On Nearly-MDS Expander Codes[1]

Ron M. Roth Vitaly Skachek
Computer Science Department,
Technion, Haifa 32000, Israel.
{ronny, vitalys}@cs.technion.ac.il

Abstract — **A construction of graph codes is presented that approaches the Singleton bound as the alphabet size goes to infinity. These codes can be decoded by a combined error-erasure decoder whose time complexity grows linearly with the code length.**

I. Introduction

We consider the following family of expander graph codes, which were studied in [1], [2]. Let $\mathcal{G} = (V, E)$ be a bipartite Δ-regular undirected connected graph with the vertex set V partitioned into two subsets, A and B, of size n, and edge set $E \subseteq A \times B$. For every $u \in V$, denote by $E(u)$ the set of edges incident with u and assume some ordering on $E(u)$. Let F be the finite field GF(q). For a word $\boldsymbol{x} = (x_e)_{e\in E}$ over an alphabet (such as F), denote by $(\boldsymbol{x})_{E(u)}$ the sub-word of $\boldsymbol{x}$ that is indexed by $E(u)$. Take $\mathcal{C}_A$ and $\mathcal{C}_B$ to be linear $[\Delta, k{=}r_A\Delta, \delta_A\Delta]$ and $[\Delta, r_B\Delta, \delta_B\Delta]$ codes over F, respectively, and define the code $\mathbb{C}$ as the following linear code of length $|E| = n\Delta$ over F:

$$\mathbb{C} = \left\{ \boldsymbol{c} \in F^{|E|} \ : \ \begin{array}{c} (\boldsymbol{c})_{E(u)} \in \mathcal{C}_A \text{ for all } u \in A \text{ and} \\ (\boldsymbol{c})_{E(u)} \in \mathcal{C}_B \text{ for all } u \in B \end{array} \right\} .$$

Let Φ denote the alphabet F^k, fix some linear one-to-one mapping $\mathcal{E}_A : \Phi \to \mathcal{C}_A$ over F, and let the mapping $\psi : \mathbb{C} \to \Phi^n$ be given by

$$\psi(\boldsymbol{c}) = \left(\mathcal{E}_A^{-1}\left((\boldsymbol{c})_{E(u)}\right)\right)_{u\in A} \ , \quad \boldsymbol{c} \in \mathbb{C} \ .$$

We now define the code $\mathbb{C}_\Phi$ of length n over Φ by

$$\mathbb{C}_\Phi = \{\psi(\boldsymbol{c}) \ : \ \boldsymbol{c} \in \mathbb{C}\} \ ,$$

and denote its rate and relative minimum distance by R_Φ and δ_Φ, respectively. The code $\mathbb{C}$, which was studied in [1], can be represented as a concatenated code with an inner code $\mathcal{C}_A$ over F and an outer code $\mathbb{C}_\Phi$ over Φ. Similarly, the codes studied in [2] can be represented as concatenated codes with $\mathbb{C}_\Phi$ as an outer code, whereas the inner codes is taken over a sub-field of F.

II. Lower bound on the minimum distance

Let $\lambda_\mathcal{G}$ be the second largest eigenvalue of the adjacency matrix of $\mathcal{G}$ and denote by $\gamma_\mathcal{G}$ the value $\lambda_\mathcal{G}/\Delta$. We show that

$$\delta_\Phi \geq \frac{\delta_B - \gamma_\mathcal{G}\sqrt{\delta_B/\delta_A}}{1-\gamma_\mathcal{G}} \ ;$$

in particular, $\delta_\Phi \to \delta_B$ whenever $\gamma_\mathcal{G} \to 0$. Using this bound, we obtain for every designed rate $R < 1$ and (small) $\epsilon > 0$ arbitrarily long codes $\mathbb{C}_\Phi$ such that $R_\Phi > R$ and $\delta_\Phi \geq 1{-}R{-}\epsilon$, thus attaining the Singleton bound when $\epsilon \to 0$. The alphabet size of $\mathbb{C}_\Phi$ is $\exp\left\{O\left((\log(1/\epsilon))/\epsilon^3\right)\right\}$, namely, the exponent here is smaller compared to [3] (yet the code in [3] is also linear-time *encodable*).

[1]This work was supported by Grant No. 94/99 from the Israel Science Foundation.

III. Decoding algorithm

Figure 1 presents an adaptation of the iterative decoder of [4] to the code $\mathbb{C}_\Phi$, with the additional feature of handling erasures (as well as errors over Φ).

Input: Received word $\boldsymbol{y} = (\boldsymbol{y}_u)_{u\in A}$ in $(\Phi \cup \{?\})^n$.

For $u \in A$ **do** $\quad (\boldsymbol{z})_{E(u)} \leftarrow \begin{cases} \mathcal{E}_A(\boldsymbol{y}_u) & \text{if } \boldsymbol{y}_u \in \Phi \\ ??\ldots? & \text{if } \boldsymbol{y}_u = ? \end{cases}$.

For $i \leftarrow 1, 2, \ldots, m$ **do** {

If i is even **then** $X \equiv A$, $\mathcal{D} \equiv \mathcal{D}_A$, **else** $X \equiv B$, $\mathcal{D} \equiv \mathcal{D}_B$.

For $u \in X$ **do** $(\boldsymbol{z})_{E(u)} \leftarrow \mathcal{D}((\boldsymbol{z})_{E(u)})$.

}

Output: $\psi(\boldsymbol{z})$ if $\boldsymbol{z} \in \mathbb{C}$ (and declare 'error' otherwise).

Figure 1: Decoder for $\mathbb{C}_\Phi$.

We use the notation '?' to stand for an erasure. The algorithm makes use of a word $\boldsymbol{z} = (z_e)_{e\in E}$ over $F \cup \{?\}$ that is initialized by the contents of the received word $\boldsymbol{y}$. Iterations $i = 2, 4, 6, \ldots$ use a decoder $\mathcal{D}_A : F^\Delta \to \mathcal{C}_A$ that recovers correctly any pattern of less than $\delta_A\Delta/2$ errors (over F), and iterations $i = 1, 3, 5, \ldots$ use a decoder $\mathcal{D}_B : (F \cup \{?\})^\Delta \to \mathcal{C}_B$ that recovers correctly any pattern of θ errors and ν erasures, provided that $2\theta + \nu < \delta_B\Delta$.

We show that the algorithm in Figure 1 corrects any pattern of μ errors and ρ erasures, provided that $\mu + \frac{1}{2}\rho < \beta n$, where

$$\beta = \frac{(\delta_B/2) - \gamma_\mathcal{G}\sqrt{\delta_B/\delta_A}}{1-\gamma_\mathcal{G}} \ ;$$

in particular, $\beta \to \delta_B/2$ when $\gamma_\mathcal{G} \to 0$. The value of m can be taken to be logarithmic in n, and the overall time complexity of the algorithm is linear in n.

IV. Applications

Using GMD decoding, $\mathbb{C}_\Phi$ can replace the MDS outer code in asymptotic concatenated code constructions that attain the Zyablov bound or the capacity of the memoryless symmetric channel. The decoding complexity of the algorithm in Figure 1 translates into a linear-time complexity of the resulting GMD decoder.

References

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

[2] A. Barg, G. Zémor, *Concatenated codes: serial and parallel,* submitted to *IEEE Trans. Inform. Theory.*

[3] V. Guruswami, P. Indyk, *Near-optimal linear-time codes for unique decoding and new list-decodable codes over smaller alphabets, Proc. STOC'2002,* Montréal, Canada, 812–821.

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