Chapter 8

Hamming Codes

To define the Hamming codes $\mathrm{Ham}(r,q)$ over $\mathbf{F}_q$, where

$$n = \frac{q^r - 1}{q - 1}, \quad r = n - k \text{ for } r = 1, 2, \ldots,$$

a parity-check matrix H is specified. First, consider the case $q = 2$.

Definition 8.1. For any positive integer r, let H be an $r \times n$ matrix, $n = 2^r - 1$, whose columns are the elements of $V(r,2) \setminus \{0\}$.

Example 8.2. (i) $r = 2$, $n = 3$, $k = 1$

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \longrightarrow H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$
$$\Longrightarrow G = [1\,1\,1] \Longrightarrow \mathrm{Ham}(2,2) = \{000, 111\},$$

the binary repetition code of length 3.

(ii) $r = 3$, $n = 7$, $k = 4$

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \longrightarrow H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$
$$\Longrightarrow G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Hence $\mathrm{Ham}(3,2)$ is equivalent to the perfect $[7,4,3]_2$ code.

Theorem 8.3. $\mathrm{Ham}(r,2)$ *is a perfect* $[2^r - 1, 2^r - 1 - r, 3]$*-code.*

Proof By definition, $\mathrm{Ham}(r,2)^\perp$ is a $[2^r - 1, r]$-code, whence $\mathrm{Ham}(r,2)$ is a $[2^r - 1, 2^r - 1 - r]$-code. Also, by definition, no two columns of H are linearly dependent but there are many sets of 3 dependent columns; for example, $(1\,0\,\ldots, 0)^T$, $(0, 1, 0, \ldots, 0)^T$, $(1, 1, 0, \ldots, 0)^T$. This gives the following:

$$n = 2^r - 1, \quad M = 2^{n-r}, \quad d = 3, \quad e = 1.$$

Hence, in Theorem 2.6 or Corollary 2.7,

$$M\left\{\binom{n}{0}+\binom{n}{1}+\ldots+\binom{n}{e}\right\}\le 2^n.$$

$$\text{LHS} = 2^{n-r}(1+n) = 2^{n-r}\,.\,2^r = 2^n = \text{RHS}.$$

So the code is perfect. □

Decoding with a binary Hamming code

$C = \mathrm{Ham}(r,2)$ is a $[2^r-1, 2^r-1-r, 3]$-code, with

$$V = V(n,2),\ |V| = 2^n,\ n = 2^r-1,\ |C| = 2^{n-r}.$$

The number of cosets is $|V|/|C| = 2^n/2^{n-r} = 2^r$. The coset leaders are $n = 2^r-1$ vectors of weight 1 and one of weight zero. The syndrome of $l_i = 0\ldots 0\,1\,0\ldots 0$, where the 1 is in the i-th place, is the i-th column of H.

I. If the received vector is y, calculate the syndrome yH^T.

II. If $yH^T = 0$, then y is a codeword.

III. If $yH^T \neq 0$, then find the column of H containing yH^T; suppose it is the i-th column.

IV. The corrected vector is $x = y + l_i$, where l_i is a vector with 1 in the i-th place and 0 elsewhere; that is, change the i-th coordinate of y,

Example 8.4. $\mathrm{Ham}(3,2):\quad r=3, n=7, k=4, d=3.$

$$H = \begin{bmatrix} 0&0&0&1&1&1&1\\ 0&1&1&0&0&1&1\\ 1&0&1&0&1&0&1 \end{bmatrix}$$

(i)

$$y = 0011111,$$
$$s_H(y) = yH^T = 011;$$

so the error is in the 3rd coordinate and

$$y + l_3 = 0001111.$$

(ii)

$$y = 1100011,$$
$$s_H(y) = 010;$$

so the error is in the 2nd coordinate, and

$$y + l_2 = 1000011.$$

Construction of $\mathrm{Ham}(r, q)$

Given any non-zero vector in $V(r, q)$, write $x \sim y$ if $y = \lambda x$ for some non-zero $\lambda \in \mathbf{F}_q$. It is immediate that this is equivalence relation. The equivalence classes are the 1-dimensional supspaces are the 1-dimensional subspaces withpout the zero.

Consider the set of equivalence classes: write the set as $PG(r-1, q)$. Pick one vector in each equivalence class. Note that

$$|PG(r-1, q)| = \frac{|V(r, q)| - 1}{q - 1}.$$

The equivalence class of $(x_1, \ldots, x_r)$ is $[x_1, \ldots, x_r]$.

Projective space $PG(r-1, q)$ over a finite field $\mathbf{F}_q$

Definition 8.5. The subspaces of $PG(r-1, q)$ are the subspaces other than $\{0\}$ of $V(r, q)$.

$V(r, q)$	$PG(r-1, q)$	proj. dim
1-dimensional subspace	point	0
2-dimensional subspace	line	1
3-dimensional subspace	plane	2
4-dimensional subspace	solid	3
i-dimensional subspace	projective $(i-1)$-diml subspace	$i-1$
$(r-1)$-dimensional subspace	hyperplane	$r-2$

Theorem 8.6. *The space $PG(r-1, q)$ contains*

(i) $(q^r - 1)/(q - 1)$ *points,*

(ii) $\dfrac{(q^r - 1)(q^{r-1} - 1)}{(q^2 - 1)(q - 1)}$ *lines,*

(iii) $q + 1$ *points on a line,*

(iv) $(q^{r-1} - 1)/(q - 1)$ *lines through a point.*

Proof (i) This is the number of 1-dimensional subspaces in $V(r, q)$.

(ii) This is the number of 2-dimensional subspaces in $V(r, q)$.

(iii) This is the number of 1-dimensional subspaces in a 2-dimensional subspace in $V(r, q)$.

(iv) This is the number of 2-dimensional subspaces through a 1-dimensional subspace in $V(r, q)$.

□

Corollary 8.7. (i) *$PG(2, q)$ contains*

(a) $q^2 + q + 1$ *points and lines,*

(b) $q + 1$ *points on a line, lines through a point.*

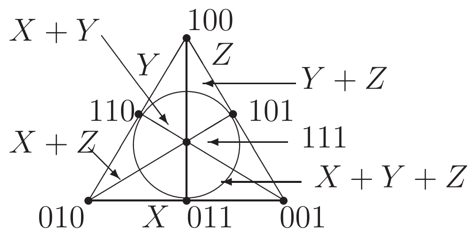
(ii) (a) *The points are* $(x, y, z) \neq (0, 0, 0)$ *where* $(\lambda x, \lambda y, \lambda z) = (x, y, z)$.

(b) *The lines are* $uX + vY + wZ = \{[x, y, z] \mid ux + vy + wz = 0\}$.

Example 8.8. $q = 2$.

The points are (x, y, z), $x, y, z \in \mathbf{F}_2$, not all zero.

The lines are $uX + vY + wZ$, $u, v, w \in \mathbf{F}_2$, not all zero.



Example 8.9. $|V(2,5)| = 5^2$, $\qquad |PG(1,5)| = (5^2 - 1)/(5 - 1) = 5 + 1 = 6$

$$V(2,5) \setminus \{0\} = \begin{array}{llll} (1,0), & (2,0), & (3,0), & (4,0) \\ (0,1), & (0,2), & (0,3), & (0,4) \\ (1,1), & (2,2), & (3,3), & (4,4) \\ (1,2), & (2,4), & (3,1), & (4,3) \\ (1,3), & (2,1), & (3,4), & (4,2) \\ (1,4), & (2,3), & (3,2), & (4,1) \end{array}$$

$PG(1,5)$ is the first column.

The construction of $\mathrm{Ham}(r, q)$

Let H be an $r \times (q^r - 1)/(q - 1)$ matrix whose columns give an element from each equivalence class, that is, the distinct points in $PG(r-1, q)$ or equivalently one vector for each 1-dimensional subspace of $V(r, q)$.

Definition 8.10. Let $\mathrm{Ham}(r, q)$ be the linear q-ary code with parity-check matrix H.

Theorem 8.11. $\mathrm{Ham}(r, q)$ *is a perfect* $\left[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3\right]$*-code.*

Proof $n = \frac{q^r-1}{q-1}$, $k = \frac{q^r-1}{q-1} - r$ by definition. Again, by definition and Theorem 9.18, $d = 3$. $M = q^k = q^{n-r}$. In Theorem 5.6,

$$\begin{aligned} q^{n-r}(1 + n(q-1)) &= q^{n-r}\left\{1 + \frac{q^r - 1}{q - 1}(q - 1)\right\} \\ &= q^{n-r}(1 + q^r - 1) \\ &= q^{n-r} \, . \, q^r \\ &= q^n. \end{aligned}$$

Hence the code is perfect. □

Note 8.12. 1. Different H give equivalent codes as they involve either a permutation of columns or the multiplication by a non-zero scalar.

2. To give a canonical H, choose the top non-zero element of each column as 1.

Lemma 8.13. (i) $|PG(1,q)| = q+1$.

(ii) $|PG(2,q)| = q^2+q+1$.

(iii) $|PG(3,q)| = (q^2+1)(q+1)$.

Example 8.14. $\text{Ham}(r,q)$ $\quad \mathbf{F}_q = \{t_1, t_2, \ldots, t_q\}$

(i) $\text{Ham}(2,q)$, $\quad H = \begin{bmatrix} 0 & 1 & 1 & \ldots & 1 \\ 1 & t_1 & t_2 & \ldots & t_q \end{bmatrix}$.

(ii) $\text{Ham}(3,q)$, $\quad H = \left[\begin{array}{c|ccc|cccc|ccc|c|ccc} 0 & 0 & \ldots & 0 & 1 & 1 & \ldots & 1 & 1 & \ldots & 1 & \ldots & 1 & \ldots & 1 \\ 0 & 1 & \ldots & 1 & t_1 & t_1 & \ldots & t_1 & t_2 & \ldots & t_2 & \ldots & t_q & \ldots & t_q \\ 1 & t_1 & \ldots & t_q & t_1 & t_2 & \ldots & t_q & t_1 & \ldots & t_q & \ldots & t_1 & \ldots & t_q \end{array}\right]$.

Decoding with a q-ary Hamming code

$C = \text{Ham}(r,q)$ is a $\left[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3\right]$ −code. It is perfect single-error correcting. Hence words of weight ≤ 1 form coset leaders.

The number of words of weight 0 is 1.

The number of words of weight 1 is $(q-1)n = q^r - 1$.

Hence the number of words of weight ≤ 1 is $q^r - 1 + 1 = q^r$. The number of cosets is $|V(n,q)|/|C| = q^n/q^k = q^n/q^{n-r} = q^r$.

I. If the received vector is y, calculate the syndrome yH^T.

II. If $yH^T = 0$, then take the correct message as y.

III. If $yH^T \neq 0$, then $yH^T = (\lambda c_j)^T$ for some column c_j of H and some λ of $\mathbf{F}_q \setminus \{0\}$.

IV. The correct message is $x = y - \lambda e_j$, where $e_j = (0\ldots010\ldots0)$ and the 1 is in the jth place; that is, subtract λ from the j-th coordinate of y.

Example 8.15. $\text{Ham}(2,5)$

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 \end{bmatrix} \longrightarrow \text{rearrange the columns} \longrightarrow H' = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 4 & 0 & 1 \end{bmatrix}.$$

Here $n = 6$, $r = 2$, $k = n - r = 4$, $d = 3$.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & -1 & -1 \\ 0 & 1 & 0 & 0 & -1 & -2 \\ 0 & 0 & 1 & 0 & -1 & -3 \\ 0 & 0 & 0 & 1 & -1 & -4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 4 & 4 \\ 0 & 1 & 0 & 0 & 4 & 3 \\ 0 & 0 & 1 & 0 & 4 & 2 \\ 0 & 0 & 0 & 1 & 4 & 1 \end{bmatrix}.$$

$\text{Ham}(2,5)$ is a $[6,4,3]$ code over $\mathbf{F}_5$; that is, it can send 625 messages.

(i) Decode $y = 123123$:

$$yH'^T = \begin{bmatrix} 1 & 2 & 3 & 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 4 & 0 & 1 \end{bmatrix}^T = (4\,1) = 4(1\,4);$$

$x = y - 4e_4 = 123223 = r_1 + 2r_2 + 3r_3 + 2r_4$, where r_i is the i-th row of G'.

(ii) Decode $y' = 111111$:

$$y'H'^T = 01,$$
$$x = y - e_6 = 111110 = r_1 + r_2 + r_3 + r_4.$$

If instead of H' we had used the **equivalent** but **not** the same parity-check matrix H,

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 \end{bmatrix} \rightarrow \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 4 & 4 & 3 & 2 & 1 & 0 \\ 1 & 2 & 3 & 4 & 0 & 1 \end{bmatrix}$$

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & -4 & -1 \\ 0 & 1 & 0 & 0 & -4 & -2 \\ 0 & 0 & 1 & 0 & -3 & -3 \\ 0 & 0 & 0 & 1 & -2 & -4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 4 \\ 0 & 1 & 0 & 0 & 1 & 3 \\ 0 & 0 & 1 & 0 & 2 & 2 \\ 0 & 0 & 0 & 1 & 3 & 1 \end{bmatrix} \begin{matrix} r_1 \\ r_2 \\ r_3 \\ r_4 \end{matrix},$$

$$\begin{aligned} y &= 123123 \Rightarrow s = 14 \Rightarrow x = 123122 = r_1 + 2r_2 + 3r_3 + r_4; \\ y' &= 111111 \Rightarrow s' = 01 \Rightarrow x = 011111 = r_2 + r_3 + r_4. \end{aligned}$$

Definition 8.16. The dual of a Hamming code is a *simplex* code.

Theorem 8.17. *The simplex code* $\text{Ham}(r,q)^\perp$ *is a* $\left[\frac{q^r-1}{q-1}, r, q^{r-1}\right]$ *code with every non-zero codeword of weight* q^{r-1}.

Proof If H is a parity-check matrix of $\text{Ham}(r,q)$ and so a generator matrix of $\text{Ham}(r,q)^\perp$, then, if $x \in \text{Ham}(r,q)^\perp \setminus \{0\}$,

$$x = \sum \lambda_i h_i,$$

where $h_1, \ldots, h_r$ are the rows of H and $\lambda_1, \ldots, \lambda_r$ are not all zero. Now, if j-th column of H is $(x_1\, x_2\, \cdots\, x_r)^\perp$, then the the j-th coordinate of x is 0 if $\sum_1^r \lambda_i x_i = 0$. As the columns vary over all points of $PG(r-1,q)$, the number of 0's in x is the number of points in a hyperplane, namely $(q^{r-1}-1)/(q-1)$. So

$$w(x) = \frac{q^r - 1}{q-1} - \frac{q^{r-1}-1}{q-1} = q^{r-1}.$$

□

Example 8.18. $C = \text{Ham}(3,2)$ is a $[7,4,3]_2$ code and so $C^\perp$ is a $[7,3]_2$ code. A parity-check matrix H for C is a generator matrix for $C^\perp$. As in Example 8.4, let

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \quad \begin{matrix} h_1 \\ h_2 \\ h_3 \end{matrix}$$

Then the elements of $C^\perp$ are $0, h_1, h_2, h_3, h_1 + h_2, h_1 + h_3, h_2 + h_3, h_1 + h_2 + h_3$; that is,

0000000, 0001111, 0110011, 1010101, 0111100, 1011010, 1100110, 1111000.

Every non-zero word of $C^\perp$ has weight 4.