EXTENDED DOUBLE-ERROR CORRECTING BINARY GOPPA CODES ARE CYCLIC

by

E. R. Berlekamp and O. Moreno

Memorandum No. ERL-M376

15 February 1973

ELECTRONICS RESEARCH LABORATORY

College of Engineering
University of California, Berkeley
94720

EXTENDED DOUBLE-ERROR CORRECTING BINARY GOPPA CODES ARE CYCLIC

by

E. R. Berlekamp and O. Moreno

Departments of Mathematics and of Electrical Engineering and
Computer Sciences and the Electronics Research Laboratory
University of California, Berkeley, California 94720

ABSTRACT

The class of codes introduced by Goppa [1,2] includes the BCH codes as a proper subset. It also includes a large subset of asymptotically good codes, each of which has an algebraic decoding algorithm for correcting some smaller number of errors. In section 7 [1], Goppa gives necessary and sufficient conditions for his codes to be isomorphic to cyclic codes under a certain correspondence. In this note, we exhibit another correspondence which reveals that certain other Goppa codes, (including the example of Goppa's See 6) become cyclic when extended by an overall parity check. In particular, the extended Goppa codes with $(n,k,d) = (2^m + 1, 2^m - 2m, 6)$ are isomorphic to the reversible cyclic codes with check polynomial $(x+1)$ $f(x)$, where $f(x)$ is an irreducible polynomial of period $2^m + 1$.

Research sponsored by the National Science Foundation Grant GK-36179.
This note is based in part on O. Moreno's Ph.D. dissertation.

The Goppa code of length 2^m consists of all codewords $C(x)$, where $x \in GF(2^m)$ and $C(x)$ takes values in $GF(2)$, which satisfy the equation in $GF(2^{mt})$

$$\sum_{x} \frac{C(x)}{z-x} = 0 \qquad (1)$$

where $z \in GF(2^{mt})$ is a root of the irreducible polynomial $G(z)$, of degree t over $GF(2^m)$. The polynomial $G(z)$ is called the Goppa polynomial, which defines the code.

The extended Goppa code of length $2^m + 1$ includes an additional position, denoted by ∞, such that

$$\sum_{x} C(x) = 0 \qquad (2)$$

where in the sum of Eq. (2), x ranges over $GF(2^m) \cup \{\infty\}$. Since $1/(z-\infty) = 0$, we may also allow the sum of Eq. (1) to have this extended range.

Let $G(z) = \sum_{i} G_i z^i$. Then $\dfrac{G(z) - G(x)}{z-x} = \sum_{i}\left(\sum_{j} G_{i+j+1} \; x^{j-i}\right) z^i$,

and since $G(z) = 0$, it follows that $\dfrac{1}{z-x} = \dfrac{-1}{G(x)} \sum_{i=0}^{t-1}\left(\sum_{j} G_{i+j+1} \; x^{j-i}\right) z^i$

and $0 = \sum_{x} \dfrac{C(x)}{z-x} = -\sum_{x} \dfrac{C(x)}{G(x)} \sum_{i=0}^{t-1}\left(\sum_{j} G_{i+j+1} \; x^{j-i}\right) z^i$

But since z satifies no equation of degree less than t over $GF(2^m)$, for each $i = 0, 1, \ldots$ $t-1$ we must have

$$0 = \sum_{x} \frac{C(x)}{G(x)}\left(\sum_{j} G_{i+j+1} \; x^{j-i}\right)$$

Since this system of equations is triangular, it also follows that

$$0 = \sum_{x} \frac{x^i C(x)}{G(x)} \quad \text{for } i = 0, 1, \ldots, t-1 \qquad (3)$$

We have shown that Eq. (1) implies Eqs. (3). It is straightforward to reverse these steps and see that Eq. (3) implies Eq. (1). Rewriting Eq. (2) as

$$0 = \sum_{x} \frac{G(x)\ C(x)}{G(x)}$$

and using Eqs. (3), we obtain

$$0 = \sum_{x} \frac{x^i\ C(x)}{G(x)} \quad \text{for } i = 0, 1, \ldots, t \qquad (4)$$

where x ranges over $GF(2^m) \cup \{\infty\}$. Eqs. (4) is equivalent to Eq. (1) and Eq. (2).

Starting from Eq. (4), it is easy to see that if H(x) is obtained from G(x) by an affine tranformation, $x \to \frac{ax+b}{cx+d}$ where $a,b,c,d \in GF(2^m)$, $ad \neq bc$ and $x \in GF(2^m) \cup \{\infty\}$, then the code with Goppa polynomial H(z) may be obtained from the code with Goppa polynomial G(z) by the corresponding affine permutation of the code's digits. Similarly, if G(z) is invariant under any affine permutation, then so is the corresponding Goppa code. As we will see in the subsequent section, some extended Goppa codes are invariant under additional symmetries.

Double error-correcting codes

Since any irreducible quadratic over $GF(2^m)$ can be transformed into any other by an appropriate affine transformation, there is only one extended 2-error correcting Goppa code of length $(2^m + 1)$. Without loss of generality, we may take

$$G(z) = z^2 + z + \beta \tag{5}$$

where $\mathrm{Tr}(\beta) = \sum_{i=0}^{m-1} \beta^{2i} = 1$.

If z is a root of $z^2 + z + \beta$, so are $z + 1$ and $\frac{\beta}{z}$. Hence, the code is invariant under the permutations

$$\rho_1\colon \; x \leftrightarrow x + 1$$
$$\rho_2\colon \; x \leftrightarrow \frac{\beta}{x}$$

It is also invariant under

$$\rho_3\colon \; x \to x^2 + \beta$$

The invariance under ρ_3 follows from squaring Eq.(1) to obtain

$$0 = \sum \frac{C(x)}{z^2 + x^2} = \sum \frac{C(x)}{z + \beta + x^2}$$

We notice that $\rho_3^m : x \to x^{2^m} + \mathrm{Tr}(\beta) = x + 1$, so that $\rho_3^m = \rho_1$.

We will now prove that the permutation $\rho_2\rho_1\colon x \to \beta/(x+1)$ is cyclic. There is a well-known homomorphism from 2 x 2 matrices onto the affine transformations, so that if

$$\sigma_1\colon \; x \to (ax+b)/(cx+d)$$
$$\sigma_2\colon \; x \to (ex+b)/(gx+h)$$

then $\sigma_1\sigma_2\colon \; x \to (ix+j)/(kx+\ell)$

where $\begin{bmatrix} i & j \\ k & \ell \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix}$

Hence, it is necessary and sufficient to show that for suitable choice of β,

$$[1\ 0]\begin{bmatrix}0 & \beta\\ 1 & 1\end{bmatrix}^{n} = k\ [1\ 0] \quad \text{where } k \in GF(2^m) \qquad (6)$$

iff $(2^m+1) \mid n$. But any eigenvalue of $\begin{bmatrix}0 & \beta\\ 1 & 1\end{bmatrix}$, say λ, must be a root of $z^2 + z + \beta$ and so in Eq. 6, $k = \lambda^n$. Let ξ be a primitive root of $z^{2^m} + 1$, so that $\xi \in GF(2^{2m})$, and for suitably chosen elements α_1, $\alpha_2 \in GF(2^{2m})$, $\xi^2 = \alpha_1 \xi + \alpha_2$. Let $\lambda = \frac{\xi}{\alpha_1}$, so that λ is a root of $z^2 + z + \beta$, where $\beta = \frac{\alpha_2}{\alpha_1^2}$. Now $\lambda^n = \xi^n \alpha_1^{-n}$, so that $\lambda \in GF(2^m)$ iff $\xi^n \in GF(2^m)$, which happens iff $(\xi^n)^{(2^m-1)} = 1$. But since $(\xi^n)^{(2^m+1)} = 1$ and (2^m+1) and (2^m-1) are relatively prime, this can happen only if $\xi^n = 1$, whence $n \equiv 0 \bmod 2^m+1$.

Q.E.D.

REFERENCES

[1] V. D. Goppa (1970) "A New Class of Linear Error-Correcting Codes" (In Russian) Problemy Peredachi Informatsy VI, (3), pp. 24-30.

[2] V. D. Goppa (1971) "Rational Representation of Codes and (L,g) Codes" (In Russian) Problemy Peredachi Informatsy VII, (3), pp. 41-49.