**ENEE 739C: Advanced Topics in Signal Processing: Coding Theory**
**Instructor: Alexander Barg**

Lecture 6a (**draft;** 9/21/03). Linear codes. Weights, supports, ranks.

http://www.enee.umd.edu/~abarg/ENEE739C/course.html

The goal of this lecture is to study general properties of linear codes. Let $\mathcal{C}$ be a $q$-ary $[n,k]$ code with weight distribution $\{A_i, i=0,1,\dots,n\}$. Let $\mathbf{G},\mathbf{H}$ be a generator and a parity-check matrix of $\mathcal{C}$. The *dual* code $\mathcal{C}^\perp$ is the set

$$\mathcal{C}^\perp = \{\mathbf{x}\in \mathscr{H}_q^n : \mathbf{H}\mathbf{x}^T = 0\}.$$

Let $i$ be a not all-zero coordinate. We have

$$|\{\mathbf{c}\in\mathcal{C} : c_i = 0\}| = \frac{1}{q}|\mathcal{C}|$$

A *shortening* of $\mathcal{C}$ on the coordinate $i$ is the $[n-1,k-1,d]$ linear code obtained by leaving only such codewords and deleting the $i$th coordinate.

Let $[n] := \{1,\dots,n\}$, $E\subset[n], \bar{E} = [n]\backslash E$. For a matrix $\mathbf{M}$ with $n$ columns we denote by $\mathbf{M}(E)$ the submatrix formed by all the columns with numbers in $E$. The *support* of a vector $\mathbf{x}\in\mathscr{H}_q^n$ is defined as $\mathrm{supp}(\mathbf{x}) = \{i : x_i\neq 0\}$. Given a subcode $\mathcal{A}\subset\mathcal{C}$, its support is

$$\mathrm{supp}(\mathcal{A}) = \{i\in[n] : \exists_{\mathbf{a}\in\mathcal{A}}\, a_i\neq 0\}$$

A *shortening* of $\mathcal{C}$ on the coordinates in $\bar{E}$ is a linear code $\mathcal{C}^E$ such that $\forall_{\mathbf{x}\in\mathcal{C}^E}\,\mathrm{supp}(\mathbf{x})\subset E$.

A projection of $\mathcal{C}$ on the coordinates in $\bar{E}$, also called *puncturing*, is a restriction of $\mathcal{C}$ to the coordinates in $E$ (simply said, deleting the coorinates in $\bar{E}$ from every codevector of $\mathcal{C}$ and deleting repeated entries from the result). The basic facts about shortenings and puncturings are given in the following

**Theorem 1.**

(i) *If $t\le d(\mathcal{C})-1$, then $\mathcal{C}_E$ is an $[n-t,k,\ge d(\mathcal{C})-t]$ code.*

(ii) $\dim\mathcal{C}^E = |E| - \mathrm{rk}(\mathbf{H}(E)), \dim(\mathcal{C}_E) = \mathrm{rk}(\mathbf{G}(E)), \dim(\mathcal{C}_E) + \dim((\mathcal{C}^\perp)^E) = |E|$.

(iii) $\mathcal{C}_E\cong\mathcal{C}/\mathcal{C}^{\bar{E}}$.

(iv) $(\mathcal{C}_E)^\perp = (\mathcal{C}^\perp)^E$; $(\mathcal{C}^E)^\perp = (\mathcal{C}^\perp)_E$.

*Proof :* (i), (iii) are obvious. (ii) is counting the number of solutions of a system of linear equations. Let us prove the first part of (iv). Let $a\in(\mathcal{C}^\perp)^E$, then $\mathbf{G}(E)a^T = 0$, so $a\in(\mathcal{C}_E)^\perp$. Further, by (ii)

$$\begin{aligned}\dim(\mathcal{C}^\perp)^E &= |E| - \mathrm{rk}(\mathbf{G}(E))\\ &= |E| - \dim\mathcal{C}_E = \dim(\mathcal{C}_E)^\perp.\end{aligned}$$

The second part of (iv) is analogous. ∎

Recall the notation for the Gaussian binomial coefficient:

$$\begin{bmatrix} n\\ k\end{bmatrix} == \prod_{i=0}^{k-1}\frac{q^{n-i}-1}{q^{k-i}-1}$$

In other words,

$$\begin{bmatrix} n\\ k\end{bmatrix} = \frac{[n]}{[k][n-k]}\quad \text{where } [u] = \prod_{i=0}^{u-1}(q^u-1).$$

**Lemma 2.** *The number of linear $[n,k]$ codes is $\begin{bmatrix} n\\ k\end{bmatrix}$.*

*Proof :* $\begin{bmatrix} n\\ k\end{bmatrix}$ equals the number of choices of $k$ linearly independent vectors in $\mathscr{H}_q^n$ divided by the number of different bases of an $[n,k]$ code. ∎

**Lemma 3.** *Let $|E| = w$. Then*

$$|E| - \mathrm{rk}(\mathbf{H}(E)) = k - \mathrm{rk}(\mathbf{G}(\bar{E})) \tag{1}$$

*Proof :* Let $\mathcal{C}_E = \mathrm{proj}_E\,\mathcal{C}$ be the projection of $\mathcal{C}$ on the coordinates in $E$. Clearly, $\dim \mathcal{C}_E = \mathrm{rk}(\mathbf{G}(E))$. On the other hand, $\mathcal{C}_E \cong \mathcal{C}/\mathcal{C}^{\bar{E}}$ by Theorem 1(iii); hence by (ii)

$$\dim \mathcal{C}_E = k - \dim \mathcal{C}^{\bar{E}} = k - |E| + \mathrm{rk}(\mathbf{H}(\bar{E})).$$

∎

This lemma bridges linear codes with the branch of combinatorics known as matroid theory. It turns out that it is possible to abstract from the linear-algebraic setting and define dependencies axiomatically. One starts with a finite set $[n]$ and calls some of its subsets independent, making sure they satisfy the same set of natural conditions that the subsets of linearly independent vectors would. Then for any subset $E \subset n$ one defines its rank as the size of a maximum independent subset contained in it. A large number of properties of independent sets and other subsets can be proved in this purely axiomatic setting, see [18]. Matroid theory finds uses in coding theory [4, 6], cryptography [5], information theory [10], multiuser communication [17] graph theory, topology [11].

Even though we will not use this here, we wish to point out that this lemma contains the MacWilliams identities in disguise. Recall that ENEE722 gives a different proof of these identities, via the Fourier transform. Both proofs are due to F. J. MacWilliams [15].

Let $n, i$ be nonnegative integers. Recall that

$$\binom{n}{i} = \begin{cases} \frac{n(n-1)\ldots(n-i+1)}{i!} & i \le n \\ 1 & i = 0 \\ 0 & \text{otherwise} \end{cases}$$

In partilucar, $\binom{0}{i} = \delta_{0,i}$.

**Lemma 4.** (The MacWilliams identities)

$$\sum_{i=0}^{n-u} A_i^{\perp} \binom{n-i}{u} = |\mathcal{C}^{\perp}| q^{-u} \sum_{i=0}^{u} A_i \binom{n-i}{n-u}. \tag{2}$$

*Proof :* We have the following chain of equalities:

$$\begin{aligned} \sum_{i=0}^{n-u} A_i^{\perp} \binom{n-i}{u} &= \sum_{|E|=n-u} |(\mathcal{C}^{\perp})^E| \\ &= \sum_{|E|=n-u} q^{n-u-\mathrm{rk}(\mathbf{G}(E))} \\ &= q^{n-k-u} \sum_{|E|=n-u} q^{u-\mathrm{rk}(\mathbf{H}(\bar{E}))} \\ &= q^{n-k-u} \sum_{i=0}^{u} A_i \binom{n-i}{n-u}. \end{aligned} \tag{3}$$

Here the first equality follows by counting in two ways the size of the set

$$\{(E, c) : |E| = n - u \text{ and } \mathbf{c} \in (\mathcal{C}^{\perp})^E, \mathrm{wt}(\mathbf{c}) \le n - u\},$$

the second one is straightforward, the third one (the central step in the proof) is implied by Lemma 3, and the final step follows by the same argument as the first one. ∎

A familiar form of these identities is obtained by using the weight enumerators of the code $\mathcal{C}$ and its dual code $\mathcal{C}^{\perp}$. We have

$$A(x, y) = \frac{1}{|\mathcal{C}^{\perp}|} A(x + (q-1)y, x - y).$$

The MacWilliams identities exist in a variety of different forms, see [13].

*Remark.* You should be aware that the linear-algebraic approach to the MacWilliams identities is only one of a number of possible points of view. First of all, a substantial portion of the results above can be extended to nonlinear codes [16, Ch.5,6]. A combinatorial perspective is given in P. Delsarte [8], see also

[16, Ch. 21], [9]. An approach via harmonic analysis is given in G. Kabatiansky and V. Levenshtein [14], see also [7, Ch.9].

Binomial moments of the weight distribution. The quantities

$$C_w = \sum_{i=0}^{w} A_i \binom{n-i}{n-w} \quad (w = 0, 1, \ldots, n)$$

are called *binomial moments* of the weight distribution of the code $\mathcal{C}$. We have seen (3) that

$$C_w = \sum_{|E|=w} q^{\dim(\mathcal{C}^E)}.$$

Clearly for an $[n, k, d]$ code, $C_0 = 1, C_w = \binom{n}{w}, w = 1, \ldots, d-1$. It is possible to express the weight coefficients via the binomial moments.

**Lemma 5.**

$$A_i = \sum_{w=0}^{i} (-1)^{i-w} \binom{n-w}{n-i} C_w.$$

*Proof :*

$$\begin{aligned}
\sum_{w=0}^{i} (-1)^{i-w} \binom{n-w}{n-i} C_w &= \sum_{w=0}^{i} (-1)^{i-w} \binom{n-w}{n-i} \sum_{j=0}^{w} \binom{n-j}{n-w} A_j \\
&= \sum_{j=0}^{i} A_j \sum_{w=0}^{j} (-1)^{i-w} \binom{n-w}{n-i} \binom{n-j}{n-w} \\
&= \sum_{j=0}^{i} A_j \binom{n-j}{n-i} \sum_{w=0}^{j} (-1)^{i-w} \binom{i-j}{i-w} \\
&= A_i
\end{aligned}$$

∎

**Lemma 6.** *Let $A(x, y)$ be the weight enumerator of $\mathcal{C}$ and let $C(x, y) = \sum_{w=0}^{n} C_w x^{n-w} y^w$.*

$$A(x, y) = C(x - y, y)$$

*Proof :*

$$\begin{aligned}
\sum_{w=0}^{n} C_w (x-y)^{n-w} y^w &= \sum_{w=0}^{n} C_w y^w \sum_{j=0}^{n-w} (-1)^{n-w-j} x^j y^{n-w-j} \binom{n-w}{j} \\
&= \sum_{j=0}^{n} x^j y^{n-j} \sum_{w=0}^{n-j} (-1)^{n-w-j} C_w \binom{n-w}{j} \\
&= \Big\{ i = n - j \Big\} = \sum_{j=0}^{n} x^j y^{n-j} \sum_{w=0}^{i} (-1)^{i-w} \binom{n-w}{n-i} C_w \\
&= \sum_{i=0}^{n} x^{n-i} y^i A_i.
\end{aligned}$$

∎

From (2)

$$C^{\perp}_{n-u} = q^{n-k-u} C_u \quad (u = 0, \ldots, n).$$

Introducing the weight enumerators $C(x, y) = \sum C_i x^{n-i} y^i, C^{\perp}(x, y) = \sum C^{\perp}_i x^{n-i} y^i$ we then have

$$\sum C^{\perp}_{n-u} x^{n-u} y^u = q^{-k} \sum C_u (xq)^{n-u} y^u$$

$$C^{\perp}(y, x) = q^{-k} C(qx, y),$$

a remarkably simple form of the MacWilliams equation.

An interesting observation about the binomial moments is that while it is not possible to bound below individual coefficients of the weight distribution, it is possible to do this for linear combinations of these coefficients (binomial moments). Here is one possibility:

**Theorem 7.**

$$C_w \geq \binom{n}{w} q^{\max(0,w-n+k)}$$

*Proof :* Let $E \subseteq [n]$. We have

$$\dim(C^E) = |E| - \mathrm{rk}(\mathbf{H}(E)) \geq \binom{n}{w} q^{w-\min(w,n-k)} = \binom{n}{w} q^{\max(0,w-n+k)}$$

∎

This result can be applied to bounding the probability of undetected error $P_u$ of a linear $[n,k]$ code. We have

**Theorem 8.** [1] *Let $\mathcal{C}$ be an $[n,k]$ linear $q$-ary code.*

$$P_u \geq \sum_{w=n-k+1}^{n} \binom{n}{w} (q^{w-n+k}-1)\Big(\frac{p}{q-1}\Big)^w \Big(1-\frac{q}{q-1}p\Big)^{n-w}.$$

*Proof :* From the previous theorem,

$$C_w - \binom{n}{w} \geq \binom{n}{w} \max(0, q^{w-n+k}-1).$$

Then

$$\begin{aligned}
P_u(\mathcal{C}) &= A(1-p, \frac{p}{q-1}) - (1-p)^n = C\Big(1-p\frac{q}{q-1}, \frac{p}{q-1}\Big) - (1-p)^n \\
&= \sum_{w=0}^{n} C_w \Big(\frac{p}{q-1}\Big)^w \Big(1-\frac{q}{q-1}p\Big)^{n-w} - \sum_{w=0}^{n} \binom{n}{w}\Big(\frac{p}{q-1}\Big)^w \Big(1-\frac{q}{q-1}p\Big)^{n-w} \\
&= \sum_{w=0}^{n} (C_w - \binom{n}{w})\Big(\frac{p}{q-1}\Big)^w \Big(1-\frac{q}{q-1}p\Big)^{n-w} \\
&\geq \sum_{w=0}^{n} \binom{n}{w} \max(0, q^{w-n+k}-1)\Big(\frac{p}{q-1}\Big)^w \Big(1-\frac{q}{q-1}p\Big)^{n-w}
\end{aligned}$$

∎

In many cases the results of the last two theorems can be improved and generalized (to nonlinear codes), see [3]. The next exercise is the first step along this way.

Exercise. (Forget the 0) Try to define binomial moments of the distance distribution $C_w$ for an unrestricted (i.e., not necessarily linear) binary code $\mathcal{C}$. Begin with the following question: what is the support of a subcode? (Hint: start with subcodes of size 2). Prove that Lemma 6 still holds true, with $A(x,y)$ replaced by the distance enumerator $B(x,y)$.

THE RANK FUNCTION. Rewrite (3) by collecting on the right-hand side subsets of one and the same rank. Namely, let

$$U_u^v = |\{E \subseteq \{1,2,\ldots,n\} \mid |E| = u, \mathrm{rk}(\mathbf{G}(E)) = v\}|.$$

For instance, $U_k^k$ is the number of information sets of the code $\mathcal{C}$.

By (3) and Theorem 1(ii) we have

$$\sum_{i=0}^{w} \binom{n-i}{n-w} A_i = \sum_{v=0}^{n-k} q^{w-v} (U^\perp)_w^v, \tag{4}$$

where the numbers $U^\perp$ are the rank coefficients of $\mathcal{C}^\perp$. Further, Lemma 3 implies that

$$(U^\perp)_u^{u-k+v} = U_{n-u}^v. \tag{5}$$

The last two equations relate the weight enumerator of $\mathcal{C}$ and its *rank distribution* $(U_u^v,\ 0 \leq u \leq n, 0 \leq v \leq k)$.

*Example.* (MDS codes) An $(n, M, d)$ code is called *maximum distance separable* (MDS) if $M = q^{n-d+1}$. Let $\mathcal{C}$ be an $[n, k, n-k+1]$ $q$-ary linear MDS code with a parity-check matrix $\mathbf{H}$. Then $\mathrm{rk}(\mathbf{H}(E)) = \min\{|E|, n-k\}$ for all $E \subseteq S$, $0 \le |E| \le n-k$. Therefore

$$(U^{\perp})_u^v = \begin{cases} \binom{n}{u} & \text{if } (0 \le v = u \le n-k) \text{ or } (u \ge n-k+1,\ v = n-k); \\ 0 & \text{otherwise.} \end{cases}$$

This enables us to compute the weight spectrum of $\mathcal{C}$. Substituting the values of $(U^{\perp})_u^v$ into (4), we obtain $A_0 = 1$, $A_i = 0$ for $1 \le i \le n-k$, and

$$A_{n-k+\ell} = \binom{n}{k-\ell} \sum_{j=0}^{\ell-1} (-1)^j \binom{n-k+\ell}{j} (q^{\ell-j} - 1) \quad (1 \le \ell \le k).$$

**Definition 1.** *The rank polynomial of a linear code $\mathcal{C}$ is*

$$U(x, y) = \sum_{u=0}^{n} \sum_{v=0}^{k} U_u^v x^u y^v.$$

Relations of the rank polynomial of $\mathcal{C}$, its dual code $\mathcal{C}^{\perp}$, and the weight polynomial of $\mathcal{C}$ are given by the following results.

**Theorem 9.**

$$U^{\perp}(x, y) = x^n y^{\dim \mathcal{C}^{\perp}} U\Big(\frac{1}{xy}, y\Big).$$

*Proof :* We have

$$\begin{aligned} U^{\perp}(x, y) &= \sum_{u=0}^{n} \sum_{v=0}^{n-k} (U^{\perp})_u^v x^u y^v = \sum_{u=0}^{n} \sum_{v=0}^{n-k} U_{n-u}^{k-u+v} x^u y^v \qquad \text{(by (5))} \\ &= x^n \sum_{u=0}^{n} \sum_{v=0}^{n-k} U_u^{k-n+u+v} x^{-u} y^v \qquad (6) \\ &= x^n y^{n-k} \sum_{u=0}^{n} \sum_{v=0}^{n-k} U_u^{u-v} (xy)^{-u} y^{u-v} \\ &= x^n y^{n-k} \sum_{u=0}^{n} \sum_{v=u-n+k}^{u} U_u^v (xy)^{-u} y^v. \qquad (7) \end{aligned}$$

Now let $|E| = n - u, \mathrm{rk}(\mathbf{G}(\bar{E})) = v$. Then $|\bar{E}| = u$ and by (1)

$$0 \le \mathrm{rk}(\mathbf{H}(E)) = |E| - k + v = v - (u - n + k).$$

Hence, for $0 \le v \le u - n + k - 1$ we have $U_u^v = 0$. Thus, the summation interval of $v$ in (7) can be extended to $0 \le v \le u$. ∎

**Theorem 10.**

$$A(x, y) = y^n |\mathcal{C}|\ U\Big(\frac{x-y}{y}, \frac{1}{q}\Big) = (x-y)^n U^{\perp}\Big(\frac{qy}{x-y}, \frac{1}{q}\Big).$$

Information profile of a linear code. Let $\mathcal{C}$ be a linear code, $[n] = \{1, \ldots, n\}$, $E \subset [n]$. Consider the average (over the choice of $E$) dimension of the code $C_E$ :

$$e_w = \binom{n}{w}^{-1} \sum_{E \in \binom{[n]}{w}} \dim(\mathcal{C}_E).$$

The number $e_w$ can be thought of an the average information content of a $w$-subset.

The numbers $(e_w, w = 1, \dots, n)$ constitute the *information profile* of the code $\mathcal{C}$. Since $\dim(C_E) = \mathrm{rk}(\mathbf{G}(E))$, where $G$ is the generator matrix of $\mathcal{C}$, we can also write

$$\binom{n}{w} e_w = \sum_{i=0}^{w} i U_w^i(\mathcal{C}).$$

The information profile was introduced for its one sake in [12] and was used recently in analyzing iterative decoding. Paper [12] also computes the average value of $e_w$ over all $[n, k]$ codes.

Minimal vectors in linear codes.

For the vectors $\mathbf{x}, \mathbf{y} \in \mathscr{H}_q^n$ we write $\mathbf{x} \prec \mathbf{y}$ ($\mathbf{x} \preceq \mathbf{y}$) if $\mathrm{supp}(\mathbf{x}) \subset \mathrm{supp}(\mathbf{y})$ (resp., $\mathrm{supp}(\mathbf{x}) \subseteq \mathrm{supp}(\mathbf{y})$).

**Definition 2.** *Let $\mathcal{C} \subset \mathscr{H}_q^n$ be a linear code. A nonzero vector $\mathbf{c} \in \mathcal{C}$ is called minimal if $0 \neq \mathbf{c}' \preceq \mathbf{c}$ implies $\mathbf{c}' = a\mathbf{c}$ where $\mathbf{c}'$ is another codevector and $a$ is a constant. In words: nonminimal vector covers a nonzero vector with a smaller support.*

Let $\mathbf{H}$ be a parity-check matrix of $\mathcal{C}$ and let $\mathcal{M}$ be the set of its minimal vectors. Let us list basic properties of minimal vectors.

**Lemma 11.**

*(i) Let $\mathbf{c} \in \mathcal{C}, U = \mathrm{supp}(\mathbf{c})$. Then $\mathbf{c} \in \mathcal{M}$ if and only if $\mathrm{rk}(\mathbf{H}(U)) = |U| - 1$.*

*(ii) ($U$ is minimal) $\Rightarrow$ ($|U| \leq n - k + 1$).*

*(iii) Every support of size $|U| \leq d(1 + \frac{1}{q-1}) - 1$ is minimal.*

*(iv) The linear span (the set of all linear combinations) of $\mathcal{M}(C)$ coincides with $C$. Moreover, if $q = 2$ then every nonzero codevector can be decomposed into a sum of minimal vectors with pairwise disjoint supports.*

*(v) Let $C$ be a binary code. Then if $\mathbf{c} \in C$, $\mathbf{c} \notin \mathcal{M}(C)$, then there is a pair of nonzero code vectors $\mathbf{c}_1 \prec \mathbf{c}$ and $\mathbf{c}_2 \prec \mathbf{c}$ with disjoint supports such that $\mathbf{c} = \mathbf{c}_1 + \mathbf{c}_2$.*

*Proof :* The *only if* part of (1) is obvious. Let us prove the converse. Let $\mathbf{h}_i$ be the $i$th column of $H(U)$. By assumption, there exist $w = |U|$ nonzero numbers $\lambda_i$ such that

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

and some $w - 1$ of these columns, say the first, are linearly independent. Suppose there exists a code vector $\mathbf{c}', \mathbf{c}' \prec \mathbf{c}$, 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,

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

with $\mu_w \neq 0$. Multiply this sum by $\lambda_w/\mu_w$ and subtract from the first one. This gives a linear dependence between the first $w - 1$ columns, a contradiction.

Part (ii) is implied by (i).

To prove part (iii), suppose that $\mathbf{c} \in \mathcal{C}$ is a nonminimal vector of weight $\mathrm{wt}(\mathbf{c}) \leq d\big(1 + \frac{1}{q-1}\big) - 1$ and let $\mathbf{c}' \prec \mathbf{c}, \mathbf{c}' \in \mathcal{C}\backslash\{0\}$. Consider $q - 1$ code vectors $\mathbf{c} - a\mathbf{c}'$, where $a$ runs over all nonzero constants. Summing up their weights, we get $(q-1)\,\mathrm{wt}(\mathbf{c}) - \mathrm{wt}(\mathbf{c}')$. Thus, their average weight is $\mathrm{wt}(\mathbf{c}) - (q-1)^{-1}\,\mathrm{wt}(\mathbf{c}')$. One of these vectors, say $\mathbf{c}''$ has weight at most the average. Together with our assumption this implies a contradiction:

$$\mathrm{wt}(\mathbf{c}'') \leq \mathrm{wt}(\mathbf{c}) - \frac{\mathrm{wt}(\mathbf{c}')}{q-1} \leq d\big(1 + \frac{1}{q-1}\big) - 1 - \frac{d}{q-1} = d - 1.$$

Part (iv) Let $\mathbf{c} \in \mathcal{C}\backslash\{0\}$. Suppose it is not minimal, then there is a minimal vector $\mathbf{m}_1$ such that $\mathrm{supp}(\mathbf{m}_1) \subset \mathrm{supp}(\mathbf{c})$. There always is a nonzero constant $a_1$ such that $(\mathbf{c} - a_1\mathbf{m}_1) \prec \mathbf{c}$. Denote $\mathbf{c}_1 = \mathbf{c} - a_1\mathbf{m}_1$. By the same argument, either $\mathbf{c}_1$ is minimal or there is an $\mathbf{m}_2 \in \mathcal{M}$ such that $(\mathbf{c}_1 - a_2\mathbf{m}_2) \prec \mathbf{c}_1$. Since the

size of the support falls by (at least) one in every step, for a certain $i$, the vector $\mathbf{c}_i$ will be minimal. Then $\mathbf{c}_i = \mathbf{c} - \sum_{j=1}^{i-1} a_j \mathbf{c}_j$.

Part (v) is obvious. ∎

How many minimal vectors are there in a typical linear code? Consider the ensemble given by random $(n-k) \times n$ parity-check matrices. Let $\mathsf{E}\, M_w$ be the expected number of minimal vectors of weight $w$.

**Theorem 12.** [2] *Let $w \le n-k+1$. Then*

$$\mathsf{E}\, M_w = \binom{n}{w} \frac{(q-1)^w}{q^{n-k}} \prod_{i=0}^{w-2} (1 - q^{-(n-k-i)}).$$

$$Var M_w \le \mathsf{E}\, M_w (1 + 2^{-d/2} \mathsf{E}\, M_w).$$

For the proof consult the source. In particular, this theorem implies that for $n \to \infty$ almost all vectors of weight $w \le n-k+1$ in a typical linear code are minimal.

The main uses of minimal vectors are in decoding of linear codes and cryptography (access structures in secret sharing schemes).

*Example*: Let $\mathcal{C}$ be an $[n = \frac{q^m-1}{q-1}, n-m-1, 3]$ Hamming code. We have

$$M_w = \frac{1}{w!} \prod_{i=0}^{w-2} (q^m - q^i), \qquad (3 \le w \le m+1).$$

*Proof:* Consider $s = w-1$ linearly independent columns in the parity-check matrix $\mathbf{H}$ 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 $\mathbf{H}$ 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 $\mathbf{H}$. This number equals

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

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

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

The substitution of the value of $n$ gives the desired result.

## References


1. K. A. S. Abdel-Ghaffar, *A lower bound on the undetected error probability and strictly optimal codes*, IEEE Trans. Inform. Theory (1997), no. 5, 1489–1502.
2. A. Ashikhmin and A. Barg, *Minimal vectors in linear codes*, IEEE Trans. Inform. Theory **44** (1998), no. 5, 2010–2017.
3. ———, *Binomial moments of the distance distribution: Bounds and applications*, IEEE Trans. Inform. Theory **45** (1999), no. 2, 438–452.
4. A. Barg, *The matroid of supports of a linear code*, Appl. Alg. Engrg. Commun. Comput. **8** (1997), 165–172.
5. E. F. Brickell and D. M. Davenport, *On the classification of ideal secret sharing schemes*, J. Cryptology **4** (1991), 123–134.
6. T Britz, *MacWilliams identities and matroid polynomials*, Electron. J. Combin. **9** (2002), #R19.
7. J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, Springer-Verlag, New York-Berlin, 1988.
8. P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Research Repts Suppl. **10** (1973), 1–97.
9. P. Delsarte and V. I. Levenshtein, *Association schemes and coding theory*, IEEE Trans. Inform. Theory **44** (1998), no. 6, 2477–2504.
10. S. Fujishige, *Entropy functions and polymatroids—combinatorial structures in information theory*, Electron. Comm. Japan **61** (1978), no. 4, 14–18.
11. I. M. Gel′fand and R. D. MacPherson, *A combinatorial formula for the Pontrjagin classes*, Bull. Amer. Math. Soc. (N.S.) **26** (1992), no. 2, 304–309.

12. T. Helleseth, T. Kløve, and V. I. Levenshtein, *On the information function of an error-correcting code*, IEEE Trans. Inform. Theory **43** (1997), no. 2, 549–557.
13. W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, New York: Cambridge University Press, 2003.
14. G. Kabatyansky and V. I. Levenshtein, *Bounds for packings on the sphere and in the space*, Problems of Information Transmission **14** (1978), no. 1, 3–25.
15. F. J. MacWilliams, *A theorem in the distribution of weights in a systematic code*, Bell Syst. Techn. Journ. **42** (1963), 79–94.
16. F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, 3 ed., North-Holland, Amsterdam, 1991.
17. D. N. C. Tse and S. V. Hanly, *Multiaccess fading channels. I. Polymatroid structure, optimal resource allocation and throughput capacities*, IEEE Trans. Inform. Theory **44** (1998), 2796–2815.
18. D. J. A. Welsh, *Matroid theory*, Academic Press, London, 1976.