INFORMATION AND CONTROL 43, 195–197 (1979)

On Vote-Taking and Complete Decoding of Certain Error-Correcting Codes

DAVID M. MANDELBAUM

P.O. Box 645, Eatontown, New Jersey 07724

It is shown how complete decoding of maximum distance separable codes can be accomplished by a vote-taking algorithm or an equivalent distance correlation method. It is also indicated where this method of decoding might find application.

I. INTRODUCTION

Maximum distance separable codes (MDS) are codes the coordinates of which are members of a field and that satisfy the distance bound $d = n - k + 1$, where n is the length of the code (number of coordinates or positions) and k is the number of information coordinates (Singleton, 1964; Forney, 1966). Important examples of MDS codes are the Reed–Solomon codes and the generalized Reed–Solomon codes (Delsarte, 1975). In this paper it is shown that MDS codes can be completely decoded by a vote-taking algorithm which is equivalent to a distance correlation method. These methods require the calculation of $\binom{n}{k}$ codewords from a received word.

II. COMPLETE DECODING

The following defining property of MDS codes is well known (Forney, 1966; MacWilliams and Sloane, 1978):

Any set of k coordinates of a (n, k) MDS code C forms an information set.

Suppose a codeword c_i in C is transmitted and errors occur, thus changing c_i into a noncodeword y differing in several coordinates from c_i. From any k coordinates of y, we can generate a codeword $\tilde{y}$ of C which may differ in at most $n - k$ coordinates from y. Each of these codewords is called an estimate of y. Define $S(y)$ to be the set of these estimates. $S(y)$ then contains $\binom{n}{k}$ estimates. Then each member $\tilde{y}$ of $S(y)$ is a codeword coinciding with y in a particular set of k coordinates. Other coordinates (but not all since y is not a codeword) may also agree with y.

0019-9958/79/110195–03$02.00/0

LEMMA. *$S(y)$ contains all code words at distance $\leqslant n - k$ from y.*

Proof. Assume that a codeword $\hat{y}$ of distance less than $n - k + 1$ from y is not included in $S(y)$. However, $\hat{y}$ agrees with y in at least one particular set of k coordinates and thus the codeword generated from these k coordinates is by definition in $S(y)$. This codeword must then equal $\hat{y}$ and thus we have a contradiction.

As a result we immediately have the following:

COROLLARY. *$S(y)$ contains the codeword or codewords at minimum distance from y. (It should be noted that the maximum weight of the coset leaders of C equals $n - k$. For suppose some coset leader L has weight w larger than $n - k$. Then the sum of L and a codeword $-c$ where c has at least k identical coordinates with L (which include the w nonzero coordinates or k of them if $k < w$) will give a coset member of weight no greater than $n - k$.)*

The complete decoding of MDS codes can now be implemented by the following algorithm which utilizes preselection and correlation.

List all $\binom{n}{k}$ codewords $\tilde{y}$ in $S(y)$ and compute the distance $d(y, \tilde{y})$ between y and $\tilde{y}$. Then the codeword $\tilde{y}$ minimizing $d(y, \tilde{y})$ is an optimal estimate assuming "nearest neighbor decoding."

The above "correlation" method of decoding is equivalent to vote-taking as follows. Assume that a given $\tilde{y}$ in $S(y)$ is such that $d(y, \tilde{y}) = \delta \leqslant n - k$. Then this $\tilde{y}$ equals y in exactly $n - \delta$ coordinates. Therefore any set of k information coordinates from these $n - \delta$ coordinates of y will generate the unique codeword $\tilde{y}$. There are exactly $\binom{n-\delta}{k}$ such sets or votes. Since $\binom{n-\delta}{k} > \binom{n-\delta'}{k}$, if $\delta' > \delta$, then minimizing δ is equivalent to taking a "plurality" vote. There may be no majority. We take the codeword or codewords in $S(y)$ receiving the most votes since these have smallest distance from y.

Thus the following has been shown:

THEOREM. *Any* MDS *code can be completely decoded by the method of vote-taking or the equivalent method of minimum distance correlation.*

It should be noted that Reed and Solomon (1969) originally used a vote-taking argument in obtaining the distance bound $d = n - k + 1$ in constructing their codes.

III. IMPLEMENTATION AND APPLICATIONS

It is obvious that to find the codeword associated with any set of k given information coordinates, elementary row operations are performed on the G generator matrix such that the columns corresponding to these k coordinates form an identity matrix I_k. The associated codeword is then obtained by multiplication.

As can be easily seen, the number of operations increases rapidly with n. However, for certain situations with moderate length codes, this method may be practical for complete decoding. These situations could be where one-way communication can be decoded by computer at leisure, such as information from space probes, etc. Consider a R–S code over $GF(2^4)$ of length $n = 15$ which corrects for four errors. Therefore $n - k = 8$ and $k = 7$. Then $\binom{n}{k} = \binom{15}{7} = 6435$ and a maximum of 6435 vote-taking operations are required for complete decoding. By contrast if complete decoding is done using a code dictionary of syndromes, then 16^8 entries are needed.

Note that the dual of any MDS code requires the same number of operations since the dual is MDS and $\binom{n}{k} = \binom{n}{n-k}$. However, using a syndrome dictionary, q^{n-k} entries are required for the dual code where q is the number of symbols in the field. For the dual of the above R–S code, this would require 16^7 entries in the dictionary.

ACKNOWLEDGMENT

The present material was originally cast in an argument using cosets. The present form, which is more direct and lucid, was suggested by the reviewer. For this and the exposure of certain errors the author is indebted.

RECEIVED: August 11, 1978; REVISED: June 13, 1979

REFERENCES

DELSARTE, P. (1975), On subfield subcodes of modified Reed–Solomon codes, *IEEE Trans. Inform. Theory* **IT-21**, 575–576.

FORNEY, G. D., JR. (1966), "Concatenated Codes," Chap. 2, MIT Press, Cambridge, Mass.

MACWILLIAMS, F. J., AND SLOANE, N. J. A. (1978), "The Theory of Error-Correcting Codes," North–Holland, Amsterdam.

REED, I. S., AND SOLOMON, G. (1960), Polynomial codes over certain finite fields, *J. SIAM* 8, 300–304.

SINGLETON, R. C. (1964), Maximum distance q-nary codes, *IEEE Trans. Inform. Theory* **IT-10**, 116–118.