Chapter 5

Golay Codes

Lecture 16, March 10, 2011

We saw in the last chapter that the linear Hamming codes are nontrivial perfect codes.

Question. Are there any other nontrivial perfect codes?

Answer. Yes, two other linear perfect codes were found by M.J.E. Golay in 1949. In addition, several nonlinear perfect codes are known that have the same n, M and d parameters as Hamming codes. $\square$

The condition for a code to be perfect is that its n, M and d values satisfy the sphere-packing bound

$$M \sum_{k=0}^{t} \binom{n}{k} (q-1)^k = q^n,$$

with $d = 2t + 1$. **Golay found three other possible integer triples (n, M, d) that do not correspond to the parameters of a Hamming or trivial perfect code.** They are $(23, 2^{12}, 7)$ and $(90, 2^{78}, 5)$ for $q = 2$ and $(11, 3^6, 5)$ for $q = 3$.

Problem 5.1. Show that the (n, M, d) triples $(23, 2^{12}, 7)$, $(90, 2^{78}, 5)$ for $q = 2$, and $(11, 3^6, 5)$ for $q = 3$ satisfy the sphere-packing bound.

It turns out that there do indeed exist linear binary $[23, 12, 7]$ (section 1) and ternary $[11, 6, 5]$ (section 2) codes; these are known as Golay codes. But, for parameters $(90, 2^{78}, 5)$ we have the following theorem

Recall the proof of Theorem 1.4 (**Sphere-Packing Bound Theorem**) If there is a q-ary $(n, M, 2t+1)$-code C, then we have

$$M \sum_{k=0}^{t} \binom{n}{k} (q-1)^k \leq q^n.$$

If the equality occurs, then C is called a perfect code.

Remark. For any $\mathbf{x} \in F_q^n$ and $t \in \mathbb{Z}_{\geq 0}$, the sphere $S(\mathbf{x}, t)$ of radius t and center $\mathbf{x}$ is the set $S(\mathbf{x}, t) = \{\mathbf{z} \in F_q^n \,|\, d(\mathbf{z}, \mathbf{x}) \leq t\}$. Then if C is a perfect q-ary $(n, M, 2t+1)$-code, then we have $\bigcup_{\mathbf{x} \in C} S(\mathbf{x}, t) = F_q^n$.

Theorem 5.1 (Nonexistence of binary $(90, 2^{78}, 5)$ codes). There exist no binary $(90, 2^{78}, 5)$ codes.

Proof. Suppose C is a binary $(90, 2^{78}, 5)$ code. By equivalence, without loss of generality we may assume that $\mathbf{0} \in C$. Let Y be the set of vectors in F_2^{90} of weight 3 that begin with two 1s. Since there are 88 possible positions for the third one, $|Y| = 88$. From **Problem 5.1**, we know that C is perfect, with $d(C) = 5$. Thus each $\mathbf{y} \in Y$ is within a distance 2 from a unique codeword $\mathbf{x}$. But then from the triangle inequality,

$$2 = d(C) - \mathrm{wt}(\mathbf{y}) \leq \mathrm{wt}(\mathbf{x}) - \mathrm{wt}(\mathbf{y}) \leq \mathrm{wt}(\mathbf{x} - \mathbf{y}) = d(\mathbf{x}, \mathbf{y}) \leq 2,$$

from which we see that $\mathrm{wt}(\mathbf{x}) = 5$ and $d(\mathbf{x}, \mathbf{y}) = \mathrm{wt}(\mathbf{x} - \mathbf{y}) = 2$. This means that $\mathbf{x}$ must have a 1 in every position that y does.

Let X be the set of all codewords of weight 5 that begin with two 1s. We know that for each $\mathbf{y} \in Y$ there is a unique $\mathbf{x} \in X$ such that $d(\mathbf{x}, \mathbf{y}) = 2$. That is, there are exactly $|Y| = 88$ elements in the set $\{(\mathbf{x}, \mathbf{y}) \,|\, \mathbf{x} \in X, \mathbf{y} \in Y, d(\mathbf{x}, \mathbf{y}) = 2\}$. But each $\mathbf{x} \in X$ contains exactly three ones after the first two positions. Thus, for each $\mathbf{x} \in X$ there are precisely three vectors $\mathbf{y} \in Y$ such that $d(\mathbf{x}, \mathbf{y}) = 2$. That is, $3|X| = 88$. This is a contradiction, since $|X|$ must be an integer. $\square$

Now let's construct the Golay codes and show some properties.

5.1 Binary Golay codes

Remark. A convenient way of finding a binary $[23, 12, 7]$ Golay code is to construct first the extended Golay $[24, 12, 8]$ code, which is just the $[23, 12, 7]$ Golay code augmented with a final parity check in the last position.

Definition 5.1 (Extended binary Golay codes). Let G be the 12×24 matrix $G = [I_{12} \,|\, A]$, where I_{12} is the 12×12 identity matrix and A is the 12×12 matrix

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}, A^t = A$$

The binary linear code with generator matrix G is called the **extended binary Golay code** and will be denoted by G_{24}.

Proposition 5.2 (Properties of the extended binary Golay code). 1). The length of G_{24} is 24 and its dimension is 12.

2). A parity-check matrix for G_{24} is the 12×24 matrix $H = [A \,|\, I_{12}]$.

3). The code G_{24} is self-dual, i.e., $G_{24}^{\perp} = G_{24}$.

4). Another parity-check matrix for G_{24} is the 12×24 matrix $H' = [I_{12} \,|\, A]$ $(= G)$.

5). Another generator matrix for G_{24} is the 12×24 matrix $G' = [A \,|\, I_{12}]$ $(= H)$.

6). The weight of every codeword in G_{24} is a multiple of 4.

7). The code G_{24} has no codeword of weight 4, so the minimum distance of G_{24} is $d = 8$.

8). The code G_{24} is an exactly three-error-correcting code.

Proof. 1). This is clear from the definition.

2). This follows from the Theorem in Chapter 3.

3). Note that the rows of G are orthogonal; i.e., if $\mathbf{r}_i$ and $\mathbf{r}_j$ are any two rows of G, then $\mathbf{r}_i \cdot \mathbf{r}_j = 0$. This implies that $G_{24} \subset G_{24}^{\perp}$. On the other hand, since both G_{24} and $G_{24}^{\perp}$ have dimension 12, we must have $G_{24} = G_{24}^{\perp}$.

4). A parity-check matrix of G_{24} is a generator matrix of $G_{24}^{\perp} = G_{24}$, and G is one such matrix.

5). A generator matrix of G_{24} is a parity-check matrix of $G_{24}^{\perp} = G_{24}$, and H is one such matrix.

6). Let $\mathbf{v}$ be a codeword in G_{24}. We want to show that $\mathrm{wt}(\mathbf{v})$ is a multiple of 4. Note that $\mathbf{v}$ is a linear combination of the rows of G. Let $\mathbf{r}_i$ denote the i-th row of G.

First, suppose $\mathbf{v}$ is one of the rows of G. Since the rows of G have weight 8 or 12, the weight of $\mathbf{v}$ is a multiple of 4.

Next, let $\mathbf{v}$ be the sum $\mathbf{v} = \mathbf{r}_i + \mathbf{r}_j$ of two different rows of G. Since G_{24} is self-dual, Exercise 3.2 in Exercise 2 for midterm shows that the weight of $\mathbf{v}$ is divisible by 4. We then continue by induction to finish the proof.

7). Note that the last row of G is a codeword of weight 8. This fact, together with statement 6) of this proposition, implies that $d = 4$ or 8. Suppose G_{24} contains a nonzero codeword $\mathbf{v}$ with $\mathrm{wt}(\mathbf{v}) = 4$. Write $\mathbf{v}$ as $(\mathbf{v}_1, \mathbf{v}_2)$, where $\mathbf{v}_1$ is the vector (of length 12) made up of the first 12 coordinates of $\mathbf{v}$, and $\mathbf{v}_2$ is the vector (also of length 12) made up of the last 12 coordinates of $\mathbf{v}$. Then one of the following situations must occur:

Case 1: $\mathrm{wt}(\mathbf{v}_1) = 0$ and $\mathrm{wt}(\mathbf{v}_2) = 4$. This cannot possibly happen since, by looking at the generator matrix G, the only such word is 0, which is of weight 0.

Case 2: $\mathrm{wt}(\mathbf{v}_1) = 1$ and $\mathrm{wt}(\mathbf{v}_2) = 3$. In this case, again by looking at G, $\mathbf{v}$ must be one of the rows of G, which is again a contradiction.

Case 3: $\mathrm{wt}(\mathbf{v}_2) = 2$ and $\mathrm{wt}(\mathbf{v}_2) = 2$. Then $\mathbf{v}$ is the sum of two of the rows of G. It is easy to check that none of such sums would give $\mathrm{wt}(\mathbf{v}_2) = 2$.

Case 4: $\mathrm{wt}(\mathbf{v}_1) = 3$ and $\mathrm{wt}(\mathbf{v}_2) = 1$. Since G' is a generator matrix, $\mathbf{v}$ must be one of the rows of G', which clearly gives a contradiction.

Case 5: $\mathrm{wt}(\mathbf{v}_1) = 4$ and $\mathrm{wt}(\mathbf{v}_2) = 1$. This case is similar to case 1, using G' instead of G.

Since we obtain contradictions in all these cases, $d = 4$ is impossible. Thus, $d = 8$.

8). This follows from statement 7) above and Theorem 1.1.

□

Definition 5.3 (Binary Golay code). Let $\hat{G}$ be the 12×23 matrix $\hat{G} = [I_{12} \mid \hat{A}]$ where I_{12} is the 12×12 identity matrix and $\hat{A}$ is the 12×11 matrix obtained from the matrix

A by deleting the last column of A. The binary linear code with generator matrix $\hat{G}$ is called the binary Golay code and will be denoted by G_{23}.

Remark. Alternatively, the binary Golay code can be defined as the code obtained from G_{24} by deleting the last digit of every codeword.

Proposition 5.4 (Properties of the binary Golay code). 1). The length of G_{23} is 23 and its dimension is 12.

2). A parity-check matrix for G_{23} is the 11×23 matrix $\hat{H} = [\hat{A}^t \,|\, I_{11}]$.

3). The extended code of G_{23} is G_{24}.

4). The distance of G_{23} is $d = 7$.

5). The code G_{23} is a perfect exactly three-error-correcting code.

Lecture 17, March 15, 2011

5.2 Ternary Golay codes

Definition 5.5 (Extended ternary Golay code). The **extended ternary Golay code**, denoted by G_{12}, is the ternary linear code with generator matrix $G = [I_6 \,|\, B]$, where B is the 6×6 matrix

$$B = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{bmatrix}, B^t = B$$

Remark. Any linear code that is equivalent to the above code is also called an extended ternary Golay code.

Definition 5.6 (Ternary Golay code). The ternary Golay code G_{11} is the code obtained by puncturing G_{12} in the last digit.

Proposition 5.7. 1). A parity-check matrix for G_{12} is the 6×12 matrix $H = [-B \,|\, I_6]$.

2). The code G_{12} is self-dual, i.e., $G_{12}^{\perp} = G_{12}$.

3). Another parity-check matrix for G_{12} is the 6×12 matrix $H' = [I_6 \,|\, B]$ $(= G)$.

4). Another generator matrix for G_{12} is the 6×12 matrix $G' = [-B \,|\, I_6]$ $(= H)$.

5). The weight of every codeword in G_{12} is a multiple of 3.

6). The code G_{12} has no codeword of weight 3, so the minimum distance of G_{12} is $d = 6$.

7). The distance of G_{11} is $d = 5$.

8). The code G_{12} is an exactly two-error-correcting code.

9). The code G_{11} is a perfect exactly two-error-correcting code.

5.3 Remarks on perfect codes

The following codes are obviously perfect codes and are called **trivial perfect codes**:

1). The linear code $C = F_q^n$ (In this case $d = 1$);

2). Any code C with $|C| = 1$ (In this case d is big enough number, such as $d = 2n + 1$);

3). Binary repetition codes of odd lengths consisting of two codewords at distance n from each other $(d = n = 2k + 1)$.

In these two chapters, we have seen that the Hamming codes and the Golay codes are examples of nontrivial perfect codes. In fact, the following result is true.

Theorem 5.2 (Tietäväinen, Van Lint). In 1973, they proved that any nontrivial perfect code over the field F_q^n must either have the parameters $(\frac{q^r-1}{q-1}, q^{n-r}, 3)$ of a Hamming code, the parameters $(23, 2^{12}, 7)$ of the binary Golay code, or the parameters $(11, 3^6, 5)$ of the ternary Golay code.