The Capacity of Matched RS Codes is Zero Over the AWGN Channel

D. E. Lazic, D. Zerfowski and Th. Beth

Universität Karlsruhe, Fakultät für Informatik,
Institut für Algorithmen und Kognitive Systeme,
Am Fasanengarten 5, D–76128 Karlsruhe, Germany
e-mail: zerfowsk@ira.uka.de

Extended Abstract
of a paper presented at the
Eurocode 1994,
l'Abbaye de La Bussière sur Ouche, Côte d'Or, France.
October 24-28, 1994

Generally, a q-ary block code $\mathcal{C} = \{\mathbf{c}_1, \ldots, \mathbf{c}_M\}$, $\mathbf{c}_m = (c_{m,1}, \ldots, c_{m,n})$, $c_{m,i} \in \mathcal{A}$, over a finite alphabet $\mathcal{A}$, $|\mathcal{A}| = q$, and of the code rate $R = \frac{\mathrm{ld}\ M}{n}$ is any subset of $\mathcal{A}^n$. In order to make encoding of block codes less spatially complex for greater values of n and M, $\mathcal{A}$ is usually provided with some algebraic structure. The most investigated family of block codes in coding theory are linear block codes $\mathcal{C}_{\mathrm{GF}} = [M, R = \frac{k}{n}]$ over finite fields $\mathcal{A} = \mathrm{GF}(q) = \{0, 1, \psi_3, \ldots, \psi_q\}$, which are k-dimensional vector subspaces of the vector space $\mathcal{A}^n$. The most attractive property of q-ary linear block codes is that all codewords (exponentially many, $M = q^{Rn}$) can be generated with linear complexity (in n) using a generator matrix, while the asymptotical performances (when $n \to \infty$) are not degraded, i.e. their capacity R_{c} and error exponent $E(R)$ are equal to the capacity and error exponent of the corresponding coding channel. Unfortunately, this is no more valid for the optimal decoding problem for $\mathcal{C}_{\mathrm{GF}}$, which is NP-complete. Only some subfamilies of these codes are suboptimally decodable with low-degree polynomial complexity. Both encoding and decoding are executable on the symbolic level, without the necessity of using a labeling of the symbols in $\mathcal{A}$ with elements in $\mathbf{N}$.

A very convenient property of $\mathcal{C}_{\mathrm{GF}}$ is that the set of Hamming distances $H_m = \{d_H(\mathbf{c}_m, \mathbf{c}_j) =$

$|\{i : c_{m,i} \neq c_{j,i}\}|\}_{j=1}^{M}$ of some codeword $\mathbf{c}_m$ to all other codewords in the code is the same for each codeword, i.e. q-ary linear block codes are *Hamming distance invariant.* Furthermore, the set H_m is a permutation of the set of Hamming weights $\mathcal{W}_H = \{w_H(\mathbf{c}_m) = d_H(\mathbf{0}, \mathbf{c}_m)\}_{m=1}^{M}$ of codewords. Accordingly, the Hamming distance between any two codewords equals the Hamming weight of their difference (which is again a codeword of the same code), i.e. q-ary linear block codes are *Hamming weight characterizable.* An inconvenient property of the Hamming distance for $q > 2$ is that it measures only the fact that the symbols at the same position in two distinguished codewords differ or not, but gives us no information on how much they differ.

Transmission of codewords of the block code $\mathcal{C}$ over waveform channels (power or band-limited) requires a mapping f of the symbol alphabet $\mathcal{A}$ into a finite dimensional Euclidean real vector space $\mathbb{R}^{\nu}$, which leads to a ν-dimensional vector (or signal point) constellation $\mathcal{S}_{\nu}$, i.e.

$$f : \mathcal{A} \rightarrow \mathcal{S}_{\nu} = \{\mathbf{s}_1, \ldots, \mathbf{s}_q\} \subset \mathbb{R}^{\nu}, \tag{1}$$

$\mathbf{s}_l = (s_{l,1}, \ldots, s_{l,\nu})$; $s_{l,\mu} \in \mathbb{R}$, $l = 1, \ldots, q$; $\mu = 1, \ldots, \nu$. The energy of the vector (or signal point) $\mathbf{s}_l$ is $E(\mathbf{s}_l) = |\mathbf{s}_l|^2 = \sum_{\mu=1}^{\nu} s_{l_\mu}^2$, while the Euclidean distance between two signal points $\mathbf{s}_l$ and $\mathbf{s}_j$ is

$$d_E(\mathbf{s}_l, \mathbf{s}_j) = \sqrt{\sum_{\mu=1}^{\nu} (s_{l,\mu} - s_{j,\mu})^2}.$$

A vector constellation $\mathcal{S}_{\nu}$ is characterized by the expected energy

$$E(\mathcal{S}_{\nu}) = \sum_{l=1}^{q} P[\mathbf{s}_l] E(\mathbf{s}_l), \tag{2}$$

(where $P[\mathbf{s}_l]$ are the prior probabilities of signal points) and by the Euclidean distance distribution

$$\mathcal{D}(\mathcal{S}_{\nu}) = \{d_E(\mathbf{s}_l, \mathbf{s}_j) \mid l < j; l, j = 1, \ldots, q\}. \tag{3}$$

Instead of the Euclidean distance very often only the minimum Euclidean distance is considered

$$d_{E_m}(\mathcal{S}_{\nu}) = \min_{\mathcal{S}_{\nu}} \mathcal{D}(\mathcal{S}_{\nu}). \tag{4}$$

The mapping f induces a mapping of the q-ary block code $\mathcal{C}$ into the $N = n \cdot \nu$ dimensional Euclidean real vector space $\mathbb{R}^N$ and defines the *Euclidean representation* $\mathcal{E}$ *of* $\mathcal{C}$, i.e.

$$\mathcal{E} = \{\mathbf{x}_m = (\mathbf{s}_{m,1}, \ldots, \mathbf{s}_{m,n}) = (x_{m,1}, \ldots, x_{m,N})\}_{m=1}^{M}. \tag{5}$$

The corresponding coded waveforms used for signaling over a waveform channel are always of the form

$$x_m(t) = \sum_{i=1}^{N} x_{m,i} \cdot \phi_i(t); \qquad m = 1, \ldots, M, \tag{6}$$

where $\Phi = \{\phi_i(t)\}_{i=1}^{N}$ are orthonormal functions of waveform duration T,

$$\int_0^T \phi_i(t)\phi_j(t)dt = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j, \end{cases} \tag{7}$$

so that the mean-square difference between two waveforms is

$$\delta_{m,j}^2 = \int_0^T [x_m(t) - x_j(t)]^2 dt = d_E^2(\mathbf{x}_m, \mathbf{x}_j) = \sum_{i=1}^{n} d_E^2(\mathbf{s}_{m,i}, \mathbf{s}_{j,i}), \tag{8}$$

and the corresponding waveform and codeword energies are

$$e_m = E(\mathbf{x}_m) = \int_0^T x_m^2(t)dt = \sum_{i=1}^{n} E(\mathbf{s}_{m,i}) = \sum_{j=1}^{N} x_{m,j}^2 \qquad m = 1, \ldots, M. \tag{9}$$

Consequently, for waveform channel models the relevant distance measure is the Euclidean distance, and the measure of the intensity of the impact of the additive channel noise $n(t)$ is the signal-to-noise ratio

$$\text{SNR} = \frac{E[\mathcal{E}]}{E[|\mathbf{n}|^2]}, \tag{10}$$

where $E[\mathcal{E}] = \sum_{m=1}^{M} P[\mathbf{x}_m]E(\mathbf{x}_m)$ is the expected energy of the codeword $\mathbf{x}_m$ in $\mathcal{E}$ and $E[|\mathbf{n}|^2]$ is the expected energy of the noise vector $\mathbf{n} = (n_1, n_2, \ldots, n_N)$ (which is the representation of $n(t)$ over the set of orthonormal functions Φ).

The Euclidean distance precisely expresses the quantity of the difference between signal points, between Euclidean representations $\mathcal{E}$ of codewords from $\mathcal{C}$, and between corresponding coded waveforms, for all values of $q \in \mathbf{N}$. Only for $q = 2$ the corresponding Hamming distance is proportional to the squared Euclidean distance for all mappings f. For $q > 2$ there exists no other distance measure on the symbolic level (metric induced only by algebraic structures on finite alphabets $\mathcal{A}$), which is generally proportional to the Euclidean metric induced through the mapping f. Thus, the very useful properties of Hamming distance, the distance invariance and weight characterization, are in general no longer valid for the induced Euclidean distance. Because of that the calculation and estimation of Euclidean distance distributions, and thereby the performances of $\mathcal{E}$ and

the corresponding waveform set, is very cumbersome, and for large N and M practically impossible. This is the true bottleneck when using nonbinary algebraic (symbolic) codes on the discrete time or waveform channel.

One possibility to overcome this incompatibility of Hamming and induced Euclidean distances could be to search for particular mappings f which preserve the distance invariance and weight characterization for induced Euclidean distances. Loeliger gives in [Loe91, Loe92] a general condition for such mappings in case the symbol alphabet $\mathcal{A}$ is provided at least with a group structure $(G, *)$ of the following form

$$d_E(f(g), f(g')) = d_E(f(g^{-1} * g'), f(e)), \qquad \forall g, g' \in G, \tag{11}$$

where e denotes the neutral element of $(G, *)$. These mappings are called *matched mappings* to the group. The corresponding vector constellation $\mathcal{S}_\nu^*$ is Euclidean distance invariant and Euclidean weight representable, where the Euclidean weights are $\{\mathcal{W}_E(\mathbf{s}_l) = d_E(f(e), f(g)) = d_E(\mathbf{s}_1, \mathbf{s}_l)\}_{l=1}^q$, when $f(e) = \mathbf{s}_1$ and $f(g) = \mathbf{s}_l$.

First examples for such matched mappings were introduced by Massey and Mittelholzer ([Mas89, MasMit89]) for linear codes over the ring $\mathcal{A} = \mathbb{Z}_m$ (the integers mod m) where the vector constellation $\mathcal{S}_2^*$ was the M-PSK point arrangement.

In this paper we will show that the asymptotical performances of one of the most popular family of linear block codes over GF(q), the Reed-Solomon (RS) codes, are bad on the AWGN channel model for all matched mappings defined on the additive group of GF(q). The construction of the proof of this statement is as follows.

1. Any vector constellation $\mathcal{S}_\nu^*$ matched to a group is a group code for the Gaussian channel (see [Loe92]).

2. Group codes for the Gaussian channel are Euclidean distance invariant spherical codes (see [Sle68]).

3. For RS codes the equality $q = n + 1$ holds, so that for any constant $\nu \in \mathbb{N}$ the minimum Euclidean distance $d_{E_m}(\mathcal{S}_\nu^*) = \epsilon$ in the vector constellation $\mathcal{S}_\nu^*$ with constant average energy $E(\mathcal{S}_\nu^*)$ tends to zero, when $n \to \infty$ and the code rate R is fixed (see [Wyn65]).

4. Matched Euclidean representations $\mathcal{E}^*$ of block codes $\mathcal{C}$ are Euclidean distance invariant (see [Loe91]). Consequently, $\mathcal{E}^*_{\mathrm{RS}}$ are also Euclidean distance invariant.

5. For the AWGN channel the signal-to-noise ratio SNR (see equation 10) is constant for $\mathcal{E}^*$, when $n \to \infty$ and ν and $E(\mathcal{S}^*_\nu)$ remain constant. According to equation (9) and the fact that $\mathcal{S}^*_\nu$ is a spherical code (so that $E(s_{m,i}) = E = \text{const}$), it follows that $\mathrm{SNR} = \frac{nE}{n\nu\sigma^2} = \frac{E}{\nu\sigma^2} = \text{const}$, where σ^2 is the constant variance of a single AWGN component. As usual, we assume here that $P[\mathbf{x}_m] = \frac{1}{M}$, $m = 1, \ldots, M$.

6. Any RS code the generator polynomial of which does not include the linear factor $(x-1)$ contains all codewords of the form $\mathbf{x}^{(l)} = (\psi_l, \psi_l, \ldots, \psi_l)$, $\psi_l \in \mathrm{GF}(q)$, $l = 1, \ldots, q$. (The proof of this statement will be given in the final version of this paper. There we also give a discussion about the RS codes with generator polynomials which include the linear factor $(x-1)$.)

7. In $\mathcal{S}^*_\nu$, let $f(\psi_l)$ and $f(\psi_j)$ be of minimum Euclidean distance ϵ. Then, according to item 6, there exist two codewords in $\mathcal{E}^*_{\mathrm{RS}}$ of the form $\mathbf{x}^{(l)}_{\mathcal{E}} = (f(\psi_l), f(\psi_l), \ldots, f(\psi_l))$ and $\mathbf{x}^{(j)}_{\mathcal{E}} = (f(\psi_j), f(\psi_j), \ldots, f(\psi_j))$, where $d^0_E(\mathbf{x}^{(l)}_E, \mathbf{x}^{(j)}_E) = n\epsilon$, so that the normalized (divided by n) Euclidean distance is $\underline{d}^0_E = \epsilon$ and tends to zero for $n \to \infty$ (according to item 3).

8. In [LazSen92] it was proved that (for constant SNR) the error exponent of constant rate distance invariant block code families is zero, and thus also the capacity, when the normalized minimum distance tends to zero as $n \to \infty$.

The items 1. to 8. imply that the family of matched Euclidean representations of Reed-Solomon codes $\mathcal{E}^*_{RS}$ have a *family error exponent*, and thus a *family capacity* for the AWGN channel, equal to zero.

References

[LazSen92] D. E. Lazic and V. Senk. A direct geometrical method for bounding the error exponent for any specific family of channel codes - part i: Cutoff rate lower bound for block codes. *IEEE Transaction on Information Theory*, 38, No. 4, pages 1548–1559, September 1992.

[Loe91] H.-A. Loeliger. Signal sets matched to groups. *IEEE Transaction on Information Theory*, 37, No. 6, pages 1675–1682, November 1991.

[Loe92] H.-A. Loeliger. *On Euclidean-Space Group Codes.* PhD thesis, ETH Zürich, No. 9720, 1992.

[Mas89] URSI ISSSE. *A Short Introduction to Coding Theory and Practice*, 1989.

[MasMit89] Proc. 4th Joint Swedish-Soviet Int. Workshop on Information Theory, Gotland, Sweden. *Convolutional Codes over Rings*, August-September 1989.

[Sle68] D. Slepian. Group codes for the gaussian channel. *Bell Systems Technical Journal*, 47, pages 575–602, April 1968.

[Wyn65] A. D. Wyner. Capabilities of bounded discrepancy decoding. *Bell Systems Technical Journal*, 44, pages 1061–1122, 1965.