A survey on proper codes

Dedicated to the memory of our friend and colleague Levon Khachatrian.

R. Dodunekova
Mathematical Sciences
Chalmers University of Technology
and Göteborg University
412 96 Göteborg, Sweden

S. M. Dodunekov
Institute of Mathematics
Bulgarian Academy of Sciences
8 G. Bountchev Str.
1113 Sofia, Bulgaria

E. Nikolova
Computer Science
Bourgas Free University
101 Aleksandrovska Str.
8000 Bourgas, Bulgaria

1 Introduction

Since the introduction of the concept of a proper code in [31], it has been accepted in the literature that proper codes perform well in error control. This statement is supported by the definition of a proper code and also by the fact that, as we will see below, many codes known to be optimal in one sense or another turn out to be proper as well.

The performance of a linear error detecting code over a symmetric memoryless channel with symbol error probability ε is characterized by the probability that a transmission error will remain undetected. This probability is a function of ε and depends on the weight distribution of the code. To find a code with the smallest undetected error probability for a given channel, one has to use exhaustive search since at the present time a general method for finding such a code does not exist. But even if it did, the problem would still remain unresolved, since very often ε is not known exactly, and a code with the smallest undetected error probability for some ε' different from ε may not have the smallest undetected error probability for ε, even when ε' is very close to ε.

The situation just described is the reason for the introduction of the property of properness: A linear code is *proper*, if its undetected error probability is an increasing function of ε. Thus the smaller the symbol error probability of the channel, the better a proper code performs in error detection. Goodness of a linear code is a weaker version of properness: A linear code is *good*, if its undetected error probability is as large as possible for the largest possible value of ε. Thus a good code performs worst in the case of worst channel condition.

In order to establish properties like properness or goodness for a parametric class of codes, one could of course attempt to study the undetected error probability analytically. Unfortunately, because of the complexity of the formulas of the weight distribution and for other reasons, such a study has shown to be effective only in a small number of cases. For example, it works well for the Maximum Distance Separable (MDS) codes, shown in [26] to be proper, but does not seem to work for the Near MDS codes. These latter codes have been studied in [17] by a different approach which was later generalized in [18] and [19] to a method presenting discrete sufficient conditions for a code to be proper or good. Although these conditions are not necessary, codes known at that time to be proper, such as the MDS codes and the Hamming codes, have turned out to satisfy them, and also other well-known parametric classes and subclasses of codes, such as Maximum Minimum Distance (MMD) codes and their duals, some Near MDS codes, and some Cyclic Redundancy-Check (CRC) codes have been shown to satisfy these sufficient conditions, see [2]–[7], [15], [17], [21], [22], and [27]. In particular, it has been shown in [27] that some non-standardized CRC codes are proper, while some standardized CRC codes are not even good.

The sufficient conditions mentioned above for a linear code to be proper are expressed in terms of certain numbers which, following [16], we refer to as *the extended binomial moments* of the code. The extended binomial moments are related synonymously to the code weight distribution and linearly to the binomial moments of the code introduced in [36]. In contrast to the latter, the extended binomial moments form a monotone sequence which, as we will see, makes them very appropriate for study of the undetected error probability. We note that [18] and [19] present sufficient conditions for goodness as well, also in terms of the extended binomial moments of the code.

The situation with error detection described above remains essentially the same when the code is used to correct errors over a symmetric memoryless channel with symbol error probability ε. The probability that a code correcting at most t symbol errors will miss a transmission error is a function of ε involving the code weight distribution together with the weight distributions of the cosets of minimum weight at most t. When the undetectable error probability is an increasing function of ε, the code is called *t-proper*. The MDS codes are examples of t-proper codes, as shown in [26], and this seems to be the only case of effective analytical study of t-properness. Another approach to this questions is the one of [20], presenting discrete sufficient conditions for t-properness, efficiently used in [2] and [7] for the study of some binary cyclic and ternary cyclic and negacyclic codes.

The sufficient conditions for t-properness are formulated in terms of certain numbers, determined by the code weight distribution and the weight distributions of the cosets of minimum weight at most t. Since these numbers become the extended binomial moments when $t = 0$, which is just the case of error detection, we will refer to them as the *t-extended binomial moments.*

After some preliminary material in Section 2, the present paper presents known sufficient conditions for properness with examples in Section 3, and in Section 4 a list of codes that are known at the presents time to be proper, many of which have been studied by the conditions in Section 3. In Section 5 special attention is paid the CRC codes, which are of real practical interest in modern communication.

For notions and results from Coding Theory used below we refer to the monographs [30], [33], and [36].

2 Preliminaries

Let C be a linear $[n, k, d]_q$ code over the finite field of q elements $GF(q)$, i.e., a k-dimensional subspace of the n-dimensional vector space $GF(q)^n$ over $GF(q)$, with minimum Hamming distance d. Suppose C is used for error detection on a discrete memoryless channel with q inputs and q outputs. Any symbol transmitted has a probability $1 - \varepsilon$ of being received correctly and a probability $\frac{\varepsilon}{q-1}$ of being transformed into each of the $q - 1$ other symbols. It is natural to assume that $0 \leq \varepsilon \leq \frac{q-1}{q}$. Such a channel model is called a q-ary symmetric channel and in the case $q = 2$ a binary symmetric channel.

Let $x \in C$ be the codeword transmitted and $y = x + e \in GF(q)^n$ be the vector received, where $e = y - x$ is the error vector resulting from the channel noise. If $e \notin C$, then $y \notin C$ and the decoder will discover the presence of an error. When $e \in C$, then $y = x + e \in C$ as well, and in this case the decoder will accept y as error free. Clearly, when $e \neq 0$ this decision is wrong, and such an error will thus remain undetected. In this way, the probability that the decoder fails to detect the existence of an error equals the probability that an undetectable error occurs, called the undetected error probability and denoted by $P_{ue}(C, \varepsilon)$. This probability is expressed in terms of the weight distribution $\{A_i,\ 0 \leq i \leq n\}$ of C and the weight distribution $\{B_i,\ 0 \leq i \leq n\}$ of $C^\perp$, the orthogonal (dual) code of C, as

$$P_{ue}(C, \varepsilon) = \sum_{i=1}^{n} A_i \Big(\frac{\varepsilon}{q-1}\Big)^i (1-\varepsilon)^{n-i}, \tag{2.1}$$

and

$$P_{ue}(C, \varepsilon) = q^{-(n-k)} \sum_{i=0}^{n} B_i \Big(1 - \frac{q\varepsilon}{q-1}\Big)^i - (1-\varepsilon)^n \tag{2.2}$$

respectively (see, for example, [33], p. 66).

To evaluate $P_{ue}(C,\varepsilon)$ by use of (2.1) and (2.2) is equivalent to determine the weight distribution of C. This is known to be a hard computational problem for large basic code parameters n, k, d, and q (see [36], Ch. 5, and [9]), and the exact weight distribution has been found only for a few classes of codes. A natural way to decide if the code C is suitable for error detection is to compare $P_{ue}(C,\varepsilon)$ with the average probability of undetected error $P_{ue}(\varepsilon)$ for the ensemble of all q-ary $[n,k]$ codes. It is known that

$$P_{ue}(\varepsilon) = q^{-(n-k)}[1-(1-\varepsilon)^k]$$

(see [46], for binary codes and [37]).

For the worst channel condition, i.e., when $\varepsilon = \frac{q-1}{q}$, the above and (2.1) give

$$P_{ue}\Big(\frac{q-1}{q}\Big) = q^{-(n-k)} - q^{-k} = P_{ue}\Big(C, \frac{q-1}{q}\Big) \tag{2.3}$$

for any q-ary $[n,k]$ code C.

Definition 1. A code C is *proper* for error detection if $P_{ue}(C,\varepsilon)$ is an increasing function of ε in the interval $[0, \frac{q-1}{q}]$.

Definition 2. A code C is *good* for error detection if $P_{ue}(C,\varepsilon) \leq P_{ue}(C, \frac{q-1}{q})$ for all ε in the interval $[0, \frac{q-1}{q}]$.

Note that a proper code is good as well. As (2.3) shows, the probability of undetected error of an $[n,k,d]_q$ proper or good code does not exceed the average undetected error probability for the ensemble of all q-ary $[n,k]$ codes for the worst channel condition.

The above ideas easily generalize to the case of error correction. Suppose an $[n,k,d]_q$ code C is used to correct t or fewer symbol errors over a q-ary symmetric channel, where $d \geq 2t+1$. For $x \in GF(q)^n$, let $V(t,x)$ denote the set of all $y \in GF(q)^n$ such that $d(x,y) \leq t$. Suppose $x' \in C$ is sent and $y \in GF(q)^n$ is received. Then one of the following cases may occur:

(i) $y \in V(t,x')$ and the decoder correctly decodes y into x'.

(ii) $y \notin V(t,x)$ for all $x \in C$ and the decoder detects an error.

(iii) $y \in V(t,x'')$ for some $x'' \in C$, $x'' \neq x'$, and the decoder incorrectly decodes y into x''. In this case the error is undetected.

Denote by $P_{ue}^{(t)}$ the probability of an undetectable error. Note that

$$P_{ue}^{(0)}(C,\varepsilon) = P_{ue}(C,\varepsilon).$$

Definition 3. An error correcting code C is *t-proper* if $P_{ue}^{(t)}(C,\varepsilon)$ is an increasing function of ε and *t-good* if

$$P_{ue}^{(t)}(C,\varepsilon) \leq P_{ue}^{(t)}\Big(C,\frac{q-1}{q}\Big)$$

for $\varepsilon \in [0,\frac{q-1}{q}]$.

It is easy to check that

$$P_{ue}^{(t)}\Big(C,\frac{q-1}{q}\Big) = (q^{-(n-k)} - q^{-n})V_q(t), \tag{2.4}$$

where $V_q(t)$ is the volume of the q-ary sphere of radius t in $GF(q)^n$.

Remark 1. As it is well known there is a relationship between the probability of undetected error for a linear code and for its dual code. In this regard an interesting question is how a property such as properness reflects the undetected error probability of the dual code. An example on p. 73 of the monograph [30] of Kløve and Korzhik shows that the dual of an proper code may not even be good.

Remark 2. A $(t-1)$-proper or $(t-1)$-good code may not be t-proper or t-good, as shown on pp. 98–99 of [30]. One may expect that a code that is t-proper or t-good is also $(t-1)$-proper or $(t-1)$-good, respectively, but this has not been shown to be true.

Remark 3. For a given matrix G, let C_G denote the code generated by G. The problem of computing $P_{ue}(C_G,p)$ as a function of a rational number p, and a generator matrix G, is an NP hard problem, as shown in [30], Theorem 3.9.1.

3 Discrete sufficient conditions for properness

As mentioned in the introduction, analytical study of the undetected error probability for properness or goodness has seldom been effective. It works for instance for the MDS codes, but not for the Near MDS codes. These latter and other classes of codes have been studied by using the discrete sufficient conditions for properness or goodness, obtained by Dodunekova and Dodunekov in [18] and [19].

The sufficient condition for properness or goodness of an $[n,k,d]_q$ code C are expressed in terms of certain numbers $\{A_0^*, A_1^*, \ldots, A_n^*\}$, synonymously related to the code weight distribution $\{A_0, A_1, \ldots, A_n\}$ of C as

$$A_0^* = 0, \quad A_\ell^* = \sum_{i=1}^{\ell} \frac{\ell_{(i)}}{n_{(i)}} A_i, \quad \ell = 1,2,\ldots,n, \tag{3.1}$$

where $j_{(i)}$ denotes the i-th factorial moment $j(j-1)\dots(j-i+1)$. Since

$$A_\ell^* = \frac{1}{\binom{n}{\ell}} \sum_{i=1}^{\ell} \binom{n-i}{n-\ell} A_i = \frac{A_\ell'}{\binom{n}{\ell}}, \quad \ell = 1, 2, \dots, n,$$

where A_ℓ', $\ell = 1, 2, \dots, n$, are the binomial moments of the code weight distribution, introduced in the monograph of MacWilliams and Sloane [36] (but see also the works of Ashikhmin and Barg [1] and [8]), we refer to the numbers A_ℓ^* as the extended binomial moments of the code, following [16].

Clearly, $A_\ell^* = 0$ for $\ell = 0, \dots, d-1$, and the rest of the extended binomial moments are monotone, i.e.,

$$A_\ell^* > A_{\ell-1}^*, \quad \ell = d, d+1, \dots, n.$$

In fact, the monotonicity of the extended binomial moments makes them appropriate for study of the undetected error probability, and the work [16] takes advantage of this.

We can now give the following sufficient conditions for properness.

Theorem 3.1 *Let C be an $[n,k,d]_q$ error detecting code. If the extended binomial moments A_ℓ^* of C satisfy*

$$A_\ell^* \geq q A_{\ell-1}^*, \quad \ell = d+1, \dots n, \tag{3.2}$$

then C is proper [18].

Equivalently, the above sufficient conditions may be stated in terms of the extended binomial moments of the dual code.

Theorem 3.2 *Let C be an $[n,k,d]_q$ error detecting code. If the extended binomial moments B_ℓ^* of the dual code $C^\perp$ satisfy*

$$B_{n-\ell}^* \geq B_{n-\ell+1}^* - q^{n-k-\ell+1}, \quad \ell = d+1, \dots, n, \tag{3.3}$$

then C is proper [19].

When the code distance of $C^\perp$ or the number of non-zero weights in it is small, conditions (3.3) are technically more convenient to use than (3.2).

We notice that the works [18] and [19] mentioned above present also sufficient conditions for goodness, in terms of the extended binomial moments as well.

The proof of Theorem 3.1 is based on the next two lemmas from [18]. The first one expresses the undetected error probability in terms of the functions

$$R_i(z) = \binom{n}{i} z^i (1-z)^{n-i}, \quad i = 1, 2, \dots, n, \quad z \in [0,1],$$

and

$$L_\ell(z) = \sum_{j=\ell}^{n} R_j(z), \quad \ell = 1, 2, \dots, n, \quad z \in [0,1].$$

Lemma 3.1 *Set $z = \frac{q}{q-1}\varepsilon$. Then*

$$P_{ue}(C, \varepsilon) = P(C, z),$$

where

$$\begin{aligned} P(C, z) &= \sum_{\ell=d}^{n} q^{-\ell} A_\ell^* R_\ell(z) \\ &= q^{-d} A_d^* L_d(z) + \sum_{\ell=d+1}^{n} q^{-\ell}(A_\ell^* - qA_{\ell-1}^*) L_\ell(z). \end{aligned}$$

Lemma 3.2 *The functions $L_\ell(z)$, $\ell = 1, 2, \ldots, n$, are strongly increasing in $z \in [0, 1]$.*

It is now easily seen that Theorem 3.1 is a direct consequence of Lemma 3.1 and Lemma 3.2. Theorem 3.2 follows from Theorem 3.1 and the following relationship between the extended binomial moments of a code and its dual, shown in [19].

Lemma 3.3 *The extended binomial moments of C and $C^\perp$ are related by*

$$A_\ell^* + 1 = q^{\ell-n+k}(B_{n-\ell}^* + 1), \quad \ell = 0, 1, \ldots, n,$$

or, equivalently, by

$$B_\ell^* + 1 = q^{\ell-n}(A_{n-\ell}^* + 1).$$

We now give some short examples.

Example 1. The MDS codes are proper, as shown by analytical methods in Kasami and Lin [26]. In this case

$$P(C, z) = (q-1) \sum_{\ell=d}^{n} q^{-\ell} L_\ell(z)$$

and, obviously, the properness of the MDS codes follows as well from Lemmas 3.1-3.2 above.

Example 2. The Near MDS codes, introduced by Dodunekov and Landgev in [14], have been studied for properness in [17] by using the above technique. One particular result there is that if C is an $[n, k]_q$ Near MDS code with

$$A_{n-k} \leq (1 - q^{-1}) \binom{n}{k}, \tag{3.4}$$

then C is proper.

In fact, for such a code

$$P(C,z)=q^{(n-k)}\frac{A_{n-k}}{\binom{n}{k}}L_{n-k}(z)$$
$$+q^{-(n-k)}\Big[1-q^{-1}-\frac{A_{n-k}}{\binom{n}{k}}\Big]L_{n-k+1}(z)+\sum_{\ell=n-k+2}^{n}q^{-\ell}L_\ell(z)$$

and the properness is a direct consequence of (3.4) and Lemmas 3.1-3.2

Example 3. All $[n,k,d]_q$ codes with

$$qd\geq(q-1)n \tag{3.5}$$

are proper.

This statement follows easily from (2.1), where the terms $(\frac{\varepsilon}{q-1})^i(1-\varepsilon)^{n-i}$ are strongly increasing in $0\leq\varepsilon\leq\frac{i}{n}$, and (3.5), implying that $\frac{i}{n}\geq\frac{q-1}{q}$ for $d\leq i\leq n$. (See Kløve and Korzhik [30], p. 49, Theorem 3.1.4, for the binary case). On the other hand,

$$A_\ell^*-qA_{\ell-1}^*=\sum_{i=d}^{\ell-1}\frac{(\ell-1)\dots(\ell-i+1)}{n_{(i)}}A_i[\ell-(\ell-i)q]+\frac{A_\ell}{\binom{n}{\ell}}\geq 0,$$

since by (3.5)

$$\ell-(\ell-i)q=iq-\ell(q-1)\geq dq-n(q-1)\geq 0$$

and the properness thus also follows from Theorem 3.1.

Note that the MacDonald codes satisfy (3.5) with equality since for them

$$n=\frac{q^k-q^u}{q-1},\quad d=q^{k-1}-q^{u-1},\ \text{ and } 1\leq u\leq k-1.$$

(see MacDonald [34], Patel [43]).

The discrete sufficient conditions for properness of [18] have been generalized in [19] to the case of error correction. Assume that C is an $[n,k,d]_q$ code correcting t or fewer errors, where $d\geq 2t+1$, and let $P_h(\varepsilon)$ be the probability for undetectable transmission error with error vector in a coset of minimum weight h, where $0\leq h\leq t$. Letting $Q_{h,\ell}$ denote the number of vectors of weight ℓ in the cosets of minimum weight h, excluding the cosets leaders, we have, according to MacWilliams [35] and Kasami and Lin [26] that

$$P_h(\varepsilon)=\sum_{\ell=0}^{n}Q_{h,\ell}\Big(\frac{\varepsilon}{q-1}\Big)^\ell(1-\varepsilon)^{n-\ell}$$

and

$$P_{ue}^{(t)}(C,\varepsilon) = \sum_{h=0}^{t} P_h(\varepsilon).$$

Let

$$\{A_i^{(t)} : A_i^{(t)} = \sum_{h=0}^{t} Q_{h,i},\ i = t+1, \dots, n\}$$

be the weight distribution of the vectors in the cosets of minimum weight at most t, excluding the leaders. The sufficient conditions for C to be t-proper are expressed in terms of the *t-extended binomial moments* of the code defined as

$$A_{\ell,t}^{*} = \sum_{i=t+1}^{\ell} \frac{\ell_{(i)}}{n_{(i)}} A_i^{(t)}, \quad \ell = t+1, \dots, n. \tag{3.6}$$

Obviously, the t-extended binomial moments $A_{t+1,t}^{*}, A_{t+2,t}^{*}, \dots, A_{n,t}^{*}$ are strictly increasing. The following theorem has been proven by Dodunekova and Dodunekov in [20].

Theorem 3.3 *Let C be an $[n,k,d]_q$ error correcting code. If the $t-$extended binomial moments $A_{\ell,t}^{*}$ of C satisfy*

$$A_{\ell,t}^{*} \geq q A_{\ell-1,t}^{*}, \quad \ell = t+2, \dots, n,$$

then C is t-proper.

Note that when $t = 0$, the case reduces to error correction and $A_{\ell,0}^{*}$ become the extended binomial moments A_{ℓ}^{*} from (3.1). Easy to see that Theorem 3.3 reduces in this case to Theorem 3.1.

4 A list of proper codes

Perfect codes

All perfect codes over finite fields, i.e., the repetition codes of odd length, the Hamming codes, the binary and ternary Golay codes, their extended codes and their dual codes are proper, see [30] and [32] for details.

Reed-Muller codes ([36])

Let $R(r,m)$ be the r-th order Reed-Muller code. Kløve [28] showed that

- The $R(0,m)$ and $R(1,m)$ codes are proper for $m \geq 1$.
- The $R(r,r)$, $R(r,r+1)$, and $R(r,r+2)$ codes are proper for $r \geq 0$.
- The $R(2,5)$ code is proper.
- The rest of $R(r,m)$ codes are not good.

BCH codes

The primitive binary t-error correcting BCH codes have been investigated intensively. The results are as follows:

- The primitive binary 2-error correcting BCH codes are proper ([31]).
- The primitive binary 3-error correcting BCH codes of length $2^m - 1$ and their extended codes are proper for m odd ([42]).
- For m even, neither the 3-error correcting BCH codes nor their extended are proper ([44]).

Maximum Distance Separable codes

The MDS codes are proper ([26]).

Near MDS codes

An $[n,k,d]_q$ code C is a Near MDS code if $d + d^{\perp} = n$ ([14], see also [10]). The parameters of C and $C^{\perp}$ are respectively $[n,k,n-k]_q$ and $[n,n-k,k]_q$.

The error detecting performance of Near MDS codes has been studied in [17], [22], and [29]. The following is known.

Theorem 4.1 *An $[n,k]_q$ Near MDS code is proper for error detection if and only if*

$$A_{n-k} \leq \min_{1-\frac{k}{n} \leq z \leq 1} (q-1) \frac{z}{z - (1 - \frac{k}{n})} \sum_{j=1}^{k} q^{-j} \binom{n-1}{k-j} \left(\frac{z}{1-z}\right)^{j-1}.$$

Theorem 4.2 *Let C be an $[n,k]_q$ Near MDS code and assume that for some ℓ, $1 \leq \ell \leq k$, the number of codewords of minimum weight in C satisfies*

$$A_{n-k} \leq (q-1)\frac{n}{k} \sum_{j=1}^{\ell} q^{-j} \binom{n-1}{k-j} \left(\frac{n-k}{k}\right)^{j-1}.$$

Then C is proper.

Corollary 4.3 *If C is an $[n,k]_q$ Near MDS code for which*

$$A_{n-k} \leq (1-q^{-1})\binom{n}{k},$$

then C is proper.

Maximum Minimum Distance (MMD) codes

For any $[n,k,d]_q$ code C holds the Singleton bound $d \leq n-k+1$. (Singleton [45]). The number $s(C) = n-k+1-d$ is called the defect of C. Clearly $s(C) = 0$ if and only if C is an MDS code.

If $k \geq m+1$ for some integer $m \geq 1$, then

$$d \leq \frac{q^m(q-1)}{q^m-1}(s+m), \quad \text{where} \quad s = s(C).$$

When

$$d = \frac{q^m(q-1)}{q^m-1}(s+m)$$

C is called a Maximum Minimum Distance (MMD) code. This class of codes has been studied by Faldum and Willems in [24], Olsson and Willems in [41], cf. also Faldum and Willems [23]. They have shown that any MMD code is formally equivalent to (i.e. has the same weight distribution as) a code from one of the classes A1-A3 below.

A1. Let C be an $[n,k,d]_q$ code of dimension $k \geq 3$ and defect $s \geq 1$. Then C is a MMD code if and only if it is formally equivalent to one of the following codes:

- The $[t\frac{q^k-1}{q-1}, k, tq^{k-1}]_q$ t-times repeated Simplex code, where $t = 1, 2, \ldots$.
- The $[q^{k-1}, k, (q-1)q^{k-2}]_q$ generalized Reed-Muller code of first order with $k \geq 4$ when $q = 2$
- The $[12,6,6]_3$ extended Golay code.
- The dual $[11,5,6]_3$ Golay code.
- The $[q^2+1, 4, q^2-q]_q$ projective elliptic quadratic code with $q \neq 2$.
- The $[(2^t-1)q+2^t, 3, (2^t-1)q]_q$ Denniston code with $1 \neq 2^t|_q$.

A2. Let C be a q-nary MMD code of dimension two and defect s. Then C is equivalent to the $[(s+1)(q+1), 2, (s+1)q]_q$ $(s+1)$-times repeated Simplex code.

A3. Let C be an MMD code of dimension k and defect $s = 0$. Then C is equivalent to the binary $[k+1, k, 2]$ MDS code.

It was shown in [21] by Dodunekova and Dodunekov that the MMD codes are proper, and in [15] by Dodunekova that the duals of MMD codes are proper as well. The main tool in the proofs are the discrete sufficient conditions (Theorems 3.1-3.2).

The error correction performance of the ternary cyclic and negacyclic codes and the binary cyclic codes of length at most 31 has been systematically studied by Baicheva in [2] by using the sufficient conditions of Theorem 3.3, and a large amount of t-proper codes have been found. One particularly interesting code, the ternary [13, 7, 5] quadratic residue code, was considered separately in [7] by Baicheva, Dodunekov, and Kötter. This code is t-proper for $t = 0, 1,$ and 2.

More particular examples on proper (and good) codes may be found in [17] and [18].

5 Application to standardized Cyclic Redundancy-Check codes

In [11], [12], [13], [25], [38], [39], and [40], a systematic study has been made on the error detection performance of standardized CRC codes including

ATM standard for ATM Header Error Control, with generator polynomial $g(x) = x^8 + x^2 + x + 1$ and code length 40;

IEC TC 57 standard, $g(x) = x^{16} + x^{14} + x^{12} + x^{11} + x^9 + x^8 + x^7 + x^4 + x + 1$;

IEEE WG 77.1 standard, $g(x) = x^{16} + x^{14} + x^{13} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^5 + x + 1$;

CCITT X.25 standard, $g(x) = x^{16} + x^{12} + x^5 + 1$;

ANSI standard, $g(x) = x^{16} + x^{15} + x^2 + 1$;

IBM-SDLC standard, $g(x) = x^{16} + x^{15} + x^{13} + x^7 + x^4 + x^2 + x + 1$;

IEEE-802 standard, $g(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$.

The following is a brief summary of the results.

CRC codes with 8 bit redundancy. Four classes of generator polynomials for this class of codes have been examined:

- The irreducible polynomials of degree 8.
- The irreducible polynomials of degree 7 multiplied by $x + 1$ (the ATM standard belongs to this class).
- The irreducible polynomials of degree 6 multiplied by $x^2 + 1$.
- The irreducible polynomials of degree 6 multiplied by $x^2 + x + 1$.

The corresponding CRC codes were tested for block lengths $10 \leq n \leq \min(127, s)$, where s is the minimum positive integer z, for which the generator polynomial divides $x^z - 1$. For $n = 40$ it turned out that the polynomials

$$f_1(x) = x^8 + x^7 + x^4 + x^3 + x^2 + x + 1$$

and

$$f_2(x) = x^8 + x^5 + x^3 + x^2 + x + 1$$

generate codes with minimum undetected error probability for $0.022266 \leq \varepsilon \leq 0.5$ and $0 \leq \varepsilon < 0.022266$ correspondingly.

The polynomial $f_3(x) = x^8+x^5+x^4+1$ is the best among weight-4 polynomials for $0 \leq \varepsilon \leq 1/2$. Note that there are several weight-4 polynomials which are better than the ATM standard. (See Baicheva, Dodunekov, and Kazakov [3])

CRC codes with 16 bit redundancy. Again, four classes of generator polynomials, omitting the reciprocal ones, have been examined for lengths $18 \leq n \leq 1024$:

- Irreducible of degree 16.
- Irreducible of degree 15, multiplied by $x + 1$.
- Irreducible of degree 14, multiplied by $x^2 + 1$.
- Irreducible of degree 14, multiplied by $x^2 + x + 1$.

The polynomial of the IEEE WG 77.1 standard gives a P_{ue} function which turns out to be minimal for the codes of lengths $n = 254$ and $n = 255$, and close to the minimal for the codes of length $181 \leq n \leq 253$, with difference from the best polynomial at $\varepsilon = 0.001$ up to 5%. For the polynomial IEC TC 57, the values of P_{ue} are close to the values of the minimal undetected error probability function for $94 \leq n \leq 128$, with difference from 1% to 5%, and attain the minimal value for $n = 19$. The performance of the standardized codes of lengths $18 \leq n \leq 1024$ has shown to be unsatisfactory. For more details we refer to the Ph.D. Thesis of P. Kazakov [27].

References

[1] A. Ashikhmin, A. Barg, Binomial moments of the distance distribution: bounds and applications. *IEEE Trans. Inform. Theory*, vol.45, no. 2, pp. 438-452, 1999.

[2] Ts. Baicheva, Binary and ternary linear codes which are good and proper for error correction. In *Proc. 7th Intern. Workshop on Algebraic and Combinatorial Coding Theory*, 18-24 June, 2000, Bansko, Bulgaria, pp. 55-60.

[3] Ts. Baicheva, S. Dodunekov, P. Kazakov, On the cyclic redundancy-check codes with 8-bit redundancy. *Comput. Commun.,* vol. 21, no. pp. 1030-1033, 1998.

[4] Ts. Baicheva, S. Dodunekov, P. Kazakov, On the cyclic redundancy-check codes with 16-bit redundancy. In *Proc. Intern. Workshop on ACCT*, Pskov, Russia, 1998, 17-21.

[5] Ts. Baicheva, S. Dodunekov, P. Kazakov, On the error detection performance of some standardized CRC codes. In *Proc. Telecom 98*, Druijba, Bulgaria, pp. 66-72, 1998.

[6] Ts. Baicheva, S. Dodunekov, P. Kazakov, On the undetected error probability performance of cyclic redundancy-check codes of 16-bit redundancy. *IEEE Trans. Commun.*, vol. 147, no. 5, pp. 253-256, 2000.

[7] Ts. Baicheva, S. Dodunekov, R. Kötter, On the performance of the ternary [13, 7, 5] quadratic residue code. *IEEE Trans. Inform. Theory*, vol.48, no. 2, pp. 562-564, 2002.

[8] A. Barg, A. Ashikhmin, Binomial moments of the distance distribution and the probability of undetected error. *Des., Codes Cryptogr.*, vol. 16, no. 2, pp. 103-116, 1999.

[9] E. R. Berlekamp, R. J. McEliece, H. C. A. van Tilborg, On the inherent intractability of certain coding problems. *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 384-386, 1978.

[10] M. A. de Boer, Almost MDS codes. *Des., Codes Cryptogr.*, vol. 9, no. 2, pp. 143-155, 1996.

[11] G. Castagnoli, B. Brauer, M. Herrmann, Optimization of Cyclic-Redundancy-Check Codes with 24 and 32 Parity Bits. *IEEE Trans. Commun.*, vol. 41, no. 6, pp. 883-892, 1993.

[12] G. Castagnoli, J. Ganz, P. Graber, Optimum cyclic redundancy-check codes with 16-bit redundancy. *IEEE Trans. Commun.*, vol. 38, no. 1, pp. 111-114, 1990.

[13] G. Castagnoli, J. Massey, Ph. Schoeller, N. Seemann, On Repeated-Root Cyclic codes. *IEEE Trans. on Inform. Theory*, vol. 37, no. 2, pp. 337-342, 1991.

[14] S. M. Dodunekov, I. Landgev, On Near MDS codes. *J. Geometry*, vol. 54, no. 1–2, pp. 30-43, 1995.

[15] R. Dodunekova, The duals of the MMD codes are proper for error detection. Preprint 2002:20, Chalmers University of Technology and Göteborg University.

[16] R. Dodunekova, The extended binomial moments of a linear code and the undetected error probability, to appear.

[17] R. Dodunekova, S. M. Dodunekov, On the probability of undetected error for Near MDS codes. Rrep. 1995-25, Dept. Math. Göteborg University, 1995.

[18] R. Dodunekova and S. M. Dodunekov, Sufficient conditions for good and proper error detecting codes, *IEEE Trans. Inform. Theory*, vol. 43, no. 6, pp. 2023-2026, 1997.

[19] R. Dodunekova, S. M. Dodunekov, Sufficient condition for good and proper error detecting codes via their duals. *Math. Balkanica*(N.S.), vol. 11, no. 3-4, pp. 375-381, 1997.

[20] R. Dodunekova, S. M. Dodunekov, Sufficient conditions for good and proper linear error correcting codes. In *Proc. II Intern. Workshop on Optimal Codes and related topics*, June 9-15, Sozopol, Bulgaria, 1998, pp. 62-67.

[21] R. Dodunekova, S. M. Dodunekov, The MMD codes are proper for error detection. *IEEE Trans. Inform. Theory*, vol. 48, no. 12, pp. 3109-3111, 2002.

[22] R. Dodunekova, S. M. Dodunekov, T. Kløve, Almost MDS and Near MDS codes for error detection. *IEEE Trans. Inform. Theory*, vol. 43, no. 1, pp. 285-290, 1997.

[23] A. Faldum, W. Willems, Codes of small defect. *Des., Codes Cryptogr.*, vol. 10, no, 3, pp. 341-350, 1997.

[24] A. Faldum, W. Willems, A characterization of MMD codes. *IEEE Trans. Inform. Theory*, vol. 44, no. 4, pp. 1555-1558, 1998.

[25] R. Glaise, A two-step computation of cyclic redundancy code CRC-32 for ATM network. *IBM J. Res. Develop.*, vol. 41, no. 6, pp. , 1997.

[26] T. Kasami, S. Lin, On the probability of undetected error for the maximum distance separable codes. *IEEE Trans. Commun.*, vol. 32, no. 9, pp. 998-1006, 1984.

[27] P. Kazakov, *Application of Polynomials to CRC and Spherical codes.* PhD Thesis. Technishe Universitet Delft, 2000.

[28] T. Kløve, Reed-Muller codes for error detection: The Good, The Bad, and The Ugly. *IEEE Trans. Inform. Theory*, vol. 42, no. 6, pp. 1615-1622, 1996.

[29] T. Kløve, Near-MDS codes for error detection. In *Proc. Int. Workshop on Optimal codes and Related Topics*, Sozopol, Bulgaria, 26 May - 1 June, 1995, pp. 103-107.

[30] T. Kløve, V. Korzhik, *Error detecting codes, General Theory and their Application in Feedback Communication Systems.* Kluwer, Boston, MA 1995.

[31] S. K. Leung-Yan-Cheong, E. R. Barnes, D. U. Friedman, On some properties of the undetected error probability of linear codes. *IEEE Trans. Inform. Theory*, vol. 25, no. 1, pp. 110-112, 1979.

[32] S. K. Leung-Yan-Cheong, M. E. Hellman, Concerning a bound on undetected error probability. *IEEE Trans. Inform. Theory*, vol. 22, no. 2, pp. 235-237, 1976.

[33] S. Lin, D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications.* Englewood Cliffs, N.J.: Prentice-Hall, 1983.

[34] J. E. MacDonald, Design methods for maximum-distance-error-correcting codes. *IBM J. Res. Devel.*, vol. 4, pp. 43-57, 1960.

[35] F.J. MacWilliams, A theorem on the distribution of weights in a systematic code. *Bell Syst. Tech. J.*, vol.42, pp. 79-94, 1963.

[36] F.J. MacWilliams, N.J.A. Sloane, *The theory of error-correcting codes.* North-Holland Publishing Company, Amsterdam, 1977.

[37] J. Massey, Coding techniques for digital data networks. In *Proc. Int. Conf. Inform. Theory and Syst.*, NTG-Fachberichte, Sept. 18-20, Berlin, Germany, vol. 65, 1978.

[38] P. Merkey, E. Posner, Optimum Cyclic Redundancy Codes for Noisy Channels. *IEEE Trans. on Inform. Theory*, vol. 30, no. 6, pp. 865-867, 1984.

[39] M. Miller, M. Wheal, M. Stevens, A. Mezhvinsky, The X.25 error detection code is a poor choice. In *Proc. Institute of Radio and Electronic Engineers Australia IREECON 85*, Sidney, 1985.

[40] M. Miller, M. Wheal, M. Stevens, S. Lin, The Reliability of Error Detection Schemes in Data Transmissions. *J. Electr. Electronics Eng.*, Australia, pp. 123-131, 1996.

[41] J. Olsson, W. Willems, A characterization of certain Griesmer codes: MMD codes in a more general sense. *IEEE Trans. Inform. Theory*, vol. 45, no. 6, pp. 2138-2142, 1999.

[42] C. Ong, C. Leung, On the undetected error probability of triple-error-correcting BCH codes. *IEEE Trans. Inform. Theory*, vol. 37, no. 3, pp. 673-678, 1991.

[43] A. M. Patel, Maximal q-ary linear codes with large minimum distance. *IEEE Trans. Inform. Theory*, vol.21, no. 1, pp. 106-110, 1975.

[44] P. Petty, Necessary condition for good error detection. *IEEE Trans. Inform. Theory*, vol. 37, no. 2, pp. 375-378, 1991.

[45] R. C. Singleton, Maximum distance q-ary codes. *IEEE Trans. Inform.Theory*, vol. 10, no. 1, pp. 116-118, 1964.

[46] J.K. Wolf, A.M. Michelson, A.H. Levesque, On the probability of undetected error for linear block codes. *IEEE Trans. Commun.*, vol. COM-30, no. 2, pp. 317-324, 1982.