# Minimal Vectors in Linear Codes and Sharing of Secrets *

Alexei Ashikhmin† Alexander Barg†, ‡

We study access structures in secret sharing schemes determined by linear codes. They are known to be characterized by the set of minimal codewords (in essence, by the set of minimal supports of the codewords). After stating some simple properties of these sets, we find them for random linear codes, the Hamming codes, and second-order Reed–Muller codes. We also extend the concept of linear secret-sharing schemes to certain finite rings.

***Keywords*** – Ideal secret-sharing schemes, vector matroids, minimal codewords.

## 1 Introduction

The concept of secret sharing has been recently extensively discussed in cryptography (an overview and relevant references are found in [1]). Informally, this concept can be described as follows. A center $D$ has to create a system of distributed access to a certain information $s_0$. Toward this end, it gives out to the users in the set $\mathcal{U} = \{p_1, \dots, p_{n-1}\}$ of the system some portions (shares) of information. The goal of the center is to ensure that only the authorized coalitions of users, putting their shares together, can learn $s_0$, while all other (unauthorized) coalitions can obtain from their joint knowledge as little information about $s_0$ as possible. In *perfect secret-sharing schemes*, this illegal information is required to be void. Suppose the shares $s_i, 1 \le i \le n-1$, and the value $s_0$ are taken from a finite set $S$ (thus, we confine ourselves to *ideal* secret-sharing schemes in which the information rate $R \triangleq \max_i(\log s_i / \log s_0)$ always equals 1). The collection of authorized coalitions is called an access structure (denoted $\Gamma, \Gamma \subseteq 2^{\mathcal{U}}$). It is natural (though not necessary) to assume that if a certain coalition can learn $s_0$ then this property is not damaged by

*The results of this paper were presented in part at the Fourth International Workshop "Algebraic and Combinatorial Coding Theory" (ACCT-4), Novgorod, 11–17 September 1994.

†Institute for Information Transmission Problems, 19 Ermolovoi st., Moscow GSP-4, 101447.

‡Faculty of Mathematics and Computer Science, University of Technology, Den Dolech 2, P.O. Box 513, 5600 MB Eindhoven. The research of this author was partially supported by the International Science Foundation under grant MEF000.

adding extra users to it. Such access structures, for which $\gamma_1 \in \Gamma$ and $\gamma_1 \subset \gamma_2$ imply $\gamma_2 \in \Gamma$, are called *monotone*. Thus, what we really need to study is the *minimal* (or Sperner) access structure, i.e., the maximal set $\Gamma^- \subseteq \Gamma$ with the property that $\gamma_1, \gamma_2 \in \Gamma^-$ implies that neither $\gamma_1 \subseteq \gamma_2$ nor $\gamma_2 \subseteq \gamma_1$. An access structure is called *connected* if for any $p \in \mathcal{U}$ there exists a $\gamma \in \Gamma^-$ such that $p \in \gamma$.

The concept of secret sharing was first introduced in [2, 3] (in a particular case) and the general definition was given in [4].

To define a secret-sharing scheme it is necessary to define a set of distribution rules, i.e., of functions that assign shares to the users. If $S$ is a finite field and those functions are linear over it, the scheme is called *linear*. Linear schemes, which form the subject of this paper, were studied in [5]–[9]

Formal definitions and a relation to error-correcting codes are given in Secs. 2, 3. This relation shows [6, 7] that the access structure of a linear secret-sharing scheme is determined by the set of so-called minimal codewords of an associated linear code, i.e., of codewords that cover no other noncollinear codewords in this code. The minimal access structure $\Gamma^-$ is formed by the users contained in supports of minimal codewords that have a nonzero first coordinate. The entire access structure $\Gamma$ is formed by all the sets of users that contain the minimal subsets $\gamma \in G^-$. Thus, a natural question[1] is to study which access structures are defined by well-known linear codes. Massey [6] and Blakley and Kabatianskii [7] suggest this question as a research problem. Interestingly, the set of minimal codewords has been studied already in [13] (for decoding purposes). There this set was called the *projecting set* of a code. For a code $C$, we denote its set of minimal codewords by $\mathcal{P}(C)$ or simply by $\mathcal{P}$. We assume that $\mathbf{0} \notin \mathcal{P}$ and suggest a notation $C^\times \triangleq C - \{\mathbf{0}\}$.

There are many binary codes with $\mathcal{P}(C) = C^\times$. They are called intersecting after [10, 11]. In our setting, if a code is intersecting, then all of its codewords with a nonzero first coordinate define minimal authorized coalitions.

In Sec. 4, we explore properties of minimal codewords and find their number in typical linear codes. The subsequent asymptotic analysis enables us to assess, from the complexity point of view, the decoding algorithm in [13]. We also find $\mathcal{P}(C)$ for $C$ the Hamming code and second-order Reed–Muller code. In Sec. 5, we extend our study to the case of $S$ a Galois ring, when the corresponding secret-sharing schemes turn out to be nonperfect. It also turns out that, especially in connection with rings, it is more accurate to speak of minimal supports (sets of coordinates) rather than of codewords themselves. In binary codes, this difference is hidden.

[1]for a coding theorist, though, probably, not for a cryptologist, who would like to construct a scheme starting from a given access structure rather than to find which structure corresponds to a scheme determined by some considerations foreign to cryptography.

## 2 Secret-Sharing Schemes

It is convenient to formally assume that there is an additional user $p_0$ that corresponds to the center $D$ and always gets $s_0$ as his share. Let $\mathcal{U} = \{p_1, \dots, p_{n-1}\}$, $\mathcal{U}' = \mathcal{U} \cup \{p_0\}$.

Let $\Gamma$ be a collection of subsets of $\mathcal{U}$ and $\mathcal{F} = \{f : \mathcal{U}' \to S\}$ be a collection of functions from $U'$ onto a finite set $S$, $|S| = q$.

Definition. A triple $< \Gamma, \mathcal{F}, S >$ is called an ideal perfect secret-sharing scheme implementing the access structure $\Gamma$ if

(1) for any $\gamma \in \Gamma$ and functions $f_1, f_2 \in F$, the condition $f_1(p_i) = f_2(p_i)$ for all $p_i \in \gamma$ necessarily implies $f_1(p_0) = f_2(p_0)$;

(2) Let $\delta \subseteq \mathcal{U}, \delta \notin \Gamma, f \in \mathcal{F}$, and $\mathcal{F}|_{s_0} = \{g \in \mathcal{F} | g(p_0) = s_0\}$. Then

$$|\{g \in \mathcal{F}|_{s_0} : g(p_i) = f(p_i) \quad \forall p_i \in \delta\}| = q.$$

Property (1) ensures that authorized coalitions can determine the secret. Property (2) is sufficient to prove [1] that the users in $\delta \notin \Gamma$ can draw no a *posteriori* information about the secret.

Associating to every $f \in \mathcal{F}$ a row of its values on $\mathcal{U}'$, we may define a secret sharing matrix.

Consider a matrix $\mathcal{M} = ||m_{fe}||, f \in \mathcal{F}, e \in \mathcal{U}'$ with entries from $S$. Let us introduce the set of distinct shares given to a selected user $a$ by all the functions $g$ that give out to the users in a certain subset $\delta$ precisely the same shares as does a function $f$:

$$N(f, a, \delta) = \{m_{ga} : \ m_{gd} = m_{fd} \text{ for all } d \in \delta\}.$$

Then $\mathcal{M}$ determines a perfect secret-sharing system if for all $\delta \subseteq \mathcal{U}'$, either $|N(f, p_0, \delta)| = 1$ for all $f$ or $|N(f, p_0, \delta)| = q$ for all $f$.

Let $\delta \in \Gamma^-, e \in \mathcal{U}' - \delta$. We say that an element $e$ depends on the set $\delta$ if $|N(f, e, \delta)| = 1$ for all rows $f$ of $\mathcal{M}$. A set $\theta$ is called an independent set of the access structure $\Gamma$ if no element $e$ of $\theta$ depends on the set $\theta - e$. In [12] it was observed that this defines a connected matroid on the set $\mathcal{U}'$ whose independent sets are the independent sets of the underlying access structure. The entries of $\Gamma^-$ are precisely the circuits of this matroid that contain the point $p_0$. This seems to be the most fundamental result on ideal secret-sharing schemes.

Thus, every ideal scheme defines an associated matroid, which is then called secret-sharing. Interestingly, the converse is not true, i.e., an example can be given of non-secret-sharing matroids [14]. However, if $S = \mathbf{F}_q$ is a finite field and a given matroid $\mathcal{V}$ is representable over it, then $\mathcal{V}$ is secret-sharing. Indeed, let $\mathcal{V}$ be represented by the column space of a matrix $H$. Then the secret-sharing matrix $\mathcal{M}$ is formed by all linear combinations of the rows of $H$.

The last remark comprises the entire theory of (one-dimensional) linear secret-sharing schemes, whose self-contained definition is found in [5]-[7].

## 3 Access Structures from Linear Codes

Let us recall the definition of linear schemes. Let $H = ||h_{ij}||, 1 \leq i \leq r, 0 \leq j \leq n-1$ be a $q$-ary matrix and $E$ an $\mathbf{F}_q$-linear space of dimension $r$. Define a linear transform $f$ on $E$ by $f(\mathbf{e}) = \mathbf{e}H, \mathbf{e} \in E$. The secret and the shares of the users are formed by coordinate 0 and coordinates 1 to $n-1$ of the vector $f(\mathbf{e})$, respectively. When $\mathbf{e}$ runs over $E$, we obtain the entire collection of distribution rules of the system defined by $H$.

*Remark.* Generally speaking, the secret and the shares may be taken from spaces of dimension greater than one [7]. Suppose the space of secrets is $m_0$-dimensional and the share spaces of $N$ users have dimensions $m_1, \ldots, m_N$. Then one should partition $H$ into the groups of columns of size $m_0, m_1, \ldots, m_N$ to ensure the necessary dimension of the corresponding spaces.

In this paper, we confine ourselves to one-dimensional schemes.

Thus, we associate the users $p_0, p_1, \ldots, p_{n-1}$ with the columns of $H$. A conference of users $p_j \in \gamma \subseteq \{p_1, \ldots, p_{n-1}\}$ can reconstruct $s_0$ iff their columns span column 0 of $H$. This follows from the Kronecker–Capelli theorem (as discussed in [5, 7]). Therefore, an access structure $\Gamma$ of the secret-sharing scheme defined by $H$ is formed by the subset of the null space of $H$ formed by vectors with a nonzero first coordinate. The minimal access structure, $\Gamma^-$, is formed by a subset of vectors in $\Gamma$ that cover no other vectors in $\Gamma$. This brings us to the concept of minimal codewords. Let $C$ be a linear code.

Definition 1. A codeword $\mathbf{c} \in C^\times$, whose leftmost nonzero coordinate is one, is called minimal if it covers no other codeword with the leftmost nonzero coordinate equal to one.

In other words, we pass from the $k$-dimensional linear space (code) $C$ to the corresponding $k-1$-dimensional projective space $\mathbf{P}(C)$ and call a vector minimal if it covers no other vectors of this space.

Definition 1′. A subset $I \subseteq \{0, 1, \ldots, n-1\}$ of the coordinate set is called minimal with respect to a given code $C$ if

(i) there exists a codeword $\mathbf{c} \in C$ with $\operatorname{supp} \mathbf{c} = I$,

(ii) there is no codeword $\mathbf{c}' \in C^\times$ with $\operatorname{supp} \mathbf{c}' \subset I$.

For $S$ a field, there is no difference in speaking of codewords with the leftmost nonzero coordinate 1 or of their supports, so $\mathcal{P}(C)$ can be also thought of as the set of minimal supports. In Sec. 5, where we deal with $S$ a ring, there is no obvious way to define minimal codewords.

As we have seen, the access structure corresponding to a linear code $C = \ker H$ is completely characterized by the set of its minimal codewords $\{(c_0, \ldots, c_{n-1})\}$ with $c_0 = 1$. Since the passage from the set $\mathcal{P}(C)$ to its subset with a nonzero first coordinate is in most cases easy, below we prefer to work with entire sets of minimal codewords.

Let us define dual access structures. Suppose $\Gamma = \{\gamma_1 = \{p_1^{(1)}, \ldots, p_{|\gamma_1|}^{(1)}\}, \gamma_2 = \{p_1^{(2)}, \ldots, p_{|\gamma_2|}^{(2)}\}, \ldots\}$ is an access structure and $F(p_1, \ldots, p_{n-1}) = p_1^{(1)} \ldots p_{|\gamma_1|}^{(1)} + p_1^{(2)} \ldots p_{|\gamma_2|}^{(2)} + \ldots$ is the associated monotone function.

Definition 2 [8]. An access structure $\Gamma^*$ is called dual to a structure $\Gamma$ if the corresponding Boolean function $F^*$ is obtained from the function $F$ by interchanging logical multiplications and additions.

In [8], it is proved that if $\mathcal{V}$ is a matroid associated to $\Gamma$ then the matroid associated to $\Gamma^*$ is the dual matroid $\mathcal{V}^*$. If $\mathcal{V}$ is representable over $\mathbf{F}_q$ then so is $\mathcal{V}^*$ (in coding terms: if some $k$ coordinates form an information set in a code $C$ then the remaining $n-k$ coordinates form an information set in the dual code $C^\perp$).

We conclude that the access structure $\Gamma^*$ dual to a structure $\Gamma$ in the linear case is determined by the dual code of the original one. The remaining part of the paper is devoted to the study of sets of minimal codewords in linear codes and their duals.

# 4 Minimal Vectors in Linear Codes

4.1. Let $C$ be a $q$-ary $[n, k, d]$-code with a parity-check matrix $H$. The following lemma, in some parts explicit already in [13], is immediate from the definition of $\mathcal{P}(C)$.

**Lemma 1**

(1). *A vector $\mathbf{c} \in C$ is minimal iff the rank of $H$ restricted to the support of $\mathbf{c}$,* $\mathrm{rk}(H|_{\mathrm{supp}\,(\mathbf{c})}) = \mathrm{wt}(\mathbf{c}) - 1$.

(2). *If $\mathbf{c}_1 \in \mathcal{P}(C)$ and $\mathrm{supp}\,\mathbf{c}_1 = \mathrm{supp}\,\mathbf{c}_2$ then $\mathbf{c}_1$ and $\mathbf{c}_2$ are collinear.*

(3). *$\mathbf{c} \in \mathcal{P}(C)$ implies $\mathrm{wt}(\mathbf{c}) \le n - k + 1$.*

(4). *If $q = 2$ then any vector $\mathbf{c} \in C$ of weight $\le 2d - 1$ is minimal.*[2]

(5). *The linear span of $\mathcal{P}(C)$ coincides with $C$.*

Proof. (1), the *if* part. Let $\mathrm{supp}\,\mathbf{c} = \{1, \ldots, w\}$; thus, there exist $w$ nonzero numbers $\lambda_i$ such that

$$\sum_{i=1}^{w} \lambda_i \mathbf{h}_i = 0. \tag{1}$$

By the assumption, there exist $w-1$ linearly independent columns. Say, they are $\mathbf{h}_1, \ldots, \mathbf{h}_{w-1}$. Suppose that there exists $\mathbf{c}'$ with $\mathrm{supp}\,\mathbf{c}' \subset \mathrm{supp}\,\mathbf{c}$, i.e., there exists a vanishing linear combination of columns that does not involve at least one of the first $w-1$ columns, for instance,

$$\sum_{i=2}^{w} \mu_i \mathbf{h}_i = 0 \tag{2}$$

[2]Note in passing that (3) and (4) imply that no binary code contains a word of weight $n - k + 2 \le w \le 2d - 1$.

with $\mu_w \neq 0$. Multiplying (2) by $\lambda_w/\mu_w$ and subtracting (2) from (1), one would get a linear dependence between the first $w-1$ columns in contradiction with the assumption.

(5) (see [13, 6]). This is seen by taking an arbitrary codeword $c \in C$ and subtracting from it any minimal codeword covered by it, appropriately scaled to reduce the size of $\operatorname{supp}\mathbf{c}$, and so on, until the difference is itself a minimal codeword. $\square$

This lemma enables one to give an immediate answer about the access structure of some codes.

*Examples.* 1. Let $C = \mathcal{G}_{23}$ be the binary $[23, 12, 7]$ Golay code. We have $n - k + 2 = 2d - 1 = 13$. Thus, $\mathcal{P}(\mathcal{G}_{23}) = \{3335 \text{ words of weight} \le 12\}$. The same argument applies to the dual $[23, 11, 8]$ code $\mathcal{G}_{23}^{\perp}$, which gives a characterization of the dual structure (the set $\mathcal{P}(\mathcal{G}_{23}^{\perp}) = \{1794 \text{ words of weights 8 and } 12\}$). For the extended code $\mathcal{G}_{24}$, we have $n - k + 2 \le 2d - 1$, and the answer is also obvious. Since puncturing any coordinate from $\mathcal{G}_{24}$ we get $\mathcal{G}_{23}$, it is also easy to find the number of codewords with a one in the first coordinate.

2. Binary intersecting codes. If $\mathcal{P}(C) = C^{\times}$, then the supports of any pair of codewords intersect since otherwise we could sum them up to get a codeword covering both of them in contradiction to that all the words are minimal. The minimal access structure $\Gamma^{-}$ is formed by all $|C|/q$ codewords with a one in the leftmost coordinate.

Let $C$ be the binary code dual to the BCH code of length $n = 2^m - 1$ with designed distance $d = 2t + 1$ and $t \le \frac{1}{3}2^{(m/2)-1}$. Then by the Carlitz–Uchiyama bound, the maximum weight $D$ of $C$ is bounded from above as $D \le 2^{m-1} + (t-1)2^{m/2}$. By the same bound, the quantity $2d \ge 2^m - 2(t-1)2^{m/2} > D$. Thus, $\mathcal{P}(C) = C^{\times}$ and $C$ is intersecting [10, Prop. 9]. To characterize the dual structure is an open question.

3. In an $[n, k, d]$ MDS-code $C$, the set of minimal codewords coincides with the set of all $\binom{n}{d}$ noncollinear codewords of weight $d$ (by Part (2) of the lemma). Of them $\binom{n-1}{d-1}$ have a one in coordinate $c_0$. This brings us back to the original threshold scheme of Shamir [3]. The dual structure in this case is also obvious.

For an $[n, k, n-k]$ code $C$, the answer is generally not as obvious. However, if $C$ is "near-MDS," i.e., if $d(C) + d(C^{\perp}) = n$, then any $k^{\perp} + 1$ columns of the parity-check matrix of $C$ have rank $k^{\perp}$ [15]. Thus, $\mathcal{P}(C) = \{\text{noncollinear words of weight } d \text{ and } d+1\}$.

4.2. Typical linear codes. Let $H$ be a randomly chosen matrix with independent entries taken from $\mathbf{F}_q$ with uniform distribution and $C = \ker H$ be the corresponding $[n, k]$ code. We want to count the average number of its minimal codewords of weight $w$.

**Theorem 1** *Let $C_w$ be the subset of words of weight $w$ in $C$. Then*

$$\mathbf{E}|C_w \cap \mathcal{P}| = \begin{cases} \binom{n}{w} \dfrac{(q-1)^{w-1}}{q^{n-k}} \displaystyle\prod_{i=0}^{w-2} (1 - q^{-(n-k-i)}), & w \le n-k+1, \\ 0 & \textit{otherwise.} \end{cases} \tag{3}$$

Proof. Let us find the probability $P\{\mathbf{c} \in C_w, \mathbf{c} \in \mathcal{P}\}$ that a given vector $\mathbf{c}$ is a codeword of weight $w$ in $C$ and is minimal. The event considered is that some (say, first) $w-1$ columns of $H$ among the chosen $w$ columns are linearly independent and the remaining column is their linear combination with $w-1$ nonzero coefficients.

The number of collections of $w$ columns that satisfy the above conditions equals

$$(q^{n-k}-1)(q^{n-k}-q)\dots(q^{n-k}-q^{w-2})(q-1)^{w-1}.$$

The total number of possible choices is $q^{w(n-k)}$. The required probability equals the quotient of these quantities and the average number of minimal vectors of weight $w$ equals $\binom{n}{w}P\{\mathbf{c} \in C_w, \mathbf{c} \in \mathcal{P}\}$. □

**Corollary 1** *Let $n \to \infty$, let $k$ grow linearly in $n$ and suppose $w = (n-k+1)-l$, $l \geq 0$. Then the average number of minimal codewords of weight $w$ in an $[n,k]$ $q$-ary linear code equals*

$$\alpha_q(l)\binom{n}{w}\frac{(q-1)^{w-1}}{q^{n-k}}, \tag{4}$$

*where for $l > 0$, $1 > \alpha_q(l) > 1-q^l$, and $\alpha(0) = 1-q^{-1}-q^{-2}+q^{-5}+q^{-7}-\dots$. Therefore, $\alpha(l) \to 1$ as $l \to \infty$.*

Proof. This amounts in the study of the asymptotic behavior of the quantity $\prod_{i=t-s+1}^{t}(1-q^{-i})$, where we have adopted the notation $t = n-k$, $s = w-1$. This product always converges since for $s \leq t-1$, one has $1 > \prod_{i=t-s+1}^{t}(1-q^{-i}) > 1-\sum_{i=t-s+1}^{t} q^{-i} > 1-q^{-(t-s)}$, which implies our claim for $l = t-s$ positive. The series expansion for $\alpha(0)$ follows from Euler's pentagonal number formula.

□

Note that the average number of noncollinear words of weight $w$ in a random $[n,k]$ $q$-ary linear code equals $\binom{n}{w}(q-1)^{w-1}/q^{n-k}$. Thus, when $w$ is not too close to $n-k$, then, on the average, virtually all noncollinear codewords are minimal. If $w = (n-k+1)-l$, $l$ a constant, the quotient $\mathbf{E}|C_w \cap \mathcal{P}|/\mathbf{E}|C_w|$ asymptotically equals $\alpha_q(l) < 1$. Precise numerical values of $\alpha_q(l)$ for $l = 0,1,2$ and $q < 11$ are given in [16]. In particular, $\alpha_q(l) > 1/2$ except for $\alpha_2(0) = 0.2887$.

This calculation is important for the assessment of a maximum-likelihood soft-decision decoding algorithm suggested by Hwang in [13]. Hwang's algorithm for binary codes is as follows. Let $C = \{\mathbf{c}_i, 1 \leq i \leq |C|\}$ be a binary linear code. For a received word $r$, calculate the vector $\varphi$ of bit log-likelihood ratio values. Pick any vector $\mathbf{c} \in C$ and for all $\mathbf{c}_s = (c_{s_1}, \dots, c_{s_n}) \in \mathcal{P}(C)$, evaluate the scalar product $\Pi$ of the vectors $\mathbf{c}_s$ and $((-1)^{c_{s1}}\varphi_1, \dots, (-1)^{c_{sn}}\varphi_n)$. If there is a vector $\mathbf{c}_s^* \in \mathcal{P}(C)$ for which $\Pi < 0$, replace $\mathbf{c}$ by $\mathbf{c}+\mathbf{c}_s^*$ and proceed as described. When $\Pi \geq 0$ for all $\mathbf{c}_s \in \mathcal{P}(C)$, the current vector $\mathbf{c}$ is the desired result.

The worst-case complexity of this algorithm is $|\mathcal{P}(C)|^2$. However, for $R < 1/2$, the number $\mathbf{E}(\mathcal{P}(C))$ is exponentially the same as the total size of the code. For $R > 1/2$, the exponential size of $\mathcal{P}(C)$ (more accurately, the exponent of $\mathbf{E}(\mathcal{P}(C))$) equals the number of the words of weight $w$ such that $w/n \sim 1 - R$. Thus, for typical code families, the complexity of Hwang's algorithm is likely to be greater than that of the conventional syndrome trellis decoding, which explains why, at least for typical codes, this suggestion was not especially successful.

*Mutatis mutandis*, this argument applies to nonbinary codes.

4.3. HAMMING CODES. Let $C$ be the $q$-ary Hamming code of length $n = (q^m - 1)/(q - 1)$.

For the binary case, the required set of vectors forms a configuration defined by J. Steiner, from which later the modern notion of Steiner systems has been coined. Formula (5) is quoted in [17] with a reference to [18]. Its proof for any $q$ is given below. Steiner's original definition is cited in the Appendix.

**Theorem 2** *The set $\mathcal{P}(C)$ is formed by $B_w$ vectors of every weight $w, 3 \le w \le m + 1$, were*

$$B_w = \frac{1}{w!(q-1)} \prod_{i=0}^{w-2} (q^m - q^i). \tag{5}$$

PROOF. Consider $s = w - 1$ linearly independent columns in the parity-check matrix $H$ of the code $C$. The total number of linear combinations of these columns with nonzero coefficients equals $(q - 1)^s$; the $1/(q - 1)$th fraction of them appear as columns in $H$ distinct from the chosen columns (since they are linearly independent). Every choice of $w$ linearly dependent columns of which $s = w - 1$ are linearly independent, defines a minimal codeword. Thus, one has to count the number of distinct choices of $s$ linearly independent columns in $H$. This number equals

$$\frac{1}{s!} n(n-1)(n - \frac{q^2-1}{q-1}) \dots (n - \frac{q^{s-1}-1}{q-1}).$$

Taking into account that all the $\binom{w}{w-1}$ choices of $w - 1$ linearly independent columns within a given support of size $w$ yield one and the same codeword, we find that the number of minimal codewords of weight $w$ in the code equals

$$B_w = \frac{1}{(w-1)!w} n(n-1)(n - \frac{q^2-1}{q-1}) \dots (n - \frac{q^{s-1}-1}{q-1})(q-1)^{s-1},$$

where we the exponent of $(q - 1)$ is $s - 1$ to rule out collinear vectors. The substitution of the value of $n$ gives the desired result. □

The dual structure in this case is determined by the set of minimal words in the $[n = (q^m - 1)/(q - 1), m, q^{m-1}]$ simplex code. The set $\mathcal{P}$ is formed by $n$ words (all pairwise noncollinear words). Of them $q^{m-1}$ have a one in coordinate $c_0$.

A similar argument in the binary case yields the following fact.

**Theorem 3** *In the extended Hamming code of length $2^m$, the number of minimal codewords of even weight $w, 4 \le w \le m+2$ equals*

$$B_w^{\text{ex}} = \frac{1}{w!} 2^m \prod_{i=0}^{w-3} (2^m - 2^i).$$

4.4. SECOND-ORDER REED–MULLER CODES.

Let $C = \text{RM}(2, m)$ be the second order binary Reed–Muller code and $A_w$ the number of its words of weight $w$. Then $A_w = 0$ except for $w = 2^{m-1}, w = 2^{m-1} \pm 2^{m-1-h}, 0 \le h \le \lfloor m/2 \rfloor$. Let $B_w = |C_w \cap \mathcal{P}|$ be the number of its minimal codewords of weight $w > 0$.

**Theorem 4** *For $w = 2^{m-1} + 2^{m-1-h}, h = 0, 1, 2$, there are no minimal codewords ($B_w = 0$). Otherwise, $B_w = A_w$, except for the case $w = 2^{m-1}$, when the number of nonminimal codewords equals*

$$A_{2^{m-1}} - B_{2^{m-1}} = 2^{m+1} - 2 + A_d(2^{m-1} - 2) \tag{6}$$

Thus, the only weights when there exist nonminimal codewords are $(3/4)n, (5/8)n$ (all codewords) and $(1/2)n$ (part of them).

PROOF. If a word $\mathbf{c}$ is nonminimal, then $\mathbf{c} = \mathbf{c}_1 + \mathbf{c}_2$ and we have for the weights $w, w_1$, and $w_2$ the equality

$$w = w_1 + w_2 \ge 2d = 2^{m-1}. \tag{7}$$

Thus, either

*(i)* $w = n/2$, in which case $w_1 = w_2 = n/4 = d$,

or $w > n/2$. Then it is possible that one of the two constituent words, $\mathbf{c}_1$ say, has weight $n/2$. In this case, Eq. (7) implies for some $h_1, h_2, 1 \le h_1, h_2 \le \lfloor m/2 \rfloor$, the following equality:

$$2^{m-1} + 2^{m-1-h} = 2^{m-1} + 2^{m-1} - 2^{m-1-h_1},$$

whence $h = h_1 = 1$.

*(ii)* $(w_1, w_2, w_3) = (\frac{3}{4}n, \frac{1}{2}n, \frac{1}{4}n)$.

If both $w_1$ and $w_2$ differ from $n/2$, then (7) yields

$$2^{m-1} + 2^{m-1-h} = 2^{m-1} - 2^{m-1-h_1} + 2^{m-1} \pm 2^{m-1-h_2}$$

or

$$2^{-h} = 1 - 2^{-h_1} \pm 2^{-h_2}, \quad h_1, h_2, h_2 \ne 0.$$

Obviously, this equality cannot be satisfied with the "+" sign whereas for the "−" the only possibilities for $(h, h_1, h_2)$ are $(1, 2, 2)$ and $(2, 2, 1)$. Thus, the two remaining cases are

$(iii)$ $(w_1, w_2, w_3) = (\frac{3}{4}n, \frac{3}{8}n, \frac{3}{8}n)$,
$(iv)$ $(w_1, w_2, w_3) = (\frac{5}{8}n, \frac{3}{8}n, \frac{1}{4}n)$.

Let us first consider cases $(ii) - (iv)$. All the words of one and the same weight $w \neq n/2$ are affinely equiavlent, i.e., if there exists one nonminimal word of weight $w$, then applying a suitable automorphism, one concludes that all words of weight $w$ are nonminimal. Suppose $(x_1, \dots, x_m)$ are the affine coordiantes on $F^m = \mathrm{EG}(m, 2)$. Then the word given by the incidence vector of the equation $x_1 x_2 = 0$ has weight $3n/4$ and covers the incidence vector (of weight $n/2$) of the hyperplane $x_1 = 0$. This shows that every word of weight $3n/4$ is nonminimal and is formed by a disjoint union of a word of weight $n/2$ and a word of weight $n/4$, while case $(iii)$ is never realized. Likewise, in case $(iv)$, the incidence vector of $x_1x_2 + x_3x_4 = 0$ has weight $5n/8$ and contains the word given by $(x_1 + x_2)(x_3 + x_4) = 1$.

The only remaining case is $(i)$. Any nonminimal word $\mathbf{c}$ of weight $n/2$ is the sum of two words of minimal weight. By [19, Thm. 13.5], the subset $X$ of $F^m$ corresponding to $\mathbf{c}$ is a disjoint union of two $(m-2)$-dimensional flats in $F^m$, say $A_1$ and $A_2$. Let $V_1$ and $V_2$ be the $(m-2)$-dimensional linear spaces parallel to $A_1$ and $A_2$, respectively. The disjointness of $A_1$ and $A_2$ implies that $\dim(V_1 + V_2) < m$. Hence either $V_1 = V_2$ and $X$ is an $(m-1)$-flat or $W = V_1 \bigcap V_2$ has dimension $m - 3$. The number $N_1$ of nonminimal words of weight $n/2$ of the first type equals the number of $(m-1)$-flats in $F^m$,

$$N_1 = 2(2^m - 1).$$

In the second case, the image of $X$ in the (3-dimensional) quotient space $F^m/W$ is a set of 4 points that do not constitute an affine plane. Hence the total number of words $X$ of this type equals

$$N_2 = \begin{bmatrix} m \\ m-3 \end{bmatrix} \Big( \binom{8}{4} - 2 \begin{bmatrix} 3 \\ 2 \end{bmatrix} \Big).$$

The sum $N_1 + N_2$ gives the claimed number (6) of nonminimal vectors of weight $n/2$ if one recalls that $A_d = (4/3)(2^m - 1)(2^{m-1} - 1)$. $\square$

*Remark.* The number of minimal vectors of weight $n/2$ in $RM(2, m)$ equals

$$B_w = \sum_{h=2}^{\lfloor m/2 \rfloor} A_{2^{m-1} - 2^{m-1-h}} (2^{m-2h+1} - 2). \tag{8}$$

# 5 Secret Sharing over Finite Rings

In this section, we shall extend the definitions of Sec. 2 to a finite commutative ring $S$ with identity $e$, whose set of zero divisors has the form $pS$ for a certain prime $p$, a.k.a. a Galois ring. After Nechaev's paper [20], Galois rings have become easy to understand for a reader with a standard background in finite fields. In particular, using the definition given, one can prove [20] that $|S| = q^m, m \geq 1$, where $q = p^s$ for some $s \geq 1$, and the characteristic of $S$ (the order of $e$ in the group $(S, +)$) equals $p^m$. Since fixing the numbers $p^m$ and $q^m$ identifies $S$ up to isomorphism, it may be also denoted as $\mathrm{GR}(q^m, p^m)$. All ideals of $S$ form the following chain:

$$N_0 = S \supset N_1 = pS \supset N_2 = p^2 S \supset \ldots \supset N_{m-1} = p^{m-1} S \supset N_m = p^m S = 0, \tag{9}$$

and $|N_i| = q^{m-i}$. The ring $S$ is constructed as a degree $s$ Galois extension of $\mathbf{Z}_{p^m}$ in much the same way as one constructs the finite field from $\mathbf{Z}_p$. Denote by $S^\times = S \setminus N_1$ the set of ring units. Consider a "linear" code $C$ over $S$, i.e., a set of rows of $n$ elements of $S$ such that if $\mathbf{c}_1, \mathbf{c}_2 \in C$ then also $a_1 \mathbf{c}_1 + a_2 \mathbf{c}_2 \in C$ for any $a_1, a_2 \in S$. The number

$$T(\mathbf{c}) = \min_{i \in \operatorname{supp} \mathbf{c}} \{u :\ c_i \in N_u\}$$

will be called the *type* of the word $\mathbf{c}$. Let us call the number $T(I) = \min_{\operatorname{supp} \mathbf{c} = I} T(\mathbf{c})$ the type of a subset $I \subseteq \{0, 1, \ldots, n-1\}$. If there is no word with support $I$, the type of $I$ is undefined.

Definition 3. A subset $I \subseteq \{0, 1, \ldots, n-1\}$ of type $t$ is called minimal if there does not exist a codeword $\mathbf{c}$ with $T(\mathbf{c}) \leq t$ and $\operatorname{supp} c \subset I$.

This yields a hierarchy of minimal subsets of types $0 \leq t \leq m-1$. The collection of type $t$ minimal subsets will be denoted by $\mathcal{P}_t(C)$.

Let us define the algorithm for generating shares. Let $\mathbf{h}_0, \ldots, \mathbf{h}_{n-1}, \mathbf{e} \in (S)^r, r \geq 1$, be vectors and suppose that at least one of the coordinates of $\mathbf{h}_0$ is a ring unit. Then the secret equals $s_0 = (\mathbf{e}, \mathbf{h}_0)$ and every user $p_i$ gets the share $s_i = (\mathbf{e}, \mathbf{h}_i), 1 \leq i \leq n-1$. The access structure $\Gamma^-$ is determined by the collection of minimal subsets of types $t, 0 \leq t \leq m-1$, for which there exists a codeword $\mathbf{c}$ whose first coordinate $c_0 \in N_t$.

We shall prove now that the coalition corresponding to a minimal subset of type $t$ can reconstruct exactly $m - t$ $q$-ary symbols of the secret; thus, the corresponding system is nonperfect.

**Theorem 5** *Suppose $I = \{i_1, \ldots, i_l\} \subset \{1, \ldots, n\}$ and $\widetilde{I} = \{0\} \cup I$ is a minimal subset of type $t$. Then the coalition $\{p_j, j \in I\}$ can reconstruct exactly $m - t$ $q$-ary symbols of $s_0$.*

Proof. Consider the matrix $H = (\mathbf{h}_1, \ldots, \mathbf{h}_{n-1})$ and let $\widetilde{H} = (\mathbf{h}_0 \mid H)$. Likewise, let us use the notation $\mathbf{s} = (s_1, \ldots, s_{n-1})$ and $\widetilde{\mathbf{s}} = (s_0, s_1, \ldots, s_{n-1})$. Let $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ be any codeword in the null space of $\widetilde{H}$ with $T(\mathbf{c}) = t, \operatorname{supp} \mathbf{c} = \widetilde{I}$, and $c_0 \in N_t$. We have $c_0 \mathbf{h}_0 = -\sum_{j=1}^{l} c_{i_j} \mathbf{h}_{i_j}$. Multiplying this equality by $\mathbf{e}$, we see that

$$s = c_0 s_0 = -\sum_{j=1}^{l} c_{i_j} s_{i_j}.$$

Clearly, $s \in N_t$ and thus, there exist not more than $|S|/|N_t| = q^t$ distinct solutions of the equation $s = c_0 x$. Hence, the users $p_j, j \in I$, can reconstruct at least $m - t$ $q$-ary symbols of the secret.

Let us show that they cannot reconstruct more than $m - t$ symbols. Toward this end, we shall prove that the number of solutions of the system

$$\mathbf{e}\widetilde{H} = \widetilde{\mathbf{s}} \tag{10}$$

is one and the same irrespective of the value of $s_0$. Denote by $L(A, \mathbf{s})$ the set of solutions of the system with coefficient matrix $A$ and right-hand side $\mathbf{s}$. Our claim is obvious if the system

$$\mathbf{e}H = \mathbf{s} \tag{11}$$

has no solutions ($|L(H, \mathbf{s})| = 0$). Suppose that $|L(H, \mathbf{s})| > 0$, then the claim will follow from the two following assertions.

**Lemma 2** *Let* $U = \mathrm{span}\,(h_j, 1 \le j \le n-1)$ *and suppose* $|U| = q^w, w \ge 0$. *Then* $|U + S\mathbf{h}_0| = q^{w+t}$, *where*

$$t = \min\{v : \exists d \in N_v \text{ such that } d\mathbf{h}_0 \in U\}. \tag{12}$$

Proof. We know that $d\mathbf{h}_0 \in U$ if and only if $d \in N_t$. Therefore, if $d_1 \not\equiv d_2 \pmod{N_t}$, any two linear combinations $\sum a_{1i}\mathbf{h}_i + d_1\mathbf{h}_0$ and $\sum a_{2i}\mathbf{h}_i + d_2\mathbf{h}_0$ are distinct. The number of elements of $S$ not congruent modulo $N_t$ equals the number of cosets in $S/N_t$, i.e., equals $q^n/q^{n-t} = q^t$. $\square$

**Lemma 3** *Suppose that* $|L(H, \mathbf{s})| > 0$, *then* $|L(\widetilde{H}, \widetilde{\mathbf{s}})| > 0$ *iff* $p^t s_0 = -\sum_{j \in I} c_j s_j$, *where* $t$ *is defined in* (12).

Proof. The *only if* part is trivial; let us prove the *if* one. Suppose that $|\mathrm{span}\,(\mathbf{h}_1, \ldots, \mathbf{h}_{n-1})| = q^w$. The size of the row space of $H$ equals that of the columns space. Therefore, there are $q^w$ vectors $\mathbf{s}$ for which system (11) has a solution. By the previous lemma, $|U + S\mathbf{h}_0| = q^{w+t}$ and hence there exist $q^t$ different ways to attach $s_0$ to $\mathbf{s}$ so that system (10) has a solution. $\square$

We conclude the proof by noticing that $|L(\widetilde{H}, \mathbf{s})| > 0$ implies that $L(\widetilde{H}, \mathbf{s})$ is a coset in the quotient structure $((S)^n, +)/L(\widetilde{H}, \mathbf{0})$. Thus, for any $\widetilde{\mathbf{s}}$ on the right-hand side of (10), this set of equations is either contradictory or has one and the same number of solutions. $\square$

Thus, we get a hierarchy of fully and partially authorized coalitions of users. A coalition $\gamma$ of type $t$ can locate the secret within $q^t$ out of $q^m$ elements of $S$. Moreover, if $\gamma$ contains a user that has earlier participated in a lower-priority coalition and has a certain knowledge of the secret, this will not allow $\gamma$ to collect more knowledge about $s_0$ than it is entitled to; thus, the system may be called reusable in a certain sense.

To illustrate the construction, let us consider two simple examples involving $\mathbf{Z}_4$-linear codes.

*Examples.* 4. Consider the 1st order Reed-Muller code $ZRM(1, v)$ of length $n = 2^v$ over $\mathbf{Z}_4$ [21]. Then there are two types of minimal words, namely, those of types 0 and 1. It can be easily seen that $\mathcal{P}_0$ consists of a single set $\widetilde{I} = \{0, 1, \dots, n-1\}$ and $\mathcal{P}_1$ consists of $2^{v+1} - 2$ subsets (supports of words) of size $n/2$. A half of minimal subsets in $\mathcal{P}_1$ involve the coordinate 0; therefore, the access structure $\Gamma^-$ in this case consists of one fully authorized coalition $(p_1, \dots, p_{n-1})$ and $2^v - 1$ half-authorized ones. Every subset in $\mathcal{P}_1$ bears exactly one codeword formed by elements of $2\mathbf{Z}_4$, i.e., consisting only of zeros and twos. If, for instance, $v = 3$, then partially authorized groups of users, i.e., those who can reconstruct only one of the two bits of secret, are the following:

| $p_1$ | $p_2$ | $p_3$ | $p_4$ | $p_5$ | $p_6$ | $p_7$ |
|---|---|---|---|---|---|---|
| • | • | • | | | | |
| • | | | • | • | | |
| | • | | • | | • | |
| • | | | | | • | • |
| | • | | | • | | • |
| | | • | • | | | • |
| | | • | | • | • | |

5. Let $C$ be the $\mathbf{Z}_4$ Kerdock code of length $n = 2^v$, $v$ odd, [20, 21]. Then $\mathcal{P}_0$ is formed by the type 0 minimal subsets of sizes $2^{v-1} + 2^{v-2} \pm 2^{(v-3)/2}$ (the number of subsets of either size is $2^{v+1}(2^v - 1)$) and $\mathcal{P}_1$ consists of $2^{v+1} - 2$ subsets of size $n/2$.

The above argument has a rather general nature since it encompasses both finite fields and integer residue rings as boundary cases. Namely, $\mathbf{F}_{p^m} = \mathrm{GR}(p^m, p)$ and $\mathbf{Z}_{p^m} = \mathrm{GR}(p^m, p^m)$.

# 6 Conclusion

The study of access structures in linear secret-sharing schemes led us to a problem of characterizing minimal codewords in linear codes. This appears to be an interesting combinatorial problem in its own, but also it has links to quite a number of topics in coding theory. For instance, as has been explained to us by Ralf Kötter, the number of minimal codewords of weight $w$ gives an upper bound on the number of noncorrectable error patterns in decoding by error-locating pairs [22]. Apart from this, it would be interesting to know to what extent does the spectrum of minimal codewords (i.e., the set of numbers $B_w$ above) fix a code and does there exist a relation between this spectrum in a code and in its dual.

*Acknowledgment.* The short and nice geometrical proof of Theorem 4 that now replaces our original (much longer) one with coordinate approach was suggested by Juriaan Simonis. We also thank Alexander Trushkin and Gilles Zémor for clarifying discussions.

Appendix

*Steiner's original problem* [18]. Given two numbers $k$ and $v$, $k \leq v$, construct a pair $(X, \mathcal{B})$, where $X$ is a finite set and $\mathcal{B}$ a collection of its subsets, which satisfies the following conditions:

(i) $|X| = v$;

(ii) $\mathcal{B} = \bigcup_{n=3}^{k} \mathcal{B}(n)$ and $|B_i| = n$ for every $B_i \in \mathcal{B}(n)$;

(iii) every pair $(x, y) \subset X$ is contained in exactly one block of $\mathcal{B}(3)$;

(iv) every $i$-subset of $X, 3 \leq i \leq k-1$, which does not contain a block of $\bigcup_{j=3}^{i} \mathcal{B}(j)$, is contained in exactly one block of $\mathcal{B}(i+1)$; no block of $\mathcal{B}(i+1)$ contains as subsets blocks of $\bigcup_{j=3}^{i} \mathcal{B}(j)$.

## References


[1] D. R. Stinson, "An explication of secret sharing schemes," *Designs, Codes and Cryptography*, **2**, no. 4 (1992), 357–390.

[2] G. R. Blakley, "Safeguarding cryptographical keys," *Proc. AFIPS 1979 Natl. Computer Conf.*, N. Y., Vol. . **48** (1979), 313–317.

[3] A. Shamir, "How to share a secret," *ACM Commun*, **22** (1979), 612–619.

[4] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," *Proc. IEEE Globecom '87* (1987), 99–102.

[5] E. F. Brickell, "Some ideal secret sharing schemes," *J. Combin. Math. Combin. Comput.*, **9** (1989), 105–114.

[6] J. Massey, "Minimal codewords and secret sharing," in: it Proc. Sixth Joint Swedish-Russian Workshop Inf. Theory, Mölle, Sweden (1993), pp. 246–249.

[7] G. R. Blakley and G. A. Kabatianskii, "Linear algebra approach to secret sharing schemes," in: *Error Control, Cryptology, and Speech Compression*, Selected papers from Int. Workshop on Inf. Protection, Moscow, Dec. 1993, Springer Lect. Notes. Comput. Sci., **829** (1994), pp. 33-40.

[8] W.-A. Jackson and K. M. Martin, "Geometric secret sharing schemes and their duals," *Designs, Codes and Cryptography*, **4** (1994), 83–95.

[9] M. Bertilsson and I. Ingemarsson, "A construction of practical secret sharing schemes using linear block codes," *Advances in Cryptology, Proc. Auscrypt '92*, Springer Lect. Notes Comput. Sci., **718** (1993), pp. 67–79.

[10] G. D. Cohen and A. Lempel, "Linear intersecting codes," *Discrete Math.*, **56** (1984), 35–43.

[11] D. Miklós, "Linear binary codes with intersection properties," *Discr. Appl. Math.*, **9** (1984), 187–196.

[12] E. F. Brickell and D. M. Davenport, "On the classification of ideal secret sharing schemes," *J. Cryptology*, **4** (1991), 123–134.

[13] T.-Y. Hwang, "Decoding linear block codes for minimizing word error rate," *IEEE Trans. Inf. Theory*, **IT-25**, No. 6 (November 1979), 733–737.

[14] P. D. Seymour, "On secret-sharing matroids," *J. Comb. Theory*, Ser. B, **56** (1992), 69–73.

[15] S. Dodunekov and I. Landgev, "On near-MDS codes," presented at the IEEE Int. Sympos. Inf. Theory, June 1994, Trondheim, Norway.

[16] F. Gerth, "Limit probabilities for coranks of matrices over GF($q$)," *Linear and Multilinear Algebra*, **19** (1986), 79–93.

[17] H. Hanani, "On the original Steiner systems," *Discrete Math.*, **51** (1984), 309–310 .

[18] J. Steiner, "Combinatorische Aufgabe," *J. Reine Angew. Math.,* **45** (1853), 181–182.

[19] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[20] A. A. Nechaev, "The Kerdock code in a cyclic form," *Diskret. Mat.*, **1**, no. 4 (1989), 123–139. English translation in *Discr. Math. Appl.*, **1** (1991), 365–384.

[21] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $\mathbf{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inf. Theory*, **40**, no. 2 (1994), 301–319.

[22] R. Pellikaan, "On decoding by error location and dependent sets of error positions," *Discrete Math.,* **106/107** (1992), 369–381.