Using Codes for Error Correction and Detection
TORLEIV KLOVE

Abstract—A linear code \( C \) over \( \mathbb{F}_q \) is good for \( t \)-error-correction and error detection if \( P(C,t;\epsilon) \leq P(C,t;(q-1)/q) \) for all \( \epsilon, 0 \leq \epsilon \leq (q-1)/q \), where \( P(C,t;\epsilon) \) is the probability of an undetected error after a codeword in \( C \) is transmitted over a \( q \)-ary symmetric channel with error probability \( \epsilon \) and correction is performed for all error patterns with \( t \) or fewer errors. A sufficient condition for a code to be good is derived. This sufficient condition is easy to check, and examples to illustrate the method are given.

I. INTRODUCTION

To control transmission errors in a data communication system, one can use a code in three ways: purely for error detection, purely for error correction, or for a combination of error correction and detection. Error-correcting codes have been widely studied, e.g., see [1]. Less is known about error-detecting codes and codes for both error correction and detection; some papers are [2]-[12]. Here we study the probability of undetected error when a code is used both for error correction and error detection. This continues work started in [2].

II. THE PROBABILITY OF UNDETECTED ERROR

We transmit symbols from the field \( \mathbb{F}_q \) over a channel; the probability that a sent symbol is received correctly is \( 1 - \epsilon \), and the probability that it is transformed into a particular one of the other \( q - 1 \) symbols is \( \epsilon/q - 1 \). Let \( C \) be a linear code of length \( n \) and dimension \( k \) over \( \mathbb{F}_q \). Let \( d = d(C) \) denote the minimum (Hamming) distance of \( C \), and let \( t \) be an integer, \( 0 \leq t < d/2 \). The code is used to correct all error patterns with \( t \) or fewer errors. Let \( P(C,t;\epsilon) \) denote the probability that after decoding there remains an undetected error. In particular, \( P(C,0;\epsilon) \) is the probability of having an undetected error when \( C \) is used purely as an error-detecting code.

It is well-known that

\[
P(C,t;\epsilon) = (1 - \epsilon)^n \sum_{j = d - t}^{n} \frac{n!}{j!(n-j)!} \frac{\epsilon^{j}}{(1 - \epsilon)^{(q - 1)j}},
\]

(2.1)

where \( A_{j} \) is the number of vectors of weight \( j \) that are within distance \( t \) of some codeword [3]. For \( \epsilon = (q - 1)/q \) (the "worst case channel") we get

\[
P(C,t;(q - 1)/q) = V_r(q^k - 1)/q^k,
\]

where \( V_r \) is the volume of a sphere of radius \( t \), i.e.,

\[
V_r = \sum_{i = 0}^{t} \binom{n}{i} (q - 1)^i.
\]

(2.2)

We say that a code \( C \) is \( t \)-good if

\[
P(C,t;\epsilon) \leq P(C,t;(q - 1)/q),
\]

for all \( \epsilon, 0 \leq \epsilon \leq (q - 1)/q \). (2.3)

A code is "good" if it is \( t \)-good for all \( t \), \( 0 \leq t < d/2 \).

Note that the definition of \( 0 \)-good differs slightly from the definitions of "good for error detection" given in [4] and [5].

In general, it is difficult to decide even if a given code is \( 0 \)-good or not. It is an open question for which values of \( n \) and \( k \) there exist \( 0 \)-good \((n,k)\)-codes. It has been shown that some classes of codes are \( 0 \)-good. These include the binary perfect codes, their dual codes, distance-5 primitive Bose-Chaudhuri-Hocquenghen (BCH) codes, distance-4 extended Hamming codes, and distance-6 extended primitive BCH codes [4] [8]. Kasami and Lin [5] recently showed that maximum-distance-separable (MDS) codes are good. These results were proved by showing that the codes in question satisfy some condition that is sufficient for a code to be \( t \)-good. One such sufficient condition is that \( P(C,t;\epsilon) \) is a monotonically increasing function of \( \epsilon \) in the interval \( [0,(q - 1)/q] \). The result on MDS codes, for instance, was shown in this way. In [4] we gave another sufficient condition in terms of the weight distribution of a binary even-weight code for it to be \( 0 \)-good. In Section III we give still another such sufficient condition that applies to all codes for all \( q \) and \( t \).

It has been shown [3], [9] that given \( q, n, k \), and \( \epsilon \), there exists an \((n,k)\) code \( C \) over \( \mathbb{F}_q \) such that

\[
P(C,0;\epsilon) \leq q^{k-n}(1 - (1 - \epsilon)^n).
\]

(2.4)

We note that the right-hand expression is an increasing function of \( \epsilon \), and that for \( \epsilon = (q - 1)/q \) it equals \( P(C,0;(q - 1)/q) \). In particular,

\[
P(C,0;\epsilon) \leq P(C,0;(q - 1)/q).
\]

(2.5)

We note, however, that the code \( C \) for which (2.4) is true depends on the particular \( \epsilon \), whereas a \( 0 \)-good code satisfies the bound for all \( \epsilon \). Moreover, the result is an existence result; it tells us nothing about how to find the code. There are a couple of similar results that sometimes sharpen the result (2.4); given \( q, n, k \), and \( \epsilon \), there exists an \((n,k)\) code \( C \) over \( \mathbb{F}_q \) such that

\[
P(C,0;\epsilon) \leq \frac{q^k - 1}{q^n - 1}(1 - (1 - \epsilon)^n),
\]

(2.6)

and even such that

\[
P(C,0;\epsilon) < \frac{q^k - 1}{q^n - 1}(1 + (q - 1)(1 - \epsilon^q/(q - 1)))
\]

(2.7)

For \( q = 2 \), (2.6) is due to Levenshtein [10] and (2.7) is due to Kasami et al. [4]. The proof for general \( q \) appears in [11]. The methods we develop herein give sufficient conditions for a code to satisfy these bounds and similar bounds for \( t > 0 \), for all \( \epsilon, 0 \leq \epsilon \leq (q - 1)/q \).

III. SUFFICIENT CONDITIONS FOR \( t \)-GOOD CODES

We use the following notations:

\[
E = \sqrt{(q - 1)},
\]

(3.1)

\[
D = 1 - \epsilon q/(q - 1),
\]

(3.2)

\( C \) is an \((n,k)\) code over \( \mathbb{F}_q \), \( A_0, A_1, A_2, \cdots \) is the Hamming weight distribution of \( C \), and \( B_0, B_1, B_2, \cdots \) is the Hamming weight distribution of the dual of \( C \). We consider the following condition, which may or may not be satisfied for particular \( C \) and \( t \):

\[
\Pi(\tau,t;\epsilon):\ 
\]

(3.3)

where

\[
\Pi(n,k,t,\tau;\epsilon) = \frac{q^k - 1}{q^n - 1} \left( 1 + (\tau - 1)D^n - \tau (1 - \epsilon)^n \right).
\]

(3.4)

For \( t = 0 \) and a fixed \( \epsilon \), this reduces to (2.6) and (2.7) when \( \tau = 1 \) and \( \tau = q \), respectively. In the following lemma, we summarize some of the properties of \( \Pi(n,k,t,\tau;\epsilon) \) whose straightforward proofs are omitted.
Lemma 1:

a) \( P(C, t; \epsilon) = \Pi(n, k, t; \epsilon) \) for \( \epsilon = 0 \) and \( \epsilon = (q - 1)/q \).

b) For any fixed \( \tau \), \( 0 \leq \tau \leq q \), \( \Pi(n, k, t; \epsilon) \) is an increasing function of \( \epsilon \) on \([0, (q - 1)/q]\).

c) For any fixed \( \epsilon \), \( 0 \leq \epsilon \leq (q - 1)/q \), \( \Pi(n, k, t; \epsilon) \) is a decreasing function of \( \tau \) on \((-\infty, \infty)\).

d) For \( 0 \leq \tau < q \), \( \Pi(n, k, t; \epsilon) = o(r) \) when \( \epsilon \to 0 \).

e) \( \Pi(n, k, t; \epsilon) = o(\epsilon^2) \) when \( \epsilon \to 0 \).

Combining a) and b) of Lemma 1, we get the following theorem, which is our reason for considering the \( \Pi(\tau, t) \)-condition.

**Theorem 1:** If \( C \) satisfies the \( \Pi(\tau, t) \)-condition for some \( \tau \), \( 0 \leq \tau \leq q \), then \( C \) is t-good.

It is a stronger condition for a code \( C \) to satisfy the \( \Pi(\tau, t) \)-condition for some \( \tau \geq 0 \) than to be t-good. However, unless \( \epsilon \) is small, \( \Pi(n, k, t; \epsilon) \) is close to \( P(C, t; (q - 1)/q) \). When \( \epsilon = 1/n \), for instance, we get \( \Pi(n, k, t; \epsilon) = O(n^2 \epsilon^2) \) when \( \epsilon \to 0 \).

Define \( \gamma(C, s, j) \) by

\[
\gamma(C, s, j) = \sum_{i=0}^{s} A(i, n, s, j) (q - 1)^i (1 - \epsilon)^{s-i}. 
\]

MacWilliams [12] gave expressions that imply that for \( s < d/2 \)

\[
\sum_{j=0}^{n} \alpha(C, s, j) = z^j 
\]

Substituting (3.9) in (2.1) and equating the right-hand sides of (2.1) and (3.3), we get, after some simple transformations,

\[
\Gamma(C, t, j) = \sum_{s=0}^{t} \gamma(C, s, j). 
\]

Starting from (3.11), we get, in the same way,

\[
\gamma(C, s, j) = q^{-n+k+1} \sum_{i=0}^{s-j} B(i, n, s, j) (q - 1)^i (1 - \epsilon)^{s-i}. 
\]

and from (2.1) we get

\[
\Gamma(C, t, j) = \sum_{m=d-t}^{j} (n-m) A_{n, m}. 
\]
Theorem 2: Let $t < d/2$ and let $0 \leq \tau \leq q$. The code $C$ satisfies the $\Pi(\tau,t)$-condition if $\Gamma(C,t,j) \leq \Delta(n,k,t,\tau,j)$ for $d - t < j < n$, where
\[
\Delta(n,k,t,\tau,j) = V_t^{\tau} q_j - 1, \quad (q^j - \tau), \quad \text{for } 0 < j < n,
\]
\[
\Gamma(C,t,j) = \sum_{m=d-t}^{j} \binom{n-m}{j-m} A_t,m - \sum_{u=0}^{d-t} \sum_{s=0}^{d-t} \binom{s}{d-t} A_t,s
\]
\[
= q^{n-k} \sum_{i=0}^{t} \binom{n-i}{j} \Psi(i,n,s) - \sum_{j=s}^{t} \binom{n-s}{j} (q-1)^j.
\]
and
\[
\Psi(i,n,s) = \sum_{j=s}^{t} \binom{n-i}{j} (q-1)^j \sum_{j=s}^{t} \binom{n-i}{j} (q-1)^j.
\]

Theorems 1 and 2 in combination give the promised criterion for $t$-goodness.

IV. CHECKING A CODE FOR THE $\Pi(\tau, t)$-CONDITION

We now take a closer look at $\Gamma$ and $\Delta$, introduce some new notations that make it easier to describe computations, and give some examples.

Lemma 3: Let $0 < j < n$. Then
a) $\Delta(n,k,t,\tau,j)$ is a decreasing function of $\tau$ on $(-\infty, q^n)$,
b) $\lim_{\tau \to -\infty} \Delta(n,k,t,\tau,j) = V_t(\tau^t - 1) \binom{n}{j}$,
c) $\Gamma(C,t,j) < V_t(\tau^t - 1) \binom{n}{j}$,
d) There exists a unique $\tau < q^n$ such that $\Gamma(C,t,j) = \Delta(n,k,t,\tau,j)$, let $C(t,j)$ denote this $\tau$.
e) $\Gamma(C,t,j) \leq \Delta(n,k,t,\tau,j)$, for $\tau \leq T(C,t,j)$.

Proof: a) and b) follow directly from (3.6). From (3.17) we get
\[
\Gamma(C,t,j) = \sum_{m=d-t}^{j} \binom{n-m}{j-m} A_t,m < \sum_{m=d-t}^{j} \binom{n-j}{j} A_t,m
\]
\[
= \binom{n}{j} V_t(\tau^t - 1),
\]
which proves c). Finally, d) follows directly from a)–c), and e) follows from a) and d).

Let $T(C,t) = \min \{ T(C,t,j) \mid 0 < j < n \}$.

Lemma 4: For any $t < d(C)/2$, $C$ satisfies the $\Pi(T(C,t),t)$-condition. In particular, if $T(C,t) > 0$, then $C$ is $t$-good.

Next we give a little lemma which, besides having some theoretical interest, also gives a useful check on the computations.

Lemma 5:

a) $T(C,t,j) = q^j$, for $1 \leq j < d - t$,
b) $T(C,0,j) = q^{n-k}$, for $n - d' < j < n$,
where $d' = d(C^\perp)$ is the minimum distance of the dual code.

Proof: a) For $j < d - t$, $\Gamma(C,t,j) = 0$, and so, by (3.6),
\[
\Gamma(C,0,j) = q^{n-k} B(n,j) \Psi(0,n,0) - \binom{n}{j}
\]
\[
= q^{n-k} \binom{n}{j} - \binom{n}{j}
\]
\[
= V_0 q^{n-k} - q^{n-k} - q^{n-k}
\]
\[
= \Delta(n,k,0,q^{n-k},j).
\]
Hence $T(C,0,j) = q^{n-k}$.

For MDS codes $d = n - k + 1$ and $d' = k + 1$, i.e., $n - d' = n - k - 1$. Hence, we get the following theorem as an immediate consequence of Lemma 5.

Theorem 3: MDS codes satisfy the $\Pi(q,0)$-condition (provided $0 < k < n$).

Theorem 3 implies that MDS codes are 0-good. As mentioned above, Kasami and Lin [5] have shown the stronger result that MDS codes are good. Their result does not imply Theorem 3, however.

We have written a program that, from a code $C$, computes $T(C,t,j)$ and $T(C',t,j)$ for all $t$ and $j$. We have run the program for a number of codes. Examples of the results follow.

Example 1: For the $(27, 11)$ Golay code we found that $T(C, t)$ is $2$ for $t = 0, 1, 2, 3$. Therefore, from Lemma 4, we conclude that the Golay code is good. As mentioned before, it has been known that it is 0-good [6].

Example 2: For a $(27, 18)$ cyclic code we found that $T(C,0) = -132838.44$, $T(C',0) = -4304523.63$, and $T(C',1) = -3667107.05$. In particular, neither $C$ nor $C'$ satisfy the $\Pi(q,0)$-condition for any $t < d/2$ (resp. $t < d'/2$).

In all the examples we have computed, we have noted that for increasing $j$, either $T(C,t,j)$ is increasing for all $j$, or it is first increasing until $j = d' - t - 1$, then decreasing until some value of $j$, and then increasing again.

REFERENCES


codes," in Globecom '82, IEEE Global Telecommun. Conf., Miami, FL,

[9] V. I. Korzhik, "Bounds on undetected error probability and optimum
group codes in a channel with feedback," Radioelektronika, 20, vol. 1,
no. 1, pp. 87-92, Jan. 1965.)

