On the Complexity of Decoding Goppa Codes

DILIP V. SARWATE, MEMBER, IEEE

***Abstract*—It is shown that i) erasures-and-errors decoding of Goppa codes can be done using $O(n \log^2 n)$ arithmetic operations, ii) long primitive binary Bose–Chaudhuri–Hocquenghem (BCH) codes can be decoded using $O(n \log n)$ arithmetic operations, and iii) Justesen's asymptotically good codes can be decoded using $O(n^2)$ bit operations. These results are based on the application of efficient computational techniques to the decoding algorithms recently discovered by Sugiyama, Kasahara, Hirasawa, and Namekawa.**

I. INTRODUCTION

Sugiyama, Kasahara, Hirasawa, and Namekawa [1]–[3] have shown that, for a t-error-correcting Goppa code [4]–[6], the key equation for errors-only decoding as well as for erasures-and-errors decoding can be solved by use of the extended version of Euclid's algorithm for the greatest common divisor (gcd) of two polynomials. This algorithm requires $O(t^2)$ arithmetic operations, as does Berlekamp's algorithm for Bose–Chaudhuri–Hocquenghem (BCH) codes [7] which also can be applied to decoding Goppa codes [8], [9]. Justesen [10] and the author [11] have independently discovered that if fast computational techniques for polynomial gcd's [12], [13] are used, then the key equation for errors-only decoding can be solved using only $O(t \log^2 t)$ arithmetic operations. In this correspondence, this result is extended to the key equation for erasures-and-errors decoding. Some other computations necessary in this case are also shown to require at most $O(t \log^2 t)$ or $O(n \log n)$ arithmetic operations. Computation of the syndrome, the error locations and error (or erasure) values all require $O(n \log n)$ arithmetic operations [10], [11]. It follows that for a fixed ratio of t/n, erasures-and-errors decoding of a Goppa code requires $O(n \log^2 n)$ arithmetic operations and is of the same order of complexity as errors-only decoding. Using Berlekamp's estimates [14] of the minimum distance of long primitive binary BCH codes, it is shown that these codes can be decoded using $O(n \log n)$ arithmetic operations. The asymptotically good codes of Justesen [15] use erasures-and-errors decoding of Reed–Solomon codes in the outer decoder. When the efficient decoding algorithm proposed here is used, the number of bit operations required by the outer decoder is reduced from $O(n^2 \log n)$ to $O(n \log^4 n)$, and the decoding of Justesen codes requires $O(n^2)$ bit operations which is the same as the order of complexity of the inner decoder.

II. COMPLEXITY OF THE DECODING ALGORITHM

Following the notation in [6], let $g(z)$ be a polynomial of degree $2t$ with coefficients in $GF(q^m)$, L the subset of elements of $GF(q^m)$ that are not roots of $g(z)$, and n the number of elements in L. Then the Goppa code of length n, symbol field $GF(q)$, location field $GF(q^m)$, and Goppa polynomial $g(z)$ is the set of all vectors $\boldsymbol{c}$ that satisfy

$$YZ\boldsymbol{c}^T = \boldsymbol{0}, \tag{1}$$

where Y is a $2t \times n$ Vandermonde matrix and Z is a $n \times n$ diagonal matrix [4]. Let M denote the set of error locations and N the set of erasure locations. The error-and-erasure locator polynomials $\sigma_e(z)$ and $\sigma_\epsilon(z)$ are as defined in [2]; for the error-and-erasure-evaluator polynomials, a slightly different definition is used, namely,

$$\eta_e(z) = -\sum_{\gamma \in M} e_\gamma \cdot \frac{\gamma^{2t}}{g(\gamma)} \prod_{\delta \in M-\{\gamma\}} (z-\delta) \tag{2}$$

$$\eta_\epsilon(z) = -\sum_{\gamma \in N} e_\gamma \cdot \frac{\gamma^{2t}}{g(\gamma)} \prod_{\delta \in N-\{\gamma\}} (z-\delta), \tag{3}$$

where the e_γ in (3) are erasure values, i.e., the difference between the arbitrary value assigned by the decoder to the symbol in the erasure location and the transmitted symbol c_γ.

Let $\boldsymbol{S} = [S_{2t-1}, S_{2t-2}, \cdots, S_1, S_0]$ be the syndrome vector defined by $\boldsymbol{S}^T = YZ\boldsymbol{r}^T$, where $\boldsymbol{r}$ is the received vector, and let $S(z) = \Sigma_{i=0}^{2t-1} S_i z^i$ be the corresponding syndrome polynomial. The key equation then becomes

$$S(z) \equiv \frac{\eta_e(z)}{\sigma_e(z)} + \frac{\eta_\epsilon(z)}{\sigma_\epsilon(z)} \bmod z^{2t}, \tag{4}$$

where the decoder knows both $S(z)$ and $\sigma_\epsilon(z)$.

The definition of $\eta_e(z)$ and $\eta_\epsilon(z)$ in (2), (3), and the corresponding key equation, (4), has been used by MacWilliams and Sloane [16] who attribute it to Helgert [17]. However, the idea is implicit in [8]. While the definitions of $\eta_e(z)$ and $\eta_\epsilon(z)$ are not exactly those of [2], it is easy to verify that all results of [2] are equally applicable to (2)–(4). In particular, the errata-evaluator polynomial $\eta(z)$ can be defined as in [2], and we get the equation

$$\sigma_e(z)\sigma_\epsilon(z)S(z) \equiv \eta(z) \bmod z^{2t}. \tag{5}$$

The modified syndrome polynomial $S_\epsilon(z)$ of degree $2t-1$ or less is defined as

$$S_\epsilon(z) \equiv \sigma_\epsilon(z)S(z) \bmod z^{2t},$$

and the key equation can be rewritten as

$$\sigma_e(z)S_\epsilon(z) \equiv \eta(z) \bmod z^{2t}. \tag{6}$$

Let $\deg \sigma_e = n_e$ and $\deg \sigma_\epsilon = n_\epsilon$ with $1 \leq 2n_e + n_\epsilon < 2t+1$. In [2] and [3], it is shown that $\deg \sigma_e \leq t - \frac{1}{2}n_\epsilon$ and $\deg \eta < t + \frac{1}{2}n_\epsilon$ and the following solution of (6) is proposed.

Algorithm: Case 1) If $n_\epsilon = 0$, i.e., if no erasures occurred, the decoder can follow the errors-only decoding procedure [1].

Case 2) $\deg S_\epsilon < n_\epsilon$ if and only if $n_e = 0$, and the solution in this case is $\sigma_e(z) = 1, \eta_e(z) = 0$, $\eta(z) = \eta_\epsilon(z) = S_\epsilon(z)$.

Case 3) Otherwise, set $r_{-1}(z) = z^{2t}$ and $r_0(z) = S_\epsilon(z)$, and let the remainder sequence $r_i(z)$ be as defined in [1] and [2]. Let k be the unique integer such that $\deg r_{k-1} \geq t + \frac{1}{2}n_\epsilon$ and $\deg r_k < t + \frac{1}{2}n_\epsilon$. Then,

$$\eta(z) = (-1)^k \delta r_k(z)$$

$$\sigma_e(z) = \delta U_k(z),$$

where δ is a nonzero constant chosen to make $\delta U_k(z)$ monic.

In applying fast computational techniques, note that Case 1 has been dealt with in [10], [11] where it is shown that $O(t \log^2 t)$ arithmetic operations are sufficient if Algorithm HGCD ([13, procedure 8.7]) is used. In Case 2, only polynomial multiplication is necessary and hence only $O(t \log t)$ arithmetic operations are required [13]. However, HGCD cannot be applied to Case 3 directly. In order to solve the key equation, one can begin with (5) rather than (6) since any solution of one is a solution of the other. Furthermore, if $2n_e + n_\epsilon < 2t+1$, the solution of (6) is unique [2, theorem 1], and hence it suffices to solve (5) for a pair of relatively prime polynomials $\sigma_e(z)$ and $\eta(z)$ of degrees at most $t - \frac{1}{2}n_\epsilon$ and less than $t + \frac{1}{2}n_\epsilon$, respectively.

Lemma 1: If at least one erasure has occurred, then the erasure value(s) can be chosen so that $\deg S = 2t - 1$.

Manuscript received August 1, 1975; revised August 24, 1976. This work was supported in part by the National Science Foundation under Grant ENG 70-01408, and in part by the Joint Services Electronics Program (U. S. Army, U. S. Navy, and U. S. Air Force) under Contract DAAB-07-72-C-0259.

The author is with the Coordinated Science Laboratory and the Department of Electrical Engineering, University of Illinois at Urbana-Champaign, Urbana, IL 61801.

Proof:

$$S_{2t-1} = \sum_{\gamma \in L} \frac{r_\gamma}{g(\gamma)}.$$

If S_{2t-1} is zero, one of the erasure values (which are arbitrarily assigned) can be changed (to $r_\gamma + 1$, for example). For this modified received vector, $S_{2t-1} \neq 0$ and $\deg S = 2t - 1$. Note that this checking and forcing of S_{2t-1} to be nonzero takes $O(n)$ arithmetic operations and can be done before the rest of the syndrome is computed.

After forcing the degree of $S(z)$ to be $2t - 1$, one sets $r_{-1}(z) = \sigma_\epsilon(z)S(z)$, $r_0(z) = z^{2t}$ and invokes Algorithm HGCD. This is a recursive procedure that computes the polynomials r_{j-1}, r_j, V_{j-1}, V_j, U_{j-1}, and U_j, where j is the unique integer such that $\deg r_{j-1} > \frac{1}{2} \deg r_{-1}$ and $\deg r_j \leq \frac{1}{2} \deg r_{-1} = \frac{1}{2}(2t - 1 + n_\epsilon) < t + \frac{1}{2}n_\epsilon$. Thus, r_j and U_j are exactly the polynomials r_k and U_k of Case 3, and the additional iteration of Euclid's algorithm, which is sometimes necessary in errors-only decoding [10], [11] is not required here. Theorem 1 below has thus been proved.

Theorem 1: The key equation for erasures-and-errors decoding of a t-error-correcting Goppa code can be solved using $O(t \log^2 t)$ arithmetic operations.

As discussed in [10] and [11], the computation of syndromes, error locations and error values all require $O(n \log n)$ arithmetic operations. Determining erasure values is no different from determining error values and also requires $O(n \log n)$ arithmetic operations. However, in erasures-and-errors decoding, there is also the following problem. The demodulator output may be either a symbol from $GF(q)$ or a special symbol denoting an erasure, for which the decoder substitutes some symbol from $GF(q)$. The decoder thus knows the erasure-locations i.e., the set N. However, the computations required of the decoder make use of $\sigma_\epsilon(z)$ and hence the decoder must first find $\sigma_\epsilon(z)$ from the set N.

Lemma 2: Given the set of erasure-locations N, the erasure-locator polynomial $\sigma_\epsilon(z)$ can be determined by procedures requiring $O(n \log n)$ and $O(t \log^2 t)$ arithmetic operations.

Proof: $n_\epsilon = |N| \leq 2t$. Consider the Goppa code of length n and minimum distance at least $4t + 1$ that has the Goppa polynomial $g^2(z)$. Suppose that the all-zeroes codeword was transmitted and that the vector $\mathbf{v}$ was received where $v_\gamma = 1$, if $\gamma \in N$ and zero otherwise. Using an errors-only decoding algorithm for this code, one can find the syndrome using $O(n \log n)$ arithmetic operations and the error-locator polynomial using $O(t \log^2 t)$ arithmetic operations. This error-locator must be $\Pi_{\gamma \in N}(z - \gamma)$, since this Goppa code has minimum distance at least $4t + 1$ and at most $2t$ errors occurred. Hence $\sigma_\epsilon(z)$ can be computed by procedures requiring $O(n \log n)$ and $O(t \log^2 t)$ arithmetic operations. Q.E.D.

The above results can be summarized as follows.

Theorem 2: For a fixed ratio of t/n, erasures-and-errors decoding of a Goppa code requires $O(n \log^2 n)$ arithmetic operations.

This result includes the results of Justesen [10] and the author [11] on errors-only decoding of Reed–Solomon and Goppa codes as special cases. We also have the following.

Corollary 1: Erasures-and-errors decoding of a long primitive binary BCH code of block length n can be done using $O(n \log n)$ arithmetic operations.

Proof: It is well-known that the BCH codes are a subclass of the Goppa codes. Berlekamp [14] has proved that for long primitive binary BCH codes of rate R and block length n, the design distance is approximately $2n \ln R^{-1}/\log_2 n$, i.e., t is $O(n/\log n)$. Hence, the solution of the key equation requires

$$\begin{aligned} O(t \log^2 t) &= O(n \log^2 (n/\log n)/\log n) \\ &= O(n (\log n - \log \log n)^2/\log n) \\ &= O(n \log n) \end{aligned}$$

arithmetic operations. All other computations necessary are also of the same order of complexity. Q.E.D.

Corollary 2: (MacWilliams–Sloane [16]). An alternant code of block length n can be decoded using $O(n \log^2 n)$ arithmetic operations.

This result is of interest since the alternant codes include the Goppa, the BCH, the Reed–Solomon, the generalized Srivastava and the Chien–Choy codes as subclasses. (See [16] for details.)

Corollary 3: Erasures-and-errors decoding of a Reed–Solomon code of block length n requires $O(n \log^2 n)$ arithmetic operations.

In [15], Justesen describes his well-known asymptotically good codes. For these, the inner decoder uses $O(n^2/\log^2 n)$ arithmetic operations while the outer decoder uses $O(n^2/\log n)$ arithmetic operations, or, equivalently, $O(n^2)$ and $O(n^2 \log n)$ bit operations, respectively. The outer decoder uses an erasures-and-errors decoding algorithm for Reed–Solomon codes. If the algorithm described in this correspondence is used, the outer decoder requires $O(n \log^2 n)$ arithmetic operations or, equivalently, $O(n \log^4 n)$ bit operations. Thus the complexity of the decoder for Justesen codes is dominated by the complexity of the inner, rather than the outer, decoder. Thus the following result has been proved.

Corollary 4: A Justesen code of block length n can be decoded in $O(n^2)$ bit operations.

Acknowledgment

It is a pleasure to acknowledge several very helpful conversations with S. J. Hong and F. P. Preparata. I am also grateful to the referees for their suggestions and comments.

References

[1] Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa, "A method for solving key equation for decoding Goppa codes," *Inform. Contr.*, vol. 27, pp. 87–99, Jan. 1975.

[2] ——, "An erasures-and-errors decoding algorithm for Goppa codes," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 238–241, Mar. 1976.

[3] ——, "Corrections to 'An erasures-and-errors decoding algorithm for Goppa Codes'," *IEEE Trans. Information Theory*, vol. IT-22, pp. 765, Nov. 1976.

[4] V. D. Goppa, "A new class of linear error-correcting codes," *Probl. Peredach. Inform.*, vol. 6, pp. 24–30, Jul.–Sept. 1970.

[5] ——, "A rational representation of codes and (L,g) codes," *Probl. Peredach. Inform.*, vol. 7, pp. 41–49, Jul.–Sept. 1971.

[6] E. R. Berlekamp, "Goppa codes," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 590–592, Sept. 1973.

[7] ——, *Algebraic Coding Theory.* New York: McGraw-Hill, 1968.

[8] C. T. Retter, "Decoding Goppa codes with a BCH decoder," *IEEE Trans. Inform. Theory*, vol. IT-21, p. 112, Jan. 1975.

[9] N. J. Patterson, "The algebraic decoding of Goppa codes," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 203–208, Mar. 1975.

[10] J. Justesen, "On the complexity of decoding Reed–Solomon codes," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 237–238, Mar. 1976.

[11] D. V. Sarwate, "On the complexity of decoders for Goppa codes," Coordinated Science Laboratory Technical Report R-719, University of Illinois, Urbana, IL, 1976.

[12] R. Moenck, "Fast computation of GCD's," in *Proceedings of the Fifth Annual ACM Symposium on the Theory of Computing*, pp. 142–151, 1973.

[13] A. V. Aho, J. E. Hopcroft, and J. D. Ullman, *The Design and Analysis of Computer Algorithms.* Reading, MA: Addison-Wesley, 1974.

[14] E. R. Berlekamp, "Long primitive binary BCH codes have distance $d \sim 2n \ln R^{-1}/\log n$," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 415–426, May 1972.

[15] J. Justesen, "A class of constructive asymptotically good algebraic codes," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 652–656, Sept. 1972.

[16] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* Amsterdam: North-Holland, (to be published).

[17] H. J. Helgert, "Alternant Codes," presented at the Information Theory Workshop, Lenox, MA, June 1975.

Some Results Related to Generalized Varshamov–Gilbert Bounds

MIKHAIL DEZA AND FREDERICK HOFFMAN

***Abstract*—Two generalizations of the Varshamov–Gilbert bound for error-correcting and error-detecting codes are developed. Sufficient intrinsic conditions are given for classes of linear codes over $GF(q)$ to include "good" codes, and these classes are related to other known classes. A lower bound on the maximal order of subspaces contained in subsets of certain finite vector spaces is given and related to a bound on error-detecting codes.**

I. Introduction

We shall discuss two concepts in this correspondence. First, we wish to consider the problem of constructing codes which correct arbitrary, but fixed, types of noise (as opposed to correcting all error patterns up to a certain weight). We prove a result analogous to the Varshamov–Gilbert bound on the size of a linear code needed for a given noise; in our case the code is selected from a *segment of self-inverse sets* or a *segment of subspaces.* These are technically defined sets of "candidates for codes" which are large enough to enable us to establish the results and small enough to be of some value. It would, of course, be desirable to find smaller sets for which the bound may be attained. The results given here include a set of sufficient conditions for a class of linear codes to contain "good" codes. Second, we prove a result on maximal subspaces contained in subsets of finite vector spaces, and employ this result to establish a bound on the size of codes to *detect* arbitrary noise, when the codes are selected from segments of subspaces.

II. Segments of Sets Correcting Noise

The problem of construction of maximal codes for correction of an arbitrary set of additive errors was posed in [4] and [5]. We let V be a vector space of dimension n over $GF(q)$, and let the set $B, 0 \in B \subset V$, be called noise. For a subset A of V, we let $A - A = \{a_1 - a_2 | a_1, a_2 \in A\}$ and $-A = \{-a | a \in A\}$. Following [4], we say that A is a *code correcting the noise* B provided that, for all $a_1, a_2 \in A$ and $b_1, b_2 \in B$, if $a_1 \neq a_2$ then $a_1 + b_1 \neq a_2 + b_2$. This condition is clearly equivalent to $(A - A) \cap (B - B) = \{0\}$. If A is a subspace (in fact if A is only a subgroup of V), this condition is equivalent to $A \cap (B - B) = \{0\}$.

Let τ be a family of subsets of V. We shall say that τ *corrects the noise* B if some element of τ corrects B. In this case, we let $C^\tau(B)$ be an element of τ of maximal cardinality which corrects B. We shall call a family τ a *segment of groups* (or *of subspaces*) if

1) every element of τ is a subgroup (subspace) of V, and
2) every subgroup (subspace) of V containing an element of τ as a subset is itself in τ.

A segment of τ is a *segment of self-inverse sets* if

1) every $A \in \tau$ satisfies $A = -A$, and
2) if $A \subset V$ satisfies $A = -A$ and A contains an element of τ as a subset, then $A \in \tau$.

Thus every segment of groups is a segment of self-inverse sets.

In [4], it is shown that $q^n/|B - B| \leq |C^\tau(B)| \leq q^n/|B|$, where q is prime and τ is the family of all subsets of V. It is clear that these estimates are generalizations of the estimates of Gilbert and of Hamming–Rao, respectively (cf. [1]). (We note that $\log_q |C^\tau(B)|$ is a generalization of the number k of information symbols.)

In [6] Goppa has shown (in other notation) that $|C^\tau(B)| \geq q^n/|B - B|$ as $n \rightarrow \infty$, if τ is the family of all irreducible Goppa codes. (The Goppa codes are described in [6] and [7] as well as in [2] and [3]). Since these codes are subgroups of V, the results of [6] generalize the theorem of Varshamov–Gilbert which establishes a bound for the class of all group-codes correcting an arbitrary additive noise. Similar results for other classes of codes appear in [9] and [10]. We shall prove an analogous result for the segments defined here. The proof is a modification of the proof of the Varshamov–Gilbert bound given in [1].

Theorem: a) If τ is a segment of self-inverse sets correcting the noise B, then $|C^\tau(B)| \geq q^n/|B - B|$.

b) If q is odd, and if τ is a segment of subspaces correcting the noise B, then $|C^\tau(B)| \geq 2q^n/(2 + (q - 1)(|B - B| - 1))$. In particular, if q is prime, this result applies when τ is a segment of groups.

Proof: a) Let $C^\tau(B) = A$. Suppose the statement of a) is false. Then, since $|A||B - B| < q^n$, $|A + (B - B)\backslash\{0\}| < q^n - 1$, so that there is a nonzero element v of V which does not belong to $A + (B - B)$. Further, $-v$ is also such an element; since, if $-v = a_1 + b_1 - b_2$ $(a_1 \in A, b_1, b_2 \in B)$, then $v = -a_1 + b_2 - b$ and $v \in A + (B - B)$, a contradiction. The set $A' = A \cup \{v, -v\}$ is in τ, since $A' = -A'$ and $A \subset A'$. Since $A' - A' = (A - A) \cup (\{v, -v\} - A)$, and since $(\{v, -v\} - A) \cap (B - B) = \emptyset$, by the choice of v, A' corrects B. But $|A'| > |A| = |C^\tau(B)|$, a contradiction. Thus a) must be true.

b) Now suppose the statement of b) is false. Then, for some segment of subspaces τ with $C^\tau(B) = A$, we have

$$|A| < 2q^n/(2 + (q - 1)(|B - B| - 1))$$

so that

$$|A|[1/(q - 1) + (|B - B| - 1)/2] < q^n/q - 1,$$

and

$$(|A| - 1)/(q - 1) + |A|(|B - B| - 1)/2 < q^n - 1/q - 1.$$

We now consider the distinct one-dimensional subspaces of V. There are precisely $q^n - 1/q - 1$ in all, and $|A|(|B - B| - 1)/2$ such subspaces intersect $A + ((B - B)\backslash\{0\})$ nontrivially since, for any $v \in A + (B - B)$, $-v \in A + (B - B)$ and $-v = v$ only for $v = 0$ (since q is odd). (We know that $0 \notin A + ((B - B)\backslash\{0\})$, since $A \cap (B - B) = \{0\}$). There must then, be a one-dimensional subspace W with $W \cap (A + (B - B)) = \{0\}$. Thus $(A + W) \cap (B - B) = \{0\}$. The subspace $A + W$ corrects the noise B and $A + W \in \tau$. Since $|A + W| > |A|$, we have a contradiction to the maximality of $|A|$, and we have proved the assertion of b).

III. The Maximal Subspace Contained in a Subset of a Finite Vector Space

We now prove a result on the size of a maximal subspace contained in a subspace of a finite vector space, which we shall apply in Section III to the problem of detecting noise. We point out that when the ground field is of prime order, the theorem can be restated for elementary Abelian groups.

Let V be a vector space of dimension n over $GF(q)$. For any positive integer b, $1 \leq b \leq q^n$, let $\mu(b)$ be the least integer m with $b \leq q^m$.

Theorem: Let A be a subset of V containing a subspace of dimension one. Then the set A contains a subspace of dimension

Manuscript received December 29, 1975.

M. Deza was with the Department of Combinatorics and Optimization, University of Waterloo, Waterloo, ON, Canada. He is now with the Department of Mathematics, University of Paris, Paris, France.

F. Hoffman was with the Department of Combinatorics and Optimization, University of Waterloo, Waterloo, ON, Canada. He is now with the Department of Mathematics, Florida Atlantic University, Boca Raton, FL 33431.

$m \geq \mu(|V|/(q-1)((|V|-|A|)+1))$. There is a set $A^* \subset V$ with $|A^*| = |A|$ and with no subspace of dimension larger than $\mu(|V|/(q-1)((|V|-|A|)+1))$.

Proof: Let W be a subspace of V of maximal dimension contained in A. Let $W = \{w_1, w_2, \cdots, w_t\}$, where $t = q^m$ and where we let $w_1 = 0$. We define a sequence $\{S_j\}$ of subsets of A as follows. $S_0 = V$; for $j = 1, \cdots, t$, we define S_j inductively by $S_j = \{s | s \in S_{j-1}$ and $w_j + \alpha s \in A$, all $\alpha \in GF(q)\}$. Clearly $W \subseteq S_t \subseteq \cdots \subseteq S_1 \subseteq A \subseteq S_0 = V$. It is also clear that for $j = 1, \cdots, t$ and for every $s \in S_{j-1} \backslash S_j$, there is $\alpha \in GF(q)$ with $g_j + \alpha s \in V \backslash A$. Thus $|S_{j-1}| - |S_j| \leq (q-1)(|V| - |A|)$, $|S_j| \geq |S_{j-1}| - (q-1)(|V| - |A|)$, $|S_j| \geq |S_0| - j(q-1)(|V| - |A|)$, so that, in particular, $|S_t| \geq |V| - t(q-1)(|V| - |A|)$. Thus $|S_t \backslash W| = |S_t| - t \geq |V| - t(q-1)$. $(|V| - |A|) - t > 0$, if and only if $t < |V|/(q-1)(|V| - |A|) + 1$. But, if $S_t \backslash W \neq \emptyset$, the subspace generated by $S_t \cup \{s\}$, for any $s \in S_t \backslash W$, is contained in A and is of dimension greater than that of W, contradicting the maximality of W. Thus $S_t \backslash W = \emptyset$ so that

$$t \geq |V|/(q-1)((|V| - |A|) + 1),$$

so that

$$m \geq \mu(|V|/(q-1)((|V| - |A|) + 1)),$$

as was asserted in the first part of the theorem.

We now let $|A|$ be fixed and let W^* be a fixed subspace of V of dimension $n - \mu(|V|/(q-1)((|V| - |A|) + 1))$. We shall form a set A^* of cardinality $|A|$ by deleting $|V| - |W^*| + 1 - |A|$ elements from $(V \backslash W^*) \cup \{0\}$. First, we must pick a subspace W of V of dimension $\mu(|V|/(q-1)((|V| - |A|) + 1))$ with $W + W^* = V$ and $W \cap W^* = \{0\}$. Since $|A| \geq |W|$ (as can be seen from the first part of the proof), we may retain the elements of W in A^*. The set A^* cannot contain a subspace of dimension larger than dim W, so the theorem is proved.

Corollary: Let G be an elementary Abelian group of order p^n, p prime. Let A be a subset of V containing a nontrivial subgroup of G. Then the set A contains a subgroup of order at least $p^n/(p-1)((p^n - |A|) + 1)$.

Proof: This is simply a restatement of the theorem for the case where q is a prime.

IV. Segments Detecting Noise

We now turn to the problem of codes detecting noise, and obtain bounds of a type similar to those of Varshamov–Gilbert.

We say that the set $A \subset V$ is a code *detecting the noise* B if, for all $a_1, a_2 \in A$ and $b \in B$, if $a_1 \neq a_2$ then $a_1 + b \neq a_2$. Clearly, this is equivalent to the condition that $(A - A) \cap B = \{0\}$. If A is a group, then the condition becomes $A \cap B = \{0\}$. If a family τ contains a nontrivial code detecting the noise B, then $D^\tau(B)$ will denote one such code which has maximal cardinality. In [4], it is shown that

$$q^n/|B \cup (-B)| \leq |D^\tau(B)| \leq q^n - |B| + 1,$$

if τ is the family of all subsets of V.

We shall say that a family τ of subspaces of V is of *Varshamov–Gilbert type* if, for every noise B ($0 \in B \subset V$) which is detected by τ, we have $|D^\tau(B)| \geq q^n/K_\tau|B|$, where K_τ is a constant. This condition is somewhat stronger than the condition $|C^\tau(B)| \geq q^n/K_\tau|B - B|$ discussed earlier, since there are subsets B with $0 \in B \subset V$ but for which no B' exists with $0 \in B' \subset V$ and $|B'| = |B' - B'|$.

Theorem: Let τ be a segment of subspaces of V; then τ is of Varshamov–Gilbert type.

Proof: If B is a noise detected by τ with $0 \in B \subset V$, then if $A = (V \backslash B) \cup \{0\}$ there is a nontrivial element U of τ contained in A. We can then apply the theorem of Section III to obtain the result, since any subspace of V contained in A will detect B. It should be pointed out that, in the proof of the theorem of Section III, W may be chosen to contain U so that W will be an element of τ in virtue of τ being a segment of subspaces of V.

We also point out a partial converse to the last theorem. Let M be an arbitrary subset of V with $0 \in M$. If M contains an element of τ as a subset, we shall designate by $G^\tau(M)$ such an element of τ of largest cardinality.

Proposition 1: Let M be a subset of V, $0 \in M$. If τ is a family of Varshamov–Gilbert type which detects the set $(V \backslash M) \cup \{0\}$, then

$$|G^\tau(M)| \geq q^n/K_\tau(q^n - |M| + 1).$$

Proof: This is clear, since $G^\tau(M) = D^\tau((V^n \backslash M) \cup \{0\})$.

Now, let us briefly consider the question, for fixed positive m, of the orders of maximal linear codes in V $(GF(q))$ correcting m-element noise. For a family τ of codes correcting at least one m-element noise, let $D^\tau(m) = \max_{|B|=m} |D^\tau(B)|$, the maximum taken over all m-element noise B detected by τ. $D(m)$ is $D^\tau(m)$ where τ is the family of all subspaces of V.

Proposition 2: $D(m)$ is the greatest power of q not exceeding $q^n - m + 1$.

Proof: This follows easily from the theorem of Section III.

References

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

[2] ——, "Goppa codes," *IEEE Trans. Inform. Theory,* vol. IT-19, pp. 590–592, Sept. 1973.

[3] I. F. Blake and R. C. Mullin, *The Mathematical Theory of Coding.* New York: Academic Press, 1975.

[4] M. Deza, "Correction of arbitrary and worst noise," *Problemy Peredatchi Informatsii,* vol. 4, pp. 26–31, 1968.

[5] ——, "Comparison of arbitrary additive noise relative to the effectiveness of detection or correction," *Problemy Peredatchi Informatsii,* vol. 1, pp. 29–38, 1965.

[6] V. D. Goppa, "A new class of linear correcting codes," *Problemy Peredatchi Informatsii,* vol. 6, pp. 24–30, Sept. 1970.

[7] ——, "Rational presentation of codes and (L,g) codes," *Problemy Peredatchi Informatsii,* vol. 7, pp. 41–49, Sept. 1971.

[8] ——, "On correcting arbitrary noise with irreducible codes," *Problemy Peredatchi Informatsii,* vol. 10, pp. 111–112, Sept. 1974.

[9] J. Justesen, "A class of constructive asymptotically good algebraic codes," *IEEE Trans. Inform. Theory,* vol. IT-18, pp. 652–656, Sept. 1972.

10] F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, "Good self-dual codes exist," *Discrete Math.,* vol. 3, pp. 153–162, 1972.

Odd Weight Symmetry in Some Binary Codes

VIJAY K. BHARGAVA

***Abstract*—If a linear binary code of length *n* contains the all-one codeword, than the weights of the code are symmetric. We consider those codes which do not contain the all-one codeword and yet have an equal number of symmetrically placed odd weight words.**

Manuscript received July 19, 1975; revised March 31, 1976. Some of this work was done while the author was with the Department of Electrical Engineering, Queen's University, Kingston, ON, Canada and was supported in part by NRC grant A-7787. An earlier version of this article was written while the author was with the Centre for Information Processing, Indian Institute of Science, Bangalore, India.

The author is with the Department of Electrical Engineering, Concordia University, Montreal, PQ, Canada.