On the Composition of Secret Sharing Schemes Related to Codes

I. Márquez-Corbella[1], E. Martínez-Moro[2] and E. Suárez-Canedo[2]

[1]Department of Algebra, Geometry and Topology, Institute of Mathematics (IMUva), University of Valladolid, Castilla, Spain.
imarquez@agt.uva.es
[2]Department of Applied Mathematics, Institute of Mathematics (IMUva), University of Valladolid, Castilla, Spain.
edgar@maf.uva.es and emiliosuarezcanedo@gmail.com

Abstract

In this paper we construct a subclass of the composite access structure introduced in [9] based on schemes realizing the structure given by the set of codewords of minimal support of linear codes. This class enlarges the iterated threshold class studied in the same paper. Furthermore all the schemes on this paper are ideal (in fact they allow a vector space construction) and we arrived to give a partial answer to a conjecture stated in [9]. Finally, as a corollary we proof that all the monotone access structures based on all the minimal supports of a code can be realized by a vector space construction.

Keywords. Cryptography, Secret Sharing Schemes, Threshold Schemes.
2000 MSC. 94A60.

1 Introduction

We will use the following notation. Let $\mathcal{P} = \{P_i\}_{i=1}^n$ be a set of participants, $\mathcal{K}$ be the set of all possible keys and $\mathcal{S}$ be the share sets. *Secret sharing schemes* are used to distribute a secret $K \in \mathcal{K}$, like a private key of a cryptosystem, among a group of individuals $\mathcal{P}$, giving to each participant a share from $\mathcal{S}$, such that only specified subsets of $\mathcal{P}$ are able to determine the secret K from joining the shares they hold.

Let $\Gamma \subseteq 2^{\mathcal{P}}$ be the family of subsets of $\mathcal{P}$ which are able to reconstructed the secret (i.e. *authorized or qualified subsets*) then Γ is called the *access structure* of the scheme. Since Γ is presupposed to satisfy the *monotone property* (that is, if $A \subseteq B \subseteq \mathcal{P}$ and $A \in \Gamma$, then $B \in \Gamma$) then the set of minimal authorized subset of Γ, denoted by Γ^m, determines a basis of Γ. The

dual of the access structure Γ on the set $\mathcal{P}$ is defined as the access structure form by the subsets whose complements are not authorized, i.e.

$$\Gamma^* = \{A \subseteq \mathcal{P} \mid \mathcal{P} \setminus A \notin \Gamma\}.$$

A *perfect* sharing scheme avoid unauthorized coalitions to learn any information about the secret. Ito, Saito and Nishizeki [7] showed that for any arbitrary monotone collection of authorized set Γ, there exists a perfect sharing scheme that realizes Γ. Moreover, a secret sharing scheme is *ideal* if it is perfect and the domain of shares of each user is $\mathcal{S}$. An access structure Γ is called *ideal* if there is an ideal scheme realizing it.

An interesting class of access structure are those admitting a *vector space construction*, this structure is due to Brickell [3]. Let $\mathbb{F}_q$ be a finite field with q elements, an access structure Γ on $\mathcal{P}$ has a *vector space construction* over $\mathbb{F}_q$ if there exists a map $\Phi : \mathcal{P} \longrightarrow \mathbb{F}_q^d$ and a vector $\mathbf{v} \in \mathbb{F}_q^d \setminus \{0\}$ such that the vector $\mathbf{v}$ can be expressed as a linear combination of vectors in the set $\{\Phi(\mathcal{P}_i) \mid \mathcal{P}_i \in A\}$ if and only if $A \in \Gamma$. Schemes realizing this structures are called *vector space secret sharing schemes*. In sake of simplicity and without lost of generality usually $\mathbf{v}$ is taken to be the vector $\mathbf{e}_1 = (1, \mathbf{0})$. Unfortunately finding a rule for deciding when an access structure Γ admits a vector space construction is still an open problem if the underlying field is not fixed.

The first examples of secret sharing schemes that appeared on the literature were examples of *threshold schemes*. The access structure of an (t, n)-threshold scheme is formed by subsets of participants whose cardinality is at least t. These schemes were introduced independently by Shamir [13] and Blakley [2] in 1979. Shamir's scheme used polynomial interpolation while Blakley's method is based on intersection properties of finite geometries, indeed both ideas where behind or related to the use of Reed-Solomon codes. Threshold schemes are ideal, admit a vector space construction and give the same opportunity to all the participants to access the secret. Indeed taking n different non-zero elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ and Φ defined by $\Phi(P_i) = (1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^{d-1}) \in \mathbb{F}_q^d$ for all $i \in \{1, \ldots, n\}$ then the (t, n)-threshold scheme can be seen as a vector space secret sharing schemes.

From now on, the expression (t, n) will denote a (t, n)-threshold scheme. In real life, not all participants are in the same hierarchy and they do not have the same privileges to access certain secrets. This idea has been adapted to secret sharing Schemes by various authors. For instance, *multilevel schemes* by Simmons [14], *bipartite structures* by Padró and Sáez [11] or *compartmented schemes* by Brickell [3].

In this article we will used a special construction of this type of schemes presented in [9] called *composition of access structures*. Let $\mathcal{P} = \mathcal{P}_1 \cup \ldots \cup \mathcal{P}_s$ be a partition of $\mathcal{P}$ into disjoints sets where $\mathcal{P}_j$ is given by the set $\{P_1^{(j)}, \ldots, P_{n_j}^{(j)}\}$ and $n = n_1 + \ldots + n_r$. Let Γ_0 be an access structure on

$\mathcal{P}$ and Γ_i be an access structure on $\mathcal{P}_i$ for $i \in \{1, \ldots, r\}$, then the *composite access structure* of $\Gamma_1, \ldots, \Gamma_r$ following Γ_0, denoted by $\Gamma_0[\Gamma_1, \ldots, \Gamma_r]$ is defined as follows:

$$\Gamma_0[\Gamma_1, \Gamma_2, \ldots, \Gamma_r] = \bigcup_{B \in \Gamma_0} \{A \subseteq \mathcal{P} \mid A \cap \mathcal{P}_i \in \Gamma_i \text{ for all } \mathcal{P}_i \in B\}. \quad (1)$$

Let us briefly fix the notation and introduce some basic definitions from coding theory. A *linear code* $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_q$, or an $[n, k]$ code for short, is a k-dimensional subspace of $\mathbb{F}_q^n$. For every codeword $\mathbf{c} \in \mathcal{C}$ its suport is define as its support as a vector in $\mathbb{F}_q$, i.e. $\text{supp}(\mathbf{c}) = \{i \mid c_i \neq 0\}$. A codeword $\mathbf{c}$ is a *minimal support codeword* of $\mathcal{C}$ if it is non-zero and $\text{supp}(\mathbf{c})$ is not contained in the support of any other codeword. We will denote by $\mathcal{C}^m$ the set of codewords of minimal support of $\mathcal{C}$. Note that describing the set of codewords with minimum hamming weight in an arbitrary linear code is an NP-hard problem [1] even if preprocessing is allowed [5]. Some improvements on their computation have been recently made in [8].

There are several ways to obtain a secret sharing using a linear code $\mathcal{C}$, we refer the reader to [6, 10, 12]. It is not difficult to show that a vector space construction is equivalent to a code in the following sense: consider the matrix whose first column is the vector assigned to the dealer and the rest of columns are the vector assigned to the participants, this matrix can be seen as a parity check matrix of a code $\mathcal{C}$ and the authorized subsets are those codeword supports containing a non-zero element on the first position.

In this paper we give a slightly different definition to the previous one. We define the access structure related to the $[n, k]$ code $\mathcal{C}$ over $\mathcal{P}$ with $|\mathcal{P}| = n$, and we denote it by $\Gamma_{\mathcal{C}}$, as the set

$$\Gamma_{\mathcal{C}} = \left\{ A \subseteq \mathcal{P} \mid \exists \mathbf{c} \in \mathcal{C} \setminus \{0\} \ : \ A = \bigcup_{i \in \text{supp}(\mathbf{c})} P_i \right\}.$$

With this definition we study the composite access structures of the form $\Gamma_0[\Gamma_{\mathcal{C}_1}, \Gamma_{\mathcal{C}_2}, \ldots, \Gamma_{\mathcal{C}_r}]$. We enlarge the well known class of iterated threshold structures in [9]. The main result is that this structure admits a vector space construction when Γ_0 admits a vector space construction. This class of structures gives a partial answer to the conjecture in [9, Open Problem 2] and they are more "natural" that the one proposed in it since the dealer appears only in one of the components and therefore there is no need of projecting the shares. As a corollary we obtain that $\Gamma_{\mathcal{C}}$ also admits a vector space construction.

2 Composition of structures related to linear codes

Let $\{\mathcal{C}_i\}_{i=1}^r$ be a set of linear $\mathbb{F}_q$ codes each one of length n_i and dimension k_i for $i = 1, \ldots, r$. For each code $\mathcal{C}_i$ we define the access structure related to $\mathcal{C}_i$ over the set of participants $\mathcal{P}_i = \{P_1^i, P_2^i, \ldots, P_{n_i}^i\}$ as the set

$$\Gamma_{\mathcal{C}_i} = \Gamma_i := \left\{\{P_{j_1}^i, \ldots P_{j_s}^i\} \mid \exists \mathbf{c} \neq 0,\, \mathbf{c} \in \mathcal{C}_i \text{ such that } \mathrm{supp}(\mathbf{c}) = \{j_1, \ldots, j_s\}\right\}. \tag{2}$$

That is, the family of qualified subsets is in one to one correspondence with the supports associated to the codewords of $\mathcal{C}_i$ and indeed Γ_i^m is determined by the minimal support codewords of $\mathcal{C}_i$.

Definition 1. *Let $\mathcal{P}_i = \{P_1^i, P_2^i, \ldots, P_{n_i}^i\}$ be the set of participants related to the code $\mathcal{C}_i$ for $i = 1, \ldots, r$ and consider all of them disjoint. Let Γ_0 be an access structure over $\{\mathcal{P}_i\}_{i=1}^r$, we define the access struture $\Gamma_0[\mathcal{C}_1, \ldots, \mathcal{C}_s]$ over the set of participants $\mathcal{P} = \bigsqcup_{i=1}^s \mathcal{P}_i$ as the composite structure (see Equation 1 for a definition of composite structure)*

$$\Gamma_0[\mathcal{C}_1, \ldots, \mathcal{C}_s] = \Gamma_0[\Gamma_{\mathcal{C}_1}, \ldots, \Gamma_{\mathcal{C}_s}]. \tag{3}$$

Remark 1. *Note that the monotone access structures $\Gamma_{\mathcal{C}_i}$ are $\mathbb{F}_q$-matroid representable structures but not in the usual sense (see for example [4]) since they do not have a distinguished participant or a dealer. In our case all the supports in $\mathcal{C}$ are considered, not only those that include the first coordinate. Thus, by definition, it is not obvious that they can be realized by a vector space construction. We will show in Corollary 1 that this last statement is true.*

Remark 2. *If each $\mathcal{C}_i$ is taken to be the Reed-Solomon code $RS(n_i, k_i)$ of parameters $[n_i, k_i]$ and Γ_0 is a threshold secret sharing scheme then we recover the class of iterated threshold access structures defined in [9].*

Proposition 1. $(\Gamma_0[\mathcal{C}_1, \ldots, \mathcal{C}_s])^\star = \Gamma_0^\star[\mathcal{C}_1^\perp, \ldots, \mathcal{C}_s^\perp]$.

Proof. We know by [9, Proposition 2] that

$$(\Gamma_0[\Gamma_{\mathcal{C}_1}, \ldots, \Gamma_{\mathcal{C}_s}])^\star = \Gamma_0^\star[\Gamma_{\mathcal{C}_1}^\star, \ldots, \Gamma_{\mathcal{C}_s}^\star].$$

But the structure $\Gamma_{\mathcal{C}_i}^\star$ is representable by a code ($\mathbb{F}_q$-representable matroid) which is given by its dual code $\mathcal{C}_i^\perp$ and the result follows. □

Recall that we will denote by Γ^m the minimal qualified subsets in the access structure Γ and by $\mathcal{C}^m$ the subsets of participants in $\Gamma_{\mathcal{C}}$ related to minimal codewords of $\mathcal{C}$.

Proposition 2. $(\Gamma_0[\mathcal{C}_1, \ldots, \mathcal{C}_s])^m = \Gamma_0^m[\mathcal{C}_1^m, \ldots, \mathcal{C}_s^m]$.

Proof. It follows straightforward from the definitions and [9, Proposition 1]. □

3 Main Theorem

Lemma 1. *Let $\mathcal{C}$ be a $\mathbb{F}_q$-linear code of parameters $[n,k]$. There exists an $\mathbb{F}_{q^s}$-linear code $\mathcal{C}'$ of parameters $[n,k]$ fulfilling the following properties:*

1. $\Gamma_{\mathcal{C}} = \Gamma_{\mathcal{C}'}$.
2. *For each minimal support $S \in \{1,\dots,n\}$ of $\mathcal{C}'$ there exists a $\mathbf{m} \in (\mathcal{C}')^m$ with $\sum_{i=1}^n m_i \neq 0$ and $\mathrm{supp}(\mathbf{m}) = S$.*

Proof. Let $\Gamma_{\mathcal{C}}^m = \{A_1, A_2, \cdots, A_\alpha\}$ be the set of minimal qualified subsets of $\Gamma_{\mathcal{C}}$ w.r.t. some ordering. Let H be a parity check matrix of $\mathcal{C}$ where $\mathbf{h}_j$ denotes the j-th column with $j = 1,\dots,n$.

By definition A_1 is related to at least a codeword support of $\mathcal{C}$. Assume that all linear combination based on A_1 over $\mathbb{F}_q$ satisfy the following expression:

$$\textstyle\sum_{j=1}^n \lambda_j \mathbf{h}_j = 0 \quad \text{with} \quad \sum_{j=1}^n \lambda_j = 0 \ .$$

Then we proceed as follows:

1. Choose an arbitrary linear combination of the above set, say $\lambda_1^1,\dots,\lambda_n^1 \in \mathbb{F}_q$, where

$$\lambda_j^1 \neq 0 \text{ if } P_j \in A_1, \quad \textstyle\sum_{j=1}^n \lambda_j^1 \mathbf{h}_j = 0 \quad \text{and} \quad \sum_{j=1}^n \lambda_j^1 = 0.$$

2. Take a column $\mathbf{h}_j$ such that $\lambda_j^1 \neq 0$ and define the vector

$$\overline{\mathbf{h}_j} = \frac{1}{\gamma_1}\mathbf{h}_j$$

   in such a way that $\lambda_j^1\gamma_1$ is neither zero nor equal to $-\sum_{i=1}^n \lambda_i^1 + \lambda_j^1$. Note that in the binary case, $q = 2$, we need to enlarge the field to some $\mathbb{F}_{2^{s_1}}$.

3. Define the matrix H^1 obtained from H by replacing the vector $\mathbf{h}_j$ by $\overline{\mathbf{h}_j}$. Observe that H^1 defines the same linear dependence relations as H, since linear dependence behaves well when extending scalars to a field extension, and therefore both matrices realize the same access structure.

At the end of this process we have found a linear combination based on A_1 over $\mathbb{F}_{q^{s_1}}$ such that

$$\textstyle\sum_{j=1}^n \lambda_j^1 \mathbf{h}_j^1 = 0 \quad \text{and} \quad \sum_{j=1}^n \lambda_j^1 \neq 0,$$

where $\mathbf{h}_j^1$ denotes the j-th column of the matrix H^1 for $j = 1,\dots,n$.

Once we have modified the original code and probably the field of definition for the set A_1 we check A_2. If all linear combination based on A_2 over $\mathbb{F}_{q^{s_1}}$ satisfy the following expression:

$$\sum_{j=1} \lambda_j \mathbf{h}_j^1 = 0 \quad \text{with} \quad \sum_{j=1}^n \lambda_j = 0 \ .$$

Then we proceed as follows (otherwise we skip this step):

1. Choose an arbitrary linear combination of the above set, say $\lambda_1^2, \ldots, \lambda_n^2$ where

$$\lambda_j^2 \neq 0 \text{ if } P_j \in A_2, \quad \sum_{j=1}^n \lambda_j^2 \mathbf{h}_j^1 = 0 \quad \text{and} \quad \sum_{j=1}^n \lambda_j^2 = 0.$$

2. Take a column $\mathbf{h}_j^1$ such that $\lambda_j^2 \neq 0$ and define the vector

$$\overline{\mathbf{h}_j^1} = \frac{1}{\gamma_2} \mathbf{h}_j^1$$

in such a way that:

   (a) If $P_j \notin A_1$ then $\lambda_j^2 \gamma_2$ is neither zero nor equal to $-\sum_{i=1}^n \lambda_i^2 + \lambda_j$.

   (b) Otherwise $\lambda_j^2 \gamma_2$ has to be different from zero and from the values

$$-\sum_{i=1}^n \lambda_i^1 + \lambda_j^1 \quad \text{and} \quad -\sum_{i=1}^n \lambda_i^2 + \lambda_j^2 \ .$$

3. Define the matrix H^2 obtained from H^1 by replacing the column $\mathbf{h}_j^1$ by $\overline{\mathbf{h}_j^1}$. Again H^2 realize the same access structure as H^1 and H.

Similarly to the previous process, we obtain a linear combination based on A_2 over $\mathbb{F}_{q^{s_2}}$ such that

$$\sum_{j=1}^n \lambda_j^2 \mathbf{h}_j^2 = 0 \quad \text{and} \quad \sum_{j=1}^n \lambda_j^2 \neq 0 \ .$$

Let us now proceed by induction. Suppose that we have a parity check matrix H^l whose code (possibly defined in an extension of the scalars) realizes the structure $\Gamma_{\mathcal{C}}$ and for each A_i with $i \leq l$ there exists a linear combination of the corresponding rows to the supports of A_i with the sum of the coefficients different from zero. Suppose that for each linear combination based on A_{l+1} over $\mathbb{F}_{q^{s_l}}$ we have

$$\sum_{j=1}^n \lambda_j \mathbf{h}_j^l = \mathbf{0} \quad \text{with} \quad \sum_{j=1}^n \lambda_j = \mathbf{0}.$$

Then we choose an arbitrary linear combination of the above set, say $\lambda_1^{l+1}, \ldots, \lambda_n^{l+1}$, we take a column $\mathbf{h}_j^l$ of H^l corresponding to the support of A_{l+1} such that $\lambda_j^{l+1} \neq 0$ and we define

$$\overline{\mathbf{h}_j^l} = \frac{1}{\gamma_{l+1}} \mathbf{h}_j^l$$

where γ_{l+1} satisfy the following properties:

- If $P_j \notin \{A_1, \ldots, A_l\}$ then $\lambda_j^{l+1} \cdot \gamma^{l+1} \notin \left\{0, -\sum_{i=1}^n \lambda_i^{l+1} + \lambda_j^{l+1}\right\}$.
- If P_j is only in A_t and A_{l+1} with $t = 1, \ldots, l$ then

$$\lambda_j^{l+1} \cdot \gamma^{l+1} \notin \left\{0, -\sum_{i=1}^n \lambda_i^{l+1} + \lambda_j^{l+1}, -\sum_{i=1}^n \lambda_i^t + \lambda_j^t\right\}.$$

- ...
- If P_j is in $A_{i_1}, \ldots, A_{i_s}$ and A_{l+1} then

$$\lambda_j^{l+1} \cdot \gamma^{l+1} \notin \left\{0, -\sum_{i=1}^n \lambda_i^{l+1} + \lambda_j^{l+1}, -\sum_{i=1}^n \lambda_i^{i_1} + \lambda_j^{i_1}, \ldots, -\sum_{i=1}^n \lambda_i^{i_s} + \lambda_j^{i_s}\right\}.$$

- ...
- If P_j is in $A_1, \ldots, A_l, A_{l+1}$ then

$$\lambda_j^{l+1} \cdot \gamma^{l+1} \notin \left\{0, -\sum_{i=1}^n \lambda_i^{l+1} + \lambda_j^{l+1}, -\sum_{i=1}^n \lambda_i^1 + \lambda_j^1, \ldots, -\sum_{i=1}^n \lambda_i^l + \lambda_j^l\right\}.$$

The steps above could require to enlarge the field in order to get enough coefficients. We define H^{l+1} to be the matrix obtained by replacing $\overline{\mathbf{h}_j^l}$ by $\mathbf{h}_j^l$ in H^l. H^{l+1} defines the same linear dependence relations as $H^l, \ldots, H^1$ and H. Thus the induction step is proved and we can conclude the proof, i.e. in at most α steps we get a parity check matrix H^α defining a code with the required properties. □

Theorem 1. *If Γ_0 admits a vector space construction then also $\Gamma_0[\mathcal{C}_1, \ldots, \mathcal{C}_s]$ admits a vector space construction.*

Proof. Consider the map $\Phi_0 : \{\mathcal{P}_i\}_{i=1}^r \to \mathbb{F}_q^d$ that endows Γ_0 with a vector space construction. For each linear code $\mathcal{C}_i$ we consider the code $\mathcal{C}_i'$ that has as parity check matrix the matrix H_i constructed in the proof of Lemma 1, probably defined in some field extension of $\mathbb{F}_q$. We denote by $\mathbf{h}_j^i$ the j-th column of H_i. Now we consider the map $\Phi : \mathcal{P} \longrightarrow \mathbb{F}_{q^s}^{d+\sum_{i=1}^s n_i}$ defined by

$$\Phi(P_j^i) = (\Phi_0(\mathcal{P}_i), \mathbf{0}_{n_1}, \ldots, \mathbf{0}_{n_{j-1}}, \underbrace{(\mathbf{h}_j^i)^t}_{j+1\text{-th position}}, \mathbf{0}_{n_{j+1}}, \ldots, \mathbf{0}_{n_s}),$$

where $\mathbf{0}_l$ denotes the zero vector of length l. We shall prove that Φ endows $\Gamma = \Gamma_0[\mathcal{C}_1', \ldots, \mathcal{C}_s']$ with a vector space construction, and therefore also $\Gamma_0[\mathcal{C}_1, \ldots, \mathcal{C}_s]$ has a vector space construction since they define the same access structure by Lemma 1. Let $A \in \Gamma$ be a qualified set and

$B = \{\mathcal{P}_i \mid \mathcal{P}_i \cap A \in \Gamma_i\} \in \Gamma_0$. Let $A_i = \{P^i_{j_1}, \ldots, P^i_{j_{l_i}}\} \neq \emptyset$ be the set $A \cap \mathcal{P}_i$ and suppose that it is a minimal qualified set (otherwise it always contains one). Thus the vectors $\{\mathbf{h}^i_{j_1}, \ldots, \mathbf{h}^i_{j_{l_i}}\}$ are linearly dependent and all subsets of them of cardinality $l_i - 1$ are linearly independent. By Lemma 1 we have that there exist a codeword in $\mathcal{C}'_i$ given by $(0, \ldots, 0, \lambda^i_{j_1}, 0, \ldots, 0, \lambda^i_{j_{l_i}}, 0, \ldots, 0)$ such that $\mathbf{0} = \sum_{k=1}^{l_i} \lambda^i_{j_k} \mathbf{h}^i_{j_k}$ and $\sum_{k=1}^{l_i} \lambda^i_{j_k} \neq 0$. Thus for each $\mathcal{P}_i \in B$ the following non-zero vector

$$\mathbf{0} \neq \sum_{k=1}^{l_i} \lambda^i_{j_k} \Phi(P^i_{j_k}) = \left(\sum_{k=1}^{l_i} \lambda^i_{j_k} \Phi_0(\mathcal{P}_i), \mathbf{0}, \ldots, \mathbf{0} \right)$$

belongs to $\langle \Phi(A) \rangle$, and since Φ_0 defines a vector space structure on Γ_0 then

$$\mathbf{e}_1 \in \left\langle \sum_{k=1}^{l_i} \lambda^i_{j_k} \Phi_0(\mathcal{P}_i) \right\rangle_{\mathcal{P}_i \in B}$$

and we have that $(\mathbf{e}_1, \mathbf{0}, \ldots, \mathbf{0}) \in \langle \Phi(A) \rangle$.

On the other hand, let now $A \subseteq \mathcal{P}$ be a participant set such that $\mathbf{e}_1 \in \langle \Phi(A) \rangle$. Then $\mathbf{e}_1 \in \langle \Phi_0(B) \rangle$ and for each $\mathcal{P}_i \in B$ if $A_i = A \cap \mathcal{P}_i$ then $\mathbf{0} \in \langle \pi_i(\Phi(B)) \rangle$ where π_i is the restriction of $\Phi(B)$ to the interval $\left[\; d + 1 + \sum_{j=1}^{i-1} n_j, \quad d + \sum_{j=1}^{i} n_j \; \right]$. Therefore there exists a codeword in $\mathcal{C}'_i$ with support corresponding to the participants of the set $A_i = A \cap \mathcal{P}_i$ for each $\mathcal{P}_i \in B$. □

Corollary 1. *$\Gamma_{\mathcal{C}}$ admits a vector space construction.*

Proof. Note that $\Gamma_{\mathcal{C}} = (1,1)[\mathcal{C}]$ so we can apply the above theorem. □

Acknowledgments

The first two authors are partially supported by Spanish MCINN under project MTM2007-64704. First author research is also supported by a FPU grant AP2008-01598 by Spanish MEC. Second author is also supported by Spanish MCINN under project MTM2010-21580-C02-02.

References

[1] E. R. Berlekamp, R. J. McEliece, and Henk C. A. van Tilborg. On the inherent intractability of certain coding problems. *IEEE Trans. Information Theory*, IT-24(3):384–386, 1978.

[2] G. R. Blakley. Safeguarding cryptographic keys. In *AFIPS 1979 National Computer Conference*, pages 313–317, 1979.

[3] E. F. Brickell. Some ideal secret sharing schemes. *J. Combin. Math. Combin. Comput.*, 6:105–113, 1989.

[4] Ernest F. Brickell and Daniel M. Davenport. On the classification of ideal secret sharing schemes (extended abstract). In *Advances in cryptology—CRYPTO '89 (Santa Barbara, CA, 1989)*, volume 435 of *Lecture Notes in Comput. Sci.*, pages 278–285. Springer, New York, 1990.

[5] J. Bruck and M. Naor. The hardness of decoding linear codes with preprocessing. *IEEE Trans. Inform. Theory*, 36(2):381–385, 1990.

[6] T. Chunming, G. Shuhong, and Z. Chengli. The Optimal Linear Secret Sharing Scheme for Any Given Access Structure. *preprint*, 2011.

[7] M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. *Electron. Comm. Japan Part III Fund. Electron. Sci.*, 72(9):56–63, 1989.

[8] I. Márquez-Corbella and E. Martínez-Moro. Algebraic structure of the minimal support codewords set of some linear codes. *Adv. Math. Commun.*, 5-2:233–244, 2011.

[9] E. Martínez-Moro, J. Mozo-Fernández, and C. Munuera. Compounding secret sharing schemes. *Australas. J. Combin.*, 30:277–290, 2004.

[10] J. L. Massey. Minimal codewords and secret sharing. In *Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory*, pages 276–279, 1993.

[11] Carles Padró and Germán Sáez. Secret sharing schemes with bipartite access structure. In *Advances in cryptology—EUROCRYPT '98 (Espoo)*, volume 1403 of *Lecture Notes in Comput. Sci.*, pages 500–511. Springer, Berlin, 1998.

[12] A. Renvall, C. Ding, J. Pieprzyk, and J. Seberry. *Information Security and Privacy*, volume 1172, pages 67–78. Springer Berlin / Heidelberg, 1996.

[13] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[14] G. J. Simmons. An introduction to shared secret and/or shared control schemes and their application. In *Contemporary cryptology*, pages 441–497. IEEE, New York, 1992.