BINARY SET FUNCTIONS AND PARITY CHECK MATRICES

W.E. CLARK
Department of Mathematics, University of South Florida, Tampa, Florida 33620, USA

L.A. DUNNING*
Department of Computer Science, Bowling Green State University, Bowling Green, Ohio 43403, USA

D.G. ROGERS
Fernley House, The Green, Croxley Green, United Kingdom, WD3 3HT

Received 8 March 1988
Revised 26 August 1988

We consider the possibility of extending to a family of sets a binary set function defined on a subfamily so that the extension is, in fact, uniquely determined. We place in this context the problem of finding the least integer \( n(r) \) such that every linear code of length \( n \) with \( n \geq n(r) \), dimension \( n - r \) and minimum Hamming distance at least 4 has a parity check matrix composed entirely of odd weight columns and answer this problem by showing that \( n(r) = 5 \cdot 2^{r-4} + 1, \quad r \geq 4. \)

This result is applied to yield new constructions and bounds for unequal error protection codes with minimum distances 3 and 4.

1. Introduction

Let \( N_r = \{1, 2, \ldots, r-1\} \) if \( r > 1 \) and \( N_1 = \emptyset \). The parity of a subset \( A \) of \( N_r \) is the number of elements in \( A \) modulo 2, which we denote by \( |A|_2 \), the number of elements itself being denoted as usual by \( |A| \). We consider functional definitions of the parity of a subset through the study of parity system defined as follows.

Let \( \mathcal{F} \) be a family of subsets of \( N_r \), with subfamily \( \mathcal{F}^* \subseteq \mathcal{F} \); and let \( \pi: \mathcal{F} \rightarrow \mathbb{Z}_2 \), where \( \mathbb{Z}_2 \) denotes the integers modulo 2. Then the pair \((\mathcal{F}, \pi)\) is said to be a parity system with base \( \mathcal{F}^* \) when

\[
\begin{align*}
(1) \quad & \pi(A) = |A|_2 \quad \text{for all } A \subseteq \mathcal{F}^*; \text{ and} \\
(2) \quad & \pi(A \oplus B) = \pi(A) + \pi(B) \quad \text{whenever } A, B \text{ and } A \oplus B \in \mathcal{F},
\end{align*}
\]

where \( A \oplus B \) denotes the symmetric difference of the sets \( A \) and \( B \). In (2), as will frequently be the case, addition in \( \mathbb{Z}_2 \) is implied by the context.

The function \( \pi \) may be thought of as a generalization of the standard parity function. These systems arose in the study of a problem in coding theory which we describe below. In that context the parameter \( r \) represents the redundancy of

* Dr. Dunning's work was supported in part by the Center for Microelectronics Design and Test, College of Engineering, University of South Florida, Tampa, Florida 33620.

a linear code. The number \( \delta \) of subsets of \( N \), not in \( \mathcal{F} \) will be called the deficiency of the system.

Of course (1) and (2) are satisfied for any \( \mathcal{F} \) and \( \mathcal{F}^* \) if the function \( \pi \) truly gives the parity of the sets \( \mathcal{F} \), that is if

\[
\pi(A) = |A|, \quad \text{for all } A \in \mathcal{F}.
\]

A system in which (3) holds will be said to be a standard system; otherwise the system \( (\mathcal{F}, \pi) \) is said to be non-standard, as is any subset \( A \in \mathcal{F} \) for which (3) fails. We observe that for given redundancy \( r \), if the deficiency is sufficiently small and the base \( \mathcal{F}^* \) in some sense generates \( \mathcal{F} \) in that the values of \( \pi \) on \( \mathcal{F}^* \) determine the values of \( \pi \) on \( \mathcal{F} \). In this case, the system has to be standard, or, put another way, (3) gives the unique extension of (1) through application of (2).

To make this observation more exact, we introduce the notion of a \((\delta, r)\)-parity system: a \((\delta, r)\)-parity system is a parity system with redundancy \( r \), deficiency \( \delta \) and base consisting of the empty set and the singletons.

Note that for a \((\delta, r)\)-parity system we always have \( 0 \leq \delta \leq 2^{r-1} - r \), since \( \mathcal{F} \) contains at least \( r \) sets. It is easy to check that if \( 1 \leq r \leq 3 \), \( \delta = 0 \) or \( \delta = 2^{r-1} - r \) then every \((\delta, r)\)-parity system is standard. Suppose a non-standard \((\delta, r)\)-parity system \((\mathcal{F}, \pi)\) exists with \( \delta < 2^{r-1} - r \), \( r > 4 \). Let \( A_0 \in \mathcal{F} \) denote a set for which (3) does not hold. If \( \delta + 1 < 2^{r-1} - r \), a non-standard \((\delta + 1, r)\)-parity system \((\mathcal{F}', \pi)\) may be derived by letting \( \mathcal{F}' \) be \( \mathcal{F} \) with any non-basis set other than \( A_0 \) removed. This shows that for a fixed redundancy \( r \) all \((\delta, r)\)-parity systems are standard until \( \delta \) grows to a certain cutoff value, say, \( \delta(r) \) and for all larger \( \delta < 2^{r-1} - r \) examples of non-standard \((\delta, r)\)-parity systems exist. This establishes the easy part of our main result on these systems:

**Theorem 1.** If \( 1 \leq r \leq 3 \), then every \((\delta, r)\)-parity system is standard. If \( r \geq 4 \) there exists an integer \( \delta(r) \) such that if \( \delta' < 2^{r-1} - r \), then every \((\delta', r)\)-parity system is standard if and only if \( \delta' \leq \delta(r) \). The number \( \delta(r) \) is given by

\[
\delta(r) = 3 \cdot 2^{r-4} - 1.
\]
Binary set functions and parity check matrices

$n(r)$ such that if $n' > r$, then every binary $(n', n' - r, 4)$ code has an odd weight column parity check matrix if and only if $n' \geq n(r)$. The number $n(r)$ is given by

$$n(r) = 5 \cdot 2^{-r} + 1.$$

The extended Hamming code employing $r$ parity check bits has length $2^{r-1}$ and protects exactly $2^{r-1} - r$ message bits. However, in practice, applications seldom call for the protection of exactly $2^{r-1} - r$ message bits. The extended Hamming code may be shortened before use by striking columns corresponding to some of its information bits from the parity check matrix. However, in some cases there are codes of the same length and redundancy that may be preferable to using a shortened extended Hamming code. Of course, if $n$ is sufficiently small relative to fixed redundancy $r$ there are codes of length $n$ with minimum distance 5 or greater. However, even without such drastic rate reduction it may be possible to correctly determine one (or possibly more) of the message bits (positions fixed in advance) despite the occurrence of two random errors. When, as in this case, the chosen message position is provided protection beyond that guaranteed by the minimum distance of the code, then that message position and the code are said to be endowed with unequal error protection (UEP). Unequal error protection [1, 5] will be addressed in greater detail in Section 5.

Consider the class of binary linear codes with a fixed number of check bits (redundancy) $r$. The extended Hamming code is the longest $d = 4$ code and has length $n = 2^{r-1}$, but it provides no additional error protection (UEP) for any of its message digits. The question arises as to how large $n$ can be and allow a code with UEP and $d = 4$. In Section 5 we answer this question by deducing from Theorem 2 that if $4 \leq r \leq n \leq 5 \cdot 2^{-r}$ then either there exists an $(n, n - r, 4)$ code with UEP or there exists an $(n, n - r, d \geq 5)$ code. Conversely, if $n > 5 \cdot 2^{-r}$ there are no $(n, n - r, 4)$ codes with UEP. A similar result is obtained for $(n, n - r, d)$ codes with $d = 3$. Define $UEP(r, d) = n + 1$ where $n$ is largest integer such that there exists an $(n, n - r, d)$ code with UEP. Then $UEP(r, d)$ will be seen to be well defined for $d = 3$ and $d = 4$ and these results can be stated as follows:

**Corollary 1.** $UEP(r, 4) = 5 \cdot 2^{-r} + 1$ for $r \geq 4$.

**Corollary 2.** $UEP(r, 3) = 5 \cdot 2^{-r-1}$ for $r \geq 4$.

We begin, in Section 2, by showing that Theorems 1 and 2 are essentially equivalent and that

$$n(r) + \delta(r) = 2^{r-1} \quad \text{for } r \geq 4,$$

by relating parity check matrices and parity systems. In Sections 3 and 4 we complete our proof of Theorem 1 by bounding $\delta(r)$ above and below so as to determine it as in (4) and so also to determine $n(r)$. 

Our interest in odd weight column codes was stimulated by a detailed study (to be reported elsewhere) of a code in [2] which has certain byte error detecting capabilities and for which knowing that an odd weight column parity check matrix is available is of considerable help. The theorems are of independent interest in that they deal, in a sense, with the connectedness of the graph of the hypercube. The applications to unequal error protection were discovered later.

2. Parity check matrices and parity check systems

Consider a binary linear code $C$ of length $n$, dimension $k$ and minimum distance at least 4; and writing $r = n - k$ (so that $r$ is the redundancy of the code), let the $r$ by $n$ matrix $H$ be a parity check matrix for $C$. For $r \geq 1$, since $H$ is a matrix of rank $r$, there are $r$ linearly independent columns $h_i$, $1 \leq i \leq r$, among the columns of $H$. Thus if $h$ is any column of $H$, then $h$ is a linear combination of the columns $h_i$, $1 \leq i \leq r$. For a subset $A$ of $N_r = \{1, \ldots, r-1\}$, we write

$$h(A) = \sum_{i \in A} h_i.$$  \hfill (5)

Note that all vector additions and scalar-vector products are over $\mathbb{Z}_2$. If $h(A)$ and $h(A) + h$, are both columns of $H$, then the columns $h_i$, $h(A)$ and $h(A) + h$, are linearly dependent, showing that $C$ has minimum distance less than 4, a contradiction. Hence, for any column $h$ of $H$, there is a unique subset $A$ of $N_r$ and a unique binary value $n(A)$ determined by $A$ and not depending on $h$ such that

$$h = h(A) + (1 + n(A)) \cdot h_r.$$ \hfill (6)

This implies first of all, that

$$n \leq 2^{r-1},$$ \hfill (7)

as there are $2^{r-1}$ subsets of $N_r$.

To continue from (6), let $\mathcal{F}$ be the family of sets $A$ arising in this representation of the columns of $H$, and let $\pi$ be the binary function obtained on $\mathcal{F}$ through representing the columns in this way. We see that, as $h_i$, $1 \leq i \leq r$, is a column of $H$,

$$(i) \in \mathcal{F}, \quad \pi(\{i\}) = 1, \quad 1 \leq i < r; \quad \emptyset \in \mathcal{F}, \quad \pi(\emptyset) = 0.$$ \hfill (8)

Further, if $A$, $B$ and $A \oplus B$ are in $\mathcal{F}$, then the associated columns of $H$ are linearly independent lest the minimum distance of the code be less than 4. But, from (5),

$$h(A \oplus B) = h(A) + h(B).$$

So, to ensure that these columns are independent, we must have

$$1 + \pi(A \oplus B) \neq (1 + \pi(A)) + (1 + \pi(B))$$

whenever $A$, $B$ and $A \oplus B \in \mathcal{F}$. 

that is,
\[ \pi(A \oplus B) = \pi(A) + \pi(B) \]  
whenever \( A, B \) and \( A \oplus B \in \mathbb{F} \). \hfill (9)

We therefore see from (7)-(9) that \( (\mathbb{F}, \pi) \) is a \((\delta, r)\)-parity system with \( \delta = 2^{r-1} - n \geq 0 \).

If the \((\delta, r)\)-parity system \( (\mathbb{F}, \pi) \) is standard then
\[ \pi(A) = |A|_2, \quad A \in \mathbb{F}, \]
and (6) implies that every column of \( H \) is a linear combination of an odd number of the columns \( h_i, 1 \leq i \leq r \). Of course, since these vectors themselves are not assumed to be of odd weight, no conclusion follows about the weight of the other columns. However, applying suitable row operations to \( H \) as necessary, we may obtain another \( r \) by \( n \) parity check matrix \( H^* \) for \( C \), where in place of the columns \( h_i, 1 \leq i \leq r \), we now have the standard basis vectors \( e_i, 1 \leq i \leq r \), which are of odd weight. The columns of \( H^* \), being linear combinations of an odd number of these replacements, have odd weight. Thus \( C \) has a parity check matrix with odd weight columns. This has shown that if every \((\delta, r)\)-parity system \( (\mathbb{F}, \pi) \) with \( \delta = 2^{r-1} - n \geq 0 \) is standard, then every linear code with length \( n \), dimension \( n - r \) and minimum distance at least 4 has a parity check matrix with odd weight columns.

In the opposite direction, beginning with a \((\delta, r)\)-parity system \( (\mathbb{F}, \pi) \) for \( r \geq 1 \), let \( h_i, 1 \leq i \leq r \), be \( r \) linearly independent, \( r \)-dimensional binary column vectors and introduce further column vectors by (compare (6))
\[ h = h(A) + (1 + \pi(A)) \cdot h_r, \] \hfill (10)
where \( h(A) \) is as in (5). Consider the matrix \( H \) with these \( n = 2^{r-1} - \delta \) vectors \( h \) as columns. Because the base of the system \( (\mathbb{F}, \pi) \) consists of the empty set and the singletons, the vectors \( h_i, 1 \leq i \leq r \), are themselves among the columns of \( H \), so that \( H \) has rank \( r \). Hence \( H \) is the parity check matrix of some binary linear code \( C \) of length \( n = 2^{r-1} - \delta \) and dimension \( k = n - r \).

The columns of \( H \) are distinct non-zero vectors, so the code \( C \) has minimum distance at least 3. Let \( A, B \in \mathbb{F} \), and consider the sum of the columns of \( H \) associated with \( A \) and \( B \):
\[ h(A) + (1 + \pi(A)) \cdot h_r + h(B) + (1 + \pi(B))h_r, \]
\[ = h(A \oplus B) + (\pi(A) + \pi(B))) \cdot h_r. \] \hfill (11)
If \( A \oplus B \) is not in \( \mathbb{F} \), then the vector in (11) is not a column of \( H \) by the definition of \( H \) given in (10). On the other hand, if \( A \oplus B \in \mathbb{F} \), then from (2)
\[ \pi(A) + \pi(B) = \pi(A \oplus B), \]
so the vector in (11) is not of the right form (10) to be a column of \( H \). Hence the sum of two columns of \( H \) is never equal to a column of \( H \) and the code \( C \) has minimum distance at least 4.
Now assume that $C$ has an odd weight column parity check matrix $H^*$. We may write $H^* = M \cdot H$ where $M$ is an $r$ by $r$ invertible matrix. This has the effect of replacing the basis vectors $h_i$ by odd weight columns $M \cdot h_i$, and a column (10) by an odd weight column

$$M \cdot h = \sum_{i \in A} M \cdot h_i + (1 + \pi(A))M \cdot h_r.$$ 

This implies that $\pi(A) = |A|_2$ for $A \in \mathcal{F}$ and so $(\mathcal{F}, \pi)$ is standard, Thus, the reverse implication that if every linear code with length $n$, dimension $n-r$ and minimum distance at least 4 has a parity check matrix with odd weight columns, then every $(\delta, r)$-parity system $(\mathcal{F}, \pi)$ with $\delta = 2^{r-1} - n \geq 0$ is standard has been shown.

This completes our discussion of the equivalence of linear codes with length $n$, dimension $n-r$ and minimum distance at least 4 and $(\delta, r)$-parity systems where $\delta = 2^{r-1} - n$, showing that such codes have odd weight column parity check matrix whenever the corresponding systems are standard. We summarize our discussion in Lemma 1 which, in turn, implies the equivalence of Theorems 1 and 2.

**Lemma 1.** (i) Every linear code of length $n$, dimension $n-r$ and minimum distance at least 4 has a parity check matrix with odd weight columns if and only if every $(\delta, r)$-parity system is standard where $\delta = 2^{r-1} - n$, $r \geq 1$.

(ii). the quantities $\delta(r)$ and $n(r)$ are related by:

$$\delta(r) + n(r) = 2^{r-1}, \quad r \geq 4.$$

Examination shows that for $1 \leq r \leq 3$, every $(\delta, r)$-parity system is standard and every $(n, n-r, 4)$ binary code has an odd weight column parity check matrix. So in these cases $\delta(r)$ and $n(r)$ are irrelevant.

In the subsequent sections we turn to the cases where $r \geq 4$.

**3. Lower bound for $n(r)$**

A parity check matrix is said to be in standard form if it contains the identity matrix among its columns. Any parity check matrix of full row rank can be placed in standard form via elementary row operations. We say that a matrix is uneven if it is in standard form and contains some columns of even weight. This terminology is suggested by the fact that a linear code has at least one uneven parity check matrix precisely when it contains at least one codeword of odd weight. It is also easy to see that a linear code has no odd weight column parity check matrix if and only if it has an uneven parity check matrix. These
Proposition 1. The following statements regarding a binary linear code \( C \) are equivalent:

(i) The codewords of \( C \) are all of even weight.

(ii) The overall parity check \( \mathbf{1} \) (the all ones vector) is a member of the dual code \( C^\perp \).

(iii) There exists a parity check matrix \( H \) for \( C \) whose columns are all of odd Hamming weight.

(iv) Every standard form parity check matrix for \( C \) is composed entirely of odd weight columns (is not uneven).

As a consequence, to establish lower bounds for \( n(r) \) it suffices to exhibit \( r \) by \( n \) uneven matrices of rank \( r \), no three columns of which are linearly dependent, for then \( n(r) > n \). The examples in Fig. 1 have all these properties so we have:

Lemma 2. \( n(4) > 5; n(5) > 10 \).

A familiar construction for codes allows us to deduce the following recursive bound.

Lemma 3. If \( n(r) > n \), then \( n(r + 1) > 2 \cdot n \).

Proof. Let \( C \) be a binary linear code of length \( n \), dimension \( n - r \) and minimum distance at least 4 with \( r \) by \( n \) parity check matrix \( H \). Consider the \( r + 1 \) by \( 2 \cdot n \) matrix \( H^* \) formed by taking two copies of \( H \) side by side, one copy bordered by an additional row of zeroes and the other by an additional row of ones:

\[
H^* = \begin{pmatrix} H & \mathbf{0} \\ \mathbf{1} & \mathbf{1} \end{pmatrix}
\]

Then \( H^* \) is of rank \( r + 1 \) and no three columns are linearly dependent. So \( H^* \) is the parity check matrix of a binary linear code \( C^* \) of length \( 2 \cdot n \), dimension \( 2 \cdot n - r - 1 \) and minimum distance at least 4.

If now \( n(r) > n \), then we may choose \( H \) to be uneven. While \( H^* \) is not uneven, replacing the penultimate row of \( H^* \) by the sum of its last two rows, gives an
uneven matrix $H^t$ which is also a parity check matrix for $C^*$. Hence $n(r + 1) > 2 \cdot n$, which proves the lemma. □

Taking Lemmas 2 and 3 together yields for $r \geq 4$, a lower bound for $n(r)$ and so, through Lemma 1(ii), an upper bound for $\delta(r)$.

**Lemma 4.** For $r \geq 4$,
\[
n(r) > 5 \cdot 2^{r-4}; \quad \delta(r) < 3 \cdot 2^{r-4}.
\]

It is interesting to note although the bounds in Lemma 2 are related as in Lemma 3 for $r = 4$, the matrix in Fig. 1(b) does not result from applying the doubling construction in the proof of Lemma 3 to the matrix in Fig. 1(a). So, for $r \geq 5$, there are at least two families of examples leading to the bounds in Lemma 4.

The construction in the proof of Lemma 3 may be interpreted in terms of parity systems in view of the equivalence established in Section 2. We record without proof in Lemma 5 a version in terms of parity systems.

**Lemma 5.** Let $(\mathcal{F}, \pi)$ be a $(\delta, r)$-parity system and define a family of subsets $\mathcal{G}$ of $N_{r+1}$ and a binary function $\rho$ on $\mathcal{G}$ by
\[
A, A \cup \{r\} \in \mathcal{G}, \quad A \in \mathcal{F};
\]
\[
\rho(A) = \pi(A), \quad \rho(A \cup \{r\}) = 1 + \pi(A), \quad A \in \mathcal{G}.
\]
Then
\begin{enumerate}
\item $(\mathcal{G}, \rho)$ is a $(2 \cdot \delta, r + 1)$-parity system;
\item $(\mathcal{G}, \rho)$ is standard if and only if $(\mathcal{F}, \pi)$ is standard.
\end{enumerate}

4. Lower bound for $\delta(r)$

Our first lemma in this section is a technical result which provides the inductive step in an argument leading to a lower bound for $\delta(r)$. The idea is to try to determine $\pi(A)$ for successively larger sets $A$ in $\mathcal{F}$ by being able to reach out further and further not just from sets in the base but from all sets in $\mathcal{G}$ about which we already know.

**Lemma 6.** Let $r - 1 \geq m \geq 2$; and suppose that $(\mathcal{F}, \pi)$ is a $(\delta, r)$-parity system such that
\[
\pi(A \oplus B) = \pi(A) + \left| B \right|_2 \quad \text{whenever } A, A \oplus B \in \mathcal{F} \text{ and } |B| < m. \quad (12)
\]
Then
\begin{enumerate}
\item $\pi(A) = |A|_2$ when $A \in \mathcal{F}$ and $|A| \leq m$; \quad (13)
\item if $r - 2 \geq m \geq 2$ and $\delta < 2^{r-m-2} \cdot (2^m - 1)$, \quad (14)
\end{enumerate}
then $\pi(A \oplus B) = \pi(A) + |B|_2$ whenever $A, A \oplus B \in \mathcal{F}$ and $|B| \leq m$. \quad (15)
The previous lemma is crucial and our central results rest directly upon it. However, the proof is lengthy and in the interest of readability we give it in the Appendix. Instead, in our next lemma, we give a sufficient condition for a \((\delta, r)\)-parity system to be standard: this condition allows Lemma 6 to be used inductively to show that (12) and so also (13) hold for \(m = r - 2\). We obtain in this way bounds for \(\delta(r)\), and so for \(n(r)\), which taken together with Lemma 4 determine these quantities as in Theorems 1 and 2, so that those theorems are then proved.

**Lemma 7.** (i) Let \(r \geq 4\); and suppose that \((F, \pi)\) is a \((\delta, r)\)-parity system such that \(\delta < 3 \cdot 2^{-r}\). Then \((F, \pi)\) is a standard parity system.

(ii) For \(r \geq 4\),
\[
\delta(r) \geq 3 \cdot 2^{-r} - 1; \quad n(r) \leq 5 \cdot 2^{-r} + 1.
\]

**Proof.** (i). Suppose that \((F, \pi)\) is a \((\delta, r)\)-parity system with \(\delta < 3 \cdot 2^{-r}\) and \(r \geq 4\). As
\[
2^{r-m-2} \cdot (2^m - 1) \geq 3 \cdot 2^{-r} \quad \text{when } r - 2 \geq m \geq 2,
\]
it follows that (14) holds for all \(m\) with \(r - 2 \geq m \geq 2\). Moreover (12) holds for \(m = 2\) since the base of \((F, \pi)\) consists of the empty set, the singletons and from (2),
\[
\pi(A \oplus B) = \pi(A) + \pi(B); \quad \pi(B) = |B|_2 \quad \text{when } A, A \oplus B \in F, \ |B| < 2.
\]
So suppose that (12) holds for some \(m\) with \(r - 2 \geq m \geq 2\). Then by Lemma 6(ii), (15) holds for \(m\), that is (12) holds for \(m\) replaced by \(m + 1\). Hence, by induction, (12) holds for \(m = r - 1\). but then, by Lemma 6(i), (13) holds for \(m = r - 1\), which is to say that \((F, \pi)\) is a standard parity system as asserted since for any set \(A\) in \(F\), \(|A| \leq r - 1\).

(ii) This follows immediately from (i). \(\square\)

5. Application to unequal error protection codes

The unequal error protection provided by an \((n, k)\) binary linear code is measured by its separation vector \([1, S]\). Let \(wt(v)\) denote the Hamming weight of a vector \(v\). The protection provided the \(i\)th message bit is measured by the \(i\)th component of the \(k\)-component separation vector \(S(G)\) which is given by
\[
S(G)_i = \min\{wt(mG) : m \in GF(2)^k, m_i = 1\}.
\]

The protection provided depends upon the generator matrix \(G\) as well as the code \(C\). The degree of protection \(S(G)_i\) provided an individual message bit \(m_i\) is interpreted in a manner analogous to minimum Hamming distance. It is known
that the minimum distance \( d \) of the code is equal to the smallest component of \( S(G) \). It is usually assumed that the rows of \( G \) have been permuted as required so that \( S(G)_i \geq S(G)_{i+1} \geq \cdots \geq S(G)_k \). Two generator matrices for the same code can then be compared by the rule \( S(G) \geq S(G') \) if and only if \( S(G)_i \geq S(G')_i \), for all \( i = 1, \ldots, k \). Given a linear code \( C \), if there exists a generator matrix \( G \) for \( C \) such that \( S(G)_i > d \) for some \( i \), then \( C \) is said to have unequal error protection (UEP). For some codes \( S(G)_i = d \) for all \( i \) and for all \( G \) and in this case we say that \( C \) has no UEP. A UEP code may be shortened by deleting a carefully chosen single column and row from a generator matrix which has been placed in a particular canonical form yielding the following result whose proof may be found in van Gils [5].

**Theorem 3** [5, Theorem 8]. Given an \( k \) by \( n \) generator matrix \( G \) with separation vector \( S(G) \) satisfying \( S(G)_i \geq \cdots \geq S(G)_k \), there exists an \((k - 1)\) by \((n - 1)\) generator matrix \( G' \) with separation vector \( S(G') \) satisfying

\[
S(G') \geq (S(G)_1, \ldots, S(G)_{k-1}).
\]

Consider the class \( \mathcal{C}(r, d) \), with \( r \geq 2, d \geq 2 \), of all binary \((n, k, d)\) codes with fixed redundancy \( r = n - k \) and minimum distance \( d = d(n, k) \) where \( d(n, k) \) is the largest obtainable minimum distance for a binary \((n, k)\) code. It is easy to see that \( d(n, k) \geq d(n + 1, k + 1) \) and hence the lengths \( n \) of the codes in \( \mathcal{C}(r, d) \) form some interval which we denote as \( m(r, d) \leq n \leq M(r, d) \). Now it follows from Theorem 3 that if there exists a code of length \( n \) in \( \mathcal{C}(r, d) \) with UEP and \( m(r, d) \leq n' \leq n \), then there exists a code in \( \mathcal{C}(r, d') \) of length \( n' \) with UEP. Hence there is an integer \( UEP(r, d) \leq M(r, d) \) such that there exists a code of length \( n \) in \( \mathcal{C}(r, d) \) with UEP if and only if

\[
m(r, d) \leq n < UEP(r, d).
\]

It may happen that none of the codes in \( \mathcal{C}(r, d) \) have UEP, in which case \( UEP(r, d) = m(r, d) \).

As was pointed out in Section 2, an \((n, n - r, 4)\) code satisfies \( n \leq 2^{r-1} \) and an \((n, n - r, 3)\) code, as is well-known, satisfies \( n \leq 2^{r} \). Thus for \( d = 2, 3, 4 \) we have:

\[
m(r, 2) = 2^r + 1, \quad M(r, 2) = \infty.
\]

\[
m(r, 3) = 2^{r-1} + 1, \quad M(r, 3) = 2^r.
\]

\[
m(r, 4) = \text{unknown}, \quad M(r, 4) = 2^{r-1}.
\]

For a few small values of \( r \) and \( d \) the values of \( m(r, d) \) and \( M(r, d) \) can be obtained from reading down the diagonals in the tables of Verhoeff [6]. Aside from the above, no general results are known although there are numerous bounds in the literature. As stated in Section 1 the numbers \( UEP(r, d) \) for \( d = 3 \) and \( 4 \) are determined by the following corollaries of Theorem 2:

**Corollary 1.** \( UEP(r, 4) = 5 \cdot 2^r + 1 \) for \( r \geq 4 \).

Corollary 2. UEP\((r, 3) = 5 \cdot 2^{r-3}\) for \(r \geq 4\).

Corollaries 1 and 2 can also be reformulated in terms of the separation vector to give Corollaries 3 and 4 which follows. Under certain conditions, Corollary 3 guarantees the existence of a code with minimum distance \(d \geq 4\) providing additional error protection for at least one message bit which must be chosen in advance. The chosen message bit will be decoded correctly despite any two random errors. Similarly, Corollary 4 guarantees additional protection for one message bit beyond that provided by a minimum distance 3 code. Whenever two random errors occur, the selected message bit will either be decoded correctly or an error will be detected. Even when this message bit is decoded correctly, other message bits may be decoded incorrectly.

Corollary 3. The exists an \((n, k)\) linear code \(c\) and generator matrix \(G\) utilizing \(n - k = r \geq 4\) check bits having \(S(G) \geq (5, 4, \ldots, 4)\) if and only if
\[
n \leq 5 \cdot 2^{r-4}.
\]

Corollary 4. There exists an \((n, k)\) linear code \(C\) and generator matrix \(G\) utilizing \(n - k = r \geq 3\) check bits having \(S(G) \geq (4, 3, \ldots, 3)\) if and only if
\[
n \leq 5 \cdot 2^{r-3} - 1.
\]

We establish Corollary 1 first and then use it to prove Corollary 2. The following lemma makes the connection between Theorem 2 and UEP.

Lemma 8. An \((n, k)\) binary linear code \(C\) with even minimum distance \(d\) which has an odd weight codeword \(c^*\) has UEP, i.e. has a generator matrix \(G\) with separation vector:
\[
S(G) \geq (d + 1, d, \ldots, d).
\]

Proof. Let \(c_1, \ldots, c_{k-1}\) be a basis for the \(k - 1\) dimensional subspace of even weight vector of \(C\). Suppose that \(C\) is encoded using the generator matrix \(G\) given by
\[
G = \begin{pmatrix}
    c^* \\
    c_1 \\
    \vdots \\
    c_{k-1}
\end{pmatrix}.
\]

Any nontrivial linear combination of rows of \(G\) has weight \(d\) implying that \(S(G)_i \geq d\) for \(i = 1, \ldots, k\). Any linear combination of rows of \(G\) involving \(c^*\) has odd weight at least \(d\) and since \(d\) is even at least \(d + 1\) implying that \(S(G)_i \geq d + 1\). This proves the lemma. \(\Box\)
**Proof of Corollary 1.** Applying Lemma 8, the codes of Lemmas 2 and 3 have the required nonconstant separation vectors when \( n = 5 \cdot 2^{-4} \). These codes can be shortened by eliminating message positions using Theorem 3 to obtain nonconstant separation vectors for \( n < 5 \cdot 2^{-4} \) while holding \( r \) fixed. Suppose \( n > 5 \cdot 2^{-4} \) and that a linear code \( C \) with \( d = 4 \) and generator matrix \( G \) with \( S(G) \geq (5, 4, \ldots, 4) \) exists. Applying Theorem 2 it follows that \( C \) is composed entirely of codewords of even weight. Thus, it follows that \( S(G) \geq (6, 4, \ldots, 4) \). Let \( \hat{G} \) be a generator matrix derived from \( G \) by changing one entry in the first row of \( G \) from 1 to 0. Denote the rows of \( \hat{G} \) by \( \hat{g}_1, \hat{g}_2, \ldots, \hat{g}_k \). The code generated by \( \hat{G} \) has odd weight codewords since \( \hat{g}_1 \) is of odd weight. This new code will violate Theorem 2 because it has minimum distance 4 and contains an odd weight codeword. To see this note that any message with \( m_1 = 0 \) encodes into the same codeword as before and hence has Hamming weight at least 4. Any message with \( m_1 = 1 \) will differ from its encoding in the original code in at most one bit position. Since such a codeword in the original code has weight at least 6, in the revised code it has weight at least 5. This completes the proof. \( \square \)

Corollary 2 can be obtained from Corollary 1 as a direct consequence of the following lemma:

**Lemma 9.** Let \( d \geq 1 \). There exists an \((n, k)\) code with redundancy \( r = n - k \) and separation vector

\[
S(G) \geq (2d + 1, 2d, \ldots, 2d) \tag{16}
\]

if and only if there exists an \((n - 1, k)\) code with redundancy \( r - 1 = n - k - 1 \) and separation vector

\[
S(G') \geq (2d, 2d - 1, \ldots, 2d - 1). \tag{17}
\]

**Proof.** Given a generator matrix \( G \) satisfying (16), a generator matrix \( G' \) satisfying (17) may be obtained by merely dropping a column from the generator matrix \( G \). The matrix \( G' \) will have maximal row rank since no nontrivial linear combination of its rows can be zero (or have weight less than \( 2d - 1 \)).

Conversely, suppose that a generator matrix \( G' \) satisfying (17) is given. Denote the rows of \( G' \) by \( g'_1, \ldots, g'_k \). Denote the parity of a vector \( v \in GF(2)^{n-1} \) by \( \rho(v) \). The desired matrix \( G \) satisfying (16) will be given by

\[
G = \begin{pmatrix}
g'_1 & 1 + \rho(g'_1) 
g'_2 & \rho(g'_2) 
\vdots & \vdots 
g'_k & \rho(g'_k)
\end{pmatrix}.
\]

Because the weights of rows 2 through \( k \) of \( G \) are even, any nontrivial linear combination of these rows will have even weight at least \( 2d - 1 \) and hence weight
at least $2d$. Any linear combination of rows of $G$ involving the first row will have weight at least $2d$ since that was true of $G'$ which is a submatrix. However, since the first row of $G$ has odd weight, any such linear combination will have odd weight and hence weight at least $2d + 1$. This completes the proof. □

A slight refinement of the arguments of Lemma 9 can be used to obtain a nearly equivalent result in terms of the UEP function:

**Proposition 2.** For $r \geq 2$ and $d \geq 2$ $\text{UEP}(r - 1, 2d - 1) = \text{UEP}(r, 2d) - 1$.

Codes of length $n$, redundancy $r$ and separation vector of the form $(4, 3, 3, \ldots, 3)$ may also be constructed using a variant of the recursive Hamming code construction as follows: For $r = 3$ and $k = 1$ take the generator matrix $G = (1 \ 1 \ 1 \ 1)$. Given a generator matrix $G$ determining a code of length $n$, redundancy $r > 3$, and separation vector $(4, 3, 3, \ldots, 3)$, define the generator matrix $G'$ for a $(2n + 1, k + n)$ code with redundancy $r + 1$ by

$$G' = \begin{pmatrix} G & 0_{k \times n} & 0_{k \times 1} \\ I_{n \times n} & I_{n \times n} & 1_{n \times 1} \end{pmatrix},$$

where constant and identity matrices have been subscripted with their sizes for clarity.

It is easy to see that $\text{UEP}(r, 2) = \infty$ for $r \geq 2$. For a few small values of $r$ and $d$, $\text{UEP}(r, d)$ may be obtained from van Gil's Table I [5]. Examination of the data in van Gil's table provokes a number of questions. For example, one might ask whether or not every code of maximal length in the class $\mathfrak{C}(r, d)$ has a constant separation vector (no UEP).

**Appendix: Proof of Lemma 6**

Let $r - 1 \geq m \geq 2$; and suppose that $(\mathcal{F}, \pi)$ is a $(\delta, r)$-parity system such that

$$\pi(A \oplus B) = \pi(A) + |B|_2 \quad \text{when } A, A \oplus B \in \mathcal{F} \text{ and } |B| < m. \quad (12)$$

**(i) Proof of (13).** We now suppose that $A$ is a set in $\mathcal{F}$ with $m$ or fewer elements and prove that

$$\pi(A) = |A|_2 \quad \text{when } A \in \mathcal{F} \text{ and } |A| \leq m. \quad (13)$$

If $|A| = 0$, that is $A$ is empty, then (13) holds since the base of the system contains the empty set. On the other hand, if $|A| > 0$, so $A$ is non-empty, take an element $a$ in $A$. Then the base of the system contains $\{a\}$ and $|A \setminus \{a\}| < m$. On appealing to (12), we have

$$\pi(A) = \pi(\{a\}) + |A \setminus \{a\}|_2,$$

from which (13) follows straightforwardly. □
(ii) Proof of (15). In proving (15), we suppose throughout that
\[ \delta < 2^{r-2} \cdot (2^m - 1), \]  
\[ (14) \]
and that \( A \) and \( A \oplus B \) are sets in \( \mathcal{F} \) where \( B \) is a set of \( m \) elements with \( r - 2 \geq m \geq 2 \). By considering various cases we show that
\[ \pi(A \oplus B) = \pi(A) + |B|_2. \]
\[ (18) \]
We find several occasions to use the following observations. For all sets \( Z \) and \( B \)
\[ |Z|_2 + |B|_2 = |Z \oplus B|_2. \]
\[ (19) \]
If \( Z \) is a proper subset of \( B \), then, from (12),
\[ \pi(W \oplus Z) = \pi(W) + |Z|_2 \quad \text{when} \ W, W \oplus Z \in \mathcal{F}. \]
\[ (20) \]
Finally, if \( Z \) is a non-empty proper subset of \( B \), then so is \( Z \oplus B \).

**Case (a) – \( A \) is a subset of \( B \).** If \( A \) is a subset of \( B \), then so is \( A \oplus B \) and,
\[ |A| \leq m; \quad |A \oplus B| \leq m. \]
As both \( A \) and \( A \oplus B \) are supposed to be in \( \mathcal{F} \), it follows from (13) that
\[ \pi(A) = |A|_2; \quad \pi(A \oplus B) = |A \oplus B|_2. \]
But also, from (19),
\[ |A|_2 + |B|_2 = |A \oplus B|_2. \]
by combining these equations, we obtain (18) in this case.

**Case (b) – \( A \) is not a subset of \( B \).** We now suppose that \( A \) is not a subset of \( B \) and consider the class \( \mathcal{A} \) of pairs \( \{X, Y\} \) of subsets \( X \) and \( Y \) of \( N_r \), such that
\[ A = X \oplus Y. \]
\[ (21) \]
For any subset \( X \) of \( N_r \), there is a unique \( Y \), namely \( Y = A \oplus X \), such that \( X \) and \( Y \) satisfy (21); this \( Y \) is distinct from \( X \) because our supposition that \( A \) is not contained in \( B \) means in particular that \( A \) is not empty. It follows therefore that the members of \( \mathcal{A} \) partition the \( 2^{r-1} \) subsets of \( N_r \) into distinct pairs, so that \( \mathcal{A} \) has \( 2^{r-2} \) members.

If \( \{X, Y\} \) is in \( \mathcal{A} \), then so is \( \{X \oplus Z, Y \oplus Z\} \) for any subset \( Z \) of \( N_r \). Thus, for any pair \( \{X, Y\} \) in \( \mathcal{A} \), we may form the subclass \( \mathcal{A}(X, Y) \) of \( \mathcal{A} \) consisting of the pairs \( \{X \oplus Z, Y \oplus Z\} \), for \( Z \) a subset of \( B \). If \( Z^* \) is a subset of \( B \), then
\[ \mathcal{A}(X, Y) = \mathcal{A}(X \oplus Z^*, Y \oplus Z^*), \]
\[ (22) \]
from which we see that such subclasses are either identical or disjoint and so give a partition of \( \mathcal{A} \).

Let \( Z_1 \) and \( Z_2 \) be distinct subsets of \( B \). Clearly for any subset \( X \) of \( N_r \), \( X \oplus Z_1 \neq X \oplus Z_2 \). Further if (21) holds then \( X \oplus Z_1 \neq Y \oplus Z_2 \), for otherwise
A \neq Z_1 \oplus Z_2$, contradicting the prevailing assumption that \( B \) does not contain \( A \). We conclude that \( \{X \oplus Z_1, Y \oplus Z_1\} \) and \( \{X \oplus Z_2, Y \oplus Z_2\} \) are distinct members of \( \mathcal{A}\{X, Y\} \) and hence that there are as many members of such subclasses as there are subsets of \( B \), that is \( 2^m \) members. Therefore \( \mathcal{A} \) is partitioned into \( 2^{r-m-2} \) subclasses of the form \( \mathcal{A}\{X, Y\} \).

Note that underlying a subclass \( \mathcal{A}\{X, Y\} \) of \( \mathcal{A} \) is the family of sets \( X \oplus Z \) and \( Y \oplus Z \) for \( Z \) a subset of \( B \); we denote this family by \( \mathcal{C}\{X, Y\} \). The family \( \mathcal{C}\{X, Y\} \) has \( 2^{m+1} \) distinct sets since \( X \oplus Z_1 = Y \oplus Z_2 \) for \( Z_1, Z_2 \) distinct subsets of \( B \) would imply \( A = X \oplus Y = Z_1 \oplus Z_2 \subseteq B \) and \( A \) is not contained in \( B \).

Now in view of (14), (at least) one of the \( 2^{m-r-2} \) disjoint subclasses in the partition of \( \mathcal{A} \), say \( \mathcal{A}\{X, Y\} \), is such that fewer than \( 2^m - 1 \) of the \( 2^{m+1} \) sets in \( \mathcal{C}\{X, Y\} \) are not in \( \mathcal{F} \). In particular, there is a subset \( Z^* \) of \( B \) such that \( X^* = X \oplus Z^* \) and \( Y^* = Y \oplus Z^* \) are both in \( \mathcal{F} \) since there are \( 2^m \) disjoint pairs of sets of these forms contained in \( \mathcal{C}\{X, Y\} \). Appealing to (22) and replacing \( X \) and \( Y \) respectively by \( X^* \) and \( Y^* \) as necessary, we obtain a subclass \( \mathcal{A}\{X, Y\} \) of \( \mathcal{A} \) such that \( \mathcal{F} \) contains \( X \) and \( Y \) and all but at most \( 2^m - 2 \) of the other members of \( \mathcal{C}\{X, Y\} \). Restricting our attention to this particular subclass, we now complete the proof (18) for case (b) by showing it to hold in each of three subcases.

**Subcase (b1) - \( X \oplus B \) not in \( \mathcal{F} \).** Suppose that \( X \oplus B \) is one of those sets in \( \mathcal{C}\{X, Y\} \) not in \( \mathcal{F} \). Then there is a non-empty proper subset \( Z \) of \( B \) such that \( X \oplus Z \) and \( Y \oplus (Z \oplus B) \) are both in \( \mathcal{F} \) because \( \mathcal{C}\{X, Y\} \) contains \( 2^m - 2 \) disjoint pairs of sets of these forms while with \( X \oplus B \) excluded there remain in \( \mathcal{C}\{X, Y\} \) at most \( 2^m - 3 \) sets not in \( \mathcal{F} \). Employing (20) and the observation that \( Z \oplus B \), as well as \( Z \), is a non-empty proper subset of \( B \), we have:

\[
\pi(X \oplus Z) = \pi(X) + |Z|_2 \\
\pi(Y \oplus (Z \oplus B)) = \pi(Y) + |Z \oplus B|_2.
\] (23) (24)

But, recalling (2) and (21), we also have

\[
\pi(A) = \pi(X) + \pi(Y); \\
\pi(A \oplus B) = \pi(X \oplus Z) + \pi(Y \oplus (Z \oplus B)),
\] (25) (26)

since all the sets mentioned in these equations are known to be in \( \mathcal{F} \). The equations (23)–(26) in conjunction with (19) enable us to compute \( \pi(A \oplus B) \) in terms of \( \pi(A) \):

\[
\pi(A \oplus B) = \pi(X \oplus Z) + \pi(Y \oplus (Z \oplus B)) \\
= \pi(X) + |Z|_2 + \pi(Y) + |Z \oplus B|_2 \\
= \pi(X) + \pi(Y) + |Z|_2 + |Z \oplus B|_2 \\
= \pi(A) + |B|_2,
\]

that is, (18) holds.
Subcase (b2) – \( Y \oplus B \) not in \( \mathcal{F} \). By argument similar to subcase (b1), we find that (18) holds if \( Y \oplus B \) is not in \( \mathcal{F} \).

Subcase (b3) – \( X \oplus B \) and \( Y \oplus B \) both in \( \mathcal{F} \). To complete our proof, suppose that \( X \oplus B \) and \( Y \oplus B \) are in \( \mathcal{F} \). This time there is a non-empty, proper subset \( Z \) of \( B \) such that (at least) one of \( X \oplus Z \) or \( Y \oplus Z \) is in \( \mathcal{F} \) since altogether there are \( 2 \cdot (2^m - 2) \) such sets in \( \mathcal{C}\{X, Y\} \), yet fewer than \( 2^m - 1 \) of these are missing from \( \mathcal{F} \). Interchanging \( X \) and \( Y \) as necessary, we may assume without loss of generality that \( X \oplus Z \) is in \( \mathcal{F} \). Thus, in these circumstances, we have (23) and (25) as before while (24) and (26) are replaced by

\[
\pi(X \oplus B) = \pi(X \oplus Z) + |Z \oplus B|_2, \quad \pi(A \oplus B) = \pi(X \oplus B) + \pi(Y).
\]

However, we are still able to use these equations with (19) to compute \( \pi(A \oplus B) \) in terms of \( \pi(A) \) and thereby confirm (18) in this case also.

The completion of these three subcases completes the proof of case (b) and in turn completes the proof of Lemma 6. □

Remarks on the above proof. Note that if the sets \( X \oplus Z \), for \( Z \) a non-empty proper subset of \( B \), together with \( Y \oplus B \) are not in \( \mathcal{F} \) then the computations confirming (18) just mentioned cannot be carried out for want of information. So if at least \( 2^m - 1 \) sets of any family \( \mathcal{C}\{X, Y\} \) are not in \( \mathcal{F} \) the method of our proof fails, showing that (14) is the best possible in terms of the arguments presented here. The examples discussed in Section 3 in which \( \delta = 3 \cdot 2^r - 4 \) are such that, for \( m = 2 \), (12) holds but (15) does not (converting the parity check matrices to parity systems as in Lemma 5). So no other argument will suffice to weaken (14), (15) for \( m = 2 \). However, this is not so in general,

Consider, for example, the case \( m = r - 2 \). If (12) holds, then, by (13),

\[
\pi(A) = |A|_2 \quad \text{when} \quad A \in \mathcal{F} \quad \text{and} \quad |A| \leq r - 2. \tag{27}
\]

If \( \delta < 2^{r-1} - r - 1 \), then there is a subset \( A^* \) in \( \mathcal{F} \) with \( 2 \leq |A^*| \leq r - 2 \). So if \( N_r \) is in \( \mathcal{F} \) then \( |N_r \oplus A^*| \leq r - 2 \) and by (18) and (27),

\[
\pi(N_r) = \pi(A^*) + |N_r \oplus A^*|_2 = |A^*|_2 + |N_r \oplus A^*|_2 = |N_r|_2.
\]

Hence, if \( \delta \leq 2^r - r - 1 \), then the system is standard since (15) holds for \( m = r - 1 \). On the other hand, if \( \mathcal{F} \) consists of the empty set, the singletons, and \( N_r \), and

\[
\pi(A) = |A|_2, \quad A \neq N_r; \quad \pi(N_r) = 1 + |N_r|_2,
\]

then \( (\mathcal{F}, \pi) \) is a non-standard \((\delta, r)\)-parity system with \( \delta = 2^r - r - 1 \). These facts seem to indicate that it is the case \( m = 2 \) which is crucial in setting a lower bound on \( \delta(r) \).
References


