A Linear Construction of Perfect Secret Sharing Schemes

Marten van Dijk

Department of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands

Abstract. In this paper, we generalize the vector space construction due to Brickell [5]. This generalization, introduced by Bertilsson [1], leads to perfect secret sharing schemes with rational information rates in which the secret can be computed efficiently by each qualified group. A one to one correspondence between the generalized construction and linear block codes is stated. It turns out that the approach of minimal codewords by Massey [15] is a special case of this construction. For general access structures we present an outline of an algorithm for determining whether a rational number can be realized as information rate by means of the generalized vector space construction. If so, the algorithm produces a perfect secret sharing scheme with this information rate. As a side-result we show a correspondence between the duality of access structures and the duality of codes.

1 Introduction

A secret sharing scheme is a method of sharing a secret among a set of participants P in such a way that certain subsets of participants are qualified to compute the secret by combining their shares. A secret sharing scheme is called perfect if in addition any non-qualified subset of participants has absolutely no information on the secret. The access structure Γ on P is the set of all qualified subsets of P. In the remainder of the paper only monotone access structures will be considered. For this reason it suffices to describe Γ by its "minimal elements": sets in Γ with the property that no proper subset is in Γ. In the following Γ is not empty and does not consist of all subsets of P. We follow the information theoretic approach of Capocelli et al. [7]. We refer to Gallager [11] for a treatment of information theory. The uncertainty about the shares of the participants in a group of participants X is denoted by $H(X)$. The set of possible secrets is denoted by S, and the uncertainty about the secret is denoted by $H(S)$. A perfect secret sharing scheme $\mathcal{PS}(\Gamma, S)$ for access structure Γ and set of possible secrets S is a sharing of secrets among participants P such that (a) any qualified subset can reconstruct the secret and (b) any non-qualified subset has absolutely no information on the secret, i.e.

$$\text{(a) } \forall_{X \in \Gamma}\ H(S|X) = 0,$$

$$\text{(b) } \forall_{X \notin \Gamma}\ H(S|X) = H(S).$$

We are interested in measures for the amount of secret information that must be given to the participants. We can use the information rate of a perfect secret sharing scheme $\mathcal{PS}(\Gamma, S)$ defined as

$$\rho(\mathcal{PS}(\Gamma, S)) = \frac{\log |S|}{\max\{\log \#(p) : p \in P\}},$$

i.e. the ratio between the size of the secret and the maximum size of the shares [6] ($\#(p)$ denotes the number of possible shares given to participant $p \in P$). Also, we can use the average information rate $\tilde{\rho}(\mathcal{PS}(\Gamma, S))$, which is the ratio between the size of the secret and the arithmetic mean of the size of all shares [4, 13, 14]. The optimal information rate of access structure Γ on P, $\rho(\Gamma)$, is defined as the supremum of $\rho(\mathcal{PS}(\Gamma, S))$ over all perfect secret sharing schemes $\mathcal{PS}(\Gamma, S)$. Similar, one can define $\tilde{\rho}(\Gamma)$, the optimal average information rate of access structure Γ on P. We notice that, by definition, $\rho(\Gamma) \leq \tilde{\rho}(\Gamma)$.

In this paper we generalize the vector space construction due to Brickell [5]. This generalization has been introduced by Bertilsson [1]. Bertilsson has investigated a special class of non-perfect secret sharing schemes (these are schemes for which only condition (a) need to be valid). We continue our investigation, started in [8], of perfect secret sharing schemes constructed by using the generalized vector space construction. This leads to perfect secret sharing schemes with rational information rates in which the secret can be computed efficiently by each qualified group. A one to one correspondence between the generalized construction and linear block codes is stated. It turns out that the approach of minimal codewords by Massey [15], and the construction of Bertilsson and Ingemarsson [2] are special cases of this construction.

Let Γ be an access structure decomposed into several "smaller" access structures. By using composition constructions (see Stinson [17] for a general description) we can compose perfect secret sharing schemes for these access structures into a perfect secret sharing scheme for the original access structure Γ. Besides composition constructions we need basic constructions. Almost all examples for basic constructions are linear, that is they use subspaces. Jackson and Martin [12] describe linear basic constructions in their most general form by using a geometrical approach. The generalized vector space construction leads to a most general description by using coding theory. In geometry subspaces are called lines, planes, and so on. In coding theory they are called codes, and they are characterized by generator matrices. As a side-result this characterization by generator matrices leads to a correspondence between the duality of access structures and the duality of codes, which leads to useful quadratic matrix equations.

Given an access structure Γ and a rational number k/p we present an outline of an algorithm for determining whether k/p can be realized as information rate by means of the generalized vector space construction for Γ. If so, the algorithm produces a corresponding perfect secret sharing scheme with information rate k/p.

The generalized vector space construction is presented in Section 2. Its code description is stated in Section 3. In Section 4 the results concerning dual access structures are presented. Finally in Section 5 we describe an algorithm constructing perfect secret sharing schemes by using the generalized vector space construction.

2 The Generalized Vector Space Construction

We denote the vector space of all k-tuples over $GF(q)$ where q is a prime power by $GF(q)^k$. Let the set of secrets be

$$S = GF(q)^k.$$

In the following $P = \{1, \ldots, n\}$ and Γ is an access structure on P. Let each participant $i \in P$ have an $l \times p_i$ matrix G_i over $GF(q)$, where l is some integer satisfying $l \geq k$. These matrices are not secret, they are public knowledge. Suppose we want to share a secret $\mathbf{s} \in S$. Then we uniformly choose a vector $\mathbf{a} \in GF(q)^{l-k}$ and we distribute to participant $i \in P$ the share

$$(\mathbf{s}, \mathbf{a})G_i.$$

This construction of a secret sharing scheme is called a generalized vector space construction. We notice that for all $i \in P$ the matrix G_i is publicly accessible and is not part of the shares of participant i. Thus one can share more secrets, $\mathbf{s}^1, \mathbf{s}^2, \ldots \in S$, by using the same secret sharing scheme, i.e. by using the same matrices G_i. In the following theorem (mentioned in [8] and independently proved by Blakley and Kabatianskii [3]) sufficient and necessary conditions are given in order to be able to define a perfect secret sharing scheme for Γ by means of the generalized vector space construction.

Theorem 1. *For $1 \leq i \leq n$ let G_i be an $l \times p_i$ matrix over $GF(q)$. For $X = \{i_1, \ldots, i_m\} \subseteq P$, with $i_1 < \ldots < i_m$, we define the $l \times p[X]$ matrix $G[X]$ over $GF(q)$, with $p[X] = \sum\limits_{i \in X} p_i$, by*

$$G[X] = (G_{i_1} | \cdots | G_{i_m}).$$

The generalized vector space construction based on the matrices $G_i, i \in P$, defines a perfect secret sharing scheme for access structure Γ on P and set of possible secrets $S = GF(q)^k$ iff

$$X \in \Gamma \Rightarrow \forall_{\mathbf{s} \in S} \, \exists_{\mathbf{b} \in GF(q)^{p[X]}} \, (\mathbf{s}, 0)^T = G[X]\mathbf{b}^T, \text{ and} \tag{1}$$

$$X \notin \Gamma \Rightarrow \forall_{\mathbf{s} \in S \setminus \{0\}} \, \forall_{\mathbf{b} \in GF(q)^{p[X]}} \, (\mathbf{s}, 0)^T \neq G[X]\mathbf{b}^T, \tag{2}$$

for all $X \subseteq P$. The information rate equals $k / \max\{p_i : i \in P\}$ and the average information rate equals $k / \frac{1}{|P|} \sum\limits_{i \in P} p_i$ of such a perfect secret sharing scheme.

A set of matrices $G_i, i \in P$, is said to be suitable (to define a perfect secret sharing scheme for access structure Γ on P) if conditions (1) and (2) are satisfied. Let the set of matrices G_i, $1 \leq i \leq n$, be suitable for Γ. Thus if X is a qualified subset of the participants then for $1 \leq i \leq k$ the unit vectors $\mathbf{e}^i \in GF(q)^l$ ($(\mathbf{e}^i)_j$ equals 1 if $i = j$ and 0 if $i \neq j$) can be expressed as a linear combination of the columns of matrix $G[X]$. If X is a non-qualified subset of the participants then none of the non-zero linear combinations of $\{\mathbf{e}^1, \ldots, \mathbf{e}^k\}$ can be expressed as a linear combination of the columns of matrix $G[X]$. We will prove that the generalized vector space construction based on the set of matrices G_i leads to a perfect secret sharing scheme. After having done this we further investigate conditions (1) and (2) of Theorem 1. In order to complete the proof of Theorem 1 we need to show that conditions (1) and (2) are necessary as well. This has been done in [9].

Let X be a qualified subset. We will show that the participants in X can compute the secret $\mathbf{s}$. The participants in X can construct $(\mathbf{s},\mathbf{a})G[X]$, because they know $(\mathbf{s},\mathbf{a})G_i$, for all $i \in X$. All unit vectors $\mathbf{e}^i$ for $1 \leq i \leq k$ can be written as linear combinations of columns in $G[X]$ (cf. (1)). Hence, the participants in X can compute a matrix B such that

$$\begin{pmatrix} I_k \\ O \end{pmatrix} = G[X]B,$$

where I_k denotes the $k \times k$ identity matrix, and O denotes the all zero matrix of size $(l-k) \times k$. Hence

$$\mathbf{s} = (\mathbf{s},\mathbf{a})G[X]B.$$

Thus the participants in X can efficiently compute $\mathbf{s}$ by combining their shares and the public matrices G_i for $i \in X$, so $H(S|X) = 0$.

Let X be a non-qualified subset. Let $\mathbf{s}$ be the secret shared among the participants by selecting a random vector $\mathbf{a}$. Then the shares distributed among the participants in X are given by the vector $(\mathbf{s},\mathbf{a})G[X] = \mathbf{c}$. We will show that for each $\mathbf{s}' \in S$ there are equally many vectors $\mathbf{a}'$ such that $(\mathbf{s}',\mathbf{a}')G[X] = \mathbf{c}$. As a consequence the shares given to the participants in X contain no information about $\mathbf{s}$, hence, $H(S|X) = H(S)$.

We denote by e the dimension of the linear span of the columns of $G[X]$. By $G[X]_1$ we denote the matrix consisting of the first k rows of $G[X]$. By $G[X]_2$ we denote the matrix consisting of the last $l-k$ rows of $G[X]$. Hence

$$G[X] = \begin{pmatrix} G[X]_1 \\ G[X]_2 \end{pmatrix}.$$

From (2) we infer that if $G[X]_2\mathbf{b}^T = \mathbf{0}$ then $G[X]\mathbf{b}^T = \mathbf{0}$. Thus the rank of matrix $G[X]$ ($= e$) equals the rank of matrix $G[X]_2$. Hence, the rows of matrix $G[X]_1$ are linear combinations of the rows of matrix $G[X]_2$.

Choose any $\mathbf{s}' \in S$, and consider the system of equations

$$(\mathbf{s}',\mathbf{a}')G[X] = \mathbf{c},$$

which is equivalent to

$$\mathbf{a}'G[X]_2 = \mathbf{c} - \mathbf{s}'G[X]_1.$$

This is a system of linear equations in the $l-k$ unknowns given by the coordinates of $\mathbf{a}'$. The coefficient matrix $G[X]_2$ has rank e. This system of linear equations is not conflicting, since there exists a vector $\mathbf{a}''$ such that $\mathbf{a}''G[X]_2 = (\mathbf{s}-\mathbf{s}')G[X]_1$, and hence $(\mathbf{a}+\mathbf{a}'')G[X]_2 = \mathbf{c} - \mathbf{s}'G[X]_1$. So, the solution space has dimension $l-k-e$. Thus there are q^{l-k-e} solutions $\mathbf{a}'$. This number is independent of the value of $\mathbf{s}'$. Hence X does not obtain any additional knowledge about S, so $H(S|X) = H(S)$.

We conclude that the generalized vector space construction describes a perfect secret sharing scheme according to the information theoretic approach of Capocelli et al. [7] (see Section 1). Since $|S| = q^k$ and $\#(i) = q^{p_i}$ for $i \in P$ the information rate equals $k/\max\{p_i : i \in P\}$ and the average information rate equals $k/\frac{1}{|P|}\sum_{i \in P} p_i$.

Example 1. Let $p_i = 1$ for $i \in P$ and let $k = 1$. Then conditions (1) and (2) are equivalent to $\mathbf{e}^1 \in \langle G_i : i \in X \rangle \Leftrightarrow X \in \Gamma$, which is the vector space construction due to Brickell [5].

We notice that the construction of Bertilsson and Ingemarsson [2] (see also [1]) is the generalized vector space construction in which $k = 1$. The following example illustrate the generalized vector space construction. In this example q is an arbitrary prime power.

Example 2. Let $P = \{1,2,3,4,5,6\}$ and let Γ be defined by its minimal elements $\{\{1,2\},\{1,3\},\{2,4\},\{2,5\},\{3,4\},\{4,5\},\{5,6\}\}$. Suppose we want to share a secret $\mathbf{s} = (s_1, s_2)$, $k = 2$. Then we choose a vector $\mathbf{a} = (a_1, a_2, a_3, a_4, a_5)$ at random and we distribute to participants

- 1 the share $(\mathbf{s},\mathbf{a})G_1 = (a_1, a_2, a_3)$ $(p_1 = 3)$,
- 2 the share $(\mathbf{s},\mathbf{a})G_2 = (s_1 + a_3, s_2 + a_2, a_4)$ $(p_2 = 3)$,
- 3 the share $(\mathbf{s},\mathbf{a})G_3 = (s_1 + a_1, s_2 + a_2, a_5)$ $(p_3 = 3)$,
- 4 the share $(\mathbf{s},\mathbf{a})G_4 = (s_1 + a_5, a_2, a_3 + a_4)$ $(p_4 = 3)$,
- 5 the share $(\mathbf{s},\mathbf{a})G_5 = (s_2 + a_4, a_3, a_5)$ $(p_5 = 3)$,
- 6 the share $(\mathbf{s},\mathbf{a})G_6 = (s_1 + a_3 + a_5, a_4)$ $(p_6 = 2)$.

The actual form of the $l \times p_i$ matrices G_i, $1 \leq i \leq 6$, can easily be determined from these relations but they are omitted for reasons of space. The reader is invited to verify (1) and (2). The information rate of this scheme is $2/3$ and the average information rate is $12/17$. The information rate is optimal (see Capocelli et al. [7] for the proof of $\rho(\Gamma) \leq 2/3$).

We notice that $s_1, s_2, a_1, \ldots$ are in $GF(q)$ in the scheme of the previous example. However, w.l.o.g. we can take them from the integer ring $\mathbb{Z}_m$! In order to use the generalized vector space construction one needs to compute a suitable set of matrices, which costs a lot of computing time. In the next section we present a description of the generalized vector space construction in terms of codes. This will finally lead to an algorithm in Section 5, and a side-result presented in Section 4.

3 Code Description

In this section we start introducing definitions in order to state some theorems about the relation between matrices defining a perfect secret sharing scheme and the linear block code C of length $k + p[P]$ over $GF(q)$ defined by its parity check matrix

$$H = \left(\begin{matrix} I_k \\ O \end{matrix} \middle| G[P] \right). \tag{3}$$

The proofs of the theorems stated in this section can be found in [9] and in the Appendix.

Definition 2. Let Γ be an access structure on P. We denote the set of minimal elements of Γ by Γ_0. Let $X \subseteq P$ then the complement of X is defined as $X^c = P \backslash X$. The complement of Γ is defined as $\Gamma^c = \{X \subseteq P : X \notin \Gamma\}$. We denote the set of maximal elements of Γ^c by Γ_1.

Definition 3. Let $\mathbf{c}^i$ be in $GF(q)^{p_i}$, $1 \le i \le n$, and $\mathbf{c} = (\mathbf{c}^1, \ldots, \mathbf{c}^n) \in GF(q)^{p[P]}$. The p-support of vector $\mathbf{c}$, $sup_p(\mathbf{c})$, is defined as the set of coordinates $i, 1 \le i \le n$, for which $\mathbf{c}^i \neq \mathbf{0}$, i.e.

$$sup_p(\mathbf{c}) = \{i : \mathbf{c}^i \neq \mathbf{0}\}.$$

Let $X = \{l_1, \ldots, l_m\} \subseteq P$, with $l_1 < \ldots < l_m$. Then the projection of vector $\mathbf{c}$ on X, $\mathbf{c}_X$ for short, is defined as

$$\mathbf{c}_X = (\mathbf{c}^{l_1}, \ldots, \mathbf{c}^{l_m}).$$

We notice that $\mathbf{c} = \mathbf{c}_P$.

Definition 4. Let Γ be an access structure on P. Let $\Gamma_0 = \{X_1, \ldots, X_r\}$. Let k and p_i, $1 \le i \le n$, be integers. We define $\mathcal{E}$ as $\mathcal{E} = \{(i,j) : 1 \le i \le r, 1 \le j \le k\}$. Then the set of vectors $C = \{\mathbf{c}^{i,j} \in GF(q)^{p[P]} : (i,j) \in \mathcal{E}\}$ is said to be suitable (to define a perfect secret sharing scheme) for access structure Γ and set of possible secrets $GF(q)^k$ if

- the Γ_0-property: $sup_p(\mathbf{c}^{i,j}) = X_i$ for all $(i,j) \in \mathcal{E}$, and
- the "Γ_1"-property: for all $r \times k$ q-ary matrices B with the property that the elements of at least one column in B do not add up to 0

$$\exists_{X \in \Gamma_0} \; X \subseteq sup_p\Big(\sum_{(i,j) \in \mathcal{E}} B_{i,j} \mathbf{c}^{i,j} \Big),$$

are satisfied by C.

At the end of this section it will be clear why the second property is called the "Γ_1"-property. Now we can state the following theorem.

Theorem 5. *Let Γ be an access structure on P. Let $\Gamma_0 = \{X_1, \ldots, X_r\}$. Let G_i, $i \in P$, be $l \times p_i$ matrices over $GF(q)$ such that the set of matrices G_i is suitable for access structure Γ and set of possible secrets $GF(q)^k$. Then there exists a suitable set of vectors $\{\mathbf{c}^{i,j} \in GF(q)^{p[P]} : (i,j) \in \mathcal{E}\}$ for Γ and set of possible secrets $GF(q)^k$ such that $G'H^T = O$, where*

$$H = \left(\begin{matrix} I_k \\ O \end{matrix} \middle| G[P] \right),$$

and G' is a generator matrix of the code defined by the linear span of the vectors $(\mathbf{e}^j, \mathbf{c}^{i,j})$, $(i,j) \in \mathcal{E}$.

Let the vectors $\mathbf{c}^{i,j} \in GF(q)^{p[P]}$, $(i,j) \in \mathcal{E}$, define a suitable set of vectors for Γ. Let H be a parity check matrix of the code defined by the linear span of the vectors $(\mathbf{e}^j, \mathbf{c}^{i,j})$, $(i,j) \in \mathcal{E}$. W.l.o.g. H is of the form

$$H = \left(\begin{matrix} I_k \\ O \end{matrix} \middle| H' \right).$$

Then the set of matrices G_i, $i \in P$, defined by $G[P] = H'$ is suitable for Γ.

By using Theorem 5 it is proved in [9] that the approach of minimal code words by Massey [15] is equivalent to the vector space construction. We want to generate a suitable set of vectors. The Γ_0-property is easy to satisfy. The "Γ_1"-property costs more effort and will be further discussed now. In the next definition the Γ_1-property for Y is defined.

Definition 6. Let $X \subseteq P$ and $Y \subseteq \mathcal{E}$. Let $\mathbf{c}^{i,j} \in GF(q)^{p[P]}, (i,j) \in \mathcal{E}$, define the set of vectors C. Then $C[X,Y]$ is defined as a matrix consisting of the $|Y|$ rows $\mathbf{c}^{i,j}_{X^c} \in GF(q)^{p[X^c]}$ with $(i,j) \in Y$. The corresponding matrix $I[X,Y]$ has rows $I[X,Y]_l \in GF(q)^k$, for $1 \leq l \leq |Y|$, defined by $I[X,Y]_l = \mathbf{e}^j$ iff there exists an i such that $C[X,Y]_l = \mathbf{c}^{i,j}_{X^c}$. Set C is said to satisfy the Γ_1-property for Y and $X \in \Gamma_1$ if the columns of $I[X,Y]$ can be written as linear combinations of the columns of $C[X,Y]$, that is if

$$\exists_{A \in GF(q)^{p[X^c] \times k}} \; I[X,Y] = C[X,Y]A.$$

Set C is said to satisfy the Γ_1-property for Y if it satisfies the Γ_1-property for Y and all $X \in \Gamma_1$.

The following theorem is about the relation between the "Γ_1"-property and the Γ_1-property for Y.

Theorem 7. *Set C satisfies the "Γ_1"-property iff C satisfies the Γ_1-property for $\mathcal{E}$.*

The last theorem is about an inductive relation with which the algorithm in Section 5 systematically searches for vectors also satisfying the "Γ_1"-property.

Theorem 8. *Let C, consisting of vectors $\mathbf{c}^{i,j}, (i,j) \in \mathcal{E}$, satisfy the Γ_1-property for $Y \neq \emptyset$ and $X \in \Gamma_1$. Let A be a matrix such that $I[X,Y] = C[X,Y]A$. Let $C_Z[X,Y]$ be defined as a matrix consisting of columns which form a basis of the zero space of $C[X,Y]$ (i.e. a basis of $\{\mathbf{c} \in GF(q)^{p[X^c]} : C[X,Y]\mathbf{c}^T = \mathbf{0}\}$). Let $(i,j) \notin Y$. Then C satisfies the Γ_1-property for $Y \cup \{(i,j)\}$ and $X \in \Gamma_1$ iff*

- $\mathbf{c}^{i,j}_{X^c} A = \mathbf{e}^j$ *or*
- *there exists a column* $\mathbf{b}$ *of* $C_Z[X,Y]$ *such that* $\mathbf{c}^{i,j}_{X^c}\mathbf{b} \neq 0$.

4 Dual Access Structures

In this section the proofs are omitted and can be found in [9]. In the next definition we define a notion of duality for an access structure (see [16]).

Definition 9. Let Γ be an access structure on P. Then the dual of Γ is defined as

$$\Gamma^\perp = \{X^c : X \in \Gamma^c\}.$$

The following properties concern the structure of $\Gamma^\perp$ (see [16, Lemma 3] as well).

Property 10. *Let Γ be an access structure. Then (i) $\Gamma^\perp$ is an access structure. (ii) $\Gamma_0^\perp = \{X^c : X \in \Gamma_1\}$. (iii) $\Gamma_1^\perp = \{X^c : X \in \Gamma_0\}$. (iv) $\Gamma^{\perp\perp} = \Gamma$. (v) $\Gamma^\perp = \{X : \forall_{Y \in \Gamma_0} X \cap Y \neq \emptyset\}$. (vi) $\Gamma_0^\perp = \{X : \forall_{x \in X} \exists_{Y \in \Gamma_0} X \cap Y = \{x\}$ and $\forall_{Y \in \Gamma_0} X \cap Y \neq \emptyset\}$.*

The following theorem characterizes suitable sets of vectors for an access structure by using the dual access structure (its proof uses Theorem 7).

Theorem 11. *Let Γ be an access structure on P. Let $\Gamma_0 = \{X_1, \ldots, X_r\}$ and $(\Gamma^\perp)_0 = \{Z_1, \ldots, Z_t\}$. We define $\mathcal{E}^\perp$ as $\mathcal{E}^\perp = \{(m,j) : 1 \leq m \leq t, 1 \leq j \leq k\}$. Let $C = \{\mathbf{c}^{i,j} \in GF(q)^{p[P]} : (i,j) \in \mathcal{E}\}$ and $H = \{\mathbf{h}^{m,j} \in GF(q)^{p[P]} : (m,j) \in \mathcal{E}^\perp\}$ be sets of vectors. Then $C[X]$, for $X \in \Gamma_0$, is defined as a $k \times p[P]$ q-ary matrix consisting of the k rows $C[X]_j = \mathbf{c}^{i,j}$, $1 \leq j \leq k$, with $X = X_i$. Similarly $H[Z]$, for $Z \in (\Gamma^\perp)_0$, is defined as a $k \times p[P]$ q-ary matrix consisting of the k rows $H[Z]_j = \mathbf{h}^{i,j}$, $1 \leq j \leq k$, with $Z = Z_i$.*

Then set C is suitable for Γ iff

- *C satisfies the Γ_0-property and*
- *there exists a set H satisfying the $(\Gamma^\perp)_0$-property such that*
- *$\forall_{Z \in (\Gamma^\perp)_0} \forall_{X \in \Gamma_0}$ $C[X]H[Z]^T = -I_k$.*

Secondly there exists a suitable set C for Γ iff there exists a suitable set H for $\Gamma^\perp$.

This immediately leads to the following corollary.

Corollary 12. *For integer k and prime power q we define $GL(k,q)$ as the set of all invertible $k \times k$ matrices over $GF(q)$. Then there exists a generalized vector space construction for Γ on $P = \{1, \ldots, n\}$ leading to an ideal perfect secret sharing scheme (i.e. a perfect secret sharing scheme for which the information rate equals 1) iff for some integer k and prime power q there exist matrices $M_0^{X,u} \in GL(k,q)$, for $X \in \Gamma_0$ and $u \in X$, and matrices $M_1^{Z,u} \in GL(k,q)$, for $Z \in (\Gamma^\perp)_0$ and $u \in Z$, such that for all $X \in \Gamma_0$ and $Z \in (\Gamma^\perp)_0$*

$$\sum_{u \in X \cap Z} M_0^{X,u} M_1^{Z,u} = I_k.$$

Hence, if there exists a prime p such that $\forall_{X \in \Gamma_0} \forall_{Y \in \Gamma_0^\perp} |X \cap Y| \equiv 1\ (p)$ then there exists an ideal perfect secret sharing scheme for Γ (e.g. $\Gamma_0 = \{ \{1,2,3\}, \{1,4,5\}, \{2,4,6\}, \{3,5,6\}\} = \Gamma_0^\perp$). As an other consequence of Theorem 11 we conclude that here exists a generalized vector space construction for access structure Γ realizing information rate r and average information rate $\tilde{r}$ iff there exists a generalized vector space construction for $\Gamma^\perp$ realizing information rate r and average information rate $\tilde{r}$. Jackson and Martin proved this result by using the geometrical approach [12]. The diagram of Figure 1 shows the relation between the generalized vector space construction for Γ, the generalized vector space construction for $\Gamma^\perp$, and their code descriptions.

5 An Algorithm

Let Γ be an access structure. We will give an outline of an algorithm which decides whether there exists a suitable set of vectors $C = \{\mathbf{c}^{i,j} : (i,j) \in \mathcal{E}\}$ or not, given q, k, and p_i for $i \in P$. If so, the algorithm produces a corresponding generalized vector space construction for Γ. The basic idea is to check if a set of vectors $\{\mathbf{c}^{i,j} : (i,j) \in$

$$\begin{tikzcd}
 & \mathcal{PS}(\Gamma, \mathcal{S}) \arrow[r, dash, "\mathrm{T11}"] \arrow[d, dash, "\mathrm{T1}"] & \mathcal{PS}(\Gamma^{\perp}, \mathcal{S}) \arrow[d, dash, "\mathrm{T1}"] & \\
\mathcal{C}^{\perp} \arrow[r, dash, "\mathrm{T5}"] \arrow[d, dash] & G \arrow[r, dash] & G' \arrow[r, dash, "\mathrm{T5}"] & \mathcal{C}'^{\perp} \supseteq \mathcal{C} \arrow[d, dash] \\
\mathcal{C} \arrow[r, dash, "\mathrm{T5}"] & C \arrow[r, dash, "\mathrm{T11}"] & C'(= H) \arrow[r, dash, "\mathrm{T5}"] & \mathcal{C}' \subseteq \mathcal{C}^{\perp}
\end{tikzcd}$$

Fig. 1. Correspondence between the duality of access structures and the duality of codes

$Y\}$ gives rise to a suitable set of vectors by using Theorem 8 and its proof (see [9] or the Appendix). We introduce two arrays, $A[X,Y]$ and $B[X,Y]$ for $X \in \Gamma_1$ and $Y \subseteq \{y_1, \ldots, y_{|\Gamma_0|k}\} = \mathcal{E}$, of global variables for which $I[X,Y] = C[X,Y]A[X,Y]$ and $C_Z[X,Y] = B[X,Y]$ are invariants. Other invariants of the algorithm are C satisfies the Γ_0-property and C satisfies the Γ_1-property for Y where $Y = \{y_1, \ldots, y_m\}$ for some m. Initially $Y = \emptyset$. The outline of the algorithm is as follows:

Step 1: If $m < |\Gamma_0|k$ take $(i,j) = y_{m+1}$ and continue with Step 2. If $m = |\Gamma_0|k$ then the set of vectors C is suitable. Hence, we can construct a perfect secret sharing scheme by using the generalized vector space construction (cf. Theorems 1 and 5). After having done this the algorithm stops.

Step 2: Check for all $X \in \Gamma_1$ if
- $\mathrm{c}^{i,j}_{X^c} A[X,Y] = e^j$ or
- $(\mathrm{c}^{i,j}_{X^c} B[X,Y])_l \neq 0$ for some l.

If so compute $B[X, Y \cup \{(i,j)\}]$ and $A[X, Y \cup \{(i,j)\}]$ (using the proof of Theorem 8), increase m, i.e. $m := m+1$ (hence, $Y := Y \cup \{(i,j)\}$), and continue with Step 1. If not continue with Step 3.

Step 3: Compute the next possible $\mathrm{c}^{i,j}$, leaving the Γ_0-property as an invariant, and continue with Step 2. If there does not exist a next possible $\mathrm{c}^{i,j}$ and $m \neq 1$ we decrease m, we take $(i,j) = y_m$, and we repeat Step 3 (this is backtracking). If there does not exist a next possible $\mathrm{c}^{i,j}$ and $m = 1$ then there does not exist a suitable set of vectors and the algorithm stops.

It is possible to speed up the algorithm by using some properties mentioned in [9]. The storage complexity is $O(p[P]^2|\Gamma_0||\Gamma_1|k)$. The worst case computing complexity of the algorithm is at most $O(p[P]^2|\Gamma_1|q^{ks})$ where $s = -p[P] + \sum_{X \in \Gamma_0} p[X]$. Thus it may be fruitful to apply the algorithm to $\Gamma^{\perp}$ and use Theorem 11 afterwards. Usage of the algorithm leads to the example of Section 2. Other examples can be found in [9]. An implementation of the algorithm can be found in [10].

6 Concluding Remarks and Acknowledgement

We have constructed perfect secret sharing schemes by using linear block codes. We show how to implement these ideas into an algorithm. As a side result we prove a correspondence between the duality of access structures and the duality of codes, which leads to useful quadratic matrix equations. The author wishes to thank Perry Moerland for implementing the algorithm of Section 5 and Henk van Tilborg for his comments which improved the presentation.

References

1. Michael Bertilsson. *Linear Codes and Secret Sharing.* PhD thesis, Linköping University, 1993.
2. Michael Bertilsson and Ingemar Ingemarsson. "A Construction of Practical Secret Sharing Schemes using Linear Block Codes". In *Advances in Cryptology – Auscrypt '92*, pages 67–79, 1992.
3. G.R. Blakley and G.A. Kabatianskii. "Linear Algebra Approach to Secret Sharing Schemes". In *PreProceedings of Workshop on Information Protection*, December 1993. Moscow.
4. C. Blundo. "Secret Sharing Schemes for Access Structures based on Graphs". Tesi di Laurea, 1991. (in Italian).
5. E.F. Brickell. "Some ideal secret sharing schemes". *J. Combin. Math. and Combin. Comput.*, 9:105–113, 1989.
6. E.F. Brickell and D.R. Stinson. "Some Improved Bounds on the Information Rate of Perfect Secret Sharing Schemes". *J. Cryptology*, 5:153–166, 1992.
7. R.M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. "On the Size of Shares for Secret Sharing Schemes". *J. Cryptology*, 6:157–167, 1993.
8. Marten van Dijk. "On the Information Rate of Perfect Secret Sharing Schemes", November 1993. submitted to Designs, Codes, and Cryptology.
9. Marten van Dijk. "A Linear Construction of Perfect Secret Sharing Schemes", April 1994. submitted to Designs, Codes, and Cryptology.
10. Marten van Dijk and Perry Moerland. "An Algorithm for finding Perfect Secret Sharing Schemes". In preparation as a technical report.
11. R.G. Gallager. *Information Theory and Reliable Communications.* John Wiley, New York, 1968.
12. W.-A. Jackson and K. Martin. "Geometric Secret Sharing Schemes and Their Duals". *Designs, Codes and Cryptology*, pages 83–95, 1994.
13. K.M. Martin. *Discrete Structures in the Theory of Secret Sharing.* PhD thesis, Royal Holloway and Bedford New College, University of London, 1991.
14. K.M. Martin. "New secret sharing schemes from old". *Journal of Combin. Math. and Combin. Comput.*, 14:65–77, 1993.
15. James L. Massey. "Minimal Codewords and Secret Sharing". In *Proc. 6th Joint Swedish-Russian Int. Workshop on Inf. Th. 1993*, pages 276–279, 1993.
16. G.S. Simmons, W.-A. Jackson, and K. Martin. "The Geometry of Shared Secret Schemes". *Bulletin of the Institute of Combinatorics and its Application*, pages 71–88, 1991.
17. D.R. Stinson. "Decomposition Constructions for Secret Sharing Schemes". *IEEE Trans. Inform. Theory*, Vol. IT-40:118–125, January 1994.

A Appendix

Proof of the first statement of Theorem 5: In the sequel $\Gamma_0 = \{X_1, \ldots, X_r\}$. We are going to investigate the structure of $\mathcal{C}$ defined by (3). We infer from (1) that for $(i,j) \in \mathcal{E}$ there exists a vector $\mathbf{b}^{i,j} \in GF(q)^{p[X_i]}$ such that $(\mathbf{e}^j, 0)^T = G[X_i]\mathbf{b}^{i,j^T}$, where $\mathbf{e}^j$ is the j-th unit vector in $GF(q)^k$. Let $\mathbf{c}^{i,j} \in GF(q)^{p[P]}$ be the vector defined by $\mathbf{c}^{i,j}_{X_i} = -\mathbf{b}^{i,j}$ and $sup_p(\mathbf{c}^{i,j}) \subseteq X_i$ (i.e. $\mathbf{c}^{i,j}_{X_i^c} = 0$). Then $(\mathbf{e}^j, \mathbf{c}^{i,j}) \in \mathcal{C}$. We will prove that $C = \{\mathbf{c}^{i,j} : (i,j) \in \mathcal{E}\}$ is a suitable set of vectors.

Let $B_{i,j} \in GF(q)$ for $(i,j) \in \mathcal{E}$. Then the linear combination

$$(\mathbf{s}, \mathbf{c}) = \sum_{(i,j)\in\mathcal{E}} B_{i,j}(\mathbf{e}^j, \mathbf{c}^{i,j}) = \Big(\sum_{1\le i\le r} B_{i,1}, \ldots, \sum_{1\le i\le r} B_{i,k}, \sum_{(i,j)\in\mathcal{E}} B_{i,j}\mathbf{c}^{i,j}\Big)$$

is in $\mathcal{C}$, and hence $(\mathbf{s}, 0)^T = -G[P]\mathbf{c}^T$ by (3). Thus

$$(\mathbf{s}, 0)^T = G[sup_p(\mathbf{c})](-\mathbf{c}_{sup_p(\mathbf{c})})^T.$$

From (2) we infer that if $sup_p(\mathbf{c}) \notin \Gamma$ then $\mathbf{s} = 0$. So either $\mathbf{s} = 0$ or $sup_p(\mathbf{c}) \in \Gamma$. Hence, either $\sum_{1\le i\le r} B_{i,j} = 0$ for all $1 \le j \le k$ or there exists a set $X \in \Gamma_0$ such that $X \subseteq sup_p(\mathbf{c})$. Hence, C satisfies the "Γ_1"-property.

Let us consider the codewords $(\mathbf{e}^j, \mathbf{c}^{i,j}) \in \mathcal{C}$ again. By the property proved in the paragraph above there exists a set $X \in \Gamma_0$ such that $X \subseteq sup_p(\mathbf{c}^{i,j})$. Also $sup_p(\mathbf{c}^{i,j}) \subseteq X_i \in \Gamma_0$, and hence $X \subseteq X_i$. Since Γ_0 consists of the minimal elements of Γ equality $X = X_i$ holds. Thus $\mathrm{sup}_p(\mathbf{c}^{i,j}) = X_i$. Hence C satisfies the Γ_0-property as well. Now we have proved that $\mathcal{C}$ contains codewords $(\mathbf{e}^j, \mathbf{c}^{i,j})$, $(i,j) \in \mathcal{E}$, such that $\{\mathbf{c}^{i,j} : (i,j) \in \mathcal{E}\}$ is a suitable set of vectors.

Proof of the second statement of Theorem 5: Let $\{\mathbf{c}^{i,j} : (i,j) \in \mathcal{E}\}$ be a suitable set of vectors. Define code $\mathcal{C}$ of length $k + p[P]$ over $GF(q)$ by the linear span of the vectors $(\mathbf{e}^j, \mathbf{c}^{i,j})$. Let H be a parity check matrix of $\mathcal{C}$. We will prove

$$H(\mathbf{s}, \mathbf{c})^T = \mathbf{0}^T \Rightarrow (\mathbf{s} = \mathbf{0} \vee sup_p(\mathbf{c}) \in \Gamma). \qquad (4)$$

If $H(\mathbf{s}, \mathbf{c})^T = \mathbf{0}^T$ then $(\mathbf{s}, \mathbf{c}) \in \mathcal{C}$. Hence, for $(i,j) \in \mathcal{E}$ there exist $B_{i,j} \in GF(q)$ such that

$$(\mathbf{s}, \mathbf{c}) = \sum_{(i,j)\in\mathcal{E}} B_{i,j}(\mathbf{e}^j, \mathbf{c}^{i,j}),$$

i.e. $\mathbf{s}_j = \sum_{1\le i\le r} B_{i,j}$ for $1 \le j \le k$ and $\mathbf{c} = \sum_{(i,j)\in\mathcal{E}} B_{i,j}\mathbf{c}^{i,j}$. If $sup_p(\mathbf{c}) \notin \Gamma$ then $\neg(\exists_{X\in\Gamma_0}\, X \subseteq sup_p(\mathbf{c}))$ and hence, by Definition 4, $\sum_{1\le i\le r} B_{i,j} = 0$ for all $1 \le j \le k$, i.e. $\mathbf{s} = \mathbf{0}$. This proves (4). Since $sup_p(\mathbf{0}) = \emptyset \notin \Gamma$

$$H(\mathbf{s}, \mathbf{0})^T = \mathbf{0}^T \Rightarrow \mathbf{s} = \mathbf{0}.$$

In other words the first k columns of H are independent. Hence, by elementary row operations H can be put into the form

$$H = \left(\begin{array}{c|c} I_k & \multirow{2}{*}{H'} \\ O & \end{array}\right).$$

Now, define the matrices $G_i, 1 \le i \le n$, by $G[P] = H'$.

Let $X \notin \Gamma$ and let $(\mathbf{s}, \mathbf{0})^T = G[X]\mathbf{b}^T$. Let vector $\mathbf{c}$ be defined by $\mathbf{c}_X = -\mathbf{b}$ and $sup_p(\mathbf{c}) \subseteq X$ (i.e. $\mathbf{c}_{X^c} = \mathbf{0}$), so $H(\mathbf{s}, \mathbf{c})^T = \mathbf{0}^T$. From (4) and $sup_p(\mathbf{c}) \notin \Gamma$ we infer that $\mathbf{s} = \mathbf{0}$. Hence (2) is satisfied.

Let $X \in \Gamma$. Then there exists a set $X_i \in \Gamma_0$ with $X_i \subseteq X$. Let $1 \leq j \leq k$. By the definition of code $\mathcal{C}$ equality $H(\mathbf{e}^j, \mathbf{c}^{i,j})^T = \mathbf{0}^T$, with $sup(\mathbf{c}^{i,j}) = X_i$, holds. Hence, $(\mathbf{e}^j, \mathbf{0}) = G[P](-\mathbf{c}^{i,j})^T$. So the j-th unit vector in $GF(q)^l$, $1 \leq j \leq k$, can be expressed as a linear combination of columns of matrix $G[X]$. Hence (1) is satisfied.

Proof of Theorem 7: We notice that the set of rows of $C[\emptyset, \mathcal{E}]$ is equal to C. The rows of $I[\emptyset, \mathcal{E}]$ are the corresponding unit vectors. Let B be a $r \times k$ q-ary matrix. Let vector $\mathbf{b} \in GF(q)^{|\mathcal{E}|}$ be defined as the concatenation of the columns of B. Thus $\mathbf{b}$ consists of all coordinates in B. Then w.l.o.g. $(\mathbf{b}I[\emptyset, \mathcal{E}])_j$ equals the addition of the elements of column j in B, and $\sum_{(i,j)\in\mathcal{E}} B_{i,j}\mathbf{c}^{i,j} = \mathbf{b}C[\emptyset, \mathcal{E}]$. So the "$\Gamma_1$"-property is equivalent to each of the following equivalent statements

$$\forall_{\mathbf{b}\in GF(q)^{|\mathcal{E}|}} \ [\mathbf{b}I[\emptyset, \mathcal{E}] \neq \mathbf{0} \Rightarrow \exists_{X\in\Gamma_0} \ X \subseteq sup_p(\mathbf{b}C[\emptyset, \mathcal{E}])],$$
$$\forall_{\mathbf{b}\in GF(q)^{|\mathcal{E}|}} \ [(\forall_{X\in\Gamma_0} \ X \nsubseteq sup_p(\mathbf{b}C[\emptyset, \mathcal{E}])) \Rightarrow \mathbf{b}I[\emptyset, \mathcal{E}] = 0],$$
$$\forall_{\mathbf{b}\in GF(q)^{|\mathcal{E}|}} \ [(\exists_{X\in\Gamma_1} \ sup_p(\mathbf{b}C[\emptyset, \mathcal{E}]) \subseteq X) \Rightarrow \mathbf{b}I[\emptyset, \mathcal{E}] = 0],$$
$$\forall_{X\in\Gamma_1} \ \forall_{\mathbf{b}\in GF(q)^{|\mathcal{E}|}} \ [sup_p(\mathbf{b}C[\emptyset, \mathcal{E}]) \subseteq X \Rightarrow \mathbf{b}I[\emptyset, \mathcal{E}] = 0],$$
$$\forall_{X\in\Gamma_1} \ \forall_{\mathbf{b}\in GF(q)^{|\mathcal{E}|}} \ [\mathbf{b}C[X, \mathcal{E}] = \mathbf{0} \Rightarrow \mathbf{b}I[X, \mathcal{E}] = 0].$$

In other words for all $X \in \Gamma_1$ the zero space of $C[X, \mathcal{E}]^T$ is contained in the zero space of $I[X, \mathcal{E}]^T$ which is by elementary matrix theory equivalent to the Γ_1-property for $\mathcal{E}$, $\forall_{X\in\Gamma_1} \ \exists_A \ I[X, \mathcal{E}] = C[X, \mathcal{E}]A$.

Proof of Theorem 8: Let

$$C[X, Y \cup \{(i,j)\}] = \begin{pmatrix} C[X, Y] \\ \mathbf{c}^{i,j}_{X^c} \end{pmatrix}.$$

If $\mathbf{c}^{i,j}_{X^c}A = \mathbf{e}^j$ then $I[X, Y \cup \{(i,j)\}] = C[X, Y \cup \{(i,j)\}]A$, i.e. C satisfies the Γ_1-property for $Y \cup \{(i,j)\}$ and X. Now we first show that if $\mathbf{c}^{i,j}_{X^c}A \neq \mathbf{e}^j$ and C satisfies the Γ_1-property for $Y \cup \{(i,j)\}$ and X then there exists a column $\mathbf{b}$ of $C_Z[X, Y]$ such that $\mathbf{c}^{i,j}_{X^c}\mathbf{b} \neq 0$. Secondly we show that if there exists a column $\mathbf{b}$ of $C_Z[X, Y]$ such that $\mathbf{c}^{i,j}_{X^c}\mathbf{b} \neq 0$ then C satisfies the Γ_1-property for $Y \cup \{(i,j)\}$ and X, which finishes the proof.

Let $\mathbf{c}^{i,j}_{X^c}A \neq \mathbf{e}^j$. Suppose that C satisfies the Γ_1-property for $Y \cup \{(i,j)\}$ and X, i.e.

$$I[X, Y \cup \{(i,j)\}] = C[X, Y \cup \{(i,j)\}]A'$$

for some matrix A'. Then $\mathbf{e}^j = \mathbf{c}^{i,j}_{X^c}A'$ and $C[X, Y](A' - A) = O$, the all zero matrix. Hence, the columns of $A' - A$ are in the zero space of $C[X, Y]$. Thus $A' = A + C_Z[X, Y]D$ for some matrix D. Also $0 \neq \mathbf{e}^j - \mathbf{c}^{i,j}_{X^c}A = \mathbf{c}^{i,j}_{X^c}(A' - A) = \mathbf{c}^{i,j}_{X^c}C_Z[X, Y]D$. Such a matrix D only exists if $\mathbf{c}^{i,j}_{X^c}C_Z[X, Y] \neq \mathbf{0}$ or equivalently if there exists a column $\mathbf{b}$ in $C_Z[X, Y]$ such that $\mathbf{c}^{i,j}_{X^c}\mathbf{b} \neq 0$.

Let $\mathbf{b}$ be a column in $C_Z[X, Y]$ such that $\mathbf{c}^{i,j}_{X^c}\mathbf{b} \neq 0$. Since $C[X, Y](A + \mathbf{b}(\mathbf{c}^{i,j}_{X^c}\mathbf{b})^{-1} (\mathbf{e}^j - \mathbf{c}^{i,j}_{X^c}A)) = I[X, Y]$ and $\mathbf{c}^{i,j}_{X^c}(A + \mathbf{b}(\mathbf{c}^{i,j}_{X^c}\mathbf{b})^{-1} (\mathbf{e}^j - \mathbf{c}^{i,j}_{X^c}A)) = \mathbf{e}^j$

$$I[X, Y \cup \{(i,j)\}] = C[X, Y \cup \{(i,j)\}](A + \mathbf{b}(\mathbf{c}^{i,j}_{X^c}\mathbf{b})^{-1}(\mathbf{e}^j - \mathbf{c}^{i,j}_{X^c}A)).$$

Hence, C satisfies the Γ_1-property for $Y \cup \{(i,j)\}$ and X.