Linear Codes and Weights

D. G. Hoffman
Auburn University   Auburn, AL 36849

Let F be a finite field with q elements. A k dimensional subspace C of the vector space F^n of all n-tuples over F is called a *linear code* of *length* n and *dimension* k. Algebraically, C is just a k-dimensional vector space over F. However, as a particular subspace of F^n, C inherits some metric properties. Specifically, for every $v \in F^n$, the *weight* of v, denoted by $wt(v)$, is defined to be the number of non-zero entries in the vector v, and the *distance* between two vectors is the weight of their difference. The interplay between the algebraic structure of C and the metric structure induced by the weight function is central to coding theory. (Should we rename it "Finite Analysis"?)

The ubiquitous triangle inequality $wt(v+w) \leq wt(v) + wt(w)$ does hold, but, as the following example shows, it is too weak to tell the whole story.

v	$wt(v)$
0	0
v_1	1
v_2	1
v_3	1
$v_1 + v_2$	2
$v_1 + v_3$	2
$v_2 + v_3$	2
$v_1 + v_2 + v_3$	1

The eight vectors of a hypothetical linear code of dimension 3 over the two-element field are listed on the left, and their weights on the right. The triangle inequality is satisfied, but it's all a sham, there is no such code!

Australasian Journal of Combinatorics 7(1993), pp.37-45

This example also illustrates our first goal here. Given an "abstract" vector space V over F, and a function ω from V to the non-negative integers, under what conditions can we realize V as a "concrete" subspace of some F^n, so that ω becomes the weight function? Our first theorem answers this question.

Theorem 1 *Let V be a vector space over F of dimension k, and for each $v \in V$, let $\omega(v)$ be a non-negative integer. Then the following three statements are equivalent:*

1) For some n, there is a linear transformation T from V into F^n, satisfying $wt(T(v)) = \omega(v)$ for all $v \in V$.

2) $\omega(0) = 0$, and $\omega(\alpha v) = \omega(v)$ for every $v \in V$, and every non-zero $\alpha \in F$. Also, if W is a subspace of V, then

$$\sum_{w \in W} \omega(w) \quad \text{is divisible by } (q-1)q^{t-1},$$

where t is the dimension of W. And if X is a coset of W in V, then

$$\sum_{w \in W} \omega(w) \leq \sum_{w \in X} \omega(w),$$

with the difference a multiple of q^t.

3) $\omega(0) = 0$, and $\omega(\alpha v) = \omega(v)$ for every $v \in V$, and every non-zero $\alpha \in F$. Also, if H is a subspace of V of dimension $k-1$, then

$$q \sum_{w \in H} \omega(w) \equiv \sum_{v \in V} \omega(v) \quad (\bmod\ q^{k-1}),$$

and

$$q \sum_{w \in H} \omega(w) \leq \sum_{v \in V} \omega(v).$$

Proof: First we assume 1), and prove 2). For each $S \subseteq V$, we form the $|S|$ by n matrix $M(S)$ as follows: the rows of $M(S)$ are indexed by the elements of S, and for each $v \in S, T(v)$ is the corresponding row of $M(S)$. Note that each of the q field elements occurs exactly q^{t-1} times in each non-zero column of $M(W)$. So if x is the number of such columns, then

$$\sum_{w \in W} \omega(w) = x(q-1)q^{t-1}.$$

If X is the coset $W+u$, then $M(X)$ is obtained from $M(W)$ by adding $T(u)$ to each row of $M(W)$. This process just permutes the entries of the x non-zero columns of $M(W)$. However, a zero column of $M(W)$ becomes a constant column in $M(X)$, and if this constant is non-zero, $M(X)$ gains weight. Thus

$$\sum_{w\in W} \omega(w) \leq \sum_{w\in X} \omega(w), \text{ and}$$

the difference is divisible by q^t, proving 2).

Obviously 2) implies 3), since the q cosets of H in V partition V.

Now we assume 3), and prove 1). We may assume that $V = F^k$, with elements written as row vectors. Thus the transformation T we seek will be of the form $T(v) = vG$, for some suitable matrix G with k rows. We proceed to construct G.

Let R be the set of all $(k-1)$-dimensional subspaces of V, and let $H \in R$. Since ω is constant on the $q-1$ non-zero vectors of any one-dimensional subspace of H, $\sum_{w\in H} \omega(w)$ is divisible by $q-1$, and so is $\sum_{v\in V} \omega(v)$, by the same reasoning.

Since $q-1$ and q^{k-1} are relatively prime, the number

$$\gamma_H := (q-1)^{-1}q^{1-k}(\sum_{v\in V} \omega(v) - q\sum_{w\in H} \omega(w))$$

is a non-negative integer. Finally, let v_H be any non-zero vector orthogonal to H.

Form the matrix G as follows: for each $H \in R$, place γ_H copies of the transpose of v_H in G as columns.

All that remains to be proved is that $wt(vG) = \omega(v)$ for all $v \in V$. This is obvious if $v = 0$, so we assume $v \neq 0$. Then

$$\begin{aligned} wt(vG) &= \sum_{\substack{H\in R\\ v\notin H}} \gamma_H = \\ & (q-1)^{-1}q^{1-k}(\sum_{u\in V} \omega(u)|\{H \in R | v \notin H\}| - \\ & q\sum_{w\in V} \omega(w)|\{H \in R | w \in H, v \notin H\}|) = \\ & (q-1)^{-1}q^{1-k}(\frac{q^k - q^{k-1}}{q-1}\sum_{u\in V} \omega(u) - q\frac{q^{k-1} - q^{k-2}}{q-1}\sum_{\substack{w\in V\\ w\notin\langle v\rangle}} \omega(w)) \\ &= (q-1)^{-1}\sum_{u\in\langle v\rangle} \omega(u) = \omega(v). \end{aligned}$$

Perhaps we have been a bit too cavalier in slinging sigmas around, and some explanation is in order.

The second equality is obtained by using the definition of γ_H, and interchanging the order of summation in the two pairs of sums.

For the third equality, we must evaluate $|\{H \in R | v \notin H\}|$ and $|\{H \in R | w \in H, v \notin H\}|$, where v and w are non-zero. The second of these is the more delicate. If w is in the one-dimensional subspace $\langle v \rangle$ spanned by v, then obviously $|\{H \in R | w \in H, v \notin H\}| = 0$. Now suppose $w \notin \langle v \rangle$. Recall that every non-zero s in V determines a unique element of R, namely the set of all vectors orthogonal to s; and conversely, every element of R is determined by $q-1$ such vectors s. So first we calculate the cardinality of the set $S = \{s \in V | s \cdot w = 0, s \cdot v \neq 0\}$. Since there are q^{k-1} vectors orthogonal to w, and q^{k-2} of these are also orthogonal to v, we have $|S| = q^{k-1} - q^{k-2}$. Thus

$$|\{H \in R | w \in H, v \notin H\}| = \frac{q^{k-1} - q^{k-2}}{q-1}.$$

A simpler argument along the same lines shows that

$$|\{H \in R | v \notin H\}| = \frac{q^k - q^{k-1}}{q-1}.$$

The fifth equality follows from the fact that for the $q-1$ non-zero elements $u \in \langle v \rangle, \omega(u) = \omega(v)$.

This concludes the proof of Theorem 1.

The matrix G constructed above is by no means unique. In fact, any sequence of the following operations applied to G produces a matrix that still has the required properties:

a) multiply some columns by non-zero field elements

b) adjoin some columns of zeros.

c) permute the columns.

However, the next theorem shows that this is all the freedom we have, the rest is forced.

Theorem 2 *Let G be a k by n matrix over F. For each $(k-1)$-dimensional subspace H of F^k, let γ_H be the number of non-zero columns of G orthogonal to H. Then*

$$\gamma_H = (q-1)^{-1}q^{1-k}(\sum_{v\in F^k} wt(vG) - q\sum_{w\in H} wt(wG)).$$

Proof: As noted in the proof of theorem 1, for each non-zero $v \in F^k$,

$$wt(vG) = \sum_{\substack{J\in R\\ v\notin J}} \gamma_J.$$

Thus, for $H \in R$,

$$\begin{aligned}
&(q-1)^{-1}q^{1-k}(\sum_{v\in F^k} wt(vG) - q\sum_{w\in H} wt(wG)) = \\
&(q-1)^{-1}q^{1-k}(\sum_{J\in R} \gamma_J|\{v \in V|v \notin J\}| - q\sum_{J\in R}\gamma_J|\{w\in H|w\notin J\}|) \\
= \; &(q-1)^{-1}q^{1-k}((q^k - q^{k-1})\sum_{J\in R}\gamma_J - q(q^{k-1}-q^{k-2})\sum_{\substack{J\in R\\ J\neq H}}\gamma_J) = \gamma_H.
\end{aligned}$$

This proves theorem 2.

A linear code C is a *constant weight code* if $wt(v) = wt(w)$ for all non-zero $v, w \in C$. As an application, we characterize constant weight codes. But first, some definitions.

If C is a linear code of length n, and m is a positive integer, for every $v \in C$, form the vector consisting of m copies of v cancatenated together. The resulting linear code of length nm is called a *replication* of C, with *multiplier* m.

If β is a non-negative integer, adjoining β zeros to the end of every vector in C results in a linear code of length $n + \beta$ called a *padding* of C.

If π is a permutation of $\{1, 2, \ldots, n\}$, and if $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a vector of non-zero field elements, for every $v = (v_1, v_2, \ldots, v_n) \in C$ form the vector $(\alpha_1 v_{\pi(1)}, \alpha_2 v_{\pi(2)}, \ldots, \alpha_n v_{\pi(n)})$. The resulting linear code is said to be *equivalent* to C.

In the notation of theorem 2, let G be any k by $n = \frac{q^k-1}{q-1}$ matrix satisfing $\gamma_H = 1$ for every $H \in R$. The code $C := \{vG|v \in F^k\}$ is called a *dual Hamming code* of dimension k.

Theorem 3 *Let C be a linear code of dimension k. Then C is a constant weight code if and only if C is equivalent to a padding of a replication of a dual Hamming code of dimension k. In this case, every non-zero $v \in C$ has weight mq^{k-1}, where m is the multiplier of the replication.*

Proof: If C is equivalent to a padding of a replication of a dual Hamming code of dimension k with multiplier m, then, in the notation of theorem 2, $\gamma_H = m$ for all $H \in R$. So for any non-zero $v \in F^k$,

$$\begin{aligned} wt(vG) &= \sum_{\substack{H \in R \\ v \notin H}} \gamma_H = m|\{H \in R | v \notin H\}| = \\ & m\frac{q^k - q^{k-1}}{q-1} = mq^{k-1}. \end{aligned}$$

Conversely, if $wt(v) = \omega$ for every non-zero $v \in C$, then by Theorem 2, for any $H \in R$,

$$\begin{aligned} \gamma_H &= (q-1)^{-1}q^{1-k}(\sum_{\substack{v \in C \\ v \neq 0}} \omega - q \sum_{\substack{w \in H \\ w \neq 0}} \omega) = \\ & \omega(q-1)^{-1}q^{1-k}(q^k - 1 - q(q^{k-1} - 1)) = \omega q^{1-k}, \end{aligned}$$

proving theorem 3.

The weight function is rather coarse; given a field element, it can only recognize whether or not it is zero. Here is a more discriminating function. If $\alpha \in F$ is non-zero, and $v \in F^n$, we define $wt(\alpha, v)$ to be the number of coordinates of v equal to α. (Perversely, we do *not* define $wt(0, v)$.) Ok, here we go again.

Theorem 4 *Let V be a vector space over F of dimension k, and for each non-zero $\alpha \in F$, and each $v \in V$, let $\omega(\alpha, v)$ be a non-negative integer. Then the following three statements are equivalent:*

1. *For some n, there is a linear transformation T from V into F^n, satisfying $wt(\alpha, T(v)) = \omega(\alpha, v)$ for every non-zero $\alpha \in F$, and every $v \in V$.*

2) *For every non-zero* $\alpha \in F, \omega(\alpha, 0) = 0$, *and* $\omega(\alpha, v) = \omega(1, \alpha^{-1}v)$ *for each* $v \in V$. *Also, if* W *is a subspace of* V, *then*

$$\sum_{w \in W} \omega(\alpha, w) \text{ is divisible by } q^{t-1},$$

where t *is the dimension of* W. *And if* X *is a coset of* W *in* V, *then*

$$\sum_{w \in W} \omega(\alpha, w) \leq \sum_{w \in X} \omega(\alpha, w),$$

with the difference a multiple of q^t.

3) *For every non-zero* $\alpha \in F, \omega(\alpha, 0) = 0$, *and* $\omega(\alpha, v) = \omega(1, \alpha^{-1}v)$ *for each* $v \in V$. *Also, if* H *is a subspace of* V *of dimension* $k - 1$, *and* X *is a coset of* H *in* V, *then*

$$\sum_{w \in H} \omega(1, w) \equiv \sum_{w \in X} \omega(1, \omega) \quad (\text{ mod } q^{k-1}),$$

and

$$\sum_{w \in H} \omega(1, w) \leq \sum_{w \in X} \omega(1, w).$$

Proof: As this proof so closely parallels the proof of Theorem 1, we content ourselves with proving that 3) implies 1).

Again, we assume $V = F^k$, and define a matrix G. For each non-zero $v \in V$, let

$$\gamma_v = q^{1-k}\Big(\sum_{\substack{w \in V \\ w \cdot v = 1}} \omega(1, w) - \sum_{\substack{w \in V \\ w \cdot v = 0}} \omega(1, w)\Big).$$

By hypothesis, γ_v is a non-negative integer.

Form the matrix G as follows: for each non-zero $v \in V$, place γ_v copies of the transpose of v in G as columns.

Now we must show that $wt(\alpha, vG) = \omega(\alpha, v)$ for all non-zero $\alpha \in F$, and all $v \in V$. This is obvious if $v = 0$, so we assume $v \neq 0$. Then

$$\begin{aligned} wt(\alpha, vG) &= \sum_{\substack{w \in V \\ w \cdot v = \alpha}} \gamma_w \\ &= q^{1-k}\Big(\sum_{u \in V} \omega(1, u) |\{w \in V | w \cdot v = \alpha, u \cdot w = 1\}| \end{aligned}$$

$$
\begin{aligned}
& - \sum_{u \in V} \omega(1,u) |\{w \in V | w \cdot v = \alpha, u \cdot w = 0\}|) \\
= \; & q^{1-k} (\sum_{\substack{\beta \in F \\ \beta \neq 0}} \omega(1, \beta v) |\{w \in V | w \cdot v = \alpha, (\beta v) \cdot w = 1\}| \\
& - \sum_{\substack{\beta \in F \\ \beta \neq 0}} \omega(1, \beta v) |\{w \in V | w \cdot v = \alpha, (\beta v) \cdot w = 0\}|) \\
= \; & q^{1-k} (q^{k-1} \omega(1, \alpha^{-1} v)) = \omega(\alpha, v).
\end{aligned}
$$

For the third equality above, we used the fact that if u is not a scalar multiple of v, then the sets

$$\{w \in V | w \cdot v = \alpha, u \cdot w = 1\} \text{ and } \{w \in V | w \cdot v = \alpha, u \cdot w = 0\}$$

have the same cardinality q^{k-2}, and so these terms cancel out.

For the fourth equality, the only non-zero summand is in the first sum, at $\beta = \alpha^{-1}$.

This concludes the proof of Theorem 4.

The matrix G is not unique, we can add zero columns and permute columns. But that's all:

Theorem 5 *Let G be a k by n matrix over F. For each non-zero v in F^k, let γ_v be the number of columns of G equal to the transpose of v. Then*

$$\gamma_v = q^{1-k} (\sum_{\substack{w \in F^k \\ w \cdot v = 1}} wt(1, wG) - \sum_{\substack{w \in F^k \\ w \cdot v = 0}} wt(1, wG)).$$

Proof: As

$$wt(1, wG) = \sum_{\substack{u \in F^k \\ u \cdot w = 1}} \gamma_u,$$

$$
\begin{aligned}
q^{1-k} (\sum_{\substack{w \in F^k \\ w \cdot v = 1}} wt(1, wG) \; & - \; \sum_{\substack{w \in F^k \\ w \cdot v = 0}} wt(1, wG)) \\
& = q^{1-k} (\sum_{u \in F^k} \gamma_u |\{w \in F^k | w \cdot v = 1, u \cdot w = 1\}| \\
& \quad - \sum_{u \in F^k} \gamma_u |\{w \in F^k | w \cdot v = 0, u \cdot w = 1\}|)
\end{aligned}
$$

$$= q^{1-k}(\sum_{\substack{\beta \in F \\ \beta \neq 0}} \gamma_{\beta v} |\{w \in F^k | w \cdot v = 1, (\beta v) \cdot w = 1\}|$$
$$- \sum_{\substack{\beta \in F \\ \beta \neq 0}} \gamma_{\beta v} |\{w \in F^k | w \cdot v = 0, (\beta v) \cdot w = 1\}|)$$
$$= q^{1-k}(q^{k-1}\gamma_v) = \gamma_v, \text{ proving Theorem 5.}$$

We leave to the reader the simple proof of the analogue of theorem 3:

Theorem 6 *Let C be a linear code of dimension k. Then $wt(\alpha, v) = wt(\beta, w) = \omega$ for all non-zero $\alpha, \beta \in F$ and all non-zero $v, w \in C$ if and only if $C = \{vG | v \in F^k\}$ where G is a matrix in which each non-zero element of F^k appears as a column of G exactly $q^{1-k}\omega$ times.*

References

[1] The Theory of Error-Correcting Codes, F. J. MacWilliams, N. J. A. Slonne, North-Holland Publishing Co. 1978.

(Received 14/11/91; revised 18/8/92)