ON A CLASS OF CODES OF DELSARTE

L. R. WELCH
University of Southern California

Summary. In reference [1], Delsarte generalized a class of codes due to Chien and Choy [2] which, in turn, are a generalization of Goppa Codes [3]. Delsarte shows that almost all of these codes meet the Gilbert-Varsharmov bound, a result which is also true of Goppa codes [4]. Both of these results are obtained by showing that the actual minimum distance is much larger than the "designed" distance and approaches the G-V bound for the designed rate.

This talk raises the question as to how large the actual rate can be for fixed design distance. No new theorems are presented but two well known theorems are proved in the context of Delsarte's presentation.

Introduction. Let $F_0 = GF(q)$ be a finite field, $F = GF(q^m)$ an extension field and $F_k[X]$ be the set of polynomials over F of degree less than k. If $S = \{\alpha_1,...,\alpha_n\}$ is an ordered set of n distinct elements of F and $a = (a_1,..., a_n)$ is an n-tuple over F of weight n, then a code may be defined:

$$C(k,a) = \{(c_1,\ldots,c_n): \sum_{i=1}^{n} c_i a_i f(\alpha_i) = 0 \text{ for } f \in F_{d-1}[X]\} \qquad (1)$$

where d = n-k+1. This definition is equivalent to Delsarte's (see Theorem 1 [1]), however the n-tuple a is his a'. The minimum distance of these codes is d = n-k+1. A subfield code can be defined [5] by

$$C|F_0 = C \cap F_0^n$$

$$= \left\{ (c_1,\ldots,c_n): \begin{array}{ll} c_i \in F_0 & 1 \le i \le n \\ \sum c_i a_i f(\alpha_i) = 0 & f \in F_{d-1}[X] \end{array} \right\}$$

It is this latter class of codes to which BCH and Goppa codes belong and for which the Gilbert-Varsharmov bound theorems have been proven. The number of linearly independent constraints on the n-tuples, c, is (d-1). In the subfield code, each constraint becomes m constraints so that the apparent number of linearly independent constraints is m(d-1) and the apparent dimension of the code is k* = n-m(d-1). However the m(d- 1)

constraints may be dependent, resulting in a larger code. In certain cases it is known that the number of linearly independent constraints is at most ((d-1)/2)m. Before investigating these cases, BCH and Goppa codes will be defined.

Let n divide q^m-1 and let α be a primitive, $n^{\underline{th}}$ root of unity in F. The ordered set S is S = $\{\alpha^1,\alpha^2,\ldots, \alpha^n\}$ and a = $(\alpha^1,\ldots, \alpha^n)$. Then

$$C_{BCH}^{n,d} = C(n-d+1)\,|F_0$$

$$= \left\{ (c_1,\ldots,c_n): \begin{array}{l} c_i \epsilon F_0 \quad 1 \le i \le n \\ \sum_{i=1}^{n} c_i \alpha^i f(\alpha^i) = 0 \text{ for } f \epsilon F_{d-1}[X] \end{array} \right\} \qquad (2)$$

Taking the powers of X as a basis for $F_{d-1}[X]$, the set of constraints become linear combinations of

$$\sum_{i=1}^{n} c_i \alpha^{(l+\ell)^i} = 0 \qquad \ell = 0, 1, \ldots, d-2$$

which can be readily seen to be the usual definition of a BCH code.

For the Goppa code with polynomial G(x), let d = deg(G) + 1 and let S contain no roots of G. Define $a_1 = [G(\alpha_i)]^{-1}$. Then the Goppa code is

$$\Gamma = C(n-d+1, a)\,|\,F_0$$

or

$$\Gamma = \left\{ (c_1,\ldots,c_n): \begin{array}{l} c_i \epsilon F_0 \quad 1 \le i \le n \\ \sum c_i [G(\alpha_i)]^{-1} f(\alpha_i) = 0 \text{ for } f \epsilon F_{d-1}[X] \end{array} \right\} \qquad (3)$$

The proof of this will not be given. here.

Two Theorems Concerning Rate. In this section GF(q) = GF(2), d is an odd integer and the constraints $c_i \epsilon$GF(2) are always implied.

It is known that the binary BCH codes have only half the redundancy of other BCH codes; that is, half of the constraint equations of Eq. (2) imply the other half. In the present context a generalization of that result can be stated and proved as follows:

Theorem 1. Let $\{\alpha_1,...,\alpha_n\}$ be a set of n distinct elements of F-{0}. Then the code defined by

$$C = \{(c_1,\ldots,c_n): \sum c_i\alpha_i f(\alpha_i) = 0, \quad f\epsilon F_{d-1}[X]\}$$

is identical with the code

$$C' = \{(c_1,\ldots,c_n): \sum c_i\alpha_i f(\alpha_i) = 0 \quad f\epsilon F_{(d-1)/2}[X^2]\}$$

Proof: Clearly C is contained in C'.

Now

$$0 = \left(\sum_{i=1}^{n} c_i\alpha_i f(\alpha_i)\right)^2 = \sum_{i=1}^{n} c_i\alpha_i^2 f^2(\alpha_i) = \sum_{i=1}^{n} c_i\alpha_i(\alpha_i f^2(\alpha_i)$$

Therefore the constraint corresponding to f(x) implies a constraint corresponding to $Xf^2(X)$. Define $(Tf)(X) = Xf^2(X)$ and for a set of polynomials, P define TP to be the space spanned by {Tf: fϵP}. Then the constraints in $F_{(d-1)/2}[X^2]=F^1$ imply the constraints in $F^2 = F^1+TF^1$. (Here, $V_1+V_2 = \{v_1+v_2:v_i\epsilon V_i\}$.) Proceeding by induction in the obvious way, F^1 implies F^d. But F^d contains $F_{d-1}[X]$. Thus C' is contained in C. Q.E.D.

Berlekamp [4] has proven a similar result concerning Goppa codes. In the present context it will be restated to emphasize code size instead of distance.

Theorem 2. Let $S = \{\alpha_1,..., \alpha_n\}$ be a set of n distinct elements of F and let H(X) be a square free polynomial in $F_{(d+1)/2}[X]$ of degree d-1/2 with no roots in S. Let Γ be the binary Goppa code with polynomial $[H(X)]^2$ and design distance d. Then Γ is identical with the code

$$G = \{(c_1,\ldots,c_n): \sum_{i=1}^{n} c_i[H(\alpha_i)]^{-2}f(\alpha_i) = 0 \quad \text{for } f\epsilon F_{(d-1)/2}[X^2]\}$$

Proof: Since G has the same construction with a subset of the constraints, Γ is contained in G. Now

$$0 = \left(\sum_{i=1}^{n} c_i[H(\alpha_i)]^{-2}f(\alpha_i)\right)^{2^{m-1}} = \sum_{i=1}^{n} c_i H(\alpha_i)^{-1} f(\alpha_i)^{2^{m-1}}$$

$$= \sum_{i=1}^{n} c_i H(\alpha_i)^{-2}[H(\alpha_i)f(\alpha_i)^{2^{m-1}}]$$

Now if $f(X) = \sum f_\ell X^{2\ell}$ and Tf is defined by

$$(Tf)(X) = \left(\sum f_\ell^{2^{m-1}} X^\ell\right) H(X)$$

then $(Tf)(\alpha_i) = H(\alpha_i) f(\alpha_i)^{2^{m-1}}$ and the constraint $f \in F_{(d-1)/2}[X^2] \subset F_{d-1}[X]$ implies the constraint $Tf \in H(X)F_{(d-1)/2}[X]$. Therefore the set $F_{(d-1)/2}[X^2]$ implies the set $F_{(d-1)/2}[X^2] + H(X)F_{(d-1)/2}[X]$. Since deg H = d-1/2, $H(X)F_{(d-1)/2}[X]$ is contained in $F_{d-1}[X]$ as is $F_{(d-1)/2}[X^2]$. Since the dimension of the two component subspaces are both (d-1)/2, the sum will be $F_{d-1}[X]$ unless $F_{(d-1)/2}[X^2] \cap H(X)F_{(d-1)/2}[X] \neq \{0\}$; that is, unless there exists non-zero polynomials, P_1, P_2 of degree less than (d-1)/2 with

$$P_1(X)^2 = H(X)P_2(X) .$$

However H is square free, so that P_2 must be of the form $H(X)P_3(X)^2$. The only such polynomial of degree less than d-1 is 0. Q. E. D.

Remark: The size of each Γ is thus at least n-((d-1)/2) m.