Goppa Codes

Invited Paper

ELWYN R. BERLEKAMP

***Abstract*—Goppa described a new class of linear noncyclic error-correcting codes in [1] and [2]. This paper is a summary of Goppa's work, which is not yet available in English.[1] We prove the four most important properties of Goppa codes. 1) There exist q-ary Goppa codes with lengths and redundancies comparable to BCH codes. For the same redundancy, the Goppa code is typically one digit longer. 2) All Goppa codes have an algebraic decoding algorithm which will correct up to a certain number of errors, comparable to half the designed distance of BCH codes. 3) For binary Goppa codes, the algebraic decoding algorithm assumes a special form. 4) Unlike primitive BCH codes, which are known to have actual distances asymptotically equal to their designed distances, long Goppa codes have actual minimum distances much greater than twice the number of errors, which are guaranteed to be correctable by the algebraic decoding algorithm. In fact, long irreducible Goppa codes asymptotically meet the Gilbert bound.**

I. Definition

LET q be a prime power, let m be any integer, let $g(z)$ be any polynomial with coefficients in GF (q^m), let L denote a subset of elements of GF (q^m) that are not roots of $g(z)$, and let $|L|$ be the number of elements in L. (Unless otherwise specified, we will take L to be the set of *all* elements of GF (q^m) that are not roots of $g(z)$.) Then there is a Goppa code with symbol field GF (q), location field GF (q^m), Goppa polynomial $g(z)$, and length $|L|$. Its coordinates are most conveniently indexed by the elements of L. The code is defined as the set of all vectors $\boldsymbol{C}$ that satisfy the condition

$$\sum_{\gamma\in L}\frac{C_\gamma}{z-\gamma}\equiv 0 \bmod g(z). \tag{1}$$

If one expands the left-hand side of this congruence in powers of z mod $g(z)$, and then equates coefficients to zero, one obtains a set of deg g linear equations in the components C_γ of $\boldsymbol{C}$, which may be viewed as parity-check equations. This immediately yields the following theorem.

Theorem 1: Goppa codes are linear. The redundancy of the code with Goppa polynomial $g(z)$ is at most deg g.

II. Algebraic Decoding

If the error vector $\boldsymbol{E}$ is added to the transmitted codeword $\boldsymbol{C}$, then the received word $\boldsymbol{R}$ is given by

$$\boldsymbol{R}=\boldsymbol{C}+\boldsymbol{E}$$

whence

$$\sum_{\gamma\in L}\frac{R_\gamma}{z-\gamma}=\sum_{\gamma\in L}\frac{C_\gamma}{z-\gamma}+\sum_{\gamma\in L}\frac{E_\gamma}{z-\gamma}.$$

Since $\boldsymbol{C}$ is a codeword, the first sum on the right-hand side vanishes mod $g(z)$, and we have

$$\sum_{\gamma\in L}\frac{R_\gamma}{z-\gamma}\equiv\sum_{\gamma\in L}\frac{E_\gamma}{z-\gamma}\bmod g(z).$$

It is therefore natural to define the *syndrome polynomial* $S(z)$ as the polynomial of degree less than deg $g(z)$ such that

$$S(z)\equiv\sum_{\gamma\in L}\frac{R_\gamma}{z-\gamma}\bmod g(z).$$

We have just shown that

$$S(z)\equiv\sum_{\gamma\in L}\frac{E_\gamma}{z-\gamma}\bmod g(z).$$

Let M be the subset of L such that $E_\gamma\neq 0$ iff $\gamma\in M$. Then

$$S(z)\equiv\sum_{\gamma\in M}\frac{E_\gamma}{z-\gamma}\bmod g(z). \tag{2}$$

As usual in algebraic coding theory, we now introduce the polynomial whose roots are the locations of the errors,

$$\sigma(z)=\prod_{\gamma\in M}(z-\gamma). \tag{3}$$

(This form of the error-locator polynomial is the reciprocal of the form used throughout [3].) We also now define a variant of the error-evaluator polynomial, which for Goppa codes is most conveniently taken as

$$\eta(z)=\sum_{\gamma\in M}E_\gamma\prod_{\partial\in M-\{\gamma\}}(z-\partial). \tag{4}$$

It is obvious that $\sigma(z)$ and $\eta(z)$ must be relatively prime. Differentiating (3) formally gives

$$\sigma'(z)=\sum_{\gamma\in M}\prod_{\partial\in M-\{\gamma\}}(z-\partial) \tag{5}$$

whence, for each $\gamma\in M$,

$$\eta(\gamma)=E_\gamma\prod_{\partial\in M-\{\gamma\}}(\gamma-\partial)=E_\gamma\sigma'(\gamma)$$

so that $E_\gamma=\eta(\gamma)/\sigma'(\gamma)$. Hence, once we have found the polynomials σ and η, the rest of the decoding is straightforward. The coordinates of the error vector are given as

$$E_\gamma=\begin{cases}0, & \text{if } \sigma(\gamma)\neq 0\\ \dfrac{\eta(\gamma)}{\sigma'(\gamma)}, & \text{if } \sigma(\gamma)=0\end{cases} \tag{6}$$

Manuscript received May 9, 1973.

The author is with the Departments of Mathematics and Electrical Engineering–Computer Science, University of California, Berkeley, Calif. 94720.

[1] Translations of the full papers will soon be available from Consultants Bureau, 227 W. 17 St., New York, N.Y., 10011, at $15 per article.

where $\sigma'(z)$ is the formal derivative of $\sigma(z)$.[2] The crux of the decoding problem is therefore to determine the coefficients of the polynomials σ and η.

To accomplish this, we must relate σ and η to the syndrome as given by (2). Multiplying (2) by (3) gives the desired relation, namely,

$$S(z) \cdot \sigma(z) \equiv \eta(z) \bmod g(z). \tag{7}$$

Following the analogy to [3, eq. (7.23)], I call congruence (7) the *key equation* for decoding Goppa codes. Given $g(z)$ and $S(z)$, the decoder's problem is to find low-degree polynomials $\sigma(z)$ and $\eta(z)$ that satisfy (7).

By reducing each power of z mod $g(z)$ and equating coefficients of $1, z, z^2, \cdots, z^{\deg g - 1}$, it becomes evident that (7) is a system of $\deg g$ linear equations in the unknown coefficients of σ and η. Hence, to prove that the decoder is able to correct all patterns of up to t errors, it is sufficient to show that (7) has no more than one solution with $\deg \sigma$ and $\deg \eta$ sufficiently small, as this uniqueness is obviously equivalent to the corresponding set of linear equations being linearly independent.

We therefore consider the conditions under which there are two different pairs of solutions to (7):

$$S(z)\sigma^{(1)}(z) \equiv \eta^{(1)}(z) \bmod g(z) \tag{8}$$

$$S(z)\sigma^{(2)}(z) \equiv \eta^{(2)}(z) \bmod g(z) \tag{9}$$

where $\sigma^{(1)}(z)$ and $\eta^{(1)}(z)$ are relatively prime, as are $\sigma^{(2)}(z)$ and $\eta^{(2)}(z)$. If $\sigma^{(1)}(z)$ and $g(z)$ had any common factor, then this factor would have to divide $\eta^{(1)}(z)$, contradicting the assumption that $\sigma^{(1)}$ and $\eta^{(1)}$ are relatively prime. Thus we may divide (8) by $\sigma^{(1)}(z)$ to obtain

$$S(z) \equiv \frac{\eta^{(1)}(z)}{\sigma^{(1)}(z)} \bmod g(z)$$

and, similarly, from (8),

$$S(z) \equiv \frac{\eta^{(2)}(z)}{\sigma^{(2)}(z)} \bmod g(z)$$

whence

$$\sigma^{(1)}(z)\eta^{(2)}(z) \equiv \sigma^{(2)}(z)\eta^{(1)}(z) \bmod g(z). \tag{10}$$

If $\deg g = 2t$ and $\deg \sigma^{(1)} \leq t$, $\deg \sigma^{(2)} \leq t$, $\deg \eta^{(2)} < t$, $\deg \eta^{(1)} < t$, then (10) becomes

$$\sigma^{(1)}(z)\eta^{(2)}(z) = \sigma^{(2)}(z)\eta^{(1)}(z). \tag{11}$$

From (11), $\sigma^{(1)}$ divides $\sigma^{(2)}\eta^{(1)}$, and since $\sigma^{(1)}$ and $\eta^{(1)}$ are relatively prime, $\sigma^{(1)}$ must divide $\sigma^{(2)}$. Similarly, $\sigma^{(2)}$ must divide $\sigma^{(1)}$. Since both are monic, it follows that $\sigma^{(1)} = \sigma^{(2)}$, whence $\eta^{(1)} = \eta^{(2)}$. This proves that if $\deg g = 2t$, then (7) has at most one solution with $\deg \eta < \deg \sigma \leq t$, and this implies that the corresponding system of linear equations in the unknown coefficients of σ and η must be nonsingular. We restate this conclusion as a theorem.

Theorem 2: If $\deg g(z) = 2t$, then there is a t-error-correcting algebraic decoding algorithm for the q-ary Goppa code with Goppa polynomial $g(z)$.

To strengthen this result in the binary case, we first observe that since all nonzero $E_\gamma = 1$, (4) and (5) coincide. Hence (10) becomes

$$\sigma^{(1)}(\sigma^{(2)})' \equiv \sigma^{(2)}(\sigma^{(1)})' \bmod g(z). \tag{12}$$

Writing $\hat{\sigma}$ for the even part of σ and $z\sigma'$ for the odd part of σ, (12) becomes

$$(\hat{\sigma}^{(1)} + z\sigma^{(1)'})\sigma^{(2)'} \equiv (\hat{\sigma}^{(2)} + z\sigma^{(2)'})\sigma^{(1)'}$$

$$\hat{\sigma}^{(1)}\sigma^{(2)'} + \hat{\sigma}^{(2)}\sigma^{(1)'} \equiv 0 \bmod g(z). \tag{13}$$

Since every polynomial on the left-hand side of (13) is even, the left-hand side is a perfect square, and (13) implies

$$\hat{\sigma}^{(1)}\sigma^{(2)'} + \hat{\sigma}^{(2)}\sigma^{(1)'} \equiv 0 \bmod \bar{g}(z) \tag{14}$$

where $\bar{g}(z)$ is the multiple of $g(z)$ of least degree such that $\bar{g}$ is a perfect square. (For example, if $g(z)$ is squarefree, then $\bar{g} = g^2$.) Hence, if $\deg \bar{g} = 2t$, $\deg \sigma^{(1)} \leq t$, and $\deg \sigma^{(2)} \leq t$, then (14) implies that

$$\hat{\sigma}^{(1)}(\sigma^{(2)})' = \hat{\sigma}^{(2)}\sigma^{(1)'}$$

from which, by relative primality, $\sigma^{(1)} = \sigma^{(2)}$. We restate this result as a theorem.

Theorem 3: If $\deg g(z) = t$, and if $g(z)$ has no repeated irreducible factors, then there is a t-error-correcting algebraic decoding algorithm for the binary Goppa code with Goppa polynomial $g(z)$.

In the special case in which $g(z)$ is a power of z, (7) reduces to [3, eq. (7.23)]. From this, it can easily be shown that the Goppa code with Goppa polynomial z^{2r} is identical to a primitive BCH code. In this case, the system of linear equations represented by (7) can be solved by the iterative algorithm given in [3, sec. 7.4]. Unfortunately, no method of comparable simplicity is known for solving (7) in the case of more general $g(z)$.

III. The Asymptotic Gilbert Bound

We have just seen that the Goppa codes include the primitive BCH codes as a special case. Of course the class of Goppa codes also includes many classes of non-BCH codes. The Goppa codes for which $g(z)$ is irreducible over GF (q^m) are called *irreducible Goppa codes.* We shall now show that most long irreducible Goppa codes satisfy the Gilbert bound on minimum distance. To this end, we let $g^{(1)}(z), g^{(2)}(z), \cdots, g^{(I)}(z)$ be the distinct irreducible polynomials of degree t over GF (q^m). According to the well-known theorem presented elsewhere [3, theorem 3.43], the number of irreducible q-ary t-tics is

$$I = \frac{1}{t} \sum_{\substack{d_1;\\ d|t}} \mu(d) q^{mt/d} \geq \frac{q^{mt}}{t}(1 - q^{-(mt/2)+1})$$

where $\mu(d)$ is the Moebius function. Now the vector V is in the Goppa code with Goppa polynomial $g^{(j)}(z)$ iff

$$\sum_{\gamma \in \mathrm{GF}(q^m)} \frac{V_\gamma}{z - \gamma} \equiv 0 \bmod g^{(j)}(z).$$

[2] Notice that (6) is an improvement over [3, eq. (10.14)], because by using σ' we are able to determine the value of each error symbol as it is located rather than first finding all error locations and then all error values.

If the Hamming weight of V is d, then

$$\sum_{\gamma \in GF(q^m)} \frac{V_\gamma}{z - \gamma}$$

is a rational function which can be written as the quotient of a numerator of degree $\leq (d - 1)$ and a denominator of degree d. The Goppa polynomial of each Goppa code containing V must divide the numerator. Since all irreducible q-ary t-tics are pairwise relatively prime, it follows that the number of irreducible Goppa codes containing V is at most $\lfloor (d - 1)/t \rfloor$. We now overbound the number of Goppa codes which contain words of weight $\leq D$ by summing over all $\binom{q^m}{d}(q - 1)^d$ vectors of weight $d \leq D$ and bounding the number of Goppa codes containing each. If

$$\sum_{d=0}^{D} \left\lfloor \frac{d - 1}{t} \right\rfloor (q - 1)^d \binom{q^m}{d} < \frac{q^{mt}}{t} (1 - q^{-(mt/2)+1}) \quad (15)$$

then the number of "bad" irreducible Goppa codes is less than the total number of irreducible Goppa codes, so there must be some remaining irreducible Goppa codes which have minimum distance $\geq D$. For large $n = q^m$, the irreducible Goppa codes have rate $\geq R$ if we set $t = [(1 - R)q^m]/m$, and inequality (15) is easily seen to be only negligibly weaker asymptotically than the classical Gilbert criterion for the existence of codes with distance D; this criterion is

$$\sum_{d=0}^{D} (q - 1)^d \binom{n}{d} < q^{(1-R)n}.$$

We state the conclusion as Theorem 4.

Theorem 4: If R is any given rate, $0 < R < (q - 1)/q$, and if ε is any small positive constant, then almost all irreducible q-ary Goppa codes of rate R and long length n have minimum distance no more than εn less than the Gilbert bound.

IV. Concluding Remarks

A number of equivalent reformulations of Goppa codes are given in [1, sec. 3] and [2, secs. 2, 3]. In [2, sec. 4] a more detailed proof of the fact that primitive BCH codes are a special class of Goppa codes is presented. In [2, sec. 5] there is a survey of a number of other types of codes, including Srivastava codes and Gabidulin codes, which are also easily seen to be weak special cases of Goppa codes.

A detailed example of the (16,8,5) binary Goppa code is presented in [1, sec. 6]. In [1, sec. 7] Goppa proves that, under certain quite restrictive hypotheses, the BCH codes are the only cyclic Goppa codes. Later, Berlekamp and Moreno [4] showed that all double-error-correcting binary Goppa codes become cyclic when extended by an overall parity check. In particular, the (16,8,5) binary Goppa code may be obtained by shortening the binary quadratic residue code of length 17. We are still investigating the possibility of close relationships between other special classes of Goppa codes and cyclic codes.

In a subsequent paper [5], Goppa introduced several new classes of codes based on the codes described here. The new classes have the following parameters: 1) q-ary codes with $n = q^m m$, $k = n - 2mt$, $d \geq 2t + 1$; 2) q-ary codes with $n = q^m - 2t + m(2t - 1) + 1$, $k = q^m - 2t$, $d \geq 2t + 1$; and 3) binary codes with $n = 2^m + mt$, $k = 2^m - t$, $d \geq 2t + 1$. This new class of binary codes includes an infinite number of codes which are better than any known Goppa code of the type discussed here, although at any fixed rate the lower bound on the distance of these new codes is asymptotically weaker than that for comparable BCH codes.

References

[1] V. D. Goppa, "A new class of linear error-correcting codes," *Probl. Peredach. Inform.*, vol. 6, no. 3, pp. 24–30, Sept. 1970.

[2] ——, "Rational representation of codes and (L,g) codes," *Probl. Peredach. Inform.*, vol. 7, no. 3, pp. 41–49, Sept. 1971.

[3] E. R. Berlekamp, *Algebraic Coding Theory.* New York: McGraw-Hill, 1968.

[4] E. R. Berlekamp and O. Moreno, "Extended double-error-correcting binary Goppa codes are cyclic," *IEEE Trans. Inform. Theory*, vol. IT-19, Nov. 1973 to be published.

[5] V. D. Goppa, "Some codes constructed on the basis of (L,g) codes," *Probl. Peredach. Inform.*, vol. 8, no. 2, pp. 107–109, June 1972.