Golay Codes

Melissa Kanemasu

Abstract. We discuss a specific type of error-control coding using Golay codes. First we introduce the basics of coding. Then we discuss the Golay code in binary form, extended binary form, and ternary form.

1. Introduction. Coding, and in particular error-control coding, is an extremely important part of applied mathematics. The sharing and the transmission of data are an integral part of communication in the world. Coding makes data transmission much easier by putting the data into a simpler form. Error-control codes help prevent the miscommunication of a message by working to correct any mistakes or scrambling of the message that occurs during transmission.

This paper introduces a particular type of error-control code, called the "Golay" code. We describe the characteristics of the code, concentrating on those that make it particularly useful. We also discuss the various forms of the code.

Golay codes have a number of different real-world applications. The binary code has been used in various communication systems, and its extended form was used in the Voyager spacecraft program during the early 1980s. For such applications, Golay codes are optimal because they are perfect or quasi-perfect, in the technical senses explained in Sections 3 and 4.

Section 2 provides a general overview of coding theory. It includes definitions and concepts necessary to understand the theory behind Golay codes. Section 3 discusses the binary form of the Golay code, and its importance as a perfect code. Section 4 discusses the extension of the binary Golay code. The effects of this extension on the characteristics of the code are also explained. Finally, Section 5 discusses the ternary form of the Golay code.

2. Definitions. Coding theory has two main types of codes: block codes and convolution codes. A *block code* is a code that uses sequences of n symbols, for some positive integer n. Each sequence of length n is a *code word* or *code block*, and contains k information digits (or bits). The remaining $n-k$ digits in the code word are called *redundant digits* or *parity-check bits*. They do not contain any additional information, but are used to make it possible to correct errors that occur in the transmission of the code. The encoder for a block code is *memoryless*, which means that the n digits in each code word depend only on each other and are independent of any information contained in previous code words. The convolution encoder is more complicated, however, because it contains memory. In a *convolution code*, the n digits of a code word also depend on the code words that were encoded previously during a fixed length of time.

The symbols that make up a code word are taken from an alphabet of q elements. A very common type of code is a *binary code* for which q is 2, and the alphabet typically consists of 0 and 1. In binary block coding, there are 2^n possible code words in a code of length n. However, each code word contains a message of only length k, so we use only 2^k of the 2^n possible words with $k < n$. This set of 2^k code words of length n is called an $(n,\ k)$ block code. The *code rate* is the ratio $R = k/n$. For a binary code, $R \leq 1$. So after encoding a k-digit message or information block, there are $n - k$ remaining redundant digits in the code word. The redundant digits give the code words the ability to reduce the effect of channel noise, which could introduce errors during the transmission of the message.

The 2^n possible code words of length n form vector space over GF(2), the finite field, or Galois field, with 2 elements. An $(n,\ k)$ block code for which the code words form a k-dimensional subspace of the vector space is called a *linear* (n, k) *block code.*

One important subclass of linear block codes is the class of *cyclic codes* or *polynomial-generated codes.* A cyclical code is a $(n,\ k)$ linear code C with the property that for any code word $\mathbf{c}$ of the form,

$$\mathbf{c} = (c_0, c_1, \ldots, c_{n-2}, c_{n-1}) \text{ where } c_i \in \{0, 1\} \text{ for } 0 \leq i \leq n-1,$$

the word $\mathbf{c}^{(1)}$ is also a code word where $\mathbf{c}^{(1)}$ has the form,

$$\mathbf{c}^{(1)} = (c_{n-1}, c_0, c_1, \ldots, c_{n-3}, c_{n-2}).$$

There is a *code polynomial*, $\mathbf{c}(X)$ of degree $n - 1$ or less, associated with each code word $\mathbf{c}$:

$$\mathbf{c}(X) = c_0 + c_1 X + c_2 X^2 + \ldots + c_{n-1} X^{n-1}.$$

The code polynomial of minimum degree in an (n, k) cyclic code is called its *generator polynomial*, and denoted by $\mathbf{g}(X)$. It can be shown, see for example [**2**, pp. 61–62], that $\mathbf{g}(X)$ has the form,

$$\mathbf{g}(X) = 1 + g_1 X + g_2 X^2 + \ldots + g_{n-k-1} X^{n-k-1} + X^{n-k}.$$

An arbitrary linear code can be specified by a generator matrix of size n by k. The rows of the generator matrix $\mathbf{G}$ are k code words from $\mathbf{c}_0$ to $\mathbf{c}_{k-1}$ that span the code:

$$\mathbf{G} = \begin{bmatrix} \mathbf{c}_0 \\ \mathbf{c}_1 \\ \vdots \\ \vdots \\ \mathbf{c}_{k-1} \end{bmatrix}.$$

Generator matrices are discussed more fully in [**4**].

The number of corresponding elements, or positions, in which two code words differ defines a metric, called the *Hamming distance.* The *Hamming weight* $w(\mathbf{c})$ of a code word $\mathbf{c}$ is the number of nonzero digits of $\mathbf{c}$. For the 2^k code words in block coding, the smallest value of the set of Hamming distances is called the *minimum distance*, denoted by $d_{\min}$. A minimum distance $d_{\min}$ for an (n, k) block code ensures that up to $t = (d_{\min} - 1)/2$ errors can be corrected by the code. The correcting capabilities of a code also depend on a number of other factors such as the code rate R, the number of code words contained in the code, and other distance properties of the code. All codes with the capacity to correct transmission errors are called *error-correcting codes.*

3. The Binary Golay Code. The binary form of the Golay code is one of the most important types of linear binary block codes. It is of particular significance since it is one of only a few examples of a nontrivial perfect code. A *t-error-correcting* code can correct a maximum of t errors. A *perfect* t-error correcting code has the property that every word lies within a distance of t to exactly one code word. Equivalently, the code has $d_{\min} = 2t + 1$, and covering radius t, where the *covering radius* r is the smallest number such that every word lies within a distance of r to a codeword.

Theorem 3-1. *If there is an (n, k) code with an alphabet of q elements, and $d_{\min} = 2t + 1$, then,*

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

Proof: There are q^k code words. For each, there are $\binom{n}{i}(q-1)^i$ words that differ from it in exactly i positions. Hence, the number on the right of the inequality is the total number of words whose distance from a code word is at most t. Since the total number of allowable words cannot exceed the total number of possible words q^n, the inequality follows immediately. □

The inequality in Theorem 3-1 is known as the *Hamming bound.* Clearly, a code is perfect precisely when it attains equality in the Hamming bound. Two Golay codes do attain equality, making them perfect codes: the (23, 12) binary code with $d_{\min} = 7$, and the (11, 6) ternary code with $d_{\min} = 5$. Both codes have the largest minimum distance for any known code with the same values of n and k. Only two other codes achieve equality in the Hamming bound: the $(2^m - 1 - m)$ Hamming code with $d_{\min} = 3$, and the binary repetition code with two code words, one all 0s and one all 1s. For more information on these other types of perfect codes, see [**4**].

Golay was in search of a perfect code when he noticed that

$$\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2^{11} = 2^{23-12},$$

which indicated the possible existence of a (23, 12) perfect binary code that could correct up to three errors. In 1949, Golay discovered such a perfect code, and it is the only one known capable of correcting any combination of three or fewer random errors in a block of 23 elements. This (23, 12) Golay code can be generated either by

$$\mathbf{g}_1(X) = 1 + X^2 + X^4 + X^5 + X^6 + X^{10} + X^{11},$$

or

$$\mathbf{g}_2(X) = 1 + X + X^5 + X^6 + X^7 + X^9 + X^{11}.$$

Both polynomials $\mathbf{g}_1(X)$ and $\mathbf{g}_2(X)$ are factors of $X^{23} + 1$ in GF(2)[X]; indeed, we have

$$X^{23} + 1 = (1 + X)\mathbf{g}_1(X)\mathbf{g}_2(X).$$

There are several different ways to decode the (23, 12) binary Golay code that maximize its error-correcting capability at $t = 3$. Two of the best methods are refined error-trapping schemes: the Kasami Decoder, and the Systematic Search Decoder. Both are explained in [**2**, pp. 102-06]. There are also other systems of decoding, but are not as good because some of the error-correcting capability of the code is lost in carrying out the decoding.

4. The Extended Golay Code. Codes can be easily extended by adding an overall parity check to the end of each code word. This fact is stated more precisely in the following lemma, which is proved in [**5**, pp. 30–31].

Lemma 4-1. *Let c be any (n, k) code whose minimum distance is odd. We can obtain a new $(n+1, k)$ code c' with the new minimum distance $d'_{min} = d_{min} + 1$ by adding a 0 at the end of each code word of even weight and a 1 at the end of each code word of odd weight.*

The (23, 12) Golay code can be extended by adding an overall parity check to each code word to form the (24, 12) extended Golay code. This code can be generated by the 12 by 24 matrix $G = [\ I\ ,\ B\ ]$ where I is the 12 by 12 identity matrix and B is the following matrix:

$$B = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

In addition, the 12 by 24 matrix $G' = [B, I]$ is also a generator for the code.

This (24, 12) extended Golay code $\mathcal{G}$ has minimum distance $d_{\min} = 8$ and has a code rate of exactly $R = \frac{1}{2}$. The weight of every code word is a multiple of 4, and $\mathcal{G}$ is invariant under a permutation of coordinates that interchanges the two halves of each code word. Unlike the (23,12) code, the (24, 12) extended Golay code is not perfect, only quasi-perfect, because all spheres of radius t are disjoint, but every vector is at most a distance of $t + 1$ from some code vector. A *quasi-perfect* code is defined to be a code which for some t has most vectors of weight t or less, a few of weight $t + 1$, and none of weight greater than $t + 1$. There are 2^{12}, or 4096, possible code words in the extended Golay code and like the unextended (23, 12) code, it can be used to correct at most three errors.

5. Ternary Golay Codes. In addition to the binary Golay codes discussed previously, there are also ternary Golay codes. The ternary (11, 6) Golay code is the only known perfect nonbinary code. Note that a Hamming sphere with radius 2 over GF(3) contains 243 vectors because

$$1 + 2\binom{11}{1} + 4\binom{11}{2} = 243.$$

Since 243 is equal to 3^5, there may be a perfect packing with 3^6 spheres (code words) of radius $t = 2$, which was discovered by Golay. The (11, 6) Golay code over the Galois field with three elements GF(3) has minimum distance of 5, and can correct up to two errors. As stated previously, like the (23, 12) binary Golay code, the (11, 6) ternary code has the largest minimum distance $d_{\min}$ of any known code with the same values of n and k.

Also, like the (23, 12) binary code, the (11, 6) ternary code can be extended by adding an overall parity check to form the extended (12, 6) ternary Golay code. Like the extended (24, 12) code, the (12, 6) code is also unique.

References

[**1**] Hoffman, D. G., and Leonard, D. A., *et.al.*, “Coding Theory: The Essentials,” Marcel Dekker, Inc., 1991.

[**2**] Lin, S., and Costello, D. J., Jr., “Error Control Coding: Fundamentals and Applications,” Prentice Hall, Inc., 1983.

[**3**] Peterson, W. W., “Error-Correcting Codes,” MIT Press, 1961.

[**4**] Rhee, M. Y., “Error-Correcting Coding Theory,” McGraw-Hill, 1989.

[**5**] Sloane, N. J. A., “A Short Course on Error Correcting Codes,” Springer-Verlag, 1975.

This page will be blank.