Symmetrically Decodable Codes

R. J. McEliece
Communications Systems Research Section

J. E. Savage
Engineering Division, Brown University

With the intention of finding binary block codes which are easily decoded, we examine decoding functions consisting of one level of symmetric functions. We find that all codes so decodable with fixed error correction capability t have rate less than $1/(2t + 1)$ and that this rate is achieved by the repetition code which has two code words and length $2t + 1$. Decoding functions consisting of two or more levels of symmetric functions include all binary functions and can therefore decode arbitrarily good binary codes.

I. Introduction

The design of error control systems often begins with the selection or invention of a code with good error correction capability, and this is followed by the invention of a decoder. Decoders invented in this fashion are often quite complex. This causes one to wonder whether this complexity is the result of an unfortunate choice for the code. In this report we invert the conventional approach to coding by fixing the decoder type and then examining the type, and characteristics of codes decodable with them. We choose to consider decoders for binary, block codes whose decoding function $f = (f_1, f_2, \cdots, f_k)$ is a collection of functions, each of which is symmetric on some subset of the components of a received word. We choose to let the code block length be n and denote by M the number of code words in a code.

When the decoding function consists of a single symmetric function ($k = 1$), we show that all codes decodable with it which have minimum distance $d = 2t + 1$ must satisfy

$$M \leq \left\lceil \frac{n+1}{2t+1} \right\rceil = \left\lfloor \frac{n}{2t+1} \right\rfloor + 1 \qquad (1)$$

It can also be shown that equality can be achieved. As a consequence of Eq. (1), if d is fixed, then the achievable code rate R decreases with increasing n. This contrasts sharply with the BCH codes, for example, where R approaches 1 with increasing n when d is fixed.

When the decoding function consists of k symmetric functions, we show with a "sphere packing"-like bound

that the maximum code rate is achieved when the domains of definition of $f_1, f_2, \cdots, f_k$ are nonoverlapping. This maximum rate is bounded by

$$R \leq \frac{1}{d}$$

and is achievable with a code which consists of the concatenation with itself n/d times of the code containing the $\overline{0}$ word and 1 word of length d. Thus the best symmetrically decodable codes are both repetitious and not very good.

Decoding functions consisting of two or more levels of symmetric functions include the majority–logic decodable codes since the first level can be used to form the syndrome of a linear code using modulo-two sums, which are symmetric functions, followed by one or more levels of majority functions which are also symmetric.

With this report we document a case study of decoders and hope to encourage interest in this unconventional approach to coding.

II. Symmetric Functions

A binary, symmetric function $f(x_1, \cdots, x_n)$ of n binary variables has the same value on all n-tuples $(x_1, x_2, \cdots, x_n)$ with the same Hamming weight. Thus,

$$f(x_1, x_2, \cdots, x_n) = f(y_1, y_2, \cdots, y_n)$$

if

$$wt(x_1, \cdots, x_n) = wt(y_1, \cdots, y_n)$$

Consequently, a binary, symmetric function can assume at most $n + 1$ values, corresponding to the $n + 1$ different weights of binary n-tuples. Also, symmetric functions are rather easy to realize with logic elements. With, at most, n counters, counting to at most n and a few additional logic elements, any symmetric function can be realized.

The symmetric functions form the only known class of functions of low complexity yet rich enough to offer some hope that they can be used to decode codes with good rate and error correction capability.

III. Symmetric Decoders

Consider a binary code C with $|C| = M$ codewords of length n. We suppose that received words R are decoded by a symmetric function of n variables, $f(x_1, \cdots, x_n)$. If the code is to correct t errors, then if E is an error pattern containing $\leq t$ *ones*, $f(c + E) = f(c)$ for each $c \epsilon C$. But since, as we have seen, the value of a symmetric function depends only on the weight of its argument and since an error pattern of weight t or less can change the weight of c by up to t, we see that the weights of the codewords C_i must satisfy

$$|w(c_i) - w(c_j)| \geq 2t + 1, \qquad i \neq j \tag{2}$$

and the maximum number of weights in the range $[0, n]$ which can be chosen to satisfy Eq. (2) is

$$M \leq \left\lceil \frac{n+1}{2t+1} \right\rceil = \left\lfloor \frac{n}{2t+1} \right\rfloor + 1 \tag{3}$$

Equality can be achieved by choosing one word of weight 0, one of weight $2t + 1, \cdots$, one of weight $q(2t + 1)$, where

$$q = \left\lfloor \frac{n}{2t+1} \right\rfloor$$

Notice that the rate of such a code is bounded by

$$R \leq \frac{1}{n} \cdot \log_2 \left\lceil \frac{n+1}{2t+1} \right\rceil \leq \frac{1}{2t+1}$$

and we can actually achieve rate $1/(2t + 1)$ with the repetition codes $\{00 \cdots 0$ and $11 \cdots 1\}$ with decoding function f = majority vote.

IV. Sub-Symmetric Decoders

We now consider a somewhat broader class of decoding functions. The decoder is to consist of k functions f_i, and each f_i is to be a symmetric function of n_i of the variables $x_1, x_2, \cdots, x_n$. We denote the domain of the function f_i by D_i.

If the code C is to correct t errors, then the projection C_i of the code onto each domain D_i will itself correct t errors and must be decodable by f_i. Hence by the results in *Section III*,

$$M_i \leq \left\lceil \frac{n_i + 1}{2t+1} \right\rceil$$

Since $M \leq M_1 M_2 \cdots M_k$ (Footnote 1),

$$M \leq \prod_{i=1}^{k} \left\lceil \frac{n_i + 1}{2t + 1} \right\rceil \tag{4}$$

If the domains D_i are disjoint, this bound can be achieved, since we have seen in *Section III* that it is achievable for $k = 1$, and so we may take $C = C_1 \times C_2 \times \cdots \times C_k$. If however, the D_i are not disjoint the various projections C_i cannot be chosen independently. Nevertheless we argue that nothing can be gained by having the D_i's overlap, as follows:

Let E be the subset of the variables $\{x_1, \cdots, x_n\}$ which are involved in more than one of the functions f_i, and let C_E be the projection of C onto E. For each word $e \epsilon E$ let C_{ie} be the set of codewords in C_i which are "compatible" with e in the sense that each codeword in C_{ie} agrees with e on $D_i \cap E$. Then the total number of codewords in C compatible with e is $\leq M_{1e} M_{2e} \cdots M_{ke}$ and so

$$M \leq \sum_{e \epsilon E} M_{1e}, M_{2e}, \cdots M_{ke} \tag{5}$$

Since all codewords in C_{ie} agree in $m_i = |D_i \cap E|$ positions, but their weights must be separated by $2t + 1$, we must have

$$M_{ie} \leq \left\lceil \frac{n_i - m_i + 1}{2t + 1} \right\rceil \tag{6}$$

Also, since $C_i = \cup C_{ie}$ and

$$M_i \leq \left\lceil \frac{n_i + 1}{2t + 1} \right\rceil$$

then

$$\Sigma M_{ie} \leq \left\lceil \frac{n_i + 1}{2t + 1} \right\rceil \tag{7}$$

Combining Eqs. (5) and (6) we obtain

$$M \leq \sum_{e} M_{1e} \cdot \left\lceil \frac{n_2 - m_2 + 1}{2t + 1} \right\rceil \cdots \left\lceil \frac{n_k - m_k + 1}{2t + 1} \right\rceil$$

which by Eq. (7) yields

$$M \leq \left\lceil \frac{n_1 + 1}{2t + 1} \right\rceil \cdot \prod_{i=2}^{k} \left\lceil \frac{n_i - m_i + 1}{2t + 1} \right\rceil$$

This is the same form as Eq. (4), with a total block length of

$$n_1 + \sum_{i=2}^{k} (n_i - m_i)$$

This is $\leq n$ since for $i \geq 2$ the sets $D_i - D_i \cap E$ are disjoint from each other and from D_i. Hence if the D_i are allowed to overlap, we can get no more codewords than we could with disjoint D_i at the same (or smaller) block length.

There remains the problem of maximizing Eq. (4) over all values of k and all choices of n_i subject to

$$n_1 + \cdots + n_k = n$$

For each i write $n_i = q_i (2t + 1) + r_i$ with $0 \leq r_i < 2t + 1$. Then we may replace each f_i with q_i functions of $2t + 1$ variables each and obtain

$$\left\lceil \frac{2t + 2}{2t + 1} \right\rceil \times \cdots \times \left\lceil \frac{2t + 2}{2t + 1} \right\rceil = 2^{q_i}$$

possible codewords instead of

$$\left\lceil \frac{n_i + 1}{2t + 1} \right\rceil = q_i + 1$$

Since $2^a \geq a + 1$ for all integers $a \geq 0$, if the product in Eq. (4) is to be maximized no n_i needs to exceed $2t + 1$. So if we write $n = q (2t + 1) + r$, $0 \leq r < 2t + 1$, and take $n_1 = \cdots = n_q = 2t + 1$, $n_{q+1} = r$, we get $M = 2^q$ as the maximum possible number of codewords, and so the rate of the code satisfies

$$R \leq \frac{1}{n} \left\lfloor \frac{n}{2t + 1} \right\rfloor \leq \frac{1}{2t + 1}$$

But since rate $1/(2t + 1)$ can be achieved by a repetition code of length $2t + 1$ and "majority vote" decoding, we see that no code that corrects t errors and is decodable by a sub-symmetric decoder is better than a repetition code. Hence, good symmetrically decodable codes are repetitious.

[1] Of course, this assumes all variables are used. If some are not, we just connect the unused ones to a symmetric function whose value is constant.