Linear Programming-Based Optimization of the Distance Spectrum of Linear Block Codes

Gianluigi Ferrari and Keith M. Chugg

1 Dip. di Ing. dell’Inform., Univ. of Parma, Parma, I-43100, Italy
2 Dept. of EE, Univ. of South. Cal., Los Angeles, CA 90089-2565 U.S.A.

Since the revolutionary work of Shannon in 1948 [1], where error-free communication was predicted by suitably coding the information to be transmitted over a noisy channel, the design of good codes has kept researchers busy for decades [2]. A multitude of codes have been designed to combat the impairments introduced by the channel. There are several ways to describe and characterize a code. The distance spectrum describes the relative distances between the code words, and reduces to the weight spectrum if the code is linear. When considering maximum likelihood (ML) decoding, the free distance, i.e., the minimum possible non-zero distance over all code words, is usually considered as a good indicator of the performance of the code. However, the discovery of the so-called turbo-like codes in the last decade has brought a deeper comprehension of the important impact of the “shape” of the whole distance spectrum of a code (not only the minimum distance) on its performance [3, 4].

Since different characteristics of the distance spectrum seem to dominate the performance at different signal-to-noise ratios (SNRs), it is reasonable to consider what is the best distance spectrum for a linear code for different channels (e.g., different SNRs). In this paper, we attempt to address this basic question in the case of a binary linear block code transmitted over different channels. As “optimality” criterion we consider the minimization of an upper bound on the word error rate (WER) \( P_W \) based on the distance spectrum \( \mathbf{a} = (a_0, \ldots, a_n) \) of a “hypothetical” group code. We correspondingly derive a linear program, where the constraints on the coefficients of the distance spectrum are derived by relying on the relationship, given by the MacWilliams-Delsarte identities [2], between a code and its dual code. The general form of the linear program is the following

\[
\begin{align*}
\text{Minimize} \quad & \Gamma = \sum_{i=d}^{n} a_i P_2(i) \\
\text{subject to} \quad & a_i \geq 0, \ i \in \{d, d+1, \ldots, n\} \\
& \sum_{i=d}^{n} a_i K_0(i) \geq -K_0(0) \\
& \sum_{i=d}^{n} a_i K_1(i) \geq -K_1(0) \\
& \cdots \\
& \sum_{i=d}^{n} a_i K_n(i) \geq -K_n(0) \\
& \sum_{i=d}^{n} a_i = M - 1,
\end{align*}
\]

where \( n \) is the code word length, \( P_2(i) \) is the pairwise error probability (PEP) between the all-zero code word and a code word of weight \( i \), \( \{K_j(i)\} \) are the so-called Krawtchouk polynomials [5] and \( d \) is a preliminary admissible minimum distance. In (1)-(2) it is implicitly assumed that \( a_0 = 1 \) and \( a_1 = \ldots = a_{d-1} = 0 \). In order to limit the complexity of the linear program, we reduce the number of unknowns by imposing a that the distance spectrum is
symmetric with respect to the central weight, i.e., $a_j = a_{n-j}$. The linear program is then solved for an AWGN channel, by specifying the PEP for the case of binary phase shift keying (BPSK) [6]. The solution of the considered upper bound-based linear program, obtained using the simplex method [7], is generally a vector with real components. In fact, the solving method does not belong to the class of integer programming techniques [8]. However, for specific values of the code word length $n$ and code rate $R = k/n$, the coefficients of the vector solution of the linear program are non-negative integers. In some cases the solutions correspond to the distance spectra of known group codes. Table 1 shows some of the obtained weight enumerators $A(x) = \sum_{i=0}^n a_i x^i$ and the corresponding known codes. In these cases, we can conclude that these codes are “optimal” in the sense of minimizing the union bound (1) on the WER. In other cases, the solution of the linear program is a vector with non-negative integers which does not correspond, to the best of the authors’ knowledge, to the distance spectrum of any known block code. This could predict the existence of still unknown group codes. For example, solving the considered linear program for $n = 34$ and $k = 15$, the obtained weight spectrum corresponds to the following weight enumerator

$$A(x) = 1 + x^{34} + 374(x^{10} + x^{24}) + 1152(x^{11} + x^{23}) + 1184(x^{12} + x^{22}) + 1848(x^{14} + x^{20}) + 7040(x^{15} + x^{19}) + 4785(x^{16} + x^{18}).$$

As one can see, the obtained distance spectrum would correspond to a (34,15) binary linear code with $d_f = 10$—provided that a search procedure found a code with such a weight spectrum. To the best of the authors’ knowledge, (34,15) group codes known up to now have at most $d_f = 9$ [9]. Starting from the knowledge of the distance spectrum and using a result presented in [10], a semi-exhaustive searching algorithm similar to that proposed in [11] could be designed. The only drawback is the computational complexity. A simplified searching algorithm, based on the a priori knowledge of the distance spectrum, is currently under study.

The PEP $P_2(i)$ in (1) depends on the SNR and the code rate. Surprisingly, we find out that the solution of the considered linear program does not depend on the SNR, provided that the other parameters remain unchanged. This is counterintuitive, since it is a common belief that the “optimality” of the distance spectrum depends on the SNR. A theorem is then proved, which gives a geometrical justification of the obtained result. In fact, one of the implications of this theorem is that the distance spectrum minimizing the upper bound on the WER depends on the expression of the PEP $P_2$ in a particular way. Defining the vector $\mathbf{p} = (P_2(1), \ldots, P_2(n)) \in \mathbb{R}^n$, the proposed theorem implies that the optimized distance spectrum depends only on the “orientation” of $\mathbf{p}$ in $\mathbb{R}^n$, but it does not depend on the magnitude of the components of $\mathbf{p}$. Increasing the SNR steepens the PEP, but the shape remains the same. In $\mathbb{R}^n$, this could be pictured by saying that the vector $\mathbf{p}$ varies in a small “cone.” In this sense, the orientation of $\mathbf{p}$ varies little, suggesting that the solution should not depend strongly on the SNR. Moreover, since the “shape” of the PEP for an AWGN channel is very similar to that for a Rayleigh flat fading channel, it is expected that the optimized distance spectra are similar in the two cases. Numerically, we found that the solution is insensitive of the particular channel—provided the other parameters do not change.
A performance analysis based on the obtained optimized distance spectra is then considered. It is shown that the optimized distance spectra guarantee asymptotically (for increasing code word length) low error probability above the SNR corresponding to the channel cut-off rate. More precisely, we evaluated the upper bounds on the WER corresponding to the obtained optimized distance spectra. In Fig. 1 the upper bounds relative to the case of transmission with BPSK with \( R = 1/2 \) over an AWGN channel are shown for increasing code word length \( n \). They cross at a specific SNR \( \gamma_b^{(co)} \), corresponding to the channel cut-off rate \( R_0 \) [6]. Similar results where obtained in the case of a Rayleigh flat fading channel, where the upper bounds on the WER cross at a SNR corresponding to the channel cut-off rate relative to this channel.

It is apparent that the proposed linear program leads to distance spectra which asymptotically (for increasing code word length) show decreasing error probability for any SNR such that \( R_0 > R \), i.e., below the channel cut-off rate. This is reasonable, since the objective function is a union bound, i.e., a sort of averaged performance measure converging above the channel cut-off rate [12]. The proposed approach could be extended in a meaningful way by considering as objective function a suitable tighter upper bound on the WER [13], possibly leading to a more complicated non-linear program.

References


Figure 1: Upper bounds on the WER, for BPSK transmission over an AWGN channel, relative to optimized distance spectra, solutions of a union bound-based linear program with symmetry condition, for $R = 1/2$ and increasing code word length $n$.


