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 $P(G)$.

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

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?

2 The Zig-Zag Product.

The Zig-Zag product is a procedure to construct a fixed-degree graph from another given graph without reducing the second's expansion too much. We slightly change the original definition and process to support biparitie grpahs with inequal left and right degree.

Definition 2.1. *Let G be a bipartite graph as defined above, and let H_l and H_r be graphs with Δ_l and Δ_r vertices, respectively. We define $G' = G \cdot_z [H_l, H_r]$, the graph obtained by multiplying the graphs G, H_l, and H_r using the Zig-Zag product, to be the graph obtained by the following steps:*

1. *For any vertex v in L, mark Δ_l new vertices on its edge, one vertex for each edge. Connect them according to the edges of H_l. Then, remove v. Each of the new vertices will have a degree of $\deg H_l + 1$, where one edge is associated with an original edge in G and the other matches the structure of H_l.*

2. *Repeat the above process, but replace each right vertex with H_R.*

3. *Now, we will color any edge associated with the smaller graphs H_l and H_r in blue, and any of the original edges of G in red. We define an edge u, v in G' if there is a path composed of a blue edge, a red edge, and another blue edge.*

Notice that G' remains bipartite and its left and right degrees are $\deg H_l \cdot \deg H_r$.

Claim 2.1 (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:*

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

Proof. Consider two checks x and y in G'. Let us abuse notation and refer to the vertices that define those checks as x and y. We will say that a vertex X of G, is the souce of x if x defiend by marking a vetex on X edges. Let X, Y be the sources of x, y respectively. Now let's split to cases:

- If $X = Y$, namely x and y have the same source. In this case, any blue-red-blue path $x \to o \to o' \to w$ from x to $w \in H_l$ that passes through a vertex $o \in H_r/\{y\}$, and $\{o, y\} \in H_r$ matches to a blue-red-blue path $y \to o \to o' \to w$ from y to w, where the first blue edge $\{x, o\}$ is replaced by $\{y, o\}$ to set y at the beginning of the path.

  So, conditioned on $X = Y$, the probability that x, y do not commute is either 0 if $\deg H_l$ is even, or $P(H_r)$.

- **[COMMENT]** Assume H_r, H_l are the complete graphs, and adding self-loops in step 1. If $X \neq Y$, then with probability $1 - P(G)$, X and Y commute in G and therefore there are even number of red edges at the form $\{o, o'\}$ to connect paths from $x, y \to w$.

$$P(G)\binom{m}{2} + Q(G)\binom{m}{2} = \frac{1}{2}mD^2$$
$$Q(G) = \binom{m}{2}^{-1} \cdot \frac{1}{2}mD^2 - P(G)$$

$$P(G') \leq \left(1 - \frac{1}{m}\right)\left(P(G) + Q(G)\frac{1}{\Delta}\right) = \left(1 - \frac{1}{m}\right)\left(\binom{m}{2}^{-1}\frac{mD^2}{2} + \left(1 - \frac{1}{\Delta}\right)P(G)\right)$$

□