Minimum-Weight Codewords in the (128,64) BCH Code

L. D. Baumert
Communications Systems Research Section

L. R. Welch
University of Southern California

In this article we determine the number of weight 22 codewords in the (128,64) BCH code which is being studied for use on future deep-space missions.

I. Introduction

Perhaps the most promising candidate deep-space telemetry coding system which is markedly superior to the short-constraint-length convolutional code on Voyager is a (128,64) BCH (Bose-Chaudhuri-Hocquenghem) block code equipped with a soft-decision decoding algorithm (Ref. 1). The minimum distance of this code is known to be 22, but in order to get accurate estimates of the code's performance it is necessary to know the exact number of codewords of weight 22. In this article we will combine techniques of combinational algebra and computer simulation, and conclude that the number of such codewords is almost certainly 243,840.

Our proof rests on the fact that the BCH code is invariant under a certain group of coordinate permutations of order $2^7 \cdot 7 \cdot 127 = 113{,}792$. Thus the words of any fixed weight are distributed into conjugacy classes under the action of this group. In this paper we will show that for weight 22 codewords one such class contains 16256 codewords, but all other classes contain 113,729 codewords. Our computer simulations of decoding algorithms have generated 85 weight-22 codewords; these have all been contained in just three classes: the small class of size 16256 and two larger classes. Thus the number of weight-22 codewords is almost surely 16256 + 113792 + 113792 = 243840.

II. Preliminary Information

The (128,64) BCH code has an automorphism group G of order $113{,}792 = 7 \times 127 \times 128$ consisting of the transformations $\tau : x \rightarrow \gamma x^{2^k} + \delta (k = 0,1, \ldots, 6; \gamma, \delta$ in $GF(2^7), \gamma \neq 0)$ acting on the elements of $GF(2^7)$ (Ref. 2). The codeword symbol position labels are $\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{126}, 0 = \alpha^\infty$, where α is a primitive root of $GF(2^7)$ and the action of τ on these labels determines the codeword permutation. So any element of G can be described in terms of a permutation of the symbols $0,1, \ldots, 126,\infty$. Thus each element of G can be described by a product of disjoint cycles of the symbols $0,1, \ldots, 126,\infty$. The order of an element is the least common multiple of the lengths of these cycles. Two conjugate permutations have the same number of cycles of each size and hence the same order. If a codeword w is fixed by the transformation τ, then the codeword $w\phi$ is fixed by the conjugate transformation $\phi^{-1}\tau\phi$.

The weight of any codeword is of course fixed by the transformations of G; thus in particular the words of minimum weight 22 are distributed into classes according to whether or not they are transformed into each other by G. Thus a collection of representative words, one from each of these classes, suffices to determine all words of weight 22 in the code. In order to determine these words of weight 22 it is useful to know whether there are any small classes (i.e., are they all of size 7 X 127 X 128 or are some smaller?).

Equivalently, one may ask whether any word w of weight 22 in the code is fixed by a transformation τ of G. We shall show that there is a single class of weight 22 codewords containing 127 X 128 = 16,256 codewords and that the other weight 22 codewords all occur in full classes of size 7 X 127 X 128.

Since conjugate elements of G perform similarly for these purposes, it suffices to examine a single element of each conjugacy class of G.

III. The Conjugacy Classes of G

Lemma. Every element of G is conjugate to one of the following transformations:

(1) Identity: $x \to x$	order 1
(2) Translation: $x \to x + 1$	order 2
(3) $x \to \gamma x, \gamma \neq 0,1$	order 127
(4) $x \to x^{2^k}, k = 1, \ldots, 6$	order 7
(5) $x \to x^{2^k} + \delta, k = 1, \ldots, 6, Tr(\delta) = 1$	order 14

In particular, if α satisfies $x^7 + x^3 + 1 = 0$ over $GF(2)$, then $Tr(\alpha^7) = 1$, and $\delta = \alpha^7$ may be used in (5). The cycle structure for (4) is 2 of length 1 and 18 of length 7, and for (5) there is one cycle of length 2 and 9 cycles of length 14.

Proof. Let us first note the general form of a conjugate $\emptyset\tau\emptyset^{-1}$. Let

$$\tau : x \to \gamma x^{2^k} + \delta \quad \emptyset : x \to ax^{2^i} + b$$

then

$$\emptyset^{-1} : x \to a^{-2^j} x^{2^j} + \left(\frac{b}{a}\right)^{2^j}$$

where $0 \leqslant j \leqslant 6$ and $i + j \equiv 0$ modulo 7. So

$$\emptyset\tau\emptyset^{-1} : x \to a^{-2^j}(\gamma^{2^j} a^{2^{k+j}} x^{2^k} + \delta^{2^j} + \gamma^{2^j} b^{2^{j+k}} + b^{2^j})$$

Note that the exponent on x is preserved by conjugation, so transformations having different exponents are necessarily in different conjugacy classes.

Trivially, the identity forms its own conjugacy class. Note that $\emptyset : x \to ax$ transforms $\tau : x \to x + 1$ into $\emptyset\tau\emptyset^{-1} : x \to x + a^{-1}$. Since a is arbitrary ($a \neq 0$) we have shown that all translations (save the identity) belong to the same conjugacy class. Obviously these translations have order 2. Let $\tau : x \to \gamma x + \delta (\gamma \neq 0,1)$ then $\emptyset : x \to x + \delta/(\gamma + 1)$ transforms τ into $\emptyset\tau\emptyset^{-1} : x \to \gamma x$. All these transformations ($\gamma \neq 0,1$) thus must have order dividing 127, and since it cannot be 1 it must be 127.

For $k = 1, \ldots, 6$, conjugate $\tau : x \to x^{2^k}$ by $\emptyset: x \to ax + b$; this yields $\emptyset\tau\emptyset^{-1} : x \to a^{2^{k-1}} x^{2^k} + a^{-1}(b^{2^k} + b)$. Since $a (a \neq 0)$ is arbitrary, so is $a^{2^k - 1}$. As b ranges over $GF(2^7)$ note that $b^{2^k} + b$ covers all elements of trace 0 exactly twice. Thus all mappings $x \to \gamma x^{2^k} + \delta$ such that $Tr(\sigma\delta) = 0$, where σ is the unique solution of $x^{2^k - 1} = \gamma$, are conjugate to $x \to x^{2^k}$.

Conjugating $\tau : x \to x^{2^k} + \delta (k = 1, \ldots, 6, Tr(\delta) = 1)$ by $\emptyset : x \to ax + b$ yields

$$\emptyset\tau\emptyset^{-1} : x \to a^{2^k - 1} x^{2^k} + a^{-1}(b^{2^k} + b + \delta)$$

Thus, as above, we get all mappings $x \to \gamma x^{2^k} + \delta$ such that $Tr(\sigma\delta) = 1$, and our lemma is proved provided we establish the cycle structures and the orders of the mappings in these last two classes.

Let $\tau : x \to x^{2^k} + \delta (k = 1, \ldots, 6)$ then $\tau^7 : x \to x + Tr(\delta)$; thus if $\delta = 0$ as in (4) we see that the order of τ must divide 7 and, as it is not 1, must indeed be 7. Since $x = 0,1$ are the only solutions of $x = x^{2^k}$ in this field, the cycle structure here must be 2 of length 1 and 18 of length 7. Similarly if $Tr(\delta) = 1$, $\tau^{14} : x \to x + 1 + Tr(\delta) = x$, thus the possible orders for τ are 1,2,7, and 14. Not 1 obviously, and $\tau^7 : x \to x + Tr(\delta) = x + 1$, so not 7. Now $\tau^2 : x \to x^{2^{2k}} + \delta^{2^k} + \delta$; but if these are equal $x^{2^{2k}} + x = \delta^{2^k} + \delta$. Since $x^{2^{2k}} + x$ maps $GF(2^7)$ doubly onto its elements of trace 0, we see that there are precisely two solutions to this equation. These two solutions must appear in a cycle of length 2 since no cycle of odd length exists (for j odd x and $\tau^j(x)$ necessarily are of different trace so they cannot be equal). Thus $\tau : x \to x^{2^k} + \delta$ where $Tr(\delta) = 1$ must have 1 cycle of length 2 and 9 cycles of length 14. In particular, it is of order 14 as asserted.

IV. The Codewords of Weight 22

If a codeword of weight 22 is fixed by a transformation τ, then τ must have distinct cycles whose lengths add to 22. Thus no transformation conjugate to (3) $x \to \gamma x (\gamma \neq 0,1)$ can fix a codeword of weight 22 since its cycle structure is necessarily 1 of length 127 and 1 of length 1. The cycle structure for (5) $x \to x^{2^k} + \delta$, $Tr(\delta) = 1$, rules these conjugacy classes out also. A translation $x \rightarrow x + \delta$ necessarily has 64 cycles of length 2 of the form (i,j) corresponding to α^i and $\alpha^j = \alpha^i + \delta$. Thus a codeword of weight 22 would have its 1's in positions specified by 11 such cycles.

So with codeword $C_0, C_1, \ldots, C_{127}$ we would have

$$\Sigma C_i \alpha^i = \sum_{i=1}^{11} \delta \neq 0$$

for $\delta \neq 0$, which contradicts the definition of a BCH code. So $x \rightarrow x + \delta (\delta \neq 0)$ fixes no words of weight 22 in this code.

Since the $\tau_k : x \rightarrow x^{2^k} (k = 1, \ldots, 6)$ are all powers of each other, they fix the same codewords, if any. Thus it suffices to examine $x \rightarrow x^2$. Since the cycle structure here (2 cycles of length 1, 18 cycles of length 7) allows codewords of weight 22, all possibilities were examined by computer and it was found that 2 such codewords exist. These are transformed into each other by $x \rightarrow x + 1$. The 127 X 128 images under G of either of these are all distinct. Thus the words of weight 22 in the (128,64) BCH code occur in full classes of size 7 X 127 X 128 = 113,792 except for the 127 X 128 = 16,256 indicated above. Testing the 85 weight 22 codewords which occurred during our simulation of this code indicates that there are just 2 further classes of size 113,792. Thus we conclude:

The (128,64) BCH code has 243,840 codewords of weight 22. These codewords may be constructed by applying G to the following representatives:

A = (0) (3,6,12,24,48,96,65) (23,46,92,57,114,101,75) (43,86,45,90,53,106,85);

B = 1,2,6,11,17,18,30,33,36,39,40,45,61,68,82,99,101, 103,106,112,115,119;

C = 1,13,22,25,26,37,44,47,56,65,67,80,83,85,86,88,99, 105,115,119,120,122

The first one (obviously) corresponds to the single small class of size 16,256.

References

1. Baumert, L. D., and McEliece, R. J., "Performance of Some Block Codes on a Gaussian Channel," Proceedings of the 1975 International Telemetering Conference, pp. 189-195, McGregor and Werner, Washington, D.C., 1975.
2. vanLint, J. H. *Coding Theory,* Springer Lecture Notes in Mathematics No. 201, Springer-Verlag, Heidelberg, 1971.