcal{P}_2}(1, \widetilde{\mathbf{k}}/\alpha) = \mathbf{0}$, when $\alpha \neq 0$. Thus we have $B \cap \mathcal{P}_1 \in \Delta_1$ or $B \cap \mathcal{P}_2 \in \Delta_2$. □

4 New Operations on and Properties of Access Structures

4.1 Element-Wise Union

We will first describe some properties of the operation for access structures, introduced in [16] and later applied to different models in [17–19]. The same operation for monotone structures was also defined by Fehr and Maurer in [9], which they call element-wise union.

Definition 7. *For any two monotone* decreasing *sets Δ_1, Δ_2 operation $\uplus$ is defined as follows: $\Delta_1 \uplus \Delta_2 = \{A = A_1 \cup A_2; A_1 \in \Delta_1, A_2 \in \Delta_2\}$.*

It is easy to check that $\Delta_1 \uplus \Delta_2$ is monotone decreasing. Note that if $A \in (\Delta_1 \uplus \Delta_2)^+$ then $A = A_1 \cup A_2$ for some $A_1 \in \Delta_1^+$ and $A_2 \in \Delta_2^+$.

Definition 8. *For any two monotone* increasing *sets Γ_1, Γ_2 operation $\uplus$ is defined as follows: $\Gamma_1 \uplus \Gamma_2 = \{A = A_1 \cup A_2; A_1 \notin \Gamma_1, A_2 \notin \Gamma_2\}^c$.*

Obviously $\Gamma_1 \uplus \Gamma_2$ is monotone increasing, since $\Gamma_1 \uplus \Gamma_2 = (\Delta_1 \uplus \Delta_2)^c$. Note that from $B \in \Gamma_1 \uplus \Gamma_2$ it follows that $B \in \Gamma_1$, $B \in \Gamma_2$ and that $B \neq A_1 \cup A_2$ with $A_1 \notin \Gamma_1, A_2 \notin \Gamma_2$.

Corollary 2. *For any two access structures Γ_1 and Γ_2, the element-wise union is subset of their product.*

$$\Gamma_1 \uplus \Gamma_2 \subset \Gamma_1 \times \Gamma_2.$$

4.2 Element-Wise Intersection

In this section we will consider operation, which is in some sense dual to the element-wise union.

Definition 9. *The* element-wise intersection *operation $\circ$ for any two monotone* increasing *sets Γ_1, Γ_2 is defined as follows: $\Gamma_1 \circ \Gamma_2 = \{B = B_1 \cap B_2; B_1 \in \Gamma_1, B_2 \in \Gamma_2\}$.*

It is easy to check that $\Gamma_1 \circ \Gamma_2$ is monotone increasing.

Lemma 2. *$B \in (\Gamma_1 \uplus \Gamma_2)^\perp$ if and only if $B = B_1 \cap B_2$ for some $B_1 \in \Gamma_1^\perp$ and $B_2 \in \Gamma_2^\perp$.*

Proof. Let us find the dual of $\Gamma_1 \uplus \Gamma_2$. Let $A \notin \Gamma_1 \uplus \Gamma_2$, i.e., $A = A_1 \cup A_2$ for some $A_1 \notin \Gamma_1$ and $A_2 \notin \Gamma_2$ (see Definition 7). Hence $A = A_1 \cup A_2; A_1^c \in \Gamma_1^\perp, A_2^c \in \Gamma_2^\perp$. Thus $A^c = A_1^c \cap A_2^c; A_1^c \in \Gamma_1^\perp, A_2^c \in \Gamma_2^c$. In other words $B \in (\Gamma_1 \uplus \Gamma_2)^\perp$ if and only if $B = B_1 \cap B_2$ for some $B_1 \in \Gamma_1^\perp$ and $B_2 \in \Gamma_2^\perp$. □

Corollary 3. *For any access structures Γ_1 and Γ_2, their element-wise intersection is the dual access structure of the element-wise union of the dual access structures $\Gamma_1^\perp$ and $\Gamma_2^\perp$.*

$$\Gamma_1 \circ \Gamma_2 = (\Gamma_1^\perp \uplus \Gamma_2^\perp)^\perp.$$

Lemma 3. *For any access structures Γ_1 and Γ_2, their sum is subset of the element-wise intersection.*

$$\Gamma_1 + \Gamma_2 \subset \Gamma_1 \circ \Gamma_2.$$

Proof. Using Definition 1 it is easy to verify that $\Gamma_1 \subseteq \Gamma_2$ if and only if $\Delta_2 \subseteq \Delta_1$ if and only if $\Gamma_2^\perp \subseteq \Gamma_1^\perp$. Now using Corollaries 2, 3 and the relation between the operations (1) we conclude that

$$\Gamma_1 + \Gamma_2 = (\Gamma_1^\perp \times \Gamma_2^\perp)^\perp \subset (\Gamma_1^\perp \uplus \Gamma_2^\perp)^\perp = \Gamma_1 \circ \Gamma_2.$$

□

4.3 Insertions in Monotone Decreasing Sets

Now we will define the operation insertion in monotone decreasing sets.

Definition 10. *Let Δ_1 and Δ_2 be two monotone decreasing sets defined on participant sets $\mathcal{P}_1$ and $\mathcal{P}_2$ respectively, and let $P_z \in \mathcal{P}_1$. Define the* insertion of monotone decreasing set *Δ_2 at player P_z in Δ_1, $\Delta_1(P_z \to \Delta_2)$, to be the monotone decreasing set defined on the set $(\mathcal{P}_1 \setminus P_z) \cup \mathcal{P}_2$ such that for $A \subseteq (\mathcal{P}_1 \setminus P_z) \cup \mathcal{P}_2$ we have*

$$A \in \Delta_1(P_z \to \Delta_2) \iff \begin{cases} A \in \Delta_1, \quad or \\ ((A \cap \mathcal{P}_1) \cup P_z \in \Delta_1 \quad and \quad A \cap \mathcal{P}_2 \in \Delta_2)\,. \end{cases}$$

Hence $\Delta_1(P_z \to \Delta_2)$ is the monotone decreasing set Δ_1 with participant P_z "replaced" by the sets of Δ_2. It is easy to verify that, $\Delta_1(P_z \to \Delta_2)$ is monotone decreasing too.

Let us consider Γ_1 defined on the set of players $\mathcal{P}$. Add one extra player P_z to the set of players $\mathcal{P}$ and form a new access structure Γ_3, such that $A \in \Delta_1^+$ if and only if $A \cup P_z \in \Delta_3^+$. Note that the player P_z is not important for reconstructing the secret.

Now combining Definition 10 and the construction above we arrive at the following lemma.

Lemma 4. *With the notions as above the following relation holds:*

$$\Delta_1 \uplus \Delta_2 = \Delta_3(P_z \to \Delta_2).$$

4.4 Some New Properties

In this section we investigate certain properties of access structures (e.g. star topology for forbidden sets and element-wise union of an access structure with its dual) .

Definition 11. *An access structure has* star topology *for forbidden sets, if there exists a player P_i such that P_i is a member of every maximal forbidden set, i.e. for any set $A \in \Delta^+$, $P_i \in A$. Call P_i to be in the center of the star.*

The next lemma follows directly from Definition 1 and Definition 11.

Lemma 5. *Access structure Γ has star topology for forbidden sets if and only if $P_i \notin B$ for any set $B \in (\Gamma^{\perp})^-$.*

Lemma 6. *Access structure Γ has star topology for forbidden sets if and only if $P_i \notin A$ for any set $A \in \Gamma^-$.*

Proof. Assume that there exists $A \in \Gamma^-$ such that $P_i \in A$. Define $B = A \setminus \{P_i\}$, so $B \in \Delta$. Thus, using the monotone decreasing property of Δ, there exists a set C such that $B \subseteq C$ and $C \in \Delta^+$. It is now easy to check that $P_i \notin C$, because otherwise it will follow that $A \subseteq C$, which is impossible since $A \in \Gamma$

and Γ is monotone increasing, implying that $C \in \Gamma$. So, $P_i \notin C$ and $C \in \Delta^+$. By Definition 11 this contradicts to the fact that Γ has a star topology for forbidden sets.

Let us now assume the opposite, i.e. $P_i \notin A$ for any set $A \in \Gamma^-$. Suppose that there exists $B \in \Delta^+$ such that $P_i \notin B$, i.e. Γ has not a star topology for forbidden sets. Define $A = B \cup \{P_i\}$, so $A \in \Gamma$. Then, using the monotone increasing property of Γ, there exists a set C such that $C \subseteq A$ and $C \in \Gamma^-$. It is now easy to check that $P_i \in C$, because otherwise it will follow that $C \subseteq B$ and Δ is monotone decreasing, implying that $C \in \Delta$. So, $P_i \in C$ and $C \in \Gamma^-$ a contradiction. □

Corollary 4. *Access structure Γ has star topology for forbidden sets if and only if the dual access structure $\Gamma^\perp$ has star topology for forbidden sets.*

Lemma 7. *Access structure Γ has star topology for forbidden sets if and only if Γ is not connected.*

Proof. Note that the following two statements are equivalent: "P_i is not in the $core(\Gamma)$" and "$P_i \notin A$ for any $A \in \Gamma^-$". So, from Lemma 6 such players P_i belong to any set $A \in \Delta^+$, i.e. the access structure Γ has star topology for the forbidden sets. □

Now we are ready to give another proof of an interesting property of access structures.

Theorem 7. *[11] For any access structure Γ $core(\Gamma) = core(\Gamma^\perp)$. Access structure Γ is connected if and only if the dual access structure $\Gamma^\perp$ is connected.*

Proof. By Lemma 7 all players P_i which are not in the $core(\Gamma)$ are in the center of the star and vice versa. Note that by Lemma 5 the same is true for the players P_i which are not in the $core(\Gamma^\perp)$. □

Remark 1. Players P_i which are not in the $core(\Gamma)$ are actually dead players for both access structures Γ and $\Gamma^\perp$ (their individual information rate is zero in both access structures).

Lemma 8. *Access structure $\Gamma \uplus \Gamma^\perp$ is not trivial (i.e., $\mathcal{P} \in \Gamma \uplus \Gamma^\perp$).*

Proof. Recall the set $\Delta \uplus \Delta^\perp = \{A = A_1 \cup A_2; A_1 \notin \Gamma, A_2 \notin \Gamma^\perp\}$ from Definition 7. Suppose that there exist A_1 and A_2, such that $A_1 \notin \Gamma$, $A_2 \notin \Gamma^\perp$ and $A_1 \cup A_2 = \mathcal{P}$. This would mean that $\Delta \uplus \Delta^\perp = P(\mathcal{P})$, i.e. $\Gamma \uplus \Gamma^\perp = \emptyset$. Without loss of generality we can assume that $A_1 \cap A_2 = \emptyset$, because otherwise we can replace A_2 with $A_2 \backslash A_1 \in \Delta^\perp$ (from the monotone decreasing property). Hence $A_1 = A_2^c$ and $A_1 = A_2^c \notin \Gamma$. From Definition 1 it follows that $A_1^c = A_2 \in \Gamma^\perp$. But $A_2 \notin \Gamma^\perp$, which contradicts our assumption. Hence there are no sets A_1 and A_2, such that $A_1 \notin \Gamma$, $A_2 \notin \Gamma^\perp$ and $A_1 \cup A_2 = \mathcal{P}$. Therefore we have $\Gamma \uplus \Gamma^\perp \neq \emptyset$. □

Now we are ready to state next interesting result in this section.

Theorem 8. *Let Γ and $\Gamma^{\perp}$ be connected access structures. Then $\Gamma \uplus \Gamma^{\perp} = \{\mathcal{P}\}$.*

Proof. We have already proved in Lemma 8 that $\mathcal{P} \in \Gamma \uplus \Gamma^{\perp}$. Hence it is sufficient to prove that except for $\{\mathcal{P}\}$ there are no other sets in $\Gamma \uplus \Gamma^{\perp}$.

For any set $A \in \Delta^{+}$ and any player $P_i \in \mathcal{P}$, $P_i \notin A$ we have $(A \cup \{P_i\}) \in \Gamma$. Set $B = (A \cup \{P_i\})^c$ then $B \in \Delta^{\perp}$. Therefore $A \cup B = (\mathcal{P} \setminus \{P_i\}) \in (\Delta \uplus \Delta^{\perp})$.

Assume that there exists a player P_j such that $(\mathcal{P} \setminus \{P_j\}) \notin (\Delta \uplus \Delta^{\perp})$. So, $P_j \in A$ for every set $A \in \Delta^{+}$, because otherwise using the construction given above we arrive at a contradiction. Hence the access structure Γ has the star topology for the forbidden sets (see Definition 11), i.e., there exists a player P_j such that for any set $A \in \Delta^{+}$, $P_j \in A$. Now using Lemma 7 we obtain that Γ is not connected – a contradiction which proves the statement of the theorem. □

References

1. G. Blakley, G. Kabatianskii. Linear Algebra Aproach to Secret Sharing Schemes, *LNCS* 829, 1994, pp. 33-40.
2. J. Benaloh, J. Leichter. Generalized Secret Sharing and Monotone Functions, *CRYPTO'88*, LNCS 403, Springer-Verlag 1990, pp. 25-35.
3. M. Bertilsson, I. Ingemarsson. A construction of Practical Secret Sharing Schemes using Linear Block Codes, *AUSCRYPT'92*, LNCS 718, Springer-Verlag 1993, pp. 67-79.
4. E. Brickell. Some ideal secret sharing schemes, *J. of Comb. Math. and Comb. Computing* **9**, 1989, pp. 105-113.
5. E. Brickell, D. Davenport. On the Classification of Ideal Secret Sharing Schemes, *Crypto'89*, LNCS 435, Springer-Verlag 1990, pp. 278-285.
6. R. Cramer, I. Damgard and U. Maurer. General Secure Multi-Party Computation from any linear secret sharing scheme, *EUROCRYPT'00*, LNCS 1807, Springer-Verlag, pp. 316-334.
7. R. Cramer, S. Fehr. Optimal Black-Box Secret Sharing over Arbitrary Abelian Groups, *CRYPTO'2002*, LNCS 2442, 2002, pp. 272-287.
8. M. van Dijk. Secret Key Sharing and Secret Key Generation, *Ph.D. thesis*, 1997, TU Eindhoven.
9. S. Fehr, U. Maurer. Linear VSS and Distributed Commitments Based on Secret Sharing and Pirwise Checks, *CRYPTO'02*, LNCS 2442, Springer-Verlag, pp. 565-580.
10. M. Ito, A. Oaito, T. Nishizeki. Secret Sharing Scheme Realizing General Access Structure, *Proc. IEEE Goblecom'87*, 1987, pp. 99-102.
11. W. -A. Jackson, K. Martin. Geometric Secret Sharing Schemes and Their Duals, *Desings Codes and Cryptography*, 4, 1994, pp. 83-95.
12. W. -A. Jackson, K. Martin, C. O'Keefe. Mutually Trusted Authority-Free Secret Sharing Schemes, *J. of Cryptology* 10, 1997, pp. 261-289.
13. M. Karchmer, A. Wigderson. On Span Programs, *Proc. 8-th Annual Structure in Complexity Theory Conference*, San Diego, California, 18-21 May 1993. IEEE Computer Society Press, pp. 102-111.
14. J. Massey. Minimal Codewords and Secret Sharing, *Proc. 6th Joint Swedish-Russian Int. Workshop on Inform. Theory* 1993, pp. 276-279.
15. K. Martin. New Secret Sharing Schemes from Old, *J. of Comb. Math. and Combin. Comput.*, **14**, 1993, pp. 65-77.

16. V. Nikov, S. Nikova, B. Preneel, J. Vandewalle. Applying General Access Structure to Proactive Secret Sharing Schemes, *Proc. of the 23rd Symposium on Information Theory in the Benelux*, May 29-31, 2002, Universite Catolique de Lovain (UCL), Lovain-la-Neuve, Belgium, pp. 197-206, *Cryptology ePrint Archive*: Report 2002/141.
17. V. Nikov, S. Nikova, B. Preneel, J. Vandewalle. On Distributed Key Distribution Centers and Unconditionally Secure Proactive Verifiable Secret Sharing Schemes based on General Access Structure, *INDOCRYPT 2002*, LNCS 2551 Springer-Verlag, 2002, pp. 422-437.
18. V. Nikov, S. Nikova, B. Preneel. On Multiplicative Linear Secret Sharing Schemes, *INDOCRYPT'2003*, LNCS 2904, 2003, pp. 135-147, *Cryptology ePrint Archive:* Report 2003/006.
19. V. Nikov, S. Nikova. On Proactive Secret Sharing Schemes, *SAC'2004*, LNCS.
20. P. Pudlak, J.Sgall. Algebraic models of computation and interpolation for algebraic proof systems, *Proc. Feasible Arithmetic and Proof Complexity*, LNCS, 1998, pp. 279-295.
21. A. Shamir. How to Share a Secret, *Communications of the ACM* 22, 1979, pp. 612-613.
22. J. Simonis, A. Ashikhmin. Almost Affine Codes, *DCC* **14**, 1998, pp. 179-197.