Construction of Asymptotically Good Low-Rate Error-Correcting Codes through Pseudo-Random Graphs

NOGA ALON*† JEHOSHUA BRUCK† JOSEPH NAOR† MONI NAOR†
RON M. ROTH†§

A new technique, based on the pseudo-random properties of certain graphs, known as expanders, is used to obtain new simple explicit constructions of asymptotically good codes. In one of the constructions (construction $\mathcal{C}_1$ below), the expanders are used to enhance Justesen codes by replicating, shuffling and then regrouping the code coordinates. For a given relative minimum distance δ and alphabet size q, the codes thus obtained have rate $R_1(\delta)$ which satisfies the inequality

$$R_1(\delta) \geq \gamma_0(1-\delta) - \frac{\gamma_1}{\log_2 q}$$

for some positive constants γ_0 and γ_1. In particular, for the low-rate neighborhood and for sufficiently large q, these codes lie above the Zyablov bound (cf. [3, Ch. 10]). For the small alphabet range (e.g., $GF(2)$), we obtain a second asymptotic good construction by using construction $\mathcal{C}_1$ as an outer code in a concatenated scheme. The resulting codes, referred to as construction $\mathcal{C}_2$, have rate $R_2(\delta)$ which is bounded from below by

$$R_2(\delta) \geq \max_{\delta \leq \mu \leq 1-\frac{1}{q}} \gamma_0\left(1 - H_q(\mu)\right)\left(1 - \frac{\delta}{\mu}\right),$$

where $H_q(x) \triangleq -x \cdot \log_q x - (1-x) \cdot \log_q(1-x) + x \cdot \log_q(q-1)$. Although construction $\mathcal{C}_2$ lies below the Zyablov bound (the constant γ_0 is approximately 0.021), they are still superior in the zero-rate neighborhood to previously-known explicit constructions, the best of which is due to Sugiyama et al. [4].

*Department of Mathematics, Tel-Aviv University, Tel-Aviv 69978, Israel.

†IBM Research Division, Almaden Research Center, 650 Harry Road, San Jose, CA 95120.

‡Computer Science Department, Stanford University, Stanford, CA 94305.

§On leave from the Computer Science Department, Technion, Haifa 32000, Israel.

These expander graphs, used in our construction, are Δ-regular undirected graphs $G = (V, E)$ such that, for any fixed real number $\delta_0 \in (0, 1]$, and for any subset of vertices $B \subseteq V$ of size $\geq \delta_0 |V|$, the fraction of vertices in V which have at least one neighbor in B approaches unity "fast" as $\Delta \to \infty$. The specific expanders used are based on those introduced by Lubotzky et al. [1] and Margulis [2].

Given such a graph with $n = |V|$ vertices and a finite field Φ, we then define a mapping $C_{\exp} : \Phi^n \to (\Phi^\Delta)^n$, such that every input n-tuple over Φ of Hamming weight $\geq \delta_0 n$ is mapped into an output n-tuple over Φ^Δ whose Hamming weight (measured over Φ^Δ) is "close" to n. The above-mentioned construction $\mathcal{C}_1$ is now obtained by applying the mapping $C_{\exp}$ to the codewords of Justesen codes, resulting in a code over the alphabet Φ^Δ whose rate is proportional to $1/\Delta$ (Δ and Φ depend on the prescribed alphabet size q and relative minimum distance δ). Construction $\mathcal{C}_2$ is obtained, in turn, by using Construction $\mathcal{C}_1$ as an outer code, with each output symbol undergoing a second level of encoding by Wozencraft's ensemble codes.

References

[1] A. Lubotzky, R. Phillips, P. Sarnak, *Ramanujan graphs, Combinatorica,* 8 (1988), 261–277.

[2] G.A. Margulis, *Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and superconcentrators, Prob. Inform. Trans.,* 24 (1988), 39–46.

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

[4] Y. Sugiyama, M. Kasahara, S. Hirasawa, T. Namekawa, *Superimposed concatenated codes, IEEE Trans. Inform. Theory,* IT-26 (1980), 735–736.