Minimum Distance Bounds for Expander Codes

VITALY SKACHEK
Claude Shannon Institute
University College Dublin
Belfield 4, Dublin, Ireland
E-mail: vitaly.skachek@ucd.ie

Open Problems Session

***Abstract*— Several expander code constructions and their parameters are surveyed. New generalized expander codes are introduced and their properties are compared with the properties of the existing constructions. Finally, some possible directions to extend the current research on expander codes are discussed.**

I. INTRODUCTION AND NOTATION

The interest in the field of coding theory has emerged with the classical work of Shannon back in 1948. A lot of research has been done since then in the framework of a 'classical' coding theory. In the recent years, however, the field has changed dramatically due to the recent advances in iterative decoding and list decoding.

The problem of finding code families with good parameters is a central problem in the field. In particular, the code families with good trade-offs between the rate and the relative minimum distance are of great interest. In the present survey, we will focus on this and the related problems.

We start with the formal definition. A set $\mathcal{C}$ of words of length n over the alphabet Σ is called a *code* over Σ of *length* n. Consider two words $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$ in Σ^n. The *Hamming distance* between $\boldsymbol{x}$ and $\boldsymbol{y}$ is defined as the number of pairs of symbols (x_i, y_i), $1 \le i \le n$, such that $x_i \neq y_i$, and is denoted by $\mathsf{d}(\boldsymbol{x}, \boldsymbol{y})$. The *minimum distance* of a code $\mathcal{C}$ is defined as

$$d = \min_{\boldsymbol{x},\boldsymbol{y} \in \mathcal{C},\ \boldsymbol{x} \neq \boldsymbol{y}} \mathsf{d}(\boldsymbol{x}, \boldsymbol{y}).$$

The *relative minimum distance* of $\mathcal{C}$ is defined as $\delta = d/n$.

Denote by $\boldsymbol{x}^T$ the transpose of the vector $\boldsymbol{x}$. A code $\mathcal{C}$ over a field $\mathbb{F} = \mathrm{GF}(q)$ is said to be a *linear* $[n, k, d]$ *code* if there exists matrix $\mathcal{H}$ with entries in $\mathbb{F}$ with n columns and rank $n - k$ such that for all $\boldsymbol{x} \in \mathbb{F}^n$

$$\mathcal{H}\boldsymbol{x}^T = \overline{0} \ \Leftrightarrow \ \boldsymbol{x} \in \mathcal{C},$$

and the minimum distance of the code $\mathcal{C}$ is d. The matrix $\mathcal{H}$ is called a *parity-check matrix* of the code $\mathcal{C}$. The value k is called the *dimension* of the code $\mathcal{C}$, and the ratio $\mathcal{R} = k/n$ is called the *rate* of the code $\mathcal{C}$.

Let $\mathcal{C}$ be a code of minimum distance d over Σ, and let $\boldsymbol{y} \in \Sigma^n$. The *unique decoding* problem consists of finding $\boldsymbol{c} \in \mathcal{C}$ (if such $\boldsymbol{c}$ exists), such that $\mathsf{d}(\boldsymbol{c}, \boldsymbol{y}) < d/2$.

II. RESULTS FOR CLASSICAL CODES

A. Gilbert-Varshamov Bound

Let $\mathsf{H}_q : [0,1] \to [0,1]$ be the q-ary entropy function defined by

$$\mathsf{H}_q(x) = x \log_q(q-1) - x \log_q x - (1-x) \log_q(1-x) \ .$$

The following classical result claims the existence of good codes.

Theorem 2.1: Let $\mathbb{F} = \mathrm{GF}(q)$, and let $\delta \in (0, 1 - 1/q]$ and $\mathcal{R} \in (0,1)$, such that

$$\mathcal{R} \le 1 - \mathsf{H}_q(\delta) \ . \qquad (1)$$

Then, for large enough values of n, there exists a linear $[n, \mathcal{R}n, \ge \delta n]$ code over $\mathbb{F}$.

The expression in (1) is often referred as the Gilbert-Varshamov bound. For the binary codes, we denote $\delta_{GV}(\mathcal{R}) = \mathsf{H}_2^{-1}(1 - \mathcal{R})$.

It should be noted that Theorem 2.1 shows only the existence of the code attaining (1). However, as of yet, there is no known general explicit way to construct such a code.

The improvements of the Gilbert-Varshamov bound were studied recently. The reader can refer to [9], [12], [22].

B. Bounds for Concatenated Codes

First, we revisit the definition of concatenated codes [8]. The following ingredients will be used:

- A linear $[\Delta, k = r\Delta, \theta\Delta]$ code $\mathcal{C}$ over $\mathbb{F} = \mathrm{GF}(q)$ (inner code).
- A linear $[n, R_\Phi n, \delta_\Phi n]$ code $\mathbb{C}_\Phi$ over $\Phi = \mathbb{F}^k$ (outer code).
- A linear one-to-one mapping $\mathcal{E} : \Phi \to \mathcal{C}$.

The respective concatenated code $\mathbb{C}$ of length $N = \Delta \cdot n$ over $\mathbb{F}$ is defined as

$$\mathbb{C} = \Big\{ (\boldsymbol{c}_1 | \boldsymbol{c}_2 | \cdots | \boldsymbol{c}_n) \in \mathbb{F}^{\Delta n} : \boldsymbol{c}_i = \mathcal{E}(a_i) \ , \\ \text{for } i \in 1, 2, \cdots, n, \ \text{ and } (a_1 a_2 \cdots a_n) \in \mathbb{C}_\Phi \Big\} \ .$$

The rate of $\mathbb{C}$ is known to be $\mathcal{R} = r R_\Phi$. The relative minimum distance of $\mathbb{C}$, δ, is at least $\delta \ge \theta \delta_\Phi$.

Generalized minimum distance (GMD) decoder was proposed in [8]. It is able to correct any error pattern of relative size less than $\frac{1}{2}\delta$.

A modified version of concatenated codes was proposed by Justesen in [13]. The proposed codes were shown to satisfy the Zyablov bound

$$\delta \geq \max_{\mathcal{R} \leq r \leq 1} \left(1 - \frac{\mathcal{R}}{r}\right) \mathsf{H}_q^{-1}(1-r) \qquad (2)$$

for a wide range of rates.

An improvement of the Zyablov bound was obtained in [6] using a *multilevel concatenation*. It was shown that multilevel binary concatenated code (almost) attain the following relation between the rate and the relative minimum distance, known as the Blokh-Zyablov bound:

$$\mathcal{R} = 1 - \mathsf{H}_2(\delta) - \delta \int_0^{1-\mathsf{H}_2(\delta)} \frac{dx}{\mathsf{H}_2^{-1}(1-x)} \; .$$

Further improvement on the minimum distance of explicitly built binary codes was obtained in [14] by using concatenation of algebraic-geometric codes with small binary codes. However, the minimum distance estimates of all these codes lie below the Gilbert-Varshamov bound.

III. Expander Codes

A. Graphs and Eigenvalues

Consider a Δ-regular undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with a vertex set $\mathcal{V}$ and an edge set $\mathcal{E}$. Denote by $A_{\mathcal{G}}$ the adjacency matrix of $\mathcal{G}$. It is easy to see that Δ is the largest eigenvalue of $A_{\mathcal{G}}$. Let λ^* be the second largest absolute value of any eigenvalue of $A_{\mathcal{G}}$. It was shown in [1] that lower ratios $\frac{\lambda^*}{\Delta}$ imply greater values of *graph expansion*.

An expander graph for which the relation

$$\lambda^* \leq 2\sqrt{\Delta - 1}$$

holds is called a *Ramanujan graph*. Ramanujan graphs have essentially the smallest possible value of λ^* (given Δ) [1]. It is known that there exist infinite families of such graphs with the number of vertices approaching infinity for fixed values of vertex degree Δ [15], [16]. We denote by $\gamma_{\mathcal{G}}$ the ratio between the second largest eigenvalue of $A_{\mathcal{G}}$ and Δ.

B. Basic Code Constructions

A method to construct codes using graphs was proposed by Tanner [21]. Expander codes were proposed in [18], and modified in [23], [4]. We recall the construction in [4].

Let $\mathcal{G}$ be a bipartite graph as above with a vertex set $\mathcal{V} = A \cup B$ such that $A \cap B = \emptyset$, $|A| = |B| = n$, and every edge has one endpoint in A and one endpoint in B. For every vertex $u \in \mathcal{V}$, we denote by $\mathcal{E}(u)$ the set of edges that are incident with u. Assume an ordering on $\mathcal{V}$, thereby inducing an ordering on the edges of $\mathcal{E}(u)$ for every $u \in \mathcal{V}$. For a field $\mathbb{F}$ and a word $\boldsymbol{z} = (z_e)_{e \in \mathcal{E}}$ in $\mathbb{F}^{|E|}$, denote by $(\boldsymbol{z})_{\mathcal{E}(u)}$ the sub-block of $\boldsymbol{z}$ that is indexed by $\mathcal{E}(u)$.

Let $\mathcal{C}_A$ and $\mathcal{C}_B$ be two linear codes of length Δ over $\mathbb{F}$. Denote $N = |\mathcal{E}| = \Delta n$. The code $\mathbb{C} = (\mathcal{G}, \mathcal{C}_A : \mathcal{C}_B)$ is defined as the following linear code of length N over $\mathbb{F}$:

$$\mathbb{C} = \Big\{ \boldsymbol{c} \in \mathbb{F}^N \; : \; (\boldsymbol{c})_{\mathcal{E}(u)} \in \mathcal{C}_A \text{ for every } u \in A \text{ and } (\boldsymbol{c})_{\mathcal{E}(v)} \in \mathcal{C}_B \text{ for every } v \in B \Big\} \; . \qquad (3)$$

C. Expander Codes Mimic Behavior of Concatenated Codes

In [2], the construction in (3) was modified by introducing so-called 'dangling edges'. It was shown that the modified construction mimics the behavior of concatenated codes. In particular, the parameters of the new codes (almost) attain the Zyablov bound. A linear-time (in N) decoding algorithm was presented that corrects a fraction of errors equaling to (almost) half of this minimum distance bound. Independently, another construction with similar properties was presented in [11].

In [17], it was shown that the construction in [2] can be thought as a concatenation of a nearly-MDS code $\mathbb{C}_\Phi$ with the appropriate inner code, thus providing another explanation for the properties of the codes in [2]. A GMD-type decoding algorithm for decoding of those codes was proposed in [20], [17].

D. Beyond the Zyablov Bound

In [3], using a more sophisticated analysis, the authors improve on the minimum-distance bounds for the codes described in [4] and [2]. In particular, for the binary codes in [4] of rate $\mathcal{R}$, they bound the relative minimum distance from below by

$$\delta(\mathcal{R}) \geq \frac{1}{4}(1-\mathcal{R})^2 \cdot \min_{\delta_{GV}((1+\mathcal{R})/2) \leq \beta \leq \frac{1}{2}} \frac{g(\beta)}{\mathsf{H}_2(\beta)} \; , \qquad (4)$$

where the function $g(\beta)$ is defined in Appendix.

For the binary codes in [2] of rate $\mathcal{R}$, the relative minimum distance is bounded from below by

$$\delta(\mathcal{R}) \geq \max_{\mathcal{R} \leq r \leq 1} \left\{ \min_{\delta_{GV}(r) \leq \beta \leq \frac{1}{2}} \left(\delta_0(\beta, r) \cdot \frac{1 - \mathcal{R}/r}{\mathsf{H}_2(\beta)} \right) \right\} , \qquad (5)$$

where the function $\delta_0(\beta, r)$ is defined in Appendix.

In particular, it follows that the relative minimum distance of these two families of codes is higher than the Zyablov bound (2) for a wide range of code rates.

Further improvement on the minimum distance of expander-based codes was obtained by elaborating on the ideas in [6]. The family of multilevel expander codes was constructed in [5], which has the minimum distance similar to that of the codes in [6]. The linear-time decoding algorithm for these codes was also presented in [5], it corrects any error pattern of size which is (almost) half of the lower bound on the minimum distance.

In Figure 1, the bounds (4) and (5) are compared with the Zyablov bound, the Blokh-Zyablov bound and the Gilbert-Varshamov bound. The bounds (4) and (5) appear in Figure 1 as "Barg-Zemor bound 1" and "Barg-Zemor bound 2", respectively.

E. Toward Gilbert-Varshamov Bound

A probabilistic construction of binary linear codes meeting the Gilbert-Varshamov bound for very low rates was presented in [10]. These codes admit polynomial-time encoding and decoding up to half minimum distance.

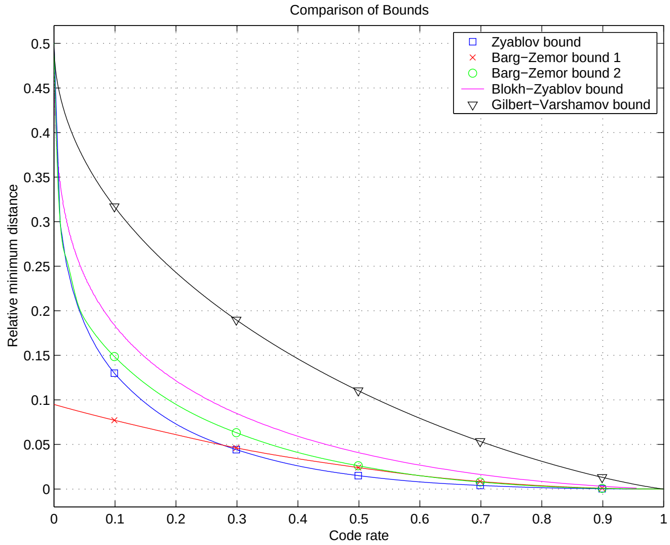

Fig. 1. Comparison of minimum distance bounds

IV. Our Approach

A. Construction of generalized expander codes

In [19, Chapter 4], we aim at improving minimum distance bounds for expander codes. We generalize the code constructions presented in [4], [2]: the codes therein, for every vertex in the set A (or B), have the same set of constraints defined by the code $\mathcal{C}_A$ (or $\mathcal{C}_B$). By contrast, for the codes described in [19, Chapter 4], there is more than one different set of constraints for the vertices in the set A (or B). We call such codes *generalized* expander codes. In the sequel, we present the results of the parameter analysis of a family of generalized expander codes. We also present a linear-time decoding algorithm for the above codes. Moreover, we obtain that the binary codes in [19, Chapter 4] have minimum distance at least as good as the minimum distance of the codes in [3], for a broad range of code rates.

We recall the definition first. Let $\mathcal{G} = (\mathcal{V} = A \cup B, \mathcal{E})$ be a bipartite Δ-regular undirected connected graph as before. We divide B into two sets, B^1 and B^2, such that $B^1 \cap B^2 = \emptyset$, $B^1 \cup B^2 = B$. Let $|B^2| = \eta n$, and thus $|B^1| = (1-\eta)n$. The value $\eta \in [0,1]$ will be defined in the sequel.

Let $\mathbb{F} = \mathrm{GF}(q)$ and assume that $\mathcal{C}_A$, $\mathcal{C}_1$ and $\mathcal{C}_2$ are linear $[\Delta, r_A\Delta, \delta_A\Delta]$, $[\Delta, r_1\Delta, \delta_1\Delta]$ and $[\Delta, r_2\Delta, \delta_2\Delta]$ codes over $\mathbb{F}$, respectively. Below, we generalize the code $\mathbb{C}$ as follows: for any codeword $\boldsymbol{c} \in \mathbb{C}$, the sub-word $(\boldsymbol{c})_{\mathcal{E}(u)}$ is in the code $\mathcal{C}_1$ if $u \in B^1$, and $(\boldsymbol{c})_{\mathcal{E}(u)}$ is in $\mathcal{C}_2$ if $u \in B^2$.

More specifically, we define the code $\mathbb{C} = (\mathcal{G}, \mathcal{C}_A, \mathcal{C}_1, \mathcal{C}_2)$ as the following linear code of length $N = \Delta n$ over $\mathbb{F}$:

$$\begin{aligned} \mathbb{C} = \Big\{ \boldsymbol{c} \in \mathbb{F}^N \quad : \; & (\boldsymbol{c})_{\mathcal{E}(u)} \in \mathcal{C}_A \text{ for every } u \in A, \\ & (\boldsymbol{c})_{\mathcal{E}(u)} \in \mathcal{C}_1 \text{ for every } u \in B^1 \\ \text{and} \quad & (\boldsymbol{c})_{\mathcal{E}(u)} \in \mathcal{C}_2 \text{ for every } u \in B^2 \; \Big\} \end{aligned} \qquad (6)$$

(for $\eta = 0, 1$, or for $\mathcal{C}_1 = \mathcal{C}_2$, the code $\mathbb{C}$ defined herein coincides with its counterpart defined in (3)).

B. Properties of generalized expander codes

Assume that $\delta_1 \geq \delta_2$. The following two theorems present simple bounds on the rate and minimum distance of generalized expander codes.

Theorem 4.1: The rate of the generalized expander code $\mathbb{C}$ is at least

$$\mathcal{R} \geq r_A + (1-\eta)r_1 + \eta r_2 - 1 \; .$$

Theorem 4.2: Let the code $\mathbb{C}$ be defined as above and let

$$\eta < \frac{\delta_A - \gamma_{\mathcal{G}}\sqrt{\delta_A/\delta_2}}{1-\gamma_{\mathcal{G}}} - \gamma_{\mathcal{G}}^{2/3} \; . \qquad (7)$$

Then, the relative minimum distance δ of $\mathbb{C}$ satisfies

$$\delta > \delta_A(\delta_1 - \tfrac{1}{2}\gamma_{\mathcal{G}}^{2/3}) \; .$$

It follows from these two theorems that for some selection of parameters the code $\mathbb{C}$ attains the Zyablov bound. In [19, Chapter 4], we present a linear-time decoding algorithm for the codes in (6). We show that if $\delta_1 > 2\gamma_{\mathcal{G}}^{2/3}$ and (7) holds, then the decoder corrects any error pattern of size up to $\mathbb{J}_{\mathbb{C}}$, where

$$\mathbb{J}_{\mathbb{C}} \triangleq \frac{\frac{1}{2}\delta_1 - \gamma_{\mathcal{G}}^{2/3}\left(1 + \sqrt{2\left(\delta_1 - 2\gamma_{\mathcal{G}}^{2/3}\right)}\right)}{1-\gamma_{\mathcal{G}}} \cdot \delta_A \Delta n \; .$$

Thus, the number of correctable errors for this algorithm is (almost) half of the Zyablov bound.

C. Better distance bounds

By using ideas from [3], we are able to prove the following theorem, which is a counterpart of Theorem 14 therein.

Theorem 4.3: Let $|\mathbb{F}|$ be a power of 2. There exists a polynomial-time constructible family of binary linear codes $\mathbb{C}$ as above of length $N = n\Delta$, $n \to \infty$, and sufficiently large but constant $\Delta = \Delta(\varepsilon)$, whose relative minimum distance satisfies

$$\delta''(\mathcal{R}) \geq \max_{\mathcal{R} \leq r_A \leq 1} \left\{ \min_{\delta_{GV}(r_A) \leq \beta \leq 1/2} \left(\delta_0(\beta, r_A) \frac{1-\mathcal{R}/r_A}{\mathsf{H}_2(\beta)} \right) \right\} - \varepsilon . \qquad (8)$$

It follows from Theorem 4.3 that the codes in (6) are at least as good (from the point of view of their rate-distance trade-offs) as the codes in [3].

D. Discussion

Consider a binary code $\mathbb{C}$ in (6) with parameter η slightly less than the right-hand side in inequality (7). From Theorem 4.3, the relative minimum distance of that code (of rate $\mathcal{R}$) is bounded from below by the expression in (8).

By contrast, consider a binary code $\mathbb{C}$ with parameter $\eta = 0$. Then, the size of the set B^2 is zero, and therefore the code $\mathbb{C}$ coincides with the code in (3). The relative minimum distance of that code (of rate $\mathcal{R}$), $\delta'(\mathcal{R})$, is shown in [3] to satisfy (4).

We can see that the bound $\delta''(\mathcal{R})$ is superior to the Zyablov bound for a wide range of rates. It is also interesting to compare the bounds $\delta'(\mathcal{R})$ and $\delta''(\mathcal{R})$. We see that the bound $\delta''(\mathcal{R})$ is superior for low rates, while the bound $\delta'(\mathcal{R})$ is superior for high rates. It would be nice to derive a combined analytical bound which will be at least as good as both these bounds. One approach could be to take a value of η 'sliding' between zero and the right-hand side of (7), and to establish the point at which the value of η maximizes the appropriate value of the relative minimum distance of the corresponding code $\mathbb{C}$. It seems that this research direction was not fully explored.

V. Open Problems

To this end, we mention some interesting research problems related to the discussed topics.

- *Minimum distance bounds.* We discussed several bounds on the minimum distance of binary classical and expander codes. Further improvements on the minimum distance bounds of the existing codes, as well as constructions of new codes with better parameters is an important open problem.
- *Bounds on error-correcting capabilities of the decoders.* Improvements on the number of correctable errors by the existing algorithms, as well as constructions of new codes having better decoders, is another related open problem.
- *Other types of expander graphs.* We discussed bounds on the minimum distance and on the number of correctable errors of expander codes. The techniques involved in the analysis were based on the eigenvalues properties of expander graphs. Recently, new explicit constructions for expander graphs were discovered, for example the zig-zag construction in [7]. This construction has better vertex-expansion properties than Ramanujan graphs have, but, on the other hand, its eigenvalue separation property is not as good as that of the Ramanujan counterparts. It would be interesting if better properties could be obtained for codes constructed from non-Ramanujan expanders, in particular from the expanders in [7].
- *Generalized expander codes.* We presented generalized expander codes and showed that their parameters are at least as good as the parameters of the expander codes in [3]. It might be interesting to further explore the properties of the generalized expander codes. An interesting question to answer is whether the generalized expander codes have any advantage over the known expander codes, similarly to the strength of irregular LDPC codes compared with regular LDPC codes.

Appendix

Let β_1 be the largest root of the equation

$$\mathsf{H}_2(\beta)\left(\beta - \mathsf{H}_2(\beta)\cdot\frac{\delta_{GV}(\mathcal{R})}{1-\mathcal{R}}\right) = -\left(\beta - \delta_{GV}(\mathcal{R})\right)\cdot\log_2(1-\beta) \ .$$

Moreover, let

$$a_1 = \frac{\beta_1}{\mathsf{H}_2(\beta_1)} - \frac{\delta_{GV}(\mathcal{R})}{\mathsf{H}_2(\delta_{GV}(\mathcal{R}))} \ ,$$

and

$$b_1 = \frac{\delta_{GV}(\mathcal{R})}{\mathsf{H}_2(\delta_{GV}(\mathcal{R}))}\cdot\beta_1 - \frac{\beta_1}{\mathsf{H}_2(\beta_1)}\cdot\delta_{GV}(\mathcal{R})) \ .$$

The function $g(\beta)$ is defined in [3] as

$$g(\beta) = \begin{cases} \dfrac{\delta_{GV}(\mathcal{R})}{1-\mathcal{R}} & \text{if } \beta \le \delta_{GV}(\mathcal{R}) \\ \dfrac{\beta}{\mathsf{H}_2(\beta)} & \text{if } \delta_{GV}(\mathcal{R}) \le \beta \text{ and } \mathcal{R} \le 0.284 \\ \dfrac{a_1\beta + b_1}{\beta_1 - \delta_{GV}(\mathcal{R})} & \begin{array}{l}\text{if } \delta_{GV}(\mathcal{R}) \le \beta \le \beta_1, \\ \quad 0.284 < \mathcal{R} \le 1\end{array} \\ \dfrac{\beta}{\mathsf{H}_2(\beta)} & \text{if } \beta_1 < \beta_1 \le 1, \ 0.284 < \mathcal{R} \le 1 \end{cases}$$

The function $\delta_0(\beta, r)$ is defined to be $\omega^{\star\star}(\beta)$ for $\delta_{GV}(r) \le \beta \le \beta_1$, where

$$\omega^{\star\star}(\beta) = r\beta + (1-r)\mathsf{H}_2^{-1}\left(1 - \frac{r}{1-r}\mathsf{H}_2(\beta)\right) \ ,$$

and β_1 is the only root of the equation

$$\delta_{GV}(r) = w^{\star}(\beta) \ ,$$

where

$$\begin{aligned} w^{\star}(\beta) \quad &= \quad (1-r)\Big(\left(2^{\mathsf{H}_2(\beta)/\beta}+1\right)^{-1} \\ &\qquad + \frac{\beta}{\mathsf{H}_2(\beta)}\left(1 - \mathsf{H}_2\left(\left(2^{\mathsf{H}_2(\beta)/\beta}+1\right)^{-1}\right)\right)\Big) \ . \end{aligned}$$

For $\beta_1 \le \beta \le \frac{1}{2}$, the function $\delta_0(\beta, r)$ is defined to be a tangent to the function $\omega^{\star\star}(\beta)$ drawn from the point $\left(\frac{1}{2}, \omega^{\star}(\frac{1}{2})\right)$.

Acknowledgement

The results in Section IV are a part of the author's Ph.D. Thesis done at the Technion – Israel Institute of Technology under the supervision of Ron M. Roth. The author is grateful to Ron M. Roth for many helpful discussions and advices.

References

[1] N. Alon, *Eigenvalues and expanders, Combinatorica, 6 (1986), pp. 83–96.*

[2] A. Barg, G. Zémor, *Concatenated codes: serial and parallel, IEEE Trans. Inform. Theory, 51 (2005), pp. 1625–1634.*

[3] A. Barg, G. Zémor, *Distance properties of expander codes, IEEE Trans. Inform. Theory, 52 (2006), pp. 78-90.*

[4] A. Barg, G. Zémor, *Error exponents of expander codes, IEEE Trans. Inform. Theory, 48 (2002), pp. 1725–1729.*

[5] A. Barg, G. Zémor, *Multilevel expander codes,* in *Algebraic Coding Theory and Information Theory,* American Math. Soc. 2005, pp. 69-83.

[6] E.L. Blokh, V.V. Zyablov, *Linear Concatenated Codes,* Nauka, Moscow, 1982 (in Russian).

[7] M. Capalbo, O. Reingold, S. Vadhan, A. Wigderson, *Randomness conductors and constant-degree lossless expanders, Proc. 34th Annual ACM Symposium on Theory of Computing (STOC), May 2002, pp. 659–668,* Montréal, Quebec, Canada.

[8] G.D. FORNEY, JR., *Concatenated Codes,* M.I.T. Press, Cambridge, Massachusetts, 1966.

[9] P. GABORIT, G. ZÉMOR, *Asymptotic improvement of the Gilbert-Varshamov bound for linear codes, Proc. IEEE International Symposium on Information Theory (ISIT) 2006,* pp.287–291, Seattle, USA.

[10] V. GURUSWAMI, P. INDYK, *Efficiently decodable low-rate codes meeting Gilbert-Varshamov bound, Proc. 15-th Symposium on Discrete Algorithms,* pp. 756–757, New Orleans, Louisiana, USA.

[11] V. GURUSWAMI, P. INDYK, *Near-optimal linear-time codes for unique decoding and new list-decodable codes over smaller alphabets, Proc. 34th Annual ACM Symposium on Theory of Computing (STOC), May 2002, pp. 812–821,* Montréal, Quebec, Canada.

[12] T. JIANG, A. VARDY, *Asymptotic improvement of the Gilbert-Varshamov bound on the size of binary codes, IEEE Trans. Inform. Theory,* vol. 50, no. 8, pp. 1655–1664, 2004.

[13] J. JUSTESEN, *A class of constructive asymptotically good algebraic codes, IEEE Trans. Inform. Theory, 18 (1972), pp. 652–656.*

[14] G.L. KATSMAN, M.A. TSFASMAN, S.G. VLĂDUT, *Modular curves and codes with a polynomial construction, IEEE Trans. Inform. Theory,* vol. 30, no. 2, pp. 353–355, March 1984.

[15] A. LUBOTSKY, R. PHILIPS, P. SARNAK, *Ramanujan graphs, Combinatorica, 8 (1988), pp. 261–277.*

[16] G.A. MARGULIS, *Explicit group theoretical constructions of combinatorial schemes and their applications to the design of expanders and concentrators, Probl. Inform. Transm., 24 (1988), pp. 39–46.*

[17] R.M. ROTH, V. SKACHEK, *Improved nearly-MDS expander codes, IEEE Trans. Inform. Theory,* vol. 52, no. 8, pp. 3650–3661, August 2006.

[18] M. SIPSER, D.A. SPIELMAN, *Expander codes, IEEE Trans. Inform. Theory, 42 (1996), pp. 1710–1722.*

[19] V. SKACHEK, *Low-Density Parity-Check Codes: Constructions and Bounds,* Ph.D. Thesis, Technion, Haifa, Israel, January 2007.

[20] V. SKACHEK, R.M. ROTH, *Generalized minimum distance iterative decoding of expander codes, Proc. IEEE Inform. Theory Workshop (ITW), Mar.-Apr. 2003, pp. 245–248,* Paris, France.

[21] R.M. TANNER, *A recursive approach to low-complexity codes, IEEE Trans. Inform. Theory, 27 (1981), pp. 533–547.*

[22] V. VU, L. WU, *Improving the Gilbert-Varshamov bound for q-ary codes, IEEE Trans. Inform. Theory,* vol. 51, no. 9, pp. 3200–3208, 2005.

[23] G. ZÉMOR, *On expander codes, IEEE Trans. Inform. Theory, 47 (2001), pp. 835–837.*