Variations on Minimal Codewords in Linear Codes

A. Ashikhmin[a], A. Barg[a,b,⋆] , G. Cohen[c], and L. Huguet[d]

[a]Institute for Information Transmission Problems, Moscow, Ermolovoy 19, GSP-4, 101447

[b] Dept. Math., Eindhoven University, Den Dolech 2, Postbus 513, 5600 MB, Eindhoven

[c] Dept. Informatique, E.N.S.T., 46 rue Barrault, 75634 Paris Cedex 13

[d] Universitat de les Illes Baleares, km. 7.5 Ctra. Valldemossa, 07071 Palma de Mallorca

Abstract. We address two topics related to the concept of minimal supports (codewords) in linear codes. In the first part we study the distribution of the number of minimal supports in random codes. In the second part, we propose a generalization of this concept for codes defined as modules over Galois rings. We determine minimal supports for some $\mathbb{Z}_4$-linear codes. Finally, we extend a recently established link between the cryptographical problem of secret sharing and minimal supports to the case of rings. The resulting secret-sharing schemes have fully and partially authorized coalitions, which permits, e.g., hierarchical access to a common resource.

1 Introduction.

Let $E = \{0, 1, \ldots, n-1\}$ be a finite set and C a linear code over a finite field $\mathbb{F}_q$ whose coordinates are numbered with the elements of E. A subset $I \subseteq E$ is called a *minimal support* w.r.t. C if there is a codeword $\mathbf{c}$ with $\operatorname{supp} \mathbf{c} = I$ and no nonzero codeword $\mathbf{b}$ satisfies $\operatorname{supp} \mathbf{b} \subset I$. Minimal supports arise naturally in the framework of matroid theory. Indeed, if $\mathcal{V}$ is a matroid on E represented over $\mathbb{F}_q$ by the column space of a parity-check matrix H of C, then the minimal supports of C are precisely the cycles of $\mathcal{V}$ (see [1]). Picking a codeword $\mathbf{c}$ with $\operatorname{supp} \mathbf{c} = I$ whose leftmost nonzero coordinate is fixed (say, to 1), we can make a bijection between codewords and supports and, thus, also speak of minimal codewords. For binary codes, there is no difference between minimal codewords and minimal supports.

Minimal supports in linear codes were studied in [2] in connection with a maximum-likelihood decoding algorithm and recently in [3]-[5] for the cryptographical problem of constructing secret-sharing schemes. The set of minimal supports of a code C will be denoted by $\mathcal{P}(C)$ or simply $\mathcal{P}$.

⋆ Supported in part by the International Science Foundation under grant MEF000.

2 A Lower Bound on the Size of $\mathcal{P}$ in Binary Codes.

Let C be a binary code with distance d. Denote $P = |\mathcal{P}(C)|$. Every codeword $\mathbf{c} \in C \setminus \{\mathbf{0}\}$ can be expanded into a sum of minimal codewords. Indeed, $\mathbf{c}$ is either minimal or covers a minimal codeword $\mathbf{u}_1$. The same applies to the word $\mathbf{c} - \mathbf{u}_1$ whose support is disjoint from $\mathbf{u}_1$, etc., until the sought expansion $\mathbf{c} = \sum \mathbf{u}_i$ is found. Clearly, the supports of the summands in this expansion are disjoint. Let $U(\mathbf{c})$ be the number of summands. Thus,

$$U(\mathbf{c}) \le \frac{\mathrm{wt}(\mathbf{c})}{d} \le \frac{n}{d}.$$

Since $\mathcal{P}(C)$ spans C, this yields

Proposition 2.1.

$$\sum_{i=1}^{n/d} \binom{P}{i} \ge |C|. \tag{2.1}$$

For $u < m/2$, we have

$$\sum_{i=1}^{u} \binom{m}{i} < \frac{m-u+1}{m-2u+1} \binom{m}{u} < \frac{m-u+1}{m-2u+1} \frac{m^u}{u!},$$

This gives lower estimates on P in (2.1). In particular, assuming the exponential growth of $|C|$, we get

$$\log P \gtrsim (d/n) \log |C|.$$

In fact, n/d is a crude upper bound on $U(\mathbf{c})$ in general. For instance, if C contains the all-one vector, then $U(\mathbf{c}) \le \dfrac{n}{2d}$ holds for at least $|C|/2$ codewords, which asymptotically yields

$$P \gtrsim (|C|/2)^{2d/n}.$$

These inequalities suggest that P tends to be quite large. In the next section, we show that this in fact holds for typical codes.

3 Distribution of Minimal Supports in Random q-ary Codes.

Let H be an $r \times n$ matrix whose entries are chosen independently with uniform distribution from $\mathbb{F}_q$. Let $\mathcal{P}$ be the set of minimal supports w.r.t. H and

$$X_w = |\{\text{minimal supports of size } w\}|.$$

First, we note that $X_w = 0$ if $w \ge r + 2$. Indeed, suppose $I \subseteq E$ is a minimal support of size w with respect to H. Then the rank of H restricted to I, $\mathrm{rk}H(I) = w - 1 \le \mathrm{rk}H \le r$. Hence $w \le r + 1$ and there are no minimal supports of size $\ge r + 2$.

In the remaining part of this section, we shall calculate the average number $E(X_w)$ and variance $D(X_w)$. Denote by d the distance of the code $\ker H$. Number all supports of size w from 1 to $\binom{n}{w}$ and denote the ith support by S_i. Let ξ_i be a random variable that equals 1 or 0 according as S_i is minimal or not. Then $X_w = \sum \xi_i$ and $E(X_w) = \sum E(\xi_i)$. Let

$$p = \Pr\{\xi_i = 1\}.$$

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

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

Since the total number of possible choices is q^{wr}, we have

$$E(\xi_i) = p = (q-1)^{w-1}\prod_{i=0}^{w-2}(q^r-q^i)/q^{wr}.$$

Let us now estimate $D(X_w)$.

$$\begin{aligned} D(X_w) = D(\sum \xi_i) &= E(\sum \xi_i)^2 - (E(\sum \xi_i))^2 \\ &= E(\sum_{i,j}\xi_i\xi_j) - (\binom{n}{w}p)^2 \\ &= E(\sum_i \xi_i^2) + E(\sum_{i\neq j}\xi_i\xi_j) - (\binom{n}{w}p^2) \\ &= E(\sum_i \xi_i) + \sum_{i\neq j}\Pr\{S_i, S_j \in \mathcal{P}\} - (\binom{n}{w}p)^2 \end{aligned} \tag{3.1}$$

We have

$$\begin{aligned} \Pr\{S_i, S_j \in \mathcal{P}\} &= \Pr\{S_i \in \mathcal{P}\}\Pr\{S_j \in \mathcal{P} | S_i \in \mathcal{P}\} \\ &= \begin{cases} p^2, & S_i \cap S_j = \emptyset \\ p\dfrac{(q^r-q^l)(q^r-q^{l+1})\dots(q^r-q^{w-2})(q-1)^{w-1}}{q^{r(w-l)}}, & |S_i \cap S_j| = l, \end{cases} \end{aligned}$$

since in the last case we know that l columns are independent. Rewrite the last line as

$$p^2\frac{q^{rl}}{(q^r-1)(q^r-q)\dots(q^r-q^{l-1})}. \tag{3.2}$$

Now,

$$\prod_{j=0}^{l-1}\frac{(q^r-q^j)}{q^r} = \prod_{u=r-l+1}^{r}(1-q^{-u}) > 1 - \sum_{u=r-l+1}^{r} q^{-u} > 1 - q^{-(r-l)}, \tag{3.3}$$

and, continuing from (3.2), one gets for the case $S_i \cap S_j \neq \emptyset$

$$\Pr\{S_i, S_j \in \mathcal{P}\} < p^2 \frac{1}{1-q^{-(r-l)}} < p^2 \frac{q}{q-1}. \tag{3.4}$$

Continue from (3.1) as follows:

$$D(X_w) < \binom{n}{w}p + \binom{n}{w}\binom{n-w}{w}p^2 + \binom{n}{w}\sum_{l=1}^{w-1}\binom{w}{l}\binom{n-w}{w-l}\frac{q}{q-1}p^2 - (\binom{n}{w}p)^2. \tag{3.5}$$

Now,

$$\sum_{l=1}^{w-1}\binom{w}{l}\binom{n-w}{w-l} = \Big[\binom{n}{w} - \binom{n-w}{w} - 1\Big]$$

and (3.5) yields

$$\begin{aligned} D(X_w) &< \binom{n}{w}p + \binom{n}{w}\binom{n-w}{w}p^2 + \frac{q}{q-1}p^2\binom{n}{w}\Big[\binom{n}{w} - \binom{n-w}{w} - 1\Big] \\ &\quad -\binom{n}{w}^2 p^2 \\ &= \binom{n}{w}p(1 - \frac{q}{q-1}p) + \frac{1}{q-1}\binom{n}{w}p^2\Big[\binom{n}{w} - \binom{n-w}{w}\Big]. \end{aligned}$$

For binary codes, this estimate can be slightly improved. Namely, $|S_i \cap S_j| = l$ implies $l \leq w - \lceil d/2 \rceil \leq r + 1 - \lceil d/2 \rceil$, and denoting $\theta = (1 - 2^{-(\lceil d/2 \rceil - 1)})^{-1}$, we get in (3.4) $\Pr\{S_i, S_j \in \mathcal{P}\} < p^2\theta$. The remaining part is performed as above.

Let us summarize these calculations as follows.

Theorem 3.1. *$X_w = 0$ if $w \geq r + 2$. Otherwise.*

$$E(X_w) = \binom{n}{w}p = \binom{n}{w}\frac{(q-1)^{w-1}}{q^r}\prod_{i=0}^{w-2}(1 - q^{-(r-i)}), \tag{3.6}$$

$$D(X_w) < \binom{n}{w}p(1 - \frac{q}{q-1}p) + \frac{1}{q-1}\binom{n}{w}p^2\Big[\binom{n}{w} - \binom{n-w}{w}\Big]. \tag{3.7}$$

For binary codes, the following estimate holds:

$$\begin{aligned} D(X_w) \ &< \binom{n}{w}p(1-\theta p) + \binom{n}{w}p^2(\theta - 1)\Big[\binom{n}{w} - \binom{n-w}{w}\Big], \\ &\theta = 1/(1 - 2^{-(\lceil d/2 \rceil - 1)}). \end{aligned} \tag{3.8}$$

Let us consider asymptotics. Suppose $n \to \infty$, $n - r$ and d grow linearly in n, and let $w = r + 1 - u$. The average number of nonproportional codewords in C equals $E(C_w) = \binom{n}{w}(q-1)^{w-1}/q^{n-k}$. Let

$$\alpha_q(u) = E(X_w)/E(C_w) = \prod_{i=u+1}^{r}(1 - q^{-i}),$$

be the average fraction of minimal codewords. Then (3.3) shows that if $u \to \infty$, then $\alpha_q(u) \to 1$. If $u = \text{const}$, then $1/2 < \lim \alpha_q(u) < 1$ except for the case $q = 2, u = 0$, when $\alpha_2(0) \to 0.2887$.

For $q = 2$, we can derive the following asymptotical approximation to $D(X_w)$ in (3.8).

$$\begin{aligned} D(X_w) &= \binom{n}{w} p + \binom{n}{w}^2 \theta p^2 - \binom{n}{w}^2 p^2 - \binom{n}{w}\binom{n-w}{w} p^2(\theta - 1) - \binom{n}{w}\theta p^2 \\ &\lesssim \binom{n}{w} p + \binom{n}{w}^2 (1 + 2^{-d/2}) p^2 - \binom{n}{w}^2 p^2 \\ &= \binom{n}{w} p (1 + 2^{-d/2} p \binom{n}{w}). \end{aligned}$$

Since

$$2^{-d/2} p \binom{n}{w} < 2^{n(H(1-R)-(1-R)-(d/2n))},$$

one observes that, at least for small rates, this term tends to 0. Thus, for small rates we can infer that, by Chebyshev's inequality, asymptotically the probability

$$\Pr\{|X_w - E(X_w)| > \gamma \sqrt{E(X_w)}\} \lesssim \gamma^{-2}.$$

Remark. The variance of the total number of codewords of weight w in a random linear code is less than $(q-1)$ times their average number. This is seen by taking X_w equal to the number of weight w codewords and proceeding as in (3.1).

4 Minimal Supports of Codes over Rings.

Our understanding of Galois rings follows the exposition in [6]. Let S be a Galois ring, i.e., a finite commutative ring with identity e, whose set of zero divisors has the form pS for a certain prime p. Denote by $S^\times$ the set of ring units (invertible elements). It is known 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. All ideals of S form the following chain:

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

and $|N_i| = q^{m-i}$. Thus, N_1 is a unique maximal ideal in S.

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

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

will be called the *type* of the word $\mathbf{c}$. Let us call the number $T(I) = \min_{\text{supp } \mathbf{c} = I} T(\mathbf{c})$ 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 4.1. 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 minimal subsets of type t will be denoted by $\mathcal{P}_t(C)$.
Examples.

1. Let $\mathcal{H}_v$ be the code over $\mathbb{Z}_4$ with the $(v+1) \times 2^v$ parity check matrix

$$\begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & 2 \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & 2 & \ldots & 2 \\ 0 & 2 & 0 & \ldots & 2 \end{bmatrix}$$

whose columns are 1 and all the $n = 2^v$ possible vectors of zeros and twos. Its binary image formed by the mapping $(0 \to 00, 1 \to 10, 2 \to 11, 3 \to 01)$ is a nonlinear $(2^{v+1}, 2^{2^{v+1}-(v+1)-1}, 4)$ code. Let $\mathcal{P} = \mathcal{P}_0 \cup \mathcal{P}_1$ be the set of minimal supports with respect to $\mathcal{H}_v$.

Theorem 4.2. *The number of minimal supports of type* 0 *and size* w *in* $\mathcal{H}_v$ *equals*

$$B_w^{(0)} = \frac{1}{w!} 2^v \prod_{i=0}^{w-3} (2^v - 2^i), \quad 4 \leq w \leq v+1, \ w \text{ even.} \tag{4.1}$$

Every pair of coordinates forms a minimal support of type 1, thus,

$$B_2^{(1)} = \binom{n}{2}. \tag{4.2}$$

Proof. All the words of weight 2 with two 2s are contained in the code, which proves (4.2). Let us prove (4.1). Suppose $I \in \mathcal{P}_0$ and $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ is a codeword with $\operatorname{supp} \mathbf{c} = I$, then all nonzero entries of $\mathbf{c}$ are units of $\mathbb{Z}_4$. For suppose not and $\mathbf{c} = (c_0, c_1, \ldots, c_{w-3}, 2, 2, 0, \ldots, 0), w = |I|$. Since $2(\mathbf{h}_{w-2} + \mathbf{h}_{w-1}) = 0$,

$$\sum_{i=0}^{w-3} c_i \mathbf{h}_i = 0.$$

Thus, I cannot be minimal. In this way we see that $\mathbf{c}$ cannot contain more than one coordinate equal to 2. Suppose $\mathbf{c} = (c_0, c_1, \ldots, c_{w-2}, 2, 0, \ldots, 0)$, then $\sum_{i=0}^{w-2} c_i = 2$. Therefore, for any I the codeword $(c_0, \ldots, -c_i, \ldots, c_{w-2}, 0 \ldots, 0)$ has for support a proper subset of I, a contradiction. Thus, all nonzero entries of $\mathbf{c}$ are either 1s or -1s. Therefore, w is even.

Generally, $\sum c_{i_j} \mathbf{h}_{i_j} = c_{i_w} \mathbf{h}_{i_w}$, where all $c_{i_j} = \pm 1$, implies $-c_{i_1} \mathbf{h}_{i_1} + \sum_{j=2}^{w-1} c_{i_j} \mathbf{h}_{i_j}$ $= -c_{i_w} \mathbf{h}_{i_w}$. Thus, any choice of the first coordinates within the ring units defines one and the same support.

Let us count the number of ways we can choose I. For I to be minimal of type 0 it is necessary that any (say, first) $w-1$ columns in it have "full rank" (i.e., the size of the space spanned by $\mathbf{h}_{i_1}, \ldots, \mathbf{h}_{i_{w-1}}$ with coefficients ± 1 is 2^{w-1}) and $\sum_{j=1}^{w-1} \mathbf{h}_{i_j} = \pm h_{i_w}$. Note that only an odd number of columns taken with coefficients ± 1 can be equal to a column of H and that the minimum Lee weight of $\mathcal{H}_v$ is 4. So we have n possibilities for i_1, $n-1$ possibilities for i_2, $n-2$ possibilities for i_3, $n-4$ possibilities for i_4, and so on,

$$n - \sum_{\substack{j=1 \\ j \text{ odd}}}^{t-1} \binom{t-1}{j} = n - 2^{t-2}$$

possibilities for i_t. Hence, the number of ways of choosing $w-1$ columns is $N = n(n-1)\ldots(n-2^{w-3})$. To prove (4.1), observe that any $w-1$ of w columns within I can be taken for the "first" ones and their order is irrelevant. Thus,

$$N = \binom{w}{w-1}(w-1)!B_w^{(0)} = w!B_w^{(0)}.$$

□

2. Consider the 1st order Reed-Muller code $ZRM(1,v)$ of length $n = 2^v$ over $\mathbb{Z}_4$ [7]. This code is orthogonal over $\mathbb{Z}_4$ to the code $\mathcal{H}_v$ of Example 1. It can be easily seen that the only codewords containing 1s and 3s are those of weight n. The remaining words of weight $n/2$ consist of 0s and 2s. Thus, $\mathcal{P}_0$ consists of a single set $\{0, 1, \ldots, n-1\}$ and $\mathcal{P}_1$ is formed by $2^{v+1}-2$ subsets (supports of words) of size $n/2$.

3. Let C be the $\mathbb{Z}_4$ "Kerdock" code of length $n = 2^v$, v odd, [6, 7], i.e., the code whose binary image is (equivalent to) the Kerdock code. 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 $n/2$.

5 An Application to Secret Sharing.

The concept of secret sharing 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 $\mathcal{U} = \{p_1, \ldots, p_{n-1}\}$ 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. If this information is void, the corresponding secret-sharing scheme is called *perfect*. A nonperfect scheme includes partially authorized coalitions of users. This could find application in banking systems,

where s_0 would be a resource rather than a secret, divided into a number of parts, and a hierarchical access to it should be organized. Thus, one should specify the amount of resource accessible to every coalition. Nonperfect schemes were studied in a number of works both from the point of view of information-theoretical security [8] and combinatorial characterization [9].

The collection of (fully and partially) authorized coalitions of the scheme is called an *access structure*.

Let us define the algorithm for generating shares. Suppose the values of shares and the secret are taken from the Galois ring S of q^m elements. Let us introduce an additional user p_0, which formally corresponds to D. Let $\mathbf{h}_0, \ldots, \mathbf{h}_{n-1}, \mathbf{e} \in (S)^r, r \geq 1$, be column vectors and suppose that at least one entry 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 value s_0 can be also viewed as the share of p_0. Let C be the code for which $\widetilde{H} = (\mathbf{h}_0, \mathbf{h}_1, \ldots, \mathbf{h}_{n-1})$ is a parity-check matrix.

A connection between minimal codewords in linear codes and access structures was pointed out in [3, 4]. Our aim is to extend this connection to codes over Galois rings. Namely, we prove that the access structure is determined by the collection of minimal supports of C of types $t, 0 \leq t \leq m-1$, for which there exists a codeword $\mathbf{c} \in C$ whose first coordinate $c_0 \in N_t$.

Theorem 5.1. *Suppose $I = \{i_1, \ldots, i_l\} \subset \{1, \ldots, n-1\}$ and $\widetilde{I} = \{0\} \cup I$ is a minimal subset of type t such that there exists a codeword $\mathbf{c} \in C$, $\operatorname{supp} \mathbf{c} = \widetilde{I}$, with $c_0 \in N_t$. Then the coalition $\{p_j, j \in I\}$ can reconstruct exactly $m-t$ q-ary symbols of s_0.*

Proof. Denote the matrix $(\mathbf{h}_1, \ldots, \mathbf{h}_{n-1})$ by 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

$$\mathbf{e}\widetilde{H} = \widetilde{\mathbf{s}} \tag{5.1}$$

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

$$\mathbf{e}H = \mathbf{s} \tag{5.2}$$

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 5.2. *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*

$$t = \min\{v : \exists d \in N_v \text{ such that } d\mathbf{h}_0 \in U\}. \tag{5.3}$$

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 $q^n/q^{n-t} = q^t$. □

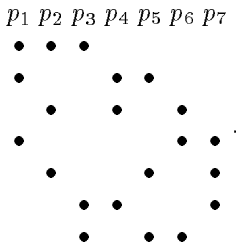
Lemma 5.3. *Suppose that* $|L(H,\mathbf{s})| > 0$, *then* $|L(\widetilde{H},\widetilde{\mathbf{s}})| > 0$ *iff* $p^t s_0 = -\sum_{j\in I} c_j s_j$, *where* t *is defined in* (5.3).

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 column space. Therefore, there are q^w vectors $\mathbf{s}$ for which system (5.2) 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 (5.1) has a solution. □

We conclude the proof of the theorem 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 (5.1), this set of equations is either contradictory or has one and the same number of solutions. □

Thus, we get a hierarchy of fully and partially authorized coalitions of users. A coalition γ of type t can locate the secret within q^t out of q^m elements of S.

Continuing from Example 2 above, we observe that in the secret-sharing scheme defined by the $ZRM(1,v)$ code, there is a single coalition of users ($\mathcal{U}$ itself) that can fully reconstruct the secret. Further, half of minimal subsets in $\mathcal{P}_1$ involve the coordinate 0; therefore, there are $2^v - 1$ half-authorized coalitions of users, i.e., those who can retrieve only one of the two bits of the secret. They are the following:



References

1. D. J. A. Welsh, *Matroid Theory*, Academic Press (1976).
2. T.-Y. Hwang, "Decoding linear block codes for minimizing word error rate," *IEEE Trans. Inf. Theory*, **IT-25**, No. 6 (November 1979), 733–737.
3. J. Massey, "Minimal codewords and secret sharing," in: *Proc. Sixth Joint Swedish-Russian Workshop Inf. Theory, Mölle, Sweden* (1993), pp. 246–249.
4. 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.
5. A. Ashikhmin and A. Barg, "Minimal vectors in linear codes and sharing of secrets," Preprint 94-113, SFB 343 "Diskrete Structure in der Mathematik," Universität Bielefeld (1994).
6. A. A. Nechaev, "Kerdock code in a cyclic form," *Diskret. Mat.*, **1**, no. 4 (1989), 123–139. English translation in *Discrete Math. Appl.*, **1** (1991), 365–384.
7. A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inf. Theory*, **40**, no. 2 (1994), 301–319.
8. G. R. Blakley and C. Meadows, "Security of ramp schemes," in: *Advances in Cryptology, Proc. CRYPTO '84*, G. R. Blakley and D. Chaum, Eds., Springer Lect. Notes Comput. Sci., **196** (1985), pp. 242–268.
9. K. Kurosawa, K. Okada, K. Sakano, W. Ogata, and S. Tsujii, "Nonperfect secret sharing schemes and matroids," in: *Proc. EUROCRYPT '93*, Springer Lect. Notes Comput. Sci., **765** (1994), pp. 126–141.

This article was processed using the LaTeX macro package with LLNCS style