On the Suboptimality of Equidistant Codes Meeting the Plotkin Bound

Po-Ning Chen, Hsuan-Yin Lin, and Stefan M. Moser
Department of Electrical & Computer Engineering
National Chiao Tung University (NCTU)
Hsinchu, Taiwan
Email: qponing@mail.nctu.edu.tw, {lin.hsuanyin, stefan.moser}@ieee.org

***Abstract*—In this paper, we re-introduce from our previous work [1] a new family of *nonlinear* codes, called *weak flip codes*, and show that its subfamily *fair weak flip codes* belongs to the class of equidistant codes, satisfying that any two distinct codewords have identical Hamming distance. It is then noted that the fair weak flip codes are related to the *binary nonlinear Hadamard codes* as both code families maximize the minimum Hamming distance and meet the Plotkin upper bound under certain blocklengths. Although the fair weak flip codes have the largest minimum Hamming distance and achieve the Plotkin bound, we find that these codes are by no means optimal in the sense of average error probability over binary symmetric channels (BSC). In parallel, this result implies that the equidistant Hadamard codes are also nonoptimal over BSCs. Such finding is in contrast to the conventional code design that aims at the maximization of the minimum Hamming distance.**

I. Introduction

In 1948, Shannon [2] ingeniously established the ultimate limit of a reliable transmission rate over noisy channels and baptized it as *channel capacity*. From then on, a new research trend for finding good codes that operate close to the channel capacity began. Implicitly from Shannon's random coding proof, such good codes call for large blocklength. Since linearity does not inhibit the achievability of channel capacity, but simplifies the analysis and implementation of codes, coding theory and practice that follow often restrict themselves to *linear codes*. Motivated by the agreement between Hamming weights of codewords and Hamming distances between codewords for linear codes, and also by the union bound that converts the global error probability into pairwise error probabilities, it then becomes common to use the *minimum Hamming distance* as a quality criterion [3] for code design.

On the other hand, due to the analytical obstacle on the determination of exact error probability, information theorists usually resort to bounds such as the random coding bound. These bounds were often derived based on certain simplifications and are by no means accurate unless the blocklength of codes is sufficiently large. In our previous work, we attempted to break away these simplifications and instead focused on *the exact error probability* of codes for practically finite blocklength [1]. This new attempt could give a practical code design and remark on whether the implication from minimum-Hamming-distance code design is consistent with the true behavior of the error performance of codes.

In this paper, we re-introduce a new class of codes from our previous work, called *fair weak flip codes* [1] [4] [5], and confirm that they are equidistant. We further show that they can achieve the Plotkin upper bound and hence have the largest minimum Hamming distance among all (possibly nonlinear) codes of equal length. We then investigate whether this optimality in minimum Hamming distance can be extended to the error performance.

Note that there exists another class of binary nonlinear codes that also meet the Plotkin bound, called *binary nonlinear Hadamard codes*. This class of binary nonlinear codes are constructed with the help of Hadamard matrices and Levenshtein's theorem [6, Ch. 2], from which the codes are named. It is thus essential to clarify the relation between the fair weak flip codes and the Hadamard codes. A simple comparison gives that if for the parameters (M, n) of a given fair weak flip code there exists a Hadamard code, then these two codes are equivalent.In this sense we can consider the fair weak flip codes to be a subclass of Hadamard codes. However, there is no guarantee that for every choice of parameters (M, n) for which fair weak flip codes exist, there also exists a corresponding Hadamard code. By this, the fair weak flip codes can also be regarded as an extension of the Hadamard codes.

The foundations of our insights lie in a new powerful way of creating and analyzing both linear and nonlinear block-codes. As is quite common, we use the *codebook matrix* containing the codewords in its rows to describe our codes. However, for our code construction and performance analysis, we look at this codebook matrix not row-wise, but *column-wise*. All our proofs and also our analysis for an equidistant code are fully based on this new approach to a code. This is another fundamental difference between our results and the binary nonlinear Hadamard codes that are constructed based on Hadamard matrices and Levenshtein's theorem [6].

II. Weak Flip Codes and the Plotkin Bound

We start with an important bound that holds for any code.

Lemma 1 (Plotkin Bound [6]): The minimum distance of an (M, n) binary code $\mathscr{C}^{(\mathsf{M},n)}$ always satisfies

$$d_{\min}\big(\mathscr{C}^{(\mathsf{M},n)}\big) \le \begin{cases} \frac{n\cdot\frac{\mathsf{M}}{2}}{\mathsf{M}-1} & \mathsf{M} \text{ even}, \\ \frac{n\cdot\frac{\mathsf{M}+1}{2}}{\mathsf{M}} & \mathsf{M} \text{ odd}. \end{cases} \tag{1}$$

Note that if an equidistant code (i.e., a code whose codewords all have identical pairwise Hamming distance) meets the Plotkin bound (1), then this code maximizes the minimum Hamming distance.

We next introduce some special families of binary codes. We start with a code with two codewords.

Definition 2: The *weak flip code* with $\mathsf{M} = 2$ codewords is defined by the following codebook matrix $\mathscr{C}^{(2,n)}$:

$$\mathscr{C}^{(2,n)} \triangleq \begin{pmatrix} \mathbf{x} \\ \bar{\mathbf{x}} \end{pmatrix} = \begin{pmatrix} 0 & \cdots & 0 \\ 1 & \cdots & 1 \end{pmatrix}. \tag{2}$$

Defining the column vector

$$\left\{ \mathbf{c}_1^{(2)} \triangleq \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\} \tag{3}$$

we see that the weak flip code with two codewords is given by a codebook matrix that consists of n columns $\mathbf{c}_1^{(2)}$.

Note that the bits of $\mathbf{c}_1^{(2)}$ are flipped versions of each other, therefore also the name of the code.

We have shown in [5] that for any blocklength n the weak flip code with two codewords is optimal among all possible codes with two codewords for the BSC and the Z-channel.

Definition 3: The *weak flip code of type* (t_2, t_3) for $\mathsf{M} = 3$ or $\mathsf{M} = 4$ codewords is defined by a codebook matrix $\mathscr{C}_{t_2,t_3}^{(\mathsf{M},n)}$ that consists of $t_1 \triangleq n - t_2 - t_3$ columns $\mathbf{c}_1^{(\mathsf{M})}$, t_2 columns $\mathbf{c}_2^{(\mathsf{M})}$, and t_3 columns $\mathbf{c}_3^{(\mathsf{M})}$, where

$$\left\{ \mathbf{c}_1^{(3)} \triangleq \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \ \mathbf{c}_2^{(3)} \triangleq \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \ \mathbf{c}_3^{(3)} \triangleq \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\} \tag{4}$$

or

$$\left\{ \mathbf{c}_1^{(4)} \triangleq \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \ \mathbf{c}_2^{(4)} \triangleq \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \ \mathbf{c}_3^{(4)} \triangleq \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right\}, \tag{5}$$

respectively.

The columns given by the sets (4) and (5) are called *candidate columns*. To be able to generalize the definition of weak flip codes to an arbitrary M, we give the following definition [1].

Definition 4: Given a number of codewords M, a length-M candidate column $\mathbf{c}$ is called a *weak flip column* if its first component is 0 and its Hamming weight equals to $\left\lfloor \frac{\mathsf{M}}{2} \right\rfloor$ or $\left\lceil \frac{\mathsf{M}}{2} \right\rceil$. The collection of all possible weak flip columns is called *weak flip candidate columns set* and is denoted by $\mathcal{C}^{(\mathsf{M})}$. Note that (4) and (5) correspond to $\mathcal{C}^{(3)}$ and $\mathcal{C}^{(4)}$, respectively. We see that a weak flip column contains an almost equal number of zeros and ones.

Defining the shorthands

$$\ell \triangleq \left\lceil \frac{\mathsf{M}}{2} \right\rceil, \qquad \mathsf{L} \triangleq \left| \mathcal{C}^{(\mathsf{M})} \right| = \binom{2\ell - 1}{\ell}, \tag{6}$$

where L represents the cardinality of the corresponding weak flip candidate columns set, we are now ready to generalize Definition 2.

Definition 5: A *weak flip code* is a codebook that is constructed only by weak flip columns.

Definition 6: A weak flip code is called *fair* if it is constructed by an equal number of all possible weak flip candidate columns in $\mathcal{C}^{(\mathsf{M})}$. Hence, the blocklength of a fair weak flip code is always a multiple of L.

Note that fair weak flip codes have been used by Shannon *et al.* for the derivation of error exponents [7].

Lemma 7 (Weak Flip Codes, Plotkin Bound, and Equidistance): A code that achieves the Plotkin bound (1) must be a weak flip code. Moreover, fair weak flip codes always meet the Plotkin bound, and they are equidistant.

Related to the weak flip codes and the fair weak flip codes are the families of Hadamard codes [6, Ch. 2]. Note that every Hadamard code is a weak flip code. Also note that for a given number of codewords M and a blocklength n, the existence of a Hadamard code is not guaranteed. For a more detailed discussion of Hadamard codes, see [1].

III. Main Results

The main result of this paper is that for many blocklengths n, equidistant codes that achieve the Plotkin bound (1) with equality, i.e., they maximize the minimum Hamming distance, are strictly suboptimal.

Theorem 8: Fair weak flip codes with an arbitrary number of codewords M and with a blocklength n such that $n \bmod \mathsf{L} = 0$, are strictly suboptimal on a BSC.

Theorem 8 can be extended to general equidistant codes that meet the Plotkin bound (1).

Theorem 9: For many blocklengths n, all equidistant codes that meet the Plotkin bound (1) with equality (in particular, all equidistant Hadamard codes) are strictly suboptimal on a BSC.

Acknowledgment

This work was supported by the National Science Council under NSC 100–2221–E–009–068–MY3.

References

[1] P.-N. Chen, H.-Y. Lin, and S. M. Moser, "Weak flip codes and applications to optimal code design on the binary erasure channel," in *Proc. 50th Allerton Conf. Commun., Contr. and Comput.*, Monticello, IL, USA, Oct. 1–5, 2012.

[2] C. E. Shannon, "A mathematical theory of communication," *Bell System Techn. J.*, vol. 27, pp. 379–423 and 623–656, Jul. and Oct. 1948.

[3] S. Lin and D. J. Costello, Jr., *Error Control Coding*, 2nd ed. Upper Saddle River, NJ: Prentice Hall, 2004.

[4] P.-N. Chen, H.-Y. Lin, and S. M. Moser, "Ultra-small block-codes for binary discrete memoryless channels," in *Proc. IEEE Inf. Theory Workshop*, Paraty, Brazil, Oct. 16–20, 2011, pp. 175–179.

[5] ——, "Optimal ultra-small block-codes for binary discrete memoryless channels," 2013, to app. in *IEEE Trans. Inf. Theory*. [Online]. Available: http://moser.cm.nctu.edu.tw/publications.html

[6] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.

[7] C. E. Shannon, R. G. Gallager, and E. R. Berlekamp, "Lower bounds to error probability for coding on discrete memoryless channels," *Inform. Contr.*, pp. 522–552, May 1967, part II.