'Perfect' Punctured Codes

by G. Solomon

& J. J. Stiffler

JET PROPULSION LABORATORY

[redacted]

International Conference on Microwaves, Circuit Theory and Information Theory, Sept. 7-11, 1964, Tokyo. ~~Japan~~

Perfect Punctured Cyclic Codes

I. Introduction.

This paper presents a class of codes which are obtained from maximal length shift register codes by deleting or puncturing certain of their coordinates. The "punctured cyclic codes" thus obtained are shown to be optimum, and an encoding and decoding procedure is outlined. In the demonstration of the optimality of these codes, a new bound on the maximum distance obtainable with an n, k group code is derived. This bound is always as good as, and generally better than, the well-known Plotkin bound (Ref. 4).

II. The Puncturing Procedure.

To begin, it is necessary to prove several theorems.

Theorem 1.

The minimum value for n for which it is possible to obtain an (n,k) group code with minimum distance d_o is greater than or equal to

$$d_o + d_1 + . . . + d_{k-1} \qquad (1)$$

where $d_i = d_{i-1}/2$ if d_{i-1} is even and $d_i = (d_{i-1} + 1)/2$ if d_{i-1} is odd.

Proof.

Designate the (n,k) group code by G. Since G contains an element with the weight d_o, it can be written, after suitable row and column permutations, in the form

$$G = \left|\begin{array}{c|c} \overbrace{\hphantom{0\,0\ldots0}}^{n - d_o} & \overbrace{\hphantom{0\ldots0}}^{d_o} \\ 0\,0\,.\,.\,.\,0 & 0\,.\,.\,.\,0 \\ 0\,0\,.\,.\,.\,0 & 1\,.\,.\,.\,1 \\ & \\ G_1 & H_1 \end{array}\right| \tag{2}$$

Since G_1 is a group and since the identity occurs exactly twice (it clearly cannot occur more than twice if G is to have minimum distance d_o) G_1 must be an $n - d_o$, $k - 1$ group with some nonzero minimum distance d_1. Further, because of the second element of G, as written above, both $g_1h_1 \epsilon G$ and $g_1\bar{h}_1 \epsilon G$ where $g_1 \epsilon G_1$, $h_1 \epsilon H$, $\bar{h}_1$ is the complement of h_1 and g_1h_1 designates the n-tuple obtained by following the $(n - d_o)$-tuple g_1 by the d_o-tuple h_1. Let d_1 be the weight of g_1 and c_1 the weight of h_1. Then:

$$w(g_1) + w(h_1) = d_1 + c_1 \geqq d_o,$$

$$w(g_1) + w(\bar{h}_1) = d_1 + d_o - c_1 \geqq d_o,$$

or

$$d_1 \geqq c_1.$$

Hence

$$d_1 \geq \left\{\frac{d_o}{2}\right\} = \begin{cases} \dfrac{d_o}{2} & d_o \text{ even} \\ \dfrac{d_o + 1}{2} & d_o \text{ odd} \end{cases} \qquad (3)$$

Continuing the same process the following groups are successively obtained. G_2, an $(n - d_o - d_1, k - 2)$ code with minimum distance $d_2 \geq \left\{d_1/2\right\}$; G_3, an $(n - d_o - d_1 - d_2, k - 3)$ code with minimum distance $d_3 \geq \left\{d_2/2\right\}$; and, in general, G_i, an $(n - d_o - d_1 - \ldots - d_{i-1}, k - i)$ code with minimum distance $d_i \geq \left\{d_{i-1}/2\right\}$. Let $i = k - 1$ and observe that for an $(m,1)$ code to have minimum distance $d, m \geq d$. Then

$$n - d_o - d_1 - , \ . \ . \ . \ , - d_{k-2} \geq d_{k-1}$$

Corollary 1.

The smallest value of n for which an (n,k) code with distance

$$d = 2^{k-1} - \sum_i 2^{\ell_i - 1} \qquad (1 \leq \ell_i \leq k - 1, \ \ell_i \neq \ell_j) \qquad (4a)$$

can exist is

$$n \geq (2^k - 1) - \sum_i (2^{\ell_i} - 1). \qquad (4b)$$

Proof.

$$d_1 = \left\{\frac{d}{2}\right\} = 2^{k-2} - \sum_i 2^{\ell_i-2},$$

where $2^{\ell_j} = 0$ for $\ell_j < 0$. With the same convention:

$$d_2 = \left\{\frac{1}{2}\left\{\frac{d}{2}\right\}\right\} = 2^{k-3} - \sum_i 2^{\ell_i-3}$$

and, in general:

$$d_j = 2^{k-j-1} - \sum_i 2^{\ell_i-j-1}.$$

Thus, since $\ell_i \leqq k - 1$, $d_{k-1} = 1$, and

$$n \geqq d + d_1 + \ldots + d_{k-1}$$

$$= -\sum_i \left[\sum_{j=0}^{\ell_i-1} 2^{\ell_i-j-1}\right] + \sum_{j=0}^{k-1} 2^{k-1-j}$$

$$= 2^k - 1 - \sum_i (2^{\ell_i} - 1).$$

Note that if $r(2^{k-1}) \geq d \geq (r-1)2^{k-1}$ for some integer r, the modified dyadic expansion

$$d = r(2^{k-1}) - \sum_{\ell_i} 2^{\ell_i - 1}$$

can be obtained resulting in the inequality

$$n \geq r(2^k - 1) - \sum_{\ell_i} (2^{\ell_i} - 1)$$

Theorem 2.

If

$$\sum_i \ell_i \leq k, \tag{6}$$

the bound obtained in Theorem 1 can be achieved.

Proof.

Assume $d \leq 2^{k-1}$. Consider the $(2^k - 1, k)$ code with distance 2^{k-1}. The columns of this code form a group on k generators from which the identity has been deleted. Now consider a subgroup of $2^{\ell_i} - 1$ columns formed from ℓ_i of these generators, again deleting the identity. The rows of this subgroup each contain exactly $2^{\ell_i - 1}$ ones. Puncturing the columns of this subgroup from the original group leaves a $\left[2^k - 1 - (2^{\ell_i} - 1)\right], k$ code with minimum distance $d = 2^{k-1} - 2^{\ell_i - 1}$. Proceeding in this fashion, distinct subgroups of order ℓ_i can be punctured for each of the values ℓ_i so long as the generators of the subgroups are all distinct. This is possible so long as

$$\sum_i \ell_i \leqq k.$$

The resulting code then has

$$n = 2^k - 1 - \sum_i (2^{\ell_i} - 1)$$

symbols and minimum distance

$$d = 2^{k-1} - \sum_i 2^{\ell_i - 1},$$

and hence achieves the bound of Theorem 1.

If $r2^{k-1} \geqq d > (r - 1)2^{k-1}$ the bound can be achieved if $\sum \ell_i \leqq rk$ in the modified expansion described above. This is accomplished by puncturing the necessary number of columns from the $r(2^k - 1), k$ code obtained by repeating the $(2^k - 1, k)$ code r times. Since each generator occurs r times, the necessary number of subgroups can be punctured so long as

$$\sum_i \ell_i \leq rk. \qquad (7)$$

The following two sections outline an encoding and decoding procedure for these "perfect" punctured cyclic codes.

III. Encoding.

Let A be an (n,k) punctured cyclic code which is optimal, i.e., $n = 2^k - 1 - m$ where

$$m = \sum_i (2^{\ell_i} - 1), \ \ell_i > \ell_{i+1}$$

and

$$\sum_i \ell_i \leq k.$$

It was shown in the previous section that such codes are obtained by puncturing or deleting **m** $(2^k - 1)^{st}$ roots of unity in the following fashion:

Choose $\alpha_1, \alpha_2, \ . \ . \ . \ , \alpha_\ell$ independent elements of $GF(2^k)$. Let G_1

be the additive group using $\alpha_1, \alpha_2, \ldots, \alpha_{\ell_1}$, as generators, G_2 the additive group using $\alpha_{\ell_1+1}, \ldots, \alpha_{\ell_1+\ell_2}$ as the generators, G_3 the additive group $\alpha_{\ell_1+\ell_2+1}, \ldots, \alpha_{\ell_1+\ell_2+\ell_3}$, and so on until all the necessary groups are formed. After omitting the zero elements in each group this procedure yields the necessary $m = \sum (2^{\ell_i} - 1)$ nonzero elements of $GF(2^k)$. This is the punctured set.

Now consider the $(2^k - 1,k)$ cyclic code. This, of course, is generated by a primitive k^{th} degree polynomial in the field F of two elements. To obtain the (n,k) code from this basic cyclic code, the values corresponding to the punctured coordinates are simply omitted. Thus, each perfect punctured code uses the primary encoding procedure and shift register device of the "parent" cyclic code $(2^k - 1,k)$ with little added complication.

Example 1.

Consider the (12,4) code. Here $m = 15 - 12 = 3$. Choose α_1 α_2, and $\alpha_1 + \alpha_2$ as the punctured elements. The (15,4) can be generated by the polynomial $f(x) = x^4 + x + 1$, a primitive 4th degree polynomial. The associated difference equation or recursion rule is then $\alpha_{i+4} + \alpha_{i+1} + \alpha_i = 0$. Let $\alpha_1 = \beta^5$, $\alpha_2 = \beta^6$ where β is a primitive 15th root of unity, and note that $\alpha_1 + \alpha_2 = \beta^5 + \beta^6 = \beta^9$. The encoding for the (15,4) code is as in the following example:

$$0\,0\,0\,1 \rightarrow 0\,0\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1$$

Deleting the 5th, 6th, and 9th coordinates, the mapping becomes

$$0\,0\,0\,1 \rightarrow 0\,0\,0\,1\,0\,1\,0\,0\,1\,1\,1\,1.$$

This is the encoding procedure for the (12,4) code with minimum distance $6 = 2^3 - 2^1$.

IV. Decoding.

Let A_i be an (n_i,k) optimal punctured cyclic code of the type given by the algorithm for "perfect" codes!

$$n_i = 2^k - 1 - m_i \text{ where } m_i = \sum_{j=1}^{r} (2^{\ell_j} - 1), \quad \sum_{j=1}^{r} \ell_j \leq k, \ \ell_j > \ell_{j+1} \geq 1,$$

and let the number of correctable errors, as determined above, be e_i. In other words, the puncturing consists of deleting the set of nonzero elements of r distinct subgroups of $GF(2^k)$. For such codes, the decoding procedure is straightforward and may be inherited from any algebraic decoding procedure used for the parent $(2^k - 1,k)$ cyclic code which enables one to determine the minimum distance explicitly, regardless of its value.

Such a decoding procedure is the Peterson decoding procedure for Bose-Chandhure codes (Ref. 3). This is a technique which determines the nearest code word (in the Hamming distance sense) if it exists.

To begin, perfect punctured codes are divided into classes in accordance with the number of groups which were punctured.

Class 1:

$m_i = 2^{\ell_1} - 1$, ℓ_1 k. This is the simplest case; only one group with ℓ_1 generators is punctured. For such a class, the decoding proceeds in two steps.

Step 1:

Since the weight of the punctured m_i-tuple is either 0 or $2^{\ell_i - 1}$, consider two separate cases. In step 1 it is assumed that the weight of the punctured word is zero, i.e., all punctured positions are zero. The received word of length n_i is then expanded into a word of length $(2^k - 1)$ by placing 0's in each of the punctured positions and the received symbols a_i in their respective unpunctured positions. Then the word is decoded as though it were a full-length unpunctured word. If possible, the nearest word is determined, and the distance d_1 between the received word and the unpunctured position of the "decoded" word is recorded.

Step 2:

Assume that the punctured position has weight $2^{\ell_1 - 1}$. In this case, place the symbol one in the $2^{\ell_1} - 1$ punctured positions. This immediately introduces an error of order $2^{\ell_1 - 1} - 1$ in the calculation. Again decode, if possible, the expanded word, and record the distance d_2 between the unpunctured positions of the decoded word and the received word.

Decision:

Compare d_1 and d_2 obtained in steps 1 and 2. Choose the word with min $(d_1,d_2) = d$. If d is not greater than the number of correctable errors e_i the received word can be uniquely decoded and is that determined in step 1 if $d_1 < d_2$ and in step 2 if $d_1 > d_2$. Note that d_1 and d_2 cannot both be less than or equal to e_i, but if e or fewer errors occur in transmission, one of them must be less than e_i.

Class II:

$$m_i = 2^{\ell_1} - 1 + 2^{\ell_2} - 1 \qquad \ell_1 > \ell_2, \ \ell_1 + \ell_2 \leq k$$

The procedure is as in Class I, except that the decoding procedure is divided into 4 steps.

Step 1:

Assume all punctured coordinates are zero.

Step 2:

Assume the $2^{\ell_1} - 1$ punctured coordinates corresponding to the first punctured group are zero and the $2^{\ell_2} - 1$ punctured coordinates corresponding to the second are one.

Step 3:

Reverse the roles of zero and one in step 2.

Step 4:

Assume all punctured coordinates are one.

As before, it is necessary to attempt to decode the words formed in each step and to determine the distance d_i between the decoded words and the received word (at the unpunctured positions only). That word is chosen which results in the minimum distance d_i. Again, if e_i or fewer errors were committed, the decoding is unique.

Class r:

In general for $m = \sum_{i=1}^{r} 2^{\ell_i} - 1$, $\sum_{i=1}^{r} \ell_i \leq k$, there will be 2^r steps to take. However since $\ell_i > \ell_{i+1}$, and $\sum \ell_i \leq k$, r remains relatively small for moderate values of k. In fact, it may be easily verified that $r < \sqrt{2k}$. Even for large values of k, this procedure may be completely practical, since most useful codes may be obtained by deleting only one or two groups from the $2^k - 1,k$ code.

Generalization to q-ary codes:

The development of this section closely parallels that of Section I and will therefore be somewhat condensed.

Theorem 1'.

The minimum value of n for which it is possible to obtain an (n,k) group code over the field of q elements with minimum distance d_0 is greater than or equal to

$$d_0 + d_1 + \dots + d_{d-1}$$

where
$$d_i = \left\{\frac{d_{i-1}}{q}\right\} = \begin{cases} \dfrac{d_{i-1}}{q} & \text{if } q \mid d_{i-1} \\ \left[\dfrac{d_{i-1}}{q}\right] + 1 & \text{otherwise} \end{cases} \tag{8}$$

Proof:

Let G represent the n,k group codes under consideration. Since G has minimum distance d_0 it can be written, after suitable column permutation, in the form

$$G = \left|\begin{array}{c|cccc}
0\;0\;\ldots\ldots\;0 & 0 & 0 & \ldots\ldots & 0 \\
G_1 & \multicolumn{4}{c}{G_2} \\
0\;0\;\ldots\ldots\;0 & \alpha_{i_1} & \alpha_{i_2} & \ldots\ldots & \alpha_{i_{d_0}} \\
G_1 & \multicolumn{4}{c}{H_2} \\
0\;0\;\ldots\ldots\;0 & (\alpha_1\alpha_{i_1}) & (\alpha_1\alpha_{i_2}) & \ldots & (\alpha_1\alpha_{i_{d_0}}) \\
\alpha_1 G_1 & \multicolumn{4}{c}{\alpha_1 H_2} \\
0\;0\;\ldots\ldots\;0 & (\alpha_2\alpha_{i_1}) & (\alpha_2\alpha_{i_2}) & \ldots & (\alpha_2\alpha_{i_{d_0}}) \\
\alpha_2 G_1 & \multicolumn{4}{c}{\alpha_2 H_2} \\
0\;0\;\ldots\ldots\;0 & (\alpha_3\alpha_{i_1}) & (\alpha_3\alpha_{i_2}) & \ldots & (\alpha_3\alpha_{i_{d_0}}) \\
\vdots & & \vdots & & \\
0\;0\;\ldots\ldots\;0 & (\alpha_{q-2}\alpha_{i_1}) & (\alpha_{q-2}\alpha_{i_2}) & . & (\alpha_{q-2}\alpha_{i_{d_0}}) \\
\alpha_{q-2} G_1 & \multicolumn{4}{c}{\alpha_{q-2} H_2}
\end{array}\right| \qquad (9)$$

where $0, 1, \alpha_1, \alpha_2, \ldots \alpha_{q-2}$ are the elements of the field, G_1 and G_2 are groups of order k-1 (the identity is written explicitly), H_2 is the coset of G_2 obtained by adding the element $\alpha_{i_1}\alpha_{i_2} \ldots \alpha_{i_{d_0}}$ to each of the elements of G_2 and $\alpha_i H_2$ is the coset obtained by multiplying each of the terms of H_2 by α_i. Note that since G has minimum weight d_0, there exists an element $0 \ldots 0 \, \alpha_{i_1}\alpha_{i_2} \ldots \alpha_{i_{d_0}}$ such that none of the last d_0 terms are zero.

Now, select an element g_1 from G(other than $0\,0 \ldots 0 \, \alpha_{i_1}\alpha_{i_2} \ldots \alpha_{i_{d_0}}$ or one of its multiples) such that a_1 of the first n-d terms are non-zero and a_2 of the last d_0 terms are non-zero. Clearly,

$$a_1 + a_2 \geqq d_0. \tag{10}$$

In addition, it will now be shown that

$$a_1 \geqq c \geqq \frac{a_2}{q-1} \tag{11}$$

where c is the maximum number of agreements between the last d_0 terms of g_1 and the corresponding terms of any of the vectors

$$\begin{array}{ccc} \alpha_{i_1} & \alpha_{i_2} \ldots & \alpha_{i_{d_0}} \\ (\alpha_1\alpha_{i_1}) & (\alpha_1\alpha_{i_2}) \ldots & (\alpha_1\alpha_{i_{d_0}}) \\ (\alpha_{q-2}\alpha_{i_1}) & (\alpha_{q-2}\alpha_{i_2}) \cdot & (\alpha_{q-2}\alpha_{i_{d_0}}). \end{array} \tag{12}$$

Since a_2 of the final d_0 terms of g_1 are non-zero and since each element of the field occurs exactly one in each position of the elements (12), the total number of agreements between these a_2 non-zero terms and the corresponding terms of all of the q-1 elements (12) is just a_2. The average number of agreements is then $\frac{a_2}{q-1}$ and $c \geq \frac{a_2}{q-1}$.

Thus, if a vector corresponding to one of the elements (12) for which $c \geq \frac{a_2}{q-1}$ is selected and subtracted from g_1, there will still be a_1 non-zero terms in this first $n-d_0$ terms of the resulting vector and the last d_0 terms will contain exactly d_0-c non-zero terms. Thus

$$a_1+d_0-c \geq d_0$$

$$\text{or } a_1 \geq c \geq \left\{\frac{a_2}{q-1}\right\} \geq \frac{a_2}{q-1}$$

as was stated above. Combining the inequalities (10) and (11) yields the result

$$a_2 \left(1+\frac{1}{q-1}\right) \geq d_0$$

$$a_2 \geq \frac{q-1}{q} d_0$$

$$a_1 \geq \left\{\frac{d_0}{q}\right\}$$

The group G_1, then, is an $(n-d_0,k-1)$ code over a field of q elements with the property that $d_1 = a_1 \geq \left\{\frac{d_0}{q}\right\}$. By repeating this argument, as before, the statement of the theorem follows.

Corollary 1':

The smallest value of n for which an (n,k) code over the field of q elements with distance

$$d = \beta_0 \, q^{k-1} - \sum \beta_i q^{\ell_i - 1} \qquad \left(\beta_i = 0,1,2, \; . \; . \; , \; q-1\right) \qquad (13a)$$
$$\left(1 \leq \ell_j \leq k-1, \; \ell_j \neq \ell_m\right)$$

can exist is

$$n \geq \frac{\beta_0 (q^k - 1)}{q-1} - \frac{\sum \beta_i (q^{\ell_i} - 1)}{q-1} \qquad (13b)$$

Proof:

This proof is completely analogous to that for q = 2 and hence will be omitted.

To obtain an analog to Theorem 2, consider the $(q^k - 1,k)$ maximal length shift register code over the q-ary alphabet with minimum distance $d = (q - 1) \; q^{k-1}$. The columns of this code form an algebra on k generators over the finite field GF(q) from which the identity has been deleted. Now consider a subalgebra of q^{ℓ} columns formed from ℓ of these generators, again deleting the identity. The rows of this subalgebra each contain exactly $q^{\ell-1} - 1$ zeroes. Puncturing the columns of this subalgebra from the original algebra leaves a $(q^k - 1 - (q^{\ell} - 1),k)$ code with minimum distance $d = (q^{k-1} - q^{\ell-1})(q - 1)$.

In addition, one may divide the algebra into (q - 1) classes with the condition that if a is in one class, no scalar multiple of a is in the same class. The weight of any row in a subclass is 1/(q - 1) times the weight of a full row of the code. Similarly, the same statement is applicable to any subalgebra of any dimension. Thus another puncturing presents itself as a possibility. Let β_k be a number less than q - 1, the number of subclasses of the k-dimensional algebra. Puncturing the columns of these β_k subclasses leaves a $\left[(q - 1 - \beta_k)(q^k - 1/q - 1),k)\right]$ code with minimum distance $d = (q - 1 - \beta_k)(q^{k-1})$. Similarly consider β_{ℓ_i} of the subclasses of an ℓ_i-dimensional subalgebra. Then an analogous puncturing yields a $\left[q^k - 1 - (q^{\ell_i} - 1/q - 1)\beta_{\ell_i},k\right]$ code with minimum distance $d = q^{k-1}(q - 1) - \beta_\ell q^{\ell_{i-1}}/q - 1$. A sufficient (though not necessary) condition for attaining the bound of Theorem 1' may now be formulated:

<u>Theorem</u> <u>2'</u>:

Let $d = \beta_0 q^{k-1} - \sum \beta_i q^{\ell_i - 1}$ $\qquad \beta_i = 0, 1, 2, . . (q - 1)$

then if $\beta_0 \geqq \max \beta_i$ and $\sum \ell_i \leq k$ $\qquad 1 \leqq \ell_j \leqq k - 1, \ \ell_i \neq \ell_j \ (i \neq j)$

the bound, $n = \beta_0 \dfrac{(q^k - 1)}{q - 1} - \sum \beta_i \dfrac{(q^{\ell_i} - 1)}{q - 1}$, is achieved by puncturing columns as described above. In this case there are obviously enough generators, algebras and subalgebras to puncture.