Amplifying the expansion while preserving a low portion of noncommuting checks.

David Ponarovsky

June 8, 2024

1 Notations and Definitions.

Let $G = (L, R, E)$ be an undirected bipartite graph, where L and R stand for the left and right vertices, and E is the set of edges connecting them. We will think of G as the Tanner graph of a linear code, constitutes the set of all possible bits assignments over the left vertices such that any right vertex sees an even number of turned-on bits (left vertices assigned to 1). The local view of the right vertex $v \in R$ is the assignment of bits to its neighbors. The bipartite graph obtained by setting L as the right vertices and R as the left vertices will be called the transposed graph, denoted by $G^\top = (R, L, E)$. n and m will be used to denote $|L|$ and $|R|$, and will often be referred to as the number of bits = code length and the number of checks. The parity check matrix of the code $H \in \mathbb{F}_2^{m\times n}$ is the adjacency matrix defined by E. This means that $H_{u,v} = 1$ only if there is an edge $u, v \in E$, and zero otherwise. It is easy to see that if the assignment $c \in \mathbb{F}_2^n$ is a codeword, then $Hc = 0$, which is why H got its name. For any $c \in \mathbb{F}_2^n$ that is not necessarily a codeword, we call $s = Hc \in \mathbb{F}_2^m$ the syndrome of c, and think of any non-zero entry of s as a check that does not pass.

Let x, y be two different rows of H, or in code language terminology, two different checks. We will say that x and y commute if $xy = 0$ and uncommute otherwise. The uncommuting rate will be defined as the probability of choosing two different uncommute checks, and will be denoted by P.

$$P = \mathbf{Pr}_{x\neq y\in \text{ rows } H}\left[xy \neq 0\right]$$

From now on, we will assume that G has a fixed left and right degree, Δ_l and Δ_r respectively. This means that any left vertex is connected to exactly Δ_l right vertices, and similarly, any right vertex is connected to exactly Δ_r left vertices. We use Δ to denote the maximum of them, $\Delta = \max\{\Delta_l, \Delta_r\}$.

For any subset of vertices $S \subset L \cup R$, we will denote the vertices connected to S by $\Gamma(S)$. G will be said to be a (τ, ε) left-expander if for any $S \subset L$ of size at most τn, it holds that $|\Gamma(S)| > (1 - \varepsilon)\Delta_l|S|$. In the same way, we define a right-expander.

We are interested in the following question: for fixed constants $\Delta, \varepsilon, \tau, \beta$, is there a family of bipartite graphs such that both G and $G^\top$ are (τ, ε) left-expanders, and their uncommuting rate is bounded above by β?

Claim 1.1 (Zig-Zag product preservs uncommuting-rate.). *Let G be a bipartite graph, and let H_l and H_r be the complete graphs with Δ_l and Δ_r vertices, respectively. Assume that $P(G) < \beta$. Then:*

$$P(G \cdot_z [H_l, H_r]) < \beta$$