CAPABILITIES OF PARITY CHECK CODES FOR NONPRIME ALPHABETS

by

JOSEPH ELLIOT LEVY

B.E.E., The Cooper Union

(1960)

SUBMITTED IN PARTIAL FULFILLMENT OF THE

REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June, 1964

Signature of Author Joseph Elliot Levy
Department of Electrical Engineering, June 5, 1964

Certified by Robert G. Gallager
Thesis Supervisor

Accepted by Truman S. Gray
Chairman, Departmental Committee on Graduate Students

CAPABILITIES OF PARITY CHECK CODES FOR NONPRIME ALPHABETS

by

JOSEPH ELLIOT LEVY

B.E.E., The Cooper Union

(1960)

SUBMITTED IN PARTIAL FULFILLMENT OF THE

REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June, 1964

Signature of Author Signature redacted
Department of Electrical Engineering, June 5, 1964

Certified by Signature redacted
Thesis Supervisor

Accepted by Signature redacted
Chairman, Departmental Committee on Graduate Students

CAPABILITIES OF PARITY CHECK CODES FOR NONPRIME ALPHABETS

by

JOSEPH ELLIOT LEVY

Submitted to the Department of Electrical Engineering on June 5, 1964 in partial fulfillment of the requirements for the degree of Master of Science.

ABSTRACT

In this paper bounds on minimum distance are derived for block parity check codes using modulo q checking arithmetic. Asymptotic expressions for the bounds on minimum distance indicate that the achievable minimum distance for a parity check code using modulo q checking arithmetic falls short of what is attainable using block codes of arbitrary construction. In contrast, parity check codes using the arithmetic of GF(q), the Galois field of q elements, have their minimum distance bounded by expressions asymptotically identical to those for arbitrary block codes.

Parity check codes using modulo q arithmetic, while deficient in Hamming distance properties, may prove to be powerful in situations where the natural restrictions upon the likely class of errors fit in with the modulo q arithmetic. A simple example involving the correction of $\pm$ 1 level errors on an 8 level channel is given; the problem is easily handled using modulo 8 checking arithmetic, and proves completely intractable when GF(8) checking arithmetic is used.

Thesis Supervisor: Robert G. Gallager
Title: Associate Professor of Electrical Engineering

Acknowledgment

I wish to thank Professor Robert G. Gallager for his many helpful suggestions and constructive criticisms during the progress of my research.

TABLE OF CONTENTS

Section I

By way of introduction to the block parity check codes on the alphabet of q symbols with which this paper concerns itself, the first paragraphs of this section present a brief sketch of the essentials of block coding.

It is easiest to begin a discussion of block codes by considering binary block codes of length n. Imagine that a person is attempting to transmit reliably one of M different messages over a noisy binary channel by sending one of M specially selected binary sequences of length n (n-tuples). In his effort to achieve reliable communication in the presence of channel noise which will unpredictably change some 0's into 1's and vice versa, he builds a certain amount of redundancy into his scheme for sending messages, i.e., his rate of transmission as defined by $R = \log_2 M / n$ is less than 1. This deliberate use of a block code of length n when, strictly speaking, a block code of length nR would have been adequate, is a procedure which should be expected to offer some protection against the incorrect decoding of messages by their recipient as a result of channel noise. Indeed, the coding theorem states that one may communicate over a discrete memoryless channel with arbitrarily small probability of error by using block codes of increasingly longer block length, as long as the rate is less than a quantity known as the channel capacity. The capacity, which is a measure of how much information the channel may reliably transmit, depends only upon the probability of a transmitted "0" being received as a "1" and the probability of a "1" being received as a "0" in the case of a binary channel.

The concept of Hamming distance is a fundamental one in understanding the error-correcting abilities of codes. The Hamming distance between two sequences is defined to be the number of places in which the two sequences differ. If a code is so constructed that the minimum Hamming distance between any two code words is 2r+1, then it is certain that any message may be correctly decoded if r or fewer errors have occurred on transmission. The recipient of the coded message can achieve this capability by comparing the received sequence to the list of possible messages in his code word dictionary, and selecting as the message sent that one which is closest to the received sequence in Hamming distance.

A common approach to the construction of redundant binary block codes is to picture that the first nR digits are chosen to represent the information to be transmitted, i.e., each of the $M = 2^{nR}$ messages has as its first nR digits one of the nR-tuples. The remaining n(1-R) digits are chosen in accordance with n(1-R) <u>parity check equations</u> expressing the dependency of the <u>check digits</u> upon the <u>information digits</u>. Such a code is called a <u>parity check code</u>; a simple example of one will make the concept more clear. Suppose that we wish to transmit any of 2^4 different messages in such a way that correct decoding may be accomplished if one or less errors have occurred on transmission. Using a code with block length of 7, where the first four digits, $x_1x_2x_3x_4$, are the information digits the following set of parity check equations for determining the check digits $x_5 x_6 x_7$ will lead to the construction of the desired single-error-correcting code:

$$x_2 \oplus x_3 \oplus x_4 \oplus x_5 = 0$$

$$x_1 \oplus x_3 \oplus x_4 \oplus x_6 = 0$$

$$x_1 \oplus x_2 \oplus x_4 \oplus x_7 = 0$$

where $\oplus$ denotes modulo 2 addition

For example, if the information digits of the message to be sent are 1000, the redundant sequence 1000011 will be transmitted. The recipient of the message can now make use of the parity check equations in his decoding procedure. He applies the three parity check equations to the received sequence; a list of the outcomes of these parity checks, called the syndrome, is made. If 1000011 were received, the syndrome would be (0,0,0).

It can be shown that a sequence is a code word in a binary parity check code if and only if its syndrome is zero. A received sequence may be thought of as the sum of two binary sequences, $\bar{m} + \bar{e}$, where $\bar{m}$ is the message and $\bar{e}$ is the "error sequence" added on (component by component, modulo 2), having 1's in those places that have been changed by channel noise and 0's elsewhere.

The syndrome can be shown to be independent of the message transmitted, and determined wholly by the error sequence occurring on transmission over the channel. For the code given above there is a unique correspondence between syndrome and error pattern for each of the eight syndromes: (0,0,0),... (1,1,1). Calculation of the syndrome results in discovery and correction of the single error, resulting in recovery of the exact sequence transmitted.

It is convenient to represent the parity check equations in terms of a matrix consisting of n(1-R) row vectors. The single-error-correcting code described above has as its <u>parity check matrix:</u>

$$\begin{Bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{Bmatrix}$$

In general, a vector is a code word if and only if its "dot product" with each of the n(1-R) rows of the parity check matrix is zero. More formally the operation is the ordinary dot product of two vectors comprised of n-tuples over the Galois field of two elements, GF(2).

It may be shown that all binary code words satisfying a given set of parity check equations form a group under the operation of modulo 2 vector addition.* Such a code is called a <u>group code</u>, and has the important property that any code word is the "difference" (or sum; in modulo 2 arithmetic, addition and subtraction are the same) of two other code words, and therefore has as its Hamming weight the Hamming distance between the two code words. For a group code the minimum distance must be equal to the weight of the minimum weight nonzero code word.

---

* A group consists of a set of elements and a defined operation upon the elements satisfying four axioms:
1) Closure: if a and b are in the set, then a+b is also in the set.
2) Associative law: a + (b+c) = (a+b) + c
3) Identity element: There is an element 0, such that a+0=a for all elements in the set
4) Unique inverse: There exists a unique inverse element for each a such that a + (-a) = 0.

These basic ideas regarding binary parity check codes may be easily extended to parity check codes with characters built on the alphabet of q symbols: 0,1,...q-1.

A parity check code on the alphabet of q symbols with block length n and rate R is defined to consist of vectors $\bar{m}_i$: $\bar{m}_i = (m_{i1},\ldots m_{in})$ which satisfy the n(1-R) independent relations:

$$\text{I-1)}\quad \sum_{k=1}^{n} m_{ik}u_{jk} = 0 \qquad j = 1,2,\ldots n(1-R)$$

The vector $\bar{u}_j = (u_{j1},\ldots u_{jn})$ is the jth row of the parity check matrix of the code; it too is composed of n-tuples from the q symbol alphabet.

Equations I-1) assume the existence of both an addition and a multiplication operation defined on the q alphabet symbols. These operations constitute the <u>checking arithmetic</u> of the code. It should be noted that if q=2, and the checking arithmetic consists of modulo 2 addition and multiplication, equations I-1) are exactly equivalent to the previously advanced definition of a binary parity check code. If the operations of the checking arithmetic obey the distributive law: (a+b)c = ac + bc, then it can be shown that the parity check code is indeed a group code for which minimum distance may be equated with minimum weight.

For block codes in general, the minimum distance between code words may be bounded from above by the Sphere Packing and Plotkin bounds and from below by the Gilbert bound. These bounds are derived in Appendix A. Analogous bounds for parity check codes using the checking arithmetic of GF(q), the Galois field of q elements, are derived in Appendix B. The expressions for these bounds in Appendices A and B are seen to agree asymptotically as block length n approaches infinity. In this sense the GF(q) checking arithmetic is an efficient one. GF(q) only exists if q is a prime number to an integral power.

In Section II bounds on minimum distance are derived for parity check codes using modulo q checking arithmetic (this is different from GF(q) arithmetic as long as q is not a prime number). When q is equal to a prime number to an integral power, both GF(q) and modulo q checking arithmetic are available as choices for the construction of parity check codes. Modulo q arithmetic will frequently seem to be a more natural choice. For example, in multiple level channels sending voltage-quantized pulses to convey information, nearly all likely error patterns will be the result of additive noise causing a one level quantization error modulo q; two level errors and up will be extremely unlikely if the spacing between quantization levels is appreciably greater than the rms noise level. Appendix C presents a simple example where quantization errors of 1 level in an 8 level channel may be easily corrected with modulo 8 checking arithmetic, but present a hopeless problem when GF(8) checking arithmetic is used.

The results of the analysis of Section II are disappointing in that the asymptotic expressions for the bounds on minimum distance indicate that the achievable minimum distance for a parity check code using modulo q checking arithmetic falls short of what is attainable for block codes in general. In terms of Hamming distance properties, modulo q checking arithmetic is inefficient and is to be avoided. Its power lies in its application to situations where restrictions upon the likely class of errors, which make Hamming distance a poor measure of error-correcting capability, fit in naturally with the modulo q arithmetic.

Section II

In this section we shall derive bounds upon the minimum distance for parity check codes employing modulo q checking arithmetic. It is easily verified that the q integers (alphabet symbols) 0,1,...q-1 form a ring under the two commutative operations of modulo q addition and modulo q multiplication. Also the distributive laws are obeyed: $a(b+c) = ab + ac$; $(a+b)c = ac + bc$. Therefore a code using modulo q checking arithmetic is a true group code for which the minimum weight for a code word is equivalent to the minimum distance of the code. Before proceeding with the actual analysis, a few basic definitions and theorems regarding modulo q arithmetic must be introduced.

Definition: In the ring of integers modulo q, any nonzero integer which is either a factor of q or has as a factor a factor of q is considered to be a <u>trivial number.</u> (Unity is <u>not</u> considered to be a trivial number.)

Definition: The symbol <u>$\nu_o(q)$</u> represents the number of trivial numbers in the set 0,1,...q-1. The remaining $q - \nu_o(q) - 1$ nonzero integers are considered to be <u>nontrivial numbers</u>.

Theorem II-1:

The product ab of two integers modulo q is trivial if either a or b is trivial; it is nontrivial if both a and b are nontrivial.

Proof: The proof of this theorem follows immediately from the definitions of trivial and nontrivial numbers.

Theorem II-2:

If a is nontrivial, then the q-1 products ab, b=1,2,...q-1, are all different and all nonzero.

Proof: ab cannot equal zero modulo q since a is not a factor of q. Now suppose that:

$$ab = ab' \quad \text{modulo } q$$

Then:

$$ab - ab' = 0$$

But, by the distributive property ab - ab' = a(b - b') =0
Thus b - b' = 0 and b must equal b'

Corollary:

Each nontrivial number a has a unique multiplicative inverse a^{-1} such that $aa^{-1} = 1$

Theorem II-3:

The nontrivial numbers form a group under modulo q multiplication.

Proof: Closure of the set follows from Theorem II-1. The identity element is 1. The existence of a unique inverse for each member of the set is stated in the corollary to Theorem II-2.

Definition: $\Omega_a(q)$, <u>the order of the trivial integer a</u> in the ring of integers modulo q, is the smallest integer such that:

$$a\Omega_a(q) = 0 \quad \text{modulo } q$$

Theorem II-4:

$\Omega_a(q)$ is a factor of q.

Proof: Since a is a trivial number it contains a factor of q which shall be denoted as g_1, such that $q=g_1g_2$. $\Omega_a(q)$ must contain g_2 as a factor if $a\Omega_a(q)$ is to equal zero modulo q. But it would be impossible for $\Omega_a(q)$ to equal $2g_2$, $3g_2$,... as these are all greater than g_2. Thus $\Omega_a(q)$ equals g_2 and is a factor of q.

Definition: f(q) is the smallest factor of q.

Corollary to Theorem II-4:

$$f(q) \le \Omega_a(q) \le q/f(q)$$

Theorem II-5:

The trivial number a has $\Omega_a(q)$ distinct multiples.

Proof: From the definition of $\Omega_a(q)$, it follows that the value of the product ab depends only upon the value of b modulo $\Omega_a(q)$.

Definition: A <u>trivial vector</u> is one having only trivial numbers for its nonzero components. A <u>nontrivial vector</u> has at least one nontrivial component.

Theorem II-6:

If the trivial vector $\bar{u}$ has components based on the ring of integers modulo $q = P^y$, a prime number to an integral power, then at least one scalar multiple of $\bar{u}$ is equal to zero.

Proof: In the ring of integers modulo $q = P^y$, all the trivial numbers are multiples of P. Thus if a is trivial, $P^{y-1}a = 0$. Therefore $P^{y-1}\bar{u} = \bar{0}$.

Theorem II-7:

Suppose that the vectors $\bar{u}_1, \ldots \bar{u}_r$ having components based on the ring of integers modulo $q = P^y$ are linearly independent, i.e., $\sum_{i=1}^{r} a_i u_i$ does not equal to zero unless all the a_i are equal to zero. Then the vector $\mathbf{u}^* = \sum_{i=1}^{r} a_i u_i$ is trivial if and only if all the a_i are trivial.

Proof: If all the a_i are trivial, then:

$$P^{y-1}u^* = P^{y-1}\sum_{i=1}^{r} a_i u_i = \sum_{i=1}^{r}(P^{y-1}a_i)u_i = 0$$

This could not happen unless u* were a trivial vector. On the other hand, assume that u* is trivial. Then:

$$P^{y-1}u^* = 0 = \sum_{i=1}^{r} (P^{y-1}a_i)u_i.$$

This implies that all the $P^{y-1}a_i$ are equal to zero; thus all the a_i are trivial numbers.

Now we may derive bounds upon the minimum distance of parity check codes using modulo q checking arithmetic ($q \neq$ a prime number). For the sake of simplicity the symbols f, ν_o, and Ω_a shall be used, their functional dependency on q being implicitly understood.

Sphere Packing Upper Bound

The alphabet contains the symbol q/f, which has only f distinct multiples. There are $\binom{n}{d}$ sequences of weight d made up of d (q/f)'s and n-d 0's. The n(1-R) parity check equations are capable of producing only $f^{n(1-R)}$ different syndromes when checking upon sequences of this type. Thus if:

$$\binom{n}{d} > f^{n(1-R)}$$

at least two sequences of this type must have the same syndrome. The difference between these two sequences, a vector of weight $\leq 2d$, must be a code word, as its syndrome is the difference of the two identical syndromes, i.e., the vector of n(1-R) 0's. The minimum distance is upperbounded by the smallest d satisfying the relation:

II-1) $$\binom{n}{d/2} > f^{n(1-R)}$$

Using equation A-1, Appendix A, the asymptotic form of II-1 as block length n approaches infinity is obtained:

II-2) $R = 1 - H_f(\delta/2)$

$$\delta = d/n; \quad H_f(x) = -x\log_f x - (1-x)\log_f(1-x)$$

Equation II-2 states the asymptote to the upper bound on the distance parameter δ as a function of the rate R.

The Plotkin Upper Bound

The proof of the Plotkin Bound is given in Appendix A. The results are summarized below:

II-3) $R \leq 1 - \frac{qd-1}{2(q-1)} - \frac{\log_q qd}{n}$

The asymptotic form of II-3) is:

II-4) $R = 1 - \frac{q\delta}{(q-1)}$

The Gilbert Lower Bound

We now consider the problem of constructing the check matrix of a code using modulo q checking arithmetic having block length n, minimum distance of at least d and a rate of at least R. The check matrix will be constructed so as to have n(1-R) rows (the rate is exactly R if all the n(1-R) parity checks are independent; otherwise it is greater than R) and n columns designated as $\bar{v}_1, \ldots . \bar{v}_n$. No linear combination of d-1 or fewer columns may equal $\bar{0}$, since this would imply the existence of a code word of weight d-1 or less. We must analyze separately two cases.

1) $q=P^y$, a prime number to an integral power

An exhaustive search procedure must be carried out for the selection of columns for the check matrix in such a way that no linear combination of d-1 or fewer columns equals zero. At the beginning of the selection procedure all $(\nu_o + 1)^{n(1-R)}$

trivial n(1-R)-tuples must be discarded. The inclusion of a trivial column in the check matrix would, by Theorem II-6, imply the existence of a weight one word in the code.

One of the nontrivial n(1-R)-tuples is selected as the first column of the check matrix. We then select the second column from those vectors remaining after excluding as ineligible all those vectors $\bar{v}'$ for which:

$$b\bar{v}' = a\bar{v}_1 \quad \text{for all a, b chosen from } 1,2,\ldots q-1$$

thereby preventing a relationship of the kind $a_1\bar{v}_1 + a_2\bar{v}_2 = \bar{0}$. In general, if the column vectors $\bar{v}_1,\ldots\bar{v}_m$, $m \leq d-2$, are among those already selected for the check matrix, then in order to make it impossible for any combination of m+1 vectors to add up to zero, those vectors v^* for which:

II-5) $bv^* = \sum_{i=1}^{m} a_i v_i$ all combinations of the a_i's chosen from: $1,2,\ldots q-1$; all choices of b from: $1,2,\ldots q-1$

must be excluded from eligibility as columns of the check matrix.

If b is nontrivial, then II-5) reduces to:

$$v^* = \sum_{i=1}^{m}(b^{-1}a_i)v_i = \sum_{i=1}^{m} a_i' v_i$$

Thus we must exclude all vectors that are linear combinations of $\bar{v}_1,\ldots\bar{v}_m$. By virtue of Theorem II-7 ν_o^m of these combinations result in trivial vectors(which were discarded at the very beginning of the procedure) and the remaining $(q-1)^m - \nu_o^m$ combinations result in nontrivial vectors.

The insertion of a trivial value of b into II-5) must now be considered. It is best to visualize II-5) as consisting of $n(1-R)$ component equations. For b trivial, only those ν_o^m combinations of $\bar{v}_1, \ldots \bar{v}_m$ yielding trivial vectors can possibly produce solutions in II-5). For any particular trivial value of b, solutions can only occur if each of the $n(1-R)$ components of $\sum_{i=1}^{m} a_i v_i$ is one of the Ω_b multiples of b. At the very worst all ν_o^m trivial combinations may produce ν_o^m distinct vectors in this category. For a given vector $\bar{v}$ in this category, there is a multiplicity of $\bar{v}^*$ satisfying $b\bar{v}^* = \bar{v}$. Suppose that d is the kth component of $\bar{v}$, and that c is the smallest integer such that $bc = d$ modulo q. Then the kth component of $\bar{v}^*$ will satisfy II-5) if it takes on any of the values: $c, c + \Omega_b, c + 2\Omega_b, \ldots$, a total of q/Ω_b possible values in all. Therefore there may be as many as $(q/\Omega_b)^{n(1-R)}$ possible values of $\bar{v}^*$ satisfying II-5) for each of the ν_o^m trivial combinations of $\bar{v}_1, \ldots \bar{v}_m$, for each trivial value of b.

Thus it is concluded that if the vectors $\bar{v}_1, \ldots \bar{v}_m$ are in the check matrix, the number of vectors that must be excluded is upperbounded by:

$$(q-1)^m - \nu_o^m + \sum_{b \text{ trivial}} (q/\Omega_b)^{n(1-R)} \nu_o^m$$

As long as the total of the number of columns selected for the matrix plus the number excluded is upperbounded by a quantity less than $q^{n(1-R)}$, another column may be added. In the worst possible case all those vectors excluded for the different possible combinations of the $\bar{v}$'s in the matrix might be distinct. Thus a code of block length n, with rate of at least R and minimum distance of at least d can surely be constructed if:

II-6)

$$\sum_{j=1}^{d-2} \binom{n-1}{j} \left\{ (q-1)^j - \nu_o^{\,j} + \sum_{b\ \text{trivial}} (q/\Omega_b)^{n(1-R)} \nu_o^{\,j} \right\} < q^{n(1-R)} - (\nu_o+1)^{n(1-R)}$$

II-6) may be simplified in form and slightly weakened by observing that the smallest value of Ω_b is f. The condition for the existence of a code having block length n, rate of at least R and minimum distance of at least d is then:

II-7)

$$\sum_{j=1}^{d-2} \binom{n-1}{j} \left\{ (q-1)^j - \nu_o^{\,j} + \frac{\nu_o^{\,j+1}\, q^{n(1-R)}}{f^{n(1-R)}} \right\} < q^{n(1-R)} - (\nu_o+1)^{n(1-R)}$$

The asymptotic form of II-7) is:

II-8) $R = 1 - H_f(\delta) - \delta \log_f \nu_o$

$\delta = d/n$; $H_f(x) = -x\log_f x - (1-x)\log_f(1-x)$

2) $\underline{q \neq P^y}$

The general argument used for the case where $q = P^y$ shall be used, but with some significant changes. We shall follow essentially the same search procedure for constructing the check matrix. The procedure is begun by excluding from eligibility as columns of the check matrix all trivial n(1-R)-tuples. This is not strictly necessary; some of the trivial n(1-R)-tuples, e.g., $\begin{bmatrix}5\\2\end{bmatrix}$ modulo 10, have no multiples equal to zero. This represents a slight weakening of the bound which will not be reflected in its asymptotic form since the trivial vectors form an infinitesimal fraction of the total number of n(1-R)-tuples as n approaches infinity.

Consider now how many vectors must be excluded if $\bar{v}_1,\ldots\bar{v}_m$ are among those chosen as columns of the check matrix. Theorem II-7) may no longer be invoked to claim that only $\nu_o^{\ m}$ of the linear combinations of $\bar{v}_1,\ldots\bar{v}_m$ are trivial; at the worst all $(q-1)^m$ combinations result in trivial vectors, each one of them accounting for the exclusion of $(q/\Omega_b)^{n(1-R)}$ distinct vectors. Thus the number of vectors excluded if $\bar{v}_1,\ldots\bar{v}_m$ are in the matrix is upperbounded by:

$$\sum_{b\ \text{trivial}} (q/\Omega_b)^{n(1-R)}\ (q-1)^m$$

The condition for the existence of a code having block length n, rate of at least R and minimum distance of at least d is:

II-9)

$$\sum_{j=1}^{d-2} \binom{n-1}{j} \left\{ \sum_{b\ \text{trivial}} (q/\Omega_b)^{n(1-R)}(q-1)^j \right\} < q^{n(1-R)} - (\nu_o+1)^{n(1-R)}$$

The asymptotic form of II-9) is:

II-10) $R = 1 - H_f(\delta) - \delta\log_f(q-1)$

Figures II-1 and II-2 are plots of the asymptotic bounds on minimum distance for parity check codes on the alphabet of four symbols using GF(4) and modulo 4 checking arithmetic respectively.

These curves show a certain superiority of the arbitrary codes and those using GF(4) checking arithmetic over those using modulo 4 checking arithmetic. They are superior in the sense that the asymptotes to the upper and lower bounds upon minimum distance for them are greater than the corresponding bounds for modulo 4 codes for $R > .08$. For $R < .08$, both classes of codes have the Plotkin bound in common.

Thus figures II-1 and II-2 provide an indication that GF(4) parity check codes are "better" than modulo 4 check codes. This is not an airtight certainty however; for all values of R, the upper bound on δ for codes using modulo 4 checking arithmetic is greater than the lower bound on δ for GF(4) check codes.

Calculations were done for the cases of q =6,8, and 10. It was found that for values of R greater than .41, .14, and .06 respectively, that the upper bound on the minimum distance for modulo q parity check codes was less than the lower bound for GF(q) and arbitrary codes, demonstrating a clear cut deficiency in Hamming distance properties for modulo q parity check codes for these rates and alphabet sizes.

Figure II-1

Bounds upon minimum distance for parity check codes using GF(4) checking arithmetic.

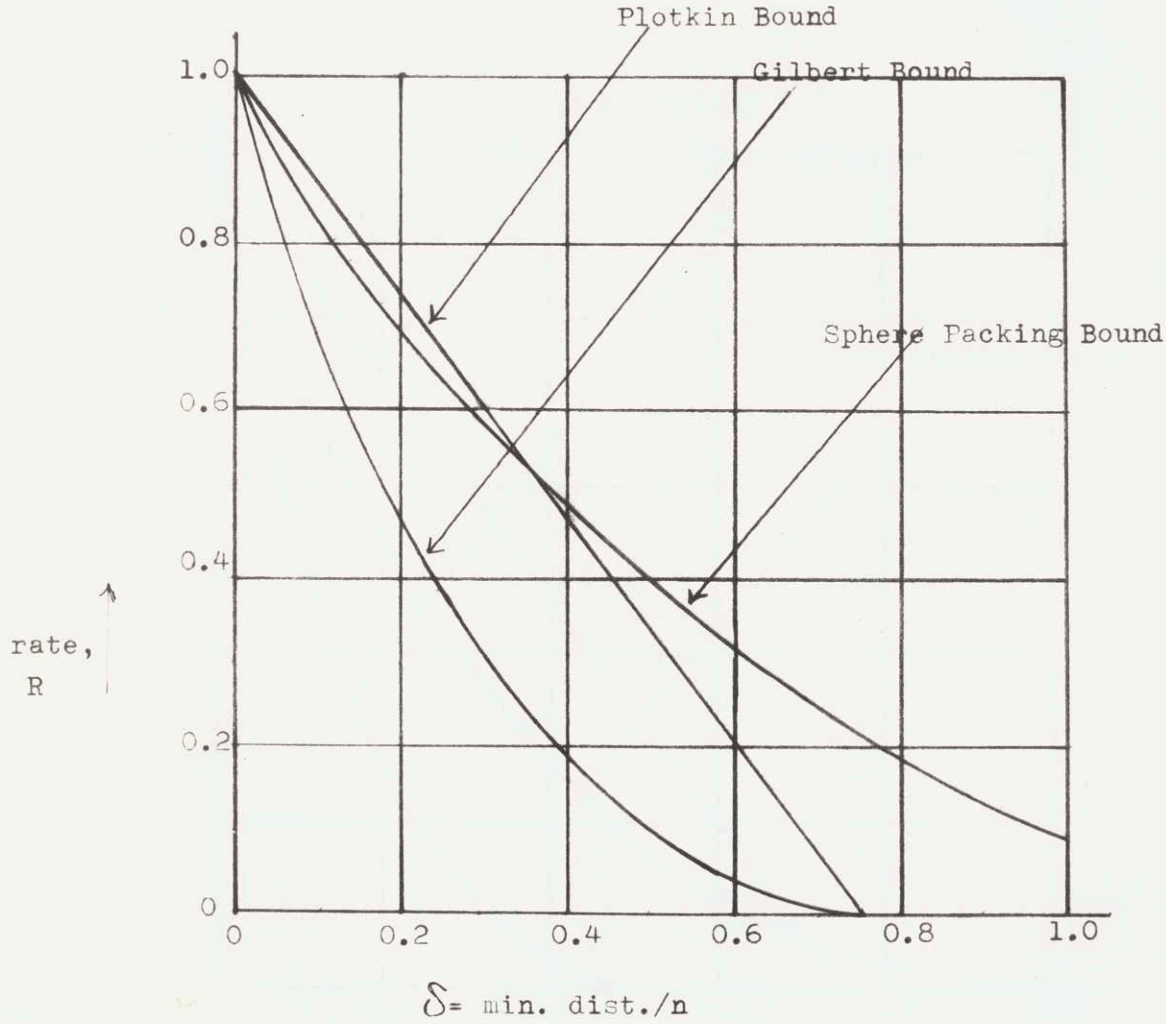
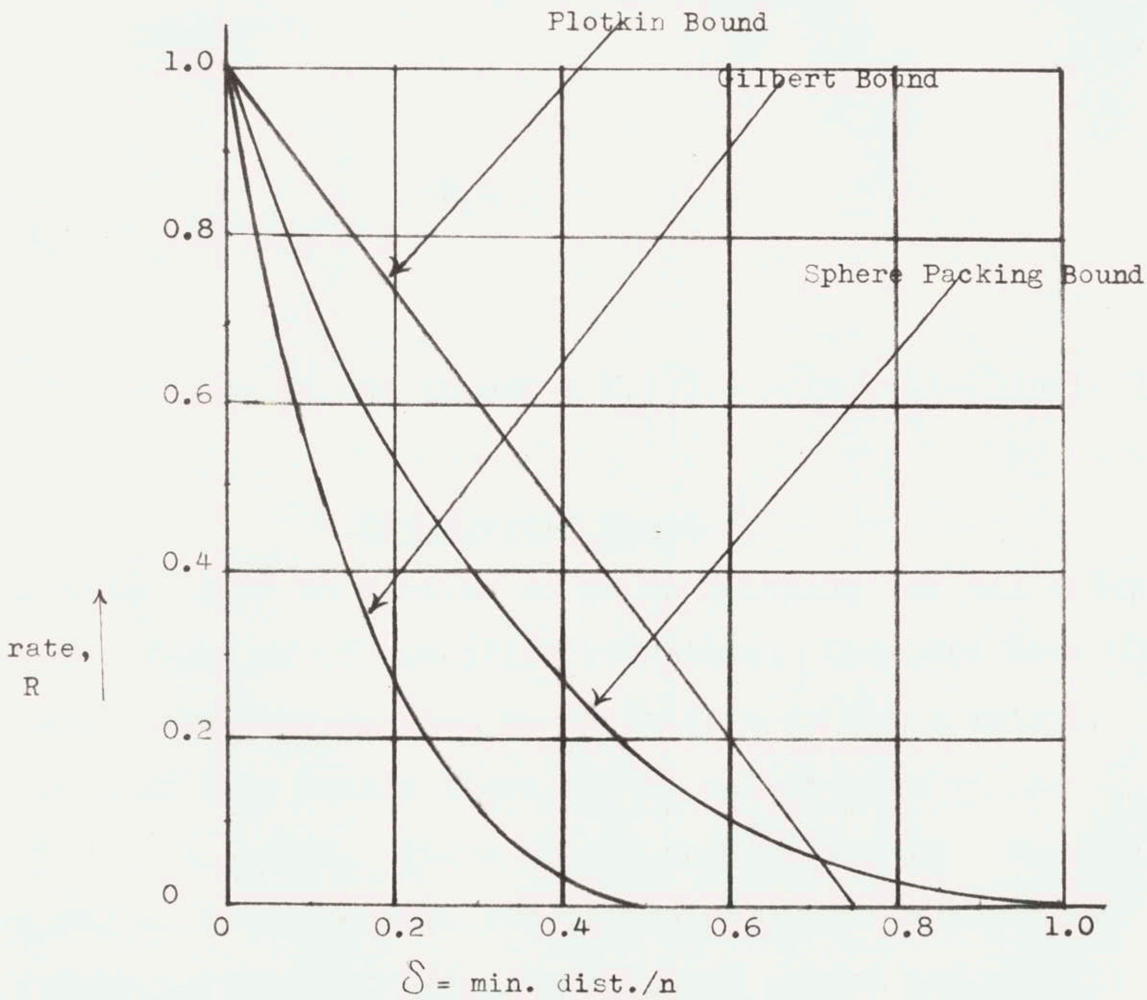


Figure II-2

Bounds upon minimum distance for parity check codes using modulo 4 checking arithmetic.



Appendix A

Bounds on minimum distance shall now be derived for arbitrary block codes of length n on the alphabet of q symbols consisting of M messages (rate, R, = $\log_q M/n$). The following asymptotic result derived on page 216 of Reference 1 shall be needed in order to express the bounds on minimum distance in their asymptotic form:

A-1) $$\binom{n}{d} \sim \left[\frac{1}{2\pi n\delta(1-\delta)}\right]^{1/2} \cdot e^{n\left[-\delta\ln\delta-(1-\delta)\ln(1-\delta)\right]}$$

or

$$\binom{n}{d} \sim \left[\frac{1}{2\pi n\delta(1-\delta)}\right]^{1/2} \cdot a^{nH_a(\delta)}$$

$\delta = d/n$; a is any number : $H_a(\delta) = -\delta\ln\delta-(1-\delta)\ln(1-\delta)$

The Plotkin Bound [4]

This bound shall be derived so as to be valid for all codes, whether arbitrary or of specified structure. Consider that all M code words are written down so as to form an M x n matrix. In each column of this matrix there are x_i occurrences of the symbol i; i=0,1,...q-1. These x_i are constrained by $\sum_{i=0}^{q-1} x_i = M$. Finding the maximum possible sum of the distances between the $\binom{M}{2}$ different pairings of characters in any column and multiplying by n gives the maximum possible sum of the distances between code words, a necessary quantity in obtaining the bound.

In any given column, there are $\binom{M}{2}$ "distances", which must be either 0 or 1. The sum of these distances is:

$$\frac{1}{2}\sum_{i=0}^{q-1} x_i(M - x_i)$$

The factor of ½ accounts for the fact that each of the different pairings is counted twice in the above expression. Application of LaGrange's method of the indeterminate multiplier shows that the expression is maximized when $x_i = 1/M$ for all i. (It may be shown that equality of all the x_i insures that the code is a group code; conversely any code which is a group code, e.g., a parity check code using modulo q checking arithmetic, has this distance maximizing property.) Thus the maximum value of the sum of the distances in a particular column is $\frac{M^2(q-1)}{2q}$.

The maximum possible sum of the distances between code words is therefore:

A-2) $$\sum \text{dist} = \frac{nM^2(q-1)}{2q}$$

The minimum distance between code words, d, must be no greater than the maximum possible average distance between code words, i.e., the quantity of expression A-2) divided by $\binom{M}{2}$:

A-3) $$d \leq \frac{nM(q-1)}{(M-1)q}$$

Let B(n,d) represent the maximum number of code words possible in a code of length n having minimum distance d. If the B(n,d) words were to be separated into q sets on the basis of the last character in each word, at least one set would contain $\frac{B(n,d)}{q}$ or more code words. Throwing away the last character of every word in this set would yield a new code of length n-1 and minimum distance d. Thus:

A-4) $B(n,d) \leq qB(n-1,d)$

Repeated application of A-4) results in:

A-5) $B(n,d) \leq q^{a}B(n-a,d)$

Equation A-3) may be rearranged and written as:

A-6) $M \cdot \left[qd - n(q-1) \right] \leq qd$

A-6) holds for B(n,d) the largest possible value of M. Substituting the value $n = \dfrac{qd - 1}{q - 1}$ into A-6) :

A-7) $B\left(\dfrac{qd - 1}{q - 1}, d\right) \leq qd$

Using A-5), with $a = n - \dfrac{qd-1}{q-1}$, we obtain :

A-8) $B(n,d) \leq qd\, q^{n - (qd-1)/(q-1)}$

or the alternate form:

A-9) $R \leq 1 - \dfrac{qd-1}{n(q-1)} - \dfrac{\log_q qd}{n}$

The asymptotic form of A-9) for large n is:

A-10) $R = 1 - \dfrac{q\delta}{(q-1)}$

The Sphere Packing Bound[5]

Consider that a code is to be constructed having minimum distance d, an even number. An n-tuple is arbitrarily selected, and all $\binom{n}{d/2-1} \cdot (q-1)^{d/2-1}$ sequences at a distance of d/2 - 1 or less from it are deleted; the process is continued until the space is exhausted. Under the most favorable circumstances possible the entire space of q^n sequences would be completely filled with nonoverlapping spheres of radius d/2 - 1. Except for a few special combinations of M and n, a perfect solution to the sphere packing problem will not exist. The minimum distance for the code so constructed must be less than the smallest d for which:

A- 11) $M \cdot \binom{n}{d/2-1} \cdot (q-1)^{d/2-1} < q^n$

The asymptotic form of A-11 is:

A-12) $R = 1 - H_q(\delta/2) - (\delta/2)\log_q(q-1)$

The Gilbert Bound[6]

A procedure is now considered which must certainly lead to the construction of a code with minimum distance d. A sequence is arbitrarily selected, and all $\binom{n}{d}(q-1)^d$ sequences at a distance of d or less from it are deleted; the process is continued until the space is exhausted. We can certainly select M message vectors in this way if:

A-13) $(M-1) \binom{n}{d} \cdot (q-1)^d < q^n$

The asymptotic form of A-13) is:

A-14) $R = 1 - H_q(\delta) - \delta\log_q(q-1)$

Appendix B

The Sphere Packing Bound[5]

There are $\binom{n}{d}\cdot(q-1)^d$ sequences of weight d in the space of n-tuples over the field of q elements. n(1-R) parity check equations are capable of producing only $q^{n(1-R)}$ syndromes. Thus if:

$$\binom{n}{d}\cdot(q-1)^d > q^{n(1-R)}$$

at least two sequences have the same syndrome. The difference between these two sequences, a vector of weight $\leq 2d$, must be a code word, as its syndrome is the difference of the two syndromes, i.e., the vector of n(1-R) 0's. The minimum distance is upper-bounded by the smallest d satisfying the relation:

$$\text{B-1)} \quad \binom{n}{d/2}\cdot(q-1)^{d/2} > q^{n(1-R)}$$

The asymptotic form of B-1) is:

$$\text{B-2)} \quad R = 1 - H_q(\delta/2) - (\delta/2)\log_q(q-1)$$

The Gilbert Bound[6]

An exhaustive search procedure is now outlined which leads to the construction of a code with minimum distance of at least d and rate of at least R. First select any nonzero n(1-R)-tuple to be a column of the parity check matrix of the code. Then select any nonzero n(1-R)-tuple not a multiple of it as the next column. Continue in this manner, selecting the jth column so that it is not a linear combination of any d-2 or fewer columns already chosen. If this procedure is followed no d - 1 or fewer columns of the matrix finally constructed can be linearly related, i.e., no linear combination of d-1 or fewer columns can be equal to the vector of all zeros. Therefore no weight d-1 or less sequence may be a code word, and the code weight must be at least d. There certainly exists a code of block length n having a rate of at least R and a minimum distance of at least d if:

B-3) $$\sum_{j=1}^{d-2} \binom{n-1}{j} \cdot (q-1)^{j} < q^{n(1-R)} - 1$$

The asymptotic form of B-3) is:

B-4) $$R = 1 - H_q(\delta) - \delta \log_q(q-1)$$

Appendix C

Consider that messages are being sent over an eight level channel where the most likely form of error is a jump of $\pm$ 1 level modulo q. Figure C-1 below shows graphically these most likely error transitions:

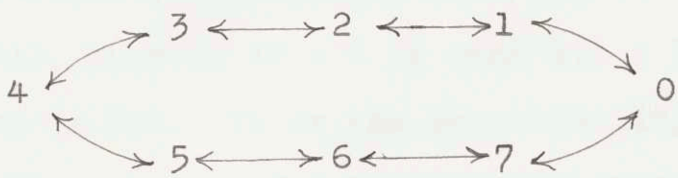


Figure C-1

A code of block length 3 correcting single errors of the type shown in figure C-1 can be designed so as to send any of 8^2 messages over the channel using a simple modulo 8 arithmetic check scheme. The first and second digits, a_1 and a_2, are information digits; the third digit is determined by $a_1 + 2a_2 + 3a_3=0$. Table C-1 below shows the simple way in which the syndrome of the single parity check equation is related to the error pattern imposed upon the transmitted message.

Table C-1

Syndrome	Error Pattern
0	no error
1	+ 1 level in first digit
2	+ 1 level in second digit
3	+ 1 level in third digit
5	- 1 level in third digit
6	- 1 level in second digit
7	- 1 level in first digit

If we tried using GF(8) checking arithmetic we would find it impossible to construct a code having two information digits and only one check digit capable of correcting single errors of $\pm$ 1 level. This is due to the structure of the additive group of GF(8), which is shown as Table C-2 below. It is seen that if the transmitted sequence is distorted by virtue of the first digit being changed from a 2 to a 3, the error pattern is 500, whereas if a 4 is sent and a 5 received the error pattern is 700. It is the impossibility of classifying all the likely variants of a transmitted message as being due to a small number of "added on" error patterns which makes the problem insoluble under GF(8) checking arithmetic.

Table C-2 The Additive Group of GF(8)

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	4	7	2	6	5	3
2	2	4	0	5	1	3	7	6
3	3	7	5	0	6	2	4	1
4	4	2	1	6	0	7	3	5
5	5	6	3	2	7	0	1	4
6	6	5	7	4	3	1	0	2
7	7	3	6	1	5	4	2	0

References

1) Fano, R.M., Transmission of Information, The M.I.T. Press and John Wiley & Sons, Inc., New York (1961).

2) Peterson, W.W., Error-Correcting Codes, The M.I.T. Press and John Wiley & Sons, Inc., New York (1961).

3) van der Waerden, B.L., Modern Algebra (2 volumes), translated by F. Blum and T.J. Benac, Frederick Ungar Publishing Co., New York (1949, 1950).

4) Plotkin, M., "Binary Codes with Specified Minimum Distance," IRE Trans., IT-6, 445-450 (1960).

5) Hamming, R.W., "Error Detecting and Error Correcting Codes," Bell System Technical Journal, 29, 147-160 (1950).

6) Sacks, G.E., "Multiple Error Correction by Means of Parity Checks," IRE Trans., IT-4, 145-147 (1958).