A conjecture on the free distance of (2,1,m) binary convolutional codes

Ph. Piret
Philips Research Laboratory, 2, av. Van Becelaere
B-1170, Brussels, Belgium

ABSTRACT. It is shown that the fixed binary (2, 1, m) convolutional codes satisfy the Costello bound if two conjectures on the weight distribution of binary shortened cyclic codes are true.

1. Introduction

Let \( C(n, k, m) \) be the class of fixed convolutional codes of length \( n \), dimension \( k \) and "constraint length" \( m \) over \( F = GF(2) \), and let \( C^*(n, k, m) \) be the class of time varying [1] convolutional codes with the same parameters. Denote the free distance of the code \( C \) by \( d(C) \) and define

\[
\delta(n, k) := \lim_{m \to \infty} \sup_{C \in \mathcal{C}(n, k, m)} \frac{d(n, k, m)}{m + 1},
\]

\[
\delta^*(n, k) := \lim_{m \to \infty} \sup_{C \in \mathcal{C}^*(n, k, m)} \frac{d^*(n, k, m)}{m + 1}.
\]

For \( R := k/n \), Costello [1] has proved the following bound

\[
\delta^*(n, k) \geq -nR/\log_2(2^{1-R} - 1),
\]

while Zigangirov [7] has recently obtained the following result

\[
\delta(n, \lfloor nR \rfloor) \geq -nR/\log_2(2^{1-R} - 1) - n\epsilon(n),
\]

with \( \lim_{n \to \infty} \epsilon(n) = 0 \). In (5) and (6), \( \log_2 \) denotes the logarithm in base 2 of its argument.

Unfortunately, (6) is meaningful only for large \( n \) and it cannot be used for the important class \( \mathcal{C}(2, 1, m) \) of fixed (2,1) binary convolutional codes. In this paper, we sketch lines along which we could perhaps prove

\[
\delta(2, 1) \geq 1/\log_2(1 + \sqrt{2}).
\]
It is easy to verify that the right hand side of (7) is nothing but the right hand side of (5) for \((n, k) = (2, 1)\). In passing we shall state two conjectures that have their own interest. Would these two conjectures become theorems then the Costello bound (5) that applies to the classes \(C^*(n, k, m)\) would also apply to the classes \(C(2, 1, m)\), which are to date the most popular classes of convolutional codes.

2. Two conjectures the truth of which would imply (7)

As an introduction to this discussion we consider first a set \(B\) of binary linear \((n, k)\) block codes. Since any \(B \in B\) is a linear code, the minimum distance \(d(B)\) of \(B\) is nothing but the minimum Hamming weight \(w_H(v)\) of all nonzero vectors \(v\) in \(B\). The question is now: is it possible to find for such a set \(B\), an integer \(d\) such that one can guarantee that at least one code \(C \in B\) satisfies \(d(C) \geq d\)? The answer is yes if something is known about the number of codes \(C \in B\) that contain an arbitrary nonzero element \(v\) of \(F^n\). Assume for example that \(B\) has the property that any nonzero \(v \in F^n\) is a codeword in at most \(M\) codes \(C \in B\). In this case, at most \(M \sum_{w=1}^{d-1} \binom{n}{w}\) codes \(C\) of \(B\) contain one or more nonzero codewords of symbol weight \(\leq d - 1\). This proves the existence of at least one code \(C \in B\) satisfying \(d(C) \geq d\), with \(d\) the largest integer for which \(\sum_{w=1}^{d-1} \binom{n}{w} \leq |B|/M\) holds.

Let us now try to apply a similar argument to the class \(C(2, 1, m)\) of binary convolutional codes generated by noncatastrophic encoders \(G\) having the form

\[
G = [g_1, g_2]; g_1 \in F[D], \text{ del } g_i = 0, \text{ deg } g_i = m, i = 1, 2, \tag{8}
\]

with \(F[D]\) the set of polynomials over \(F\) in the indeterminate \(D\), which represents the delay operator. In (8), del and deg denote respectively the delay and the degree of their argument, i.e. the lowest and the highest power of \(D\) with a nonzero coefficient.

We denote by \(E(G)\) the code generated by \(G\), and by \(\alpha(m)\) the fraction of noncatastrophic encoders among all encoders \(G\) satisfying (8). Rosenberg has shown that one has \(\lim_{m \to \infty} \alpha(m) = 1/3\), [6]. On the other hand, if \(G\) is a noncatastrophic encoder, then for sufficiently large \(m\), its free distance \(d[E(G)]\) is achieved by a polynomial information sequence \(a = \sum_{i=0}^{\ell} a_i D^i, a_i \in F, a_0 = a_\ell = 1, \) of degree \(\ell \leq m^2\) and such that \(v = aG\) has the property to be a simple sequence with respect to \(G\). (A polynomial code sequence \(v = aG\), with \(a = 1 + \sum_{j=1}^{\ell-1} a_j D^j + D^\ell\) is called a simple sequence with respect to a \((2,1,m)\) encoder, if for \(1 \leq j \leq \ell - 1\), the information sequence \(a\) does not contain any subsequence of \(m\) consecutive symbols \(a_j\) that are zero.) That this must be the case follows from the following remarks.