Non-linear Cyclic Codes that Attain the Gilbert-Varshamov Bound

Ishay Haviv*, Michael Langberg†, Moshe Schwartz‡, and Eitan Yaakobi§
*School of Computer Science, The Academic College of Tel Aviv-Yaffo,
Tel Aviv 61083, Israel, ishayhav@mta.ac.il
†Department of Electrical Engineering, State University of New-York at Buffalo,
Buffalo, NY 14260, USA, mikel@buffalo.edu
‡Department of Electrical and Computer Engineering, Ben-Gurion University of the Negev,
Beer Sheva 8410501, Israel, schwartz@ee.bgu.ac.il
§Department of Computer Science, Technion – Israel Institute of Technology,
Haifa 32000, Israel, yaakobi@cs.technion.ac.il

***Abstract*—We prove that there exist non-linear binary cyclic codes that attain the Gilbert-Varshamov bound.**

***Index Terms*—Cyclic codes, non-linear codes, Gilbert-Varshamov bound, good family of codes**

I. Introduction

For a finite field $\mathbb{F}_q$, a *cyclic code* of length n is a linear subspace $C \subseteq \mathbb{F}_q^n$ that is closed under cyclic permutations, i.e., for every codeword $x \in C$, all cyclic permutations of x are also included in C. Cyclic codes have been extensively studied over the last decades exhibiting a rich algebraic structure with immense applications in storage and communication, e.g., [3], [7], [11], [13].

A code over alphabet Σ is said to have *(normalized) minimum distance* at least $\delta \in [0,1]$ if any two distinct codewords in $C \subseteq \Sigma^n$ are of Hamming distance at least δn. It is also said to have *rate* $R(C) \triangleq \frac{1}{n}\log_{|\Sigma|}|C|$. Of particular interest are *good families of codes*, which are sequences of codes $C_1, C_2, \ldots$, with C_i of length n_i, rate R_i, and minimum normalized distance δ_i, such that simultaneously,

$$\lim_{i\to\infty} n_i = \infty, \qquad \lim_{i\to\infty} R_i > 0, \quad \text{and} \qquad \lim_{i\to\infty} \delta_i > 0.$$

One of the most fundamental challenges in coding theory is to construct good families of codes. Several such families were presented in the literature over the years. This includes, for example, the Gilbert-Varshamov (GV) codes [8], [15] and the algebraic constructions of Justesen [10] and Goppa [9] (see also [11]). However, the existence of a good family of *cyclic* (linear) codes is a long-standing open problem, see e.g., [2], [5], [6], [12].

In an attempt to shed some light on the problem of good cyclic codes, some works considered close variants to cyclic codes. Quasi-cyclic and double-circulant codes are one example, created by interleaving cyclic codes. These families were shown to contain families of good codes [11, Ch. 16]. Another such example is the family of module skew codes, which are almost cyclic except for a slight twist in the permutation. These were recently shown to contain a good family of codes [1].

In this work, we study another variant of cyclic codes – *non-linear* cyclic codes[1]. For simplicity of presentation we consider only the binary case. We will show that this family of codes contains a good family which asymptotically meets the GV bound [8], [15], i.e., of normalized distance δ and asymptotic rate approaching $1 - H(\delta)$, where H stands for the binary entropy function. This matches the best known lower bound for binary codes of minimum normalized distance δ that are not necessarily cyclic. To the best of our knowledge, good families of non-linear binary cyclic codes have not been previously presented in the literature.

Our construction of good binary non-linear cyclic codes is conceptually very simple and includes two steps. In the first step we construct a high-rate binary code which we call *auto-cyclic*. (All formal definitions are given below in Section II.) An auto-cyclic code is a non-linear cyclic code in which the set of cyclic permutations of any given codeword is of (normalized) minimum distance at least δ. In this context, we refer to δ as the *auto-cyclic* distance. Auto-cyclic codes are reminiscent of *orthogonal* or low *auto-correlation* codes, e.g. [4], [14]. Using a probabilistic argument, we show the existence of a subset of $\{0,1\}^n$ of asymptotic rate 1 which is auto-cyclic with auto-cyclic distance δ arbitrarily close to $\frac{1}{2}$. Once a high-rate auto-cyclic code is established, we greedily remove some of its elements (using a slight variant of the well known greedy process that leads to the GV bound) to obtain the desired non-linear cyclic code C of rate $1 - H(\delta)$ and minimum distance δ.

The remainder of this note is structured as follows. In Section II we present our formal definitions. In Section III we prove the existence of binary non-linear cyclic codes that meet the GV bound. Section IV includes concluding remarks and open questions.

Authors appear in alphabetical order. Research supported in part by NSF grant 1526771, the Israel Science Foundation (ISF) grants No. 130/14, and No. 1624/14.

[1]It is common in the literature to define cyclic codes as linear. Thus, we shall make it a point to emphasize the fact that the codes we consider *may be* non-linear by naming them *non-linear cyclic codes*.

II. Preliminaries

Let $[n] \triangleq \{0,1,\ldots,n-1\}$. In the context of indices, all addition and multiplication operations are done modulo n.

Definition 1. *Let $x = x_0,\ldots,x_{n-1} \in \{0,1\}^n$. For all $i \in [n]$, the cyclic shift of x i-locations to the left is defined as*

$$E^i(x) \triangleq x_i,\ldots,x_{n-1},x_0,\ldots,x_{i-1}.$$

Definition 2. *Let $x = x_0,\ldots,x_{n-1}, y = y_0,\ldots,y_{n-1} \in \{0,1\}^n$. The (normalized) Hamming distance between x and y is defined as*

$$d(x,y) \triangleq \frac{|\{i \in [n] : x_i \neq y_i\}|}{n}.$$

The cyclic Hamming-distance between x and y is defined as

$$d_{\text{cyc}}(x,y) \triangleq \min_{i\in[n]} d(E^i(x),y) = \min_{i\in[n]} d(x,E^i(y)).$$

The auto-cyclic Hamming-distance between x and itself is defined as

$$d^*_{\text{cyc}}(x,x) \triangleq \min_{i:E^i(x)\neq x} d(E^i(x),x).$$

Notice that in the definition of the auto-cyclic distance we only consider shifts $E^i(x)$ that differ from x. For the all-0 vector 0^n and the all-1 vector 1^n we define the auto-cyclic distance to be n.

Definition 3. *A subset $C \subseteq \{0,1\}^n$ is* cyclic *if for every $x \in C$ and every $i \in [n]$ it holds that $E^i(x) \in C$.*

Definition 4. *We say that $C \subseteq \{0,1\}^n$ is an $[n,\delta]$ binary* auto-cyclic code *if C is cyclic and in addition for every $x \in C$ it holds that $d^*_{\text{cyc}}(x,x) \geqslant \delta$.*

Definition 5. *We say that $C \subseteq \{0,1\}^n$ is an $[n,\delta]$ binary non-linear* cyclic code *if C is cyclic and in addition, for every $x,y \in C$, $x \neq y$, it holds that $d(x,y) \geqslant \delta$.*

Definition 6. *The rate of a subset $C \subseteq \{0,1\}^n$ is defined by*

$$R(C) \triangleq \frac{\log_2 |C|}{n}.$$

Definition 7. *The asymptotic rate of an infinite sequence of codes $\mathcal{C} = \{C_i\}_{i=1}^{\infty}$, where $C_i \subseteq \{0,1\}^{n_i}$, $n_i < n_{i+1}$ for all i, is defined as*

$$\mathcal{R}(\mathcal{C}) \triangleq \limsup_{i\to\infty} R(C_i) = \limsup_{i\to\infty} \frac{\log_2 |C_i|}{n_i}.$$

III. Non-linear Cyclic Codes

We start with the following lemma that provides a probabilistic construction of binary auto-cyclic codes of high rate.

Lemma 8. *For every $0 \leqslant \delta < \frac{1}{2}$ and every sufficiently large prime n, there exists a code $C \subseteq \{0,1\}^n$ of rate at least $1 - \frac{1}{n}$ satisfying $d(E^i(x),x) \geqslant \delta$ for every $x \in C$ and $i \in [n] \setminus \{0\}$. In particular, there exists a sequence of binary auto-cyclic codes of normalized minimum distance δ and asymptotic rate 1.*

Proof: Let n be a sufficiently large prime. Consider choosing a random element $x = x_0,\ldots,x_{n-1}$ in $\{0,1\}^n$ from the uniform distribution. Namely, each entry of x is chosen i.i.d. uniformly over $\{0,1\}$. Let $i \in [n] \setminus \{0\}$. We first analyze the probability

$$\Pr_x \left[d(E^i(x),x) \geqslant \delta\right].$$

In our analysis we will use the fact that for a prime n, the sequence $0, i, 2i, 3i, \ldots, (n-1)i$ consists of elements that are all distinct modulo n. For $k \in [n]$, let A_k be the indicator of the event that the ki-th coordinate (modulo n) of x differs from that of $E^i(x)$, namely that x_{ki} differs from $x_{(k+1)i}$. As n is prime it holds that

$$\Pr_x \left[d(E^i(x),x) \geqslant \delta\right] = \Pr_x \left[\sum_{k\in[n]} A_k \geqslant \delta n\right].$$

Let $a = a_0,\ldots,a_{n-1} \in \{0,1\}^n$ be an arbitrary vector, and consider the probability

$$\Pr[\forall k : A_k = a_k] = \prod_{k=0}^{n-1} \Pr[A_k = a_k \mid A_0 = a_0,\ldots,A_{k-1} = a_{k-1}].$$

Notice that each A_k depends only on x_{ki} and $x_{(k+1)i}$. Using the fact that the sequence $0, i, 2i, 3i, \ldots, (n-1)i$ consists of elements that are all distinct modulo n, we conclude that for $k \in \{0,\ldots,n-2\}$:

$$\Pr[A_k = a_k \mid A_0 = a_0,\ldots,A_{k-1} = a_{k-1}] = \frac{1}{2}.$$

Here, we used the fact that each entry x_i of x is uniform over $\{0,1\}$ and that $x_{(k+1)i}$ is independent of the entries $\{x_{\ell i}\}_{\ell\in[k]}$ that determine the events $A_0,\ldots,A_{k-1}$. Thus,

$$\Pr[\forall k : A_k = a_k] \leqslant \frac{1}{2^{n-1}}.$$

We now conclude that for any $i \in [n] \setminus \{0\}$,

$$\begin{aligned}\Pr_x \left[d(E^i(x),x) < \delta\right] &= \Pr_x \left[\sum_{k\in[n]} A_k < \delta n\right] \\ &\leqslant \sum_{\substack{a\in\{0,1\}^n \\ d(a,0)<\delta}} \Pr_x[\forall k : A_k = a_k] \\ &\leqslant \frac{2^{H(\delta)n}}{2^{n-1}}.\end{aligned}$$

Above, we upper bound the Hamming ball of radius δn by $2^{H(\delta)n}$, where H stands for the binary entropy function. By the union bound over $i \in [n] \setminus \{0\}$, we have

$$\Pr_x \left[\exists i \in [n] \setminus \{0\}, d(E^i(x),x) < \delta\right] \leqslant 2(n-1) \cdot 2^{(H(\delta)-1)n}. \tag{1}$$

Finally, define

$$C \triangleq \left\{x \in \{0,1\}^n : \forall i \in [n] \setminus \{0\}, d(E^i(x),x) \geqslant \delta\right\}.$$

By (1) we have

$$|C| \geqslant 2^n - 2(n-1) \cdot 2^{H(\delta)n} \geqslant 2^{n-1},$$

for $\delta < \frac{1}{2}$ and a sufficiently large n, so the rate of C is at least $1 - 1/n$. In addition, if $x \in C$ then any cyclic shift of x is also in C. ∎

Equipped with Lemma 8, we are ready to prove our main result stated below.

Theorem 9. *For every $0 < \delta < \frac{1}{2}$ and $R < 1 - H(\delta)$ there exists a sequence of binary non-linear cyclic codes of normalized minimum distance at least δ and asymptotic rate at least R.*

Proof: Fix $\varepsilon > 0$ and let $R \triangleq 1 - H(\delta) - \varepsilon$. We construct for every sufficiently large prime n an $[n, \delta]$ binary non-linear cyclic code C of rate at least R. Our construction has two steps. In the first step, using Lemma 8, we construct an $[n, \delta]$ auto-cyclic code C' of rate at least $1 - \varepsilon$. Specifically,

$$C' = \left\{ x \in \{0,1\}^n : \forall i \in [n] \setminus \{0\}, d(E^i(x), x) \geqslant \delta \right\}.$$

In the second step we construct C by a greedy procedure similar to that used in the standard GV bound. Specifically, we start with $C = \emptyset$. Let x be any word in C'. Add x and all its cyclic shifts $\left\{E^i(x)\right\}_{i \in [n]}$ to C and remove them from C'. In addition, remove from C' all words y for which $d_{\text{cyc}}(x, y) < \delta$. In this process, since $d_{\text{cyc}}(x, y) = \min_i d(E^i(x), y)$, we remove at most $n 2^{H(\delta)n}$ words from C'. Here, as before, we upper bound the Hamming ball of radius δn by $2^{H(\delta)n}$. Note that for any y removed, we also remove all its cyclic shifts.

We now continue in iterations, in each iteration we add an element $x \in C'$ and all its cyclic shifts to C and remove all y for which $d_{\text{cyc}}(x, y) < \delta$ from C' (including x and its cyclic shifts). We continue in this fashion until C' is empty.

As in every iteration we add n words to the code C, it follows that its final size is at least

$$|C| \geqslant n \cdot \frac{|C'|}{n \cdot 2^{H(\delta)n}} = \frac{|C'|}{2^{H(\delta)n}},$$

and thus its rate satisfies

$$R(C) \geqslant 1 - H(\delta) - \varepsilon = R.$$

The code C is an $[n, \delta]$ binary non-linear cyclic code. Namely, by construction, for each $x \in C$ and $i \in [n]$ it holds that $E^i(x) \in C$. Moreover, by the iterative procedure, any distinct $x, x' \in C$ satisfy $d(x, x') \geqslant \delta$. ∎

IV. Conclusion

In this work we proved the existence of a good family of binary non-linear cyclic codes of normalized distance δ and asymptotic rate $1 - H(\delta)$ (i.e., codes that meet the GV bound). The codes we construct are non-linear. Specifically, for $\delta < \frac{1}{2}$, the code C' obtained in the first step of our construction is the collection of all codewords x with auto-cyclic distance greater or equal to δ. This code is not linear. To see this, consider any x for which for all $i \in [n] \setminus \{0\}$ it holds that $d(x, E^i(x)) \geqslant \delta + \frac{2}{n}$. The proof of Lemma 8 shows the existence of several such x. Consider now the codeword $y = x + 0^{n-1}1$. The codeword y satisfies the slightly weaker condition that for all $i \in [n] \setminus \{0\} : \ d(y, E^i(y)) \geqslant \delta$. So both x and y have auto-cyclic distance at least δ however $x + y = 0^{n-1}1$ has auto-cyclic distance of $\frac{2}{n}$. The second step of our construction, which removes elements from C' to obtain the cyclic code C of distance δ and rate arbitrarily close to $1 - H(\delta)$, is greedy and does not necessarily yield linear codes. Whether the first step of our construction can be refined using algebraic techniques to yield a linear auto-cyclic code, or whether the second step of our construction (assuming a linear C') can yield a linear code C, are intriguing problems left open in this work. Problems that, if solved, may shed light on the existence of good binary linear cyclic codes.

V. Acknowledgment

The authors would like to thank Alexander Barg for his valuable comments on an earlier draft of this work.

References

[1] A. Alahmadi, A. Leroy, and P. Solé, "Long module skew codes are good," *Discrete Mathematics*, vol. 339, no. 5, pp. 1624–1627, 2016.
[2] L. M. J. Bazzi and S. K. Mitter, "Some randomized code constructions from group actions," *IEEE Transactions on Information Theory*, vol. 52, no. 7, pp. 3210–3219, 2006.
[3] R. Chien, "Cyclic decoding procedures for Bose-Chaudhuri-Hocquenghem codes," *IEEE Transactions on Information Theory*, vol. 10, no. 4, pp. 357–363, 1964.
[4] F. R. K. Chung, J. A. Salehi, and V. K. Wei, "Optical orthogonal codes: design, analysis and applications," *IEEE Transactions on Information theory*, vol. 35, no. 3, pp. 595–604, 1989.
[5] C. Ding and Z. Zhou, "Binary cyclic codes from explicit polynomials over GF(2^m)," *Discrete Mathematics*, vol. 321, pp. 76–89, 2014.
[6] S. T. Dougherty, J. Kim, and P. Solé, "Open problems in coding theory," *Contemp. Math*, vol. 634, pp. 79–99, 2015.
[7] G. D. Forney, "On decoding BCH codes," *IEEE Transactions on Information Theory*, vol. 11, no. 4, pp. 549–557, 1965.
[8] E. N. Gilbert, "A comparison of signalling alphabets," *Bell System Technical Journal*, vol. 31, no. 3, pp. 504–522, 1952.
[9] V. D. Goppa, "A new class of linear error-correcting codes," *Probl. Peredachi Inf.*, vol. 6, no. 3, pp. 24–30, 1970.
[10] J. Justesen, "Class of constructive asymptotically good algebraic codes," *IEEE Transactions on Information Theory*, vol. 18, no. 5, pp. 652–656, 1972.
[11] F. J. MacWilliams and N. J. A. Sloane, *The theory of error correcting codes*. Elsevier, 1977.
[12] C. Martínez-Pérez and W. Willems, "Is the class of cyclic codes asymptotically good?" *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 696–700, 2006.
[13] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE Transactions on Information Theory*, vol. 15, no. 1, pp. 122–127, 1969.
[14] D. Sarwate, "Bounds on crosscorrelation and autocorrelation of sequences," *IEEE Transactions on Information Theory*, vol. 25, no. 6, pp. 720–724, 1979.
[15] R. R. Varshamov, "Estimate of the number of signals in error correcting codes," *Dokl. Acad. Nauk*, vol. 117, pp. 739–741, 1957.