Electronic Colloquium on Computational Complexity, Report No. 133 (2024)

Two-Sided Lossless Expanders in the Unbalanced Setting

Eshan Chattopadhyay*
Cornell University
eshan@cs.cornell.edu

Mohit Gurumukhani*
Cornell University
mgurumuk@cs.cornell.edu

Noam Ringach †
Cornell University
nomir@cs.cornell.edu

Yunya Zhao*
Cornell University
yunya@cs.cornell.edu

Abstract

We present the first explicit construction of *two-sided* lossless expanders in the unbalanced setting (bipartite graphs that have many more nodes on the left than on the right). Prior to our work, all known explicit constructions in the unbalanced setting achieved only one-sided lossless expansion.

Specifically, we show that the one-sided lossless expanders constructed by Kalev and Ta-Shma (RANDOM'22)—that are based on multiplicity codes introduced by Kopparty, Saraf, and Yekhanin (STOC'11)—are, in fact, two-sided lossless expanders.

Using our unbalanced bipartite expander, we easily obtain lossless (non-bipartite) expander graphs with high degree and a free group action. As far as we know, this is the first explicit construction of lossless (non-bipartite) expanders with N vertices and degree $\ll N$.

1 Introduction

Lossless expanders are graphs in which small sets of vertices have almost as many neighbors as possible. Formally, we say that a d-regular graph $G = (V, E)$ is a (K, A)-*expander* if for all sets $S \subseteq V$ of size at most K we have that $|\Gamma(S)| \geq A\,|S|$ where $\Gamma(S)$ is the neighborhood of S. Generally, we desire that K is as large as possible with $K = \Omega(|V|\,/d)$. When $A = (1-\varepsilon)d$ for some small ε, we say that G is a (K, ε)-*lossless expander* since only a small fraction of the total number of possible neighbors is lost. As with other pseudorandom objects, it is well-known that a random graph is a lossless expander with high probability [Vad12].

A reasonable question after seeing this definition is whether other notions of expansion, such as spectral or edge expansion, can be used to derive such graphs. Unfortunately, while Ramanujan graphs (optimal spectral expanders) do have expansion factor arbitrarily close to $A = d/2$, there also exist examples of Ramanujan graphs with expansion factor exactly $A = d/2$, showing that spectral expansion does not necessarily give rise to lossless expansion [Kah95].

One can view these graphs as bipartite graphs $G = (L \sqcup R, E)$ with $L = R = V$ and edges across the two sets of vertices according to whether two vertices shared an edge in the original graph. This yields a balanced bipartite graph with expansion from both the left and right sets of vertices. [LH22] showed that such graphs with constant degree and lossless expansion from both sides that have certain algebraic properties are known to have applications to good quantum low-density parity check (qLDPC) codes. Moreover, these qLDPC codes are easier to analyze than the ones of [PK22; DHLV23], which are the only known good qLDPC constructions known to date. However, current explicit constructions of balanced lossless expanders only achieve expansion from one side of the bipartite graph [CRVW02; CRT23; Gol24]. In this balanced setting,

*Supported by a Sloan Research Fellowship and NSF CAREER Award 2045576.
†Supported by NSF GRFP grant DGE – 2139899, NSF CAREER Award 2045576 and a Sloan Research Fellowship.

ISSN 1433-8092

lossless expansion from both the left and right, termed *two-sided lossless expansion*, is only known for small sets of size $K = \Omega(\exp(\sqrt{\log |V|}))$ [HMMP24].

Amazingly, lossless expansion is even possible in the unbalanced setting with $|L| \gg |R|$. Morally, it is surprising that lossless expansion is still possible from a much larger set of vertices to a much smaller set of vertices. Unsurprisingly then, these graphs also find many applications. Often in this setting, lossless expanders are termed *lossless condensers* since the neighbor function that takes in a left vertex and the index of a neighbor and outputs the right vertex has a much shorter output length than input length. In this context as in the balanced setting, current constructions are similarly only able to achieve lossless expansion from the left to the right [TU06; TUZ07; GUV09; KT22], with the best parameters achieved by [GUV09; KT22]. The constructions from these papers have found a wide array of applications in coding theory [SS96], extractor constructions [TU06; TUZ07; GUV09; DKSS13], derandomization [DT23],[1] and probabilistic data structures [UW87; BMRV02], with the unbalanced nature of the graph being essential.

As our first main result, we fill a gap in this line of work by showing that the unbalanced bipartite graph of [KT22] based on the multiplicity codes of [KSY14] is a two-sided lossless expander (Theorem 1). We use this result, in a relatively straightforward way, to obtain two-sided lossless expanders in the balanced setting and, in fact, non-bipartite lossless expanders with high degree, which is our second main result (Theorem 2).

We now define a two-sided lossless expander as:

Definition 1.1 (Two-sided lossless expander)**.** *We say that a (D_L, D_R)-regular bipartite graph $G = (L \sqcup R, E)$ is a* two-sided (K_L, A_L, K_R, A_R)-expander *if for any subset $S_L \subseteq L$ such that $|S_L| \le K_L$ we have that $|\Gamma_{\to}(S_L)| \ge A_L |S_L|$ and similarly that for any subset $S_R \subseteq R$ such that $|S_R| \le K_R$ we have that $|\Gamma_{\leftarrow}(S_R)| \ge A_R |S_R|$. When $A_L = (1-\varepsilon_L)D_L$ and $A_R = (1-\varepsilon_R)D_R$ for small $\varepsilon_L, \varepsilon_R > 0$, we say that G is a* two-sided $(K_L, \varepsilon_L, K_R, \varepsilon_R)$-lossless expander.

With this definition, our main theorem can be informally stated as follows.

Theorem 1 (Informal version of Theorem 5.1)**.** *For infinitely many N and all constant $0 < \delta \le 0.49$, there exists an explicit biregular, two-sided $(K_L, \varepsilon_L = 0.01, K_R, \varepsilon_R = 0.01)$ lossless expander $\Gamma_{\to} : [N] \times [D_L] \to [M]$ where $D_L = \mathrm{poly}(\log N)$, $N^{1.01\delta - o(1)} \le M \le D_L \cdot N^{1.01\delta}$, $K_L = N^{\delta}$, and $K_R = O(M/D_L)$.*

Remark 1.2. *Because [KT22] has optimal left degree of their bipartite graph (up to polynomial factors), we achieve optimal left-degree as well and, with respect to this, achieve optimal right degree, optimal size of sets of vertices on both sides that losslessly expand,*[2] *and the expansion constant.*

Remark 1.3. *Interestingly, while [GUV09] constructed the first unbalanced one-sided lossless expander, our methods do not work to show that the [GUV09] also expands losslessly from the right.*[3] *Determining whether the [GUV09] can also be shown or modified to expand losslessly from the right is an interesting open question.*

We obtain our second main result by taking the bipartite half (see Section 2.2 for more details) of the [KT22] graph, using the fact that it is a two-sided lossless expander:

Theorem 2 (Informal version of Theorem 6.1)**.** *For infinitely many N, there exists an explicit $(K, \varepsilon = 0.01)$ lossless expander $G = (V, E)$ where $|V| = N$, each node has degree in range $[0.99D, D]$ where $N^{0.51} \le D \le N^{0.51+o(1)}$ and $K = N^{0.48}$. Moreover, G is endowed with a free group action from $\mathbb{F}_q$ where $q = \mathrm{poly}(\log N)$.*

One can show that there exist non-bipartite lossless expanders with even constant degree. So, the degree of our lossless graph obtained is far from optimal. Nevertheless, as far as we know, this is the first explicit construction of a lossless (non-bipartite) expander apart from trivial constructions which have either $D = 1$ or $K = O(1)$.

[1] [DT23] instantiated Goldreich's PRG [Gol11] with the lossless expander of [KT22].

[2] To see that this setting of K_R is indeed optimal, note that in a (D_L, D_R)-biregular graph it must be that $N \cdot D_L = M \cdot D_R$ and so $\frac{M}{D_L} = \frac{N}{D_R}$. Hence, $K_R = O(M/D_L) = O(N/D_R)$, the largest possible size.

[3] In fact, the [GUV09] construction is not even right-regular. See Appendix B for details.

2 Proof Overview

In this section, we first outline the proof of Theorem 1—our two-sided lossless expander. Using it, we construct high degree non-bipartite lossless expanders, proving Theorem 2.

2.1 Two-sided lossless expander

We show that the bipartite graph defined in [KT22] based on multiplicity codes is a two-sided lossless expander. The left-to-right lossless expansion was shown in [KT22]. Our main contribution is showing that the KT graph also expands losslessly from right to left. To do this, we first show that the KT graph is right-regular. Second, for any pair of right vertices, we compute the exact number of common left neighbors they have. Finally, for any not-too-large subset on the right, we lower bound the number of its left neighbors by using the inclusion-exclusion principle to subtract all possible double counted common left neighbors from the total number of outgoing edges.

We state an informal version of our result and present details on the strategy sketched above.

Theorem 2.1 (Informal version of Theorem 4.1)**.** *For every field $\mathbb{F}_q$ and $n, s \in \mathbb{N}$ with $15 \leq 2(s+1) < n < char(\mathbb{F}_q)$, and any $\delta > 0$, there exists an explicit bipartite graph $G = (L \sqcup R, E)$ with $L = \mathbb{F}_q^n, R = \mathbb{F}_q^{s+2}$ with left degree $d_L = q$ and right degree $d_R = q^{n-(s+1)}$ such that G is a two-sided (K_L, A_L, K_R, A_R) expander where $K_L = \Omega(q^{s+1})$, $A_L = q - n(s+2)$, $K_R = \delta q^{s+1}$, $A_R = \left(1 - O\left(\delta \cdot \frac{q-1}{q}\right)\right) q^{n-(s+1)}$.*

Theorem 1 is obtained from Theorem 2.1 by instantiating the parameters appropriately (see Section 5 for more details). We now define the KT graph and then claim that it is a lossless right expander.

Definition 2.2 (The KT graph [KT22])**.** *Let $q, n, s \in \mathbb{N}$ be such that q is a prime power, characteristic of the finite field $\mathbb{F}_q \geq n$ and $s \leq n/2$. We define $G = (L \sqcup R, E)$ where $L = \mathbb{F}_q^n, R = \mathbb{F}_q^{s+2}$. The left degree is q and for any $f \in \mathbb{F}_q^n$ and $y \in \mathbb{F}_q$, the y'th neighbor of f is defined as follows: Identify f as member of $\mathbb{F}_q[X]$ with degree of f at most $n-1$; then, the neighbor $\Gamma_{\rightarrow}(f, y)$ will be $(y, f^{(0)}(y), \dots, f^{(s)}(y))$ where $f^{(i)}$ is the i'th iterative derivative of f.*

Theorem 2.3 (The KT graph losslessly expands from the right)**.** *The KT graph G is a right (K_R, A_R)-lossless expander where $K_R = \delta\,|R|$, $\varepsilon_R = O(\delta \cdot \frac{q-1}{q})$ for arbitrary $0 < \delta < 1$. In other words, for any subset $T \subseteq R$, $|T| \leq K_R$, T has at least $(1 - \varepsilon_R) d_R |T|$ neighbors on the left.*

Theorem 2.1 immediately follows from left expansion shown by [KT22] and Theorem 2.3. For the rest of this section, we focus on proving Theorem 2.3 that relies on the following two key lemmas.

Lemma 2.4 (Right regularity)**.** *The KT graph G is right-regular and has right-degree $d_R = q^{n-(s+1)}$.*

Lemma 2.5 (Number of common left neighbors)**.** *For any pair of right-vertices $w_1, w_2 \in \mathbb{F}_q^{s+2}$ such that $w_1 = (y_1, z_1), w_2 = (y_2, z_2)$ where $y_1 \neq y_2 \in \mathbb{F}_q$ and $z_1, z_2 \in \mathbb{F}_q^{s+1}$, we have $|\Gamma_{\leftarrow}(y_1, z_1) \cap \Gamma_{\leftarrow}(y_2, z_2)| = q^{n-(2s+2)}$.*

Theorem 2.3 then follows by an application of the inclusion-exclusion principle—subtracting the maximum number of common neighbors between any pair of vertices in T from the total number of edges leaving T—we get the required lower bound on the size of T's left neighborhood.

We now discuss the proof techniques for showing Lemma 2.4 and Lemma 2.5. We start by making a simple but useful observation on the structure of the KT graph G.

Observation 2.6. *Fix $w = (y, z_0, \cdots, z_s) \in R$ and let $f \in L$ be any left-neighbor of w. Then it must be the case that w is the y'th neighbor of f. Now for any $w' \in R$ such that $w' = (y, z'_0, \cdots, z'_s)$, it holds that $f \notin \Gamma_{\leftarrow}(w')$. This is saying that any pair of right vertices (w, w') that come from the same seed [4] must have disjoint left neighborhoods.*

[4] We sometimes refer to $y \in \mathbb{F}_q$ as the "seed", like in the condensers literature.

Central to our analysis of the right degree and the number of common left neighbors are the following linear maps.

Definition 2.7. *For $y \in \mathbb{F}_q$, define the map $\psi_y(f) : \mathbb{F}_q^n \to \mathbb{F}_q^{s+1}$ as follows: Interpret $f \in \mathbb{F}_q[X]$ as a degree $\leq n-1$ polynomial and map it to $(f^{(0)}(y), \ldots, f^{(s)}(y))$ where $f^{(i)}$ is the i'th iterative derivative of f.*

We note that ψ_y is a $\mathbb{F}_q$-linear map, for any $y \in \mathbb{F}_q$.

Definition 2.8. *For $y_1, y_2 \in \mathbb{F}_q$, $y_1 \neq y_2$, define the map $\psi_{y_1,y_2}(f) : \mathbb{F}_q^n \to \mathbb{F}_q^{2(s+1)}$ as the concatenation of the respective linear maps, that is, $\psi_{y_1,y_2}(f) = (\psi_{y_1}(f), \psi_{y_2}(f))$.*

Observe that the y'th neighbor of a left-vertex f is then given by $(y, \psi_y(f))$. Proving the above lemmas (about the KT graph) now boils down to showing that both ψ_y and ψ_{y_1,y_2} are full rank for all $y, y_1, y_2 \in \mathbb{F}_q$.

1. *ψ_y is full rank implies Lemma 2.4*: Let $w = (y, z_0, \cdots, z_s) \in R$ be any right vertex, then the set of its left neighbor is $\{f \in L \mid (y, \psi_y(f)) = w\} = \psi_y^{-1}(z_0, \cdots, z_s)$. Because of Observation 2.6 and surjectivity, the right degree $D_R = \left|\psi_y^{-1}(z_0, \cdots, z_s)\right| = q^n/q^{s+1} = q^{n-(s+1)}$.
2. *ψ_{y_1,y_2} is full rank implies Lemma 2.5*: Similar to above, let $w_1 = (y_1, z_1) \in R$ and $w_2 = (y_2, z_2) \in R$, $y_1 \neq y_2$, be any pair of right vertices from *different* seeds. We extend Observation 2.6 to see that the number of $f \in L$ such that $(y_1, \psi_{y_1}(f)) = w_1$ and $(y_2, \psi_{y_2}(f)) = w_2$ is exactly $\left|\psi_{y_1,y_2}^{-1}(z_1, z_2)\right|$. By surjectivity, the number of left neighbors shared by w_1 and w_2 is $q^{n-(2s+2)}$.

To conclude the proof, it remains to show that these linear maps are full rank. For the linear map ψ_y, the associated matrix is lower triangular, and we show the determinant is non-zero through straightforward calculation. Proving that the map ψ_{y_1,y_2} is full rank requires more work. The main insight for computing the determinant of the matrix is to factor it into a lower triangular matrix and a matrix, the determinant of which reduces to computing the determinant of a Vandermonde matrix after a change of basis between the falling factorial basis and the monomial basis. We refer the reader to Section 3.5 for more details on the conversion of polynomial basis, and Section 4.3 for the complete proof of Lemma 2.5.

2.2 Non-bipartite lossless expander

We show that the bipartite half of the KT graph (from the previous section) yields a non-bipartite lossless expander. The bipartite half is an operation of bipartite graphs that transforms them into a non-bipartite graph, and is defined as follows: given a bipartite graph $G = (L \sqcup R, E)$, its bipartite half $G^2[L]$ is a graph with vertex set L where there is an edge $(u, v) \in G^2[L]$ iff u and v share a common neighbor in G.

One nuance of the bipartite half is that applying it to a biregular bipartite graph does not necessarily mean that the bipartite half will be regular itself. Thus, we must define what it means for a graph to be lossless in this non-regular setting. A natural definition just involves summing the total number of neighbors of a set.

Definition 2.9. *An irregular graph $G = (V, E)$ is a (K, ε)-*lossless expander[5] *if for any set $S \subseteq V$ of size at most K we have that $|\Gamma(S)| \geq (1-\varepsilon) \sum_{v \in S} d(v)$ where $d(v)$ represents the degree of vertex v.*

A stronger notion of lossless expansion is with respect to the highest degree of a node present in a graph.

Definition 2.10. *An irregular graph $G = (V, E)$ is a* max-degree (K, ε)-lossless expander *if for any set $S \subseteq V$ of size at most K we have that $|\Gamma(S)| \geq (1-\varepsilon) D |S|$ where $D = \max_{v \in V} d(v)$, the maximum degree of any vertex in G.*

Using this definition, our main observation is that the bipartite half of any two-sided lossless bipartite expander yields a non-bipartite, max-degree lossless expander.

[5] We abuse notation between the regular and irregular cases of graphs since this definition of lossless expansion for an irregular graph captures our previous definition of lossless expansion for regular graphs.

Lemma 2.11 (Lemma 6.3 restated)**.** *Let $G = (L \sqcup R, E)$ be a (D_L, D_R)-regular (K_L, A_L, K_R, A_R)-two-sided lossless expander. Then $G^2[L]$ is a max-degree (K, A)-expander where each node has a degree in $[D_L A_R, D_L D_R]$, and with $K = \min(K_L, K_R/D_L)$ and $A = A_L A_R$.*

The proof of this lemma essentially follows from expanding twice in the underlying two-sided expander G. Since we force our initial set to be at most K_L and K_R/D_L, we are guaranteed that we can use the left-to-right expansion of G and then additionally the right-to-left expansion of G, where at each step we expand by A_L and A_R, respectively.

Finally, we use the bipartite two-sided lossless expander from Theorem 1 as the base graph in Lemma 2.11 to obtain Theorem 2.

Theorem 2.12 (Informal version of Theorem 6.1)**.** *For infinitely many N, there exists an explicit $(K, \varepsilon = 0.01)$ lossless expander $G = (V, E)$ where $|V| = N$, each node has degree in range $[0.99D, D]$ where $N^{0.51} \leq D \leq N^{0.51+o(1)}$ and $K = N^{0.48}$. Moreover, G is endowed with a free group action from $\mathbb{F}_q$, where $q = \mathrm{poly}(\log N)$.*

In this setting, observe that $D_L A_R \approx 0.999 D_L D_R$ so $G^2[L]$ is very close to regular. Furthermore, $A = A_L A_R \approx 0.99 D_L D_R$, implying $G^2[L]$ is indeed a max-degree lossless expander. Additionally, because the vertices in the bipartite half of the KT graph are elements of $\mathbb{F}_q^n$, we get a free group action from $\mathbb{F}_q$ on them by scalar multiplication. One needs to be careful here since $G^2[L]$ contains the zero polynomial vertex; we remove this vertex and observe that removing one vertex still preserves the expansion properties.

Organization We use Section 3 to introduce necessary preliminaries. Then in Section 4.1 we show how our main theorem is proved assuming right regularity and knowing the overlap between two neighborhoods of right vertices. These facts are then proved in Section 4.2 and Section 4.3, respectively. In Section 5, we plug in parameters to get our two-sided lossless expander. Finally, in Section 6 we show how the bipartite half of the KT graph is a non-bipartite lossless expander with a free group action.

We prove that our constructions are explicit in Appendix A, and discuss why we were not able to show that the [GUV09] graph expands losslessly from the right in Appendix B.

3 Preliminaries

3.1 Notation

For a function $f \in \mathbb{F}_q[X]$, we we use $f^{(j)}$ to denote the j'th iterated derivative of f. We will often use the notation b_i for $i \in \mathbb{N}$ to refer to the polynomial $x^i \in \mathbb{F}_q[x]$ and we will often use the fact that $(b_0, \ldots, b_n)$ form a basis for the polynomials of degree at most n. For a (d_L, d_R)-biregular bipartite graph $G = (L \sqcup R)$, we use $\Gamma_\rightarrow : L \times [D_L] \to R$ to be the function that maps vertices in L to their neighbors in R as given by G; we use $\Gamma_\leftarrow : R \times [D_R] \to L$ to be the function that maps vertices in R to their neighbors in L as given by G. Often, we will define graph G by only defining the associated $\Gamma_\rightarrow$. When clear from context, we sometimes abuse notation and use $\Gamma_\rightarrow(w)$ to denote the right neighborhood of $w \in L$, and similarly $\Gamma_\leftarrow(w)$ for the left neighborhood of $w \in R$.

3.2 Lossless expansion

Throughout this paper, we will be focusing on the notion of vertex expansion as opposed to other definitions (e.g., edge, spectral) of expansion. Defining vertex expansion of a regular graph is straightforward.

Definition 3.1. *A D-regular graph $G = (V, E)$ is a (K, A)-*expander *if for all $S \subseteq V$ such that $|S| \leq K$ we have that $|\Gamma(S)| \geq A|S|$. If $A = 1 - \varepsilon$, then we say that G is a (K, ε)-*lossless expander*.*

For biregular bipartite graphs, we must consider the degree of each side to define expansion.

Definition 3.2. *A (D_L, D_R)-biregular graph $G = (L \sqcup R, E)$ is a (K_L, A_L, K_R, A_R)-*two-sided expander *if for all $S \subseteq L$ of size at most K_L we have $|\Gamma_{\rightarrow}(S)| \geq A_L |S|$ and for all $S \subseteq R$ of size at most K_R we have $|\Gamma_{\leftarrow}(S)| \geq A_R |S|$. If $A_L = 1 - \varepsilon_L$ and $A_R = 1 - \varepsilon_R$, then we call G a $(K_L, \varepsilon_L, K_R, \varepsilon_R)$-*lossless two-sided expander*.*

For irregular graphs, we can generalize Definition 3.1 in two ways. The first way is considering expansion with respect to the maximum number of neighbors of a set.

Definition 3.3. *An irregular graph $G = (V, E)$ is a (K, ε)-*lossless expander *(where we abuse the word "expander" for both regular and irregular graphs) if for any set $S \subseteq V$ of size at most K we have that $|\Gamma(S)| \geq (1 - \varepsilon) \sum_{v \in S} d(v)$ where $d(v)$ represents the degree of vertex v.*

The second, stronger notion of lossless expansion is with respect to the highest degree of a node present in a graph.

Definition 3.4. *An irregular graph $G = (V, E)$ is a* max-degree (K, ε)-lossless expander *if for any set $S \subseteq V$ of size at most K we have that $|\Gamma(S)| \geq (1 - \varepsilon) D |S|$ where $D = \max_{v \in V} d(v)$, the maximum degree of any vertex in G.*

3.3 The KT graph

Throughout the paper, we will use construction of bipartite (left) lossless expanders from [KT22] based on multiplicity codes from [KSY14]. We will often refer to this graph 'the KT graph':

Definition 3.5 (The KT graph)**.** *Let $q, n, s \in \mathbb{N}$ be such that q is a prime power, characteristic of the finite field $\mathbb{F}_q \geq n$ and $s \leq n/2$. Define $G = (L \sqcup R, E)$ where $L = \mathbb{F}_q^n, R = \mathbb{F}_q^{s+2}$. The left degree is q and for any $f \in \mathbb{F}_q^n$ and $y \in \mathbb{F}_q$, the y'th neighbor of f is defined as follows: Identify f as member of $\mathbb{F}_q[X]$ with degree of f at most $n-1$; then, the neighbor $\Gamma_{\rightarrow}(f, y)$ will be $(y, f^{(0)}(y), \ldots, f^{(s)}(y))$ where $f^{(j)}$ is the j'th iterative derivative of f.*

Remark 3.6. *In the paper [KT22], the final lossless expander graph construction slightly differs from ours. While they do construct the KT-graph G defined as above and show it has great (left) expanding properties, the final (left) lossless expander graph actually is defined as $H = (L \sqcup R, E)$ where $L = 2^n, R = \mathbb{F}_q^{s+2}$ and the left degree is q. H is constructed by considering the subgraph of G induced by vertices on the left side corresponding to $\{0,1\}^n$. For us, the final two-sided lossless expander graph will be G itself. This is why, our two-sided lossless expander graph has slightly worse parameters (worse constants) compared to the left lossless expander graph from [KT22].*

3.4 A useful inequality

We will use the following inequality based on an application of the Cauchy-Schwarz inequality:

Claim 3.7. *Fix $n \in \mathbb{N}, S \in \mathbb{R}$. Let $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ be such that $\sum_{1 \leq i \leq n} x_i = S$. Then,*

$$\sum_{1 \leq i < j \leq n} x_i x_j \leq \frac{(n-1)S^2}{2n}$$

Proof. Recall the Cauchy-Schwarz inequality: $\left(\sum_{1 \leq i \leq n} a_i b_i\right)^2 \leq \left(\sum_{1 \leq i \leq n} a_i^2\right)\left(\sum_{1 \leq i \leq n} b_i^2\right)$. We apply this with $a_1 = x_1, \ldots, a_n = x_n$ and $b_1 = b_2 = \cdots = b_n = 1$ to infer that

$$S^2 \leq \left(\sum_{1 \leq i \leq n} x_i^2\right) \cdot n \leq \left(S^2 - 2 \sum_{1 \leq i < j \leq n} x_i x_j\right) \cdot n$$

Rearranging, we infer that

$$\sum_{1\le i<j\le n} x_i x_j \le \frac{(n-1)S^2}{2n}$$

as desired. □

3.5 Falling factorial basis and Stirling numbers

We will use well known facts regarding converting between falling factorial basis for polynomials and the standard monomial basis using Stirling numbers. For formal reference of these claims, refer to [AA07]. Our viewpoint is inspired by an exposition of these results that appeared in a blog post by Terence Tao [Ter19].

We begin by defining falling factorials:

Definition 3.8. *The falling factorial of degree n is defined to be the polynomial*

$$x^{\underline{n}} = (x-n+1)(x-n+2)\cdots(x-1)x$$

We record the following well known fact:

Fact 3.9. *Falling factorials $(x^{\underline{n}},\ldots,x^{\underline{0}})$ form a basis for the polynomials in $\mathbb{F}_q[x]$ of degree at most n.*

Falling factorials are related to the monomial basis through Stirling numbers:

Definition 3.10 (Stirling numbers of the first kind)**.** *The* Stirling number of the first kind $st_1(n,k)$ *is the coefficient of x^k in the expansion of $x^{\underline{n}}$ where $k,n\in\mathbb{N}$. In particular,*

$$x^{\underline{n}} = \sum_{k=0}^{n} st_1(n,k)x^k$$

. Let $\begin{bmatrix} n \\ k \end{bmatrix}$ denote the number of permutations on n elements with k cycles, then

$$st_1(n,k) = (-1)^{n-k}\begin{bmatrix} n \\ k \end{bmatrix}$$

Definition 3.11 (Stirling numbers of the second kind)**.** *The* Stirling number of the second kind $st_2(n,k)$ *is the coefficient for $x^{\underline{k}}$ in the expansion of x^n where $n,k\in\mathbb{N}$ are arbitrary. In particular,*

$$x^n = \sum_{k=1}^{n} st_2(n,k)x^{\underline{k}}.$$

Moreover,

$$st_2(n,k) = \sum_{i=0}^{k}\frac{(-1)^{k-i}i^n}{(k-i)!i!}.$$

Fact 3.12. *If we let $\mathcal{S}\in\mathbb{F}_q^{n\times n}$ be defined by the Stirling numbers of the second kind as $\mathcal{S}(i,j)=st_2(j,i)$, then it is easy to check from Definition 3.11 that $(x^{\underline{0}},x^{\underline{1}},\ldots,x^{\underline{n}})\mathcal{S} = (x^0,x^1,\ldots,x^n)$. Notice that since $st_2(j,i)=0$ when $i>j$, and $st_2(j,i)=1$ when $i=j$, the matrix $\mathcal{S}$ is upper triangular and its determinant is the product of its diagonal entries, meaning* $\det(\mathcal{S})=1$.

$$\mathcal{S} = \begin{bmatrix} st_2(0,0) & st_2(1,0) & st_2(2,0) & \cdots & st_2(n,0) \\ 0 & st_2(1,1) & st_2(2,1) & \cdots & st_2(n,1) \\ 0 & 0 & st_2(2,2) & \cdots & st_2(n,2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & st_2(n,n) \end{bmatrix}$$

3.6 Free group actions on graphs

Here we recall basic notions about group actions on graphs. First, we define an abstract group notion.

Definition 3.13. *Let G be a group and X a set. A* group action $\cdot : G \times X \to X$ *(where we write the $\cdot$ in infix notation) is a function that has the following two properties:*

1. *Identity: The identity element 1_G of G always acts trivially as $1_G \cdot x = x$ for any $x \in X$.*
2. *Compatibility: The group action and multiplication of G are compatible. That is, for any $g, h \in G$ and $x \in X$ we have $(gh) \cdot x = g \cdot (h \cdot x)$ where gh is the product of g and h in G.*

Next, we recall another abstract notion about group actions.

Definition 3.14. *We say that a group action of G on X is* free *if $g \cdot x = x$ for some $x \in X$ implies that $g = 1_G$.*

Finally, we consider what it means for a graph to be invariant with respect to a group action.

Definition 3.15. *Let G be a group and $H = (V, E)$ a graph with a group action from G. We say that H is* G-invariant *if for all $(v, w) \in E$ and $g \in G$ we have that $(g \cdot v, g \cdot w) \in E$.*

4 An Explicit Two-sided Lossless Expander

In this section, we first describe how to prove our main theorem using right regularity and the size of the overlap in neighborhoods between any two right vertices. Then we prove these two facts in Section 4.2 and Section 4.3, respectively.

4.1 Main theorem

Putting together all of our results with the left-to-right expansion of [KT22] yields our main theorem.

Theorem 4.1. *For all finite fields $\mathbb{F}_q$ and $n, s \in \mathbb{N}$ with $15 \le 2(s+1) < n < char(\mathbb{F}_q)$, there exists an explicit bipartite graph $G = (L \sqcup R, E)$ with $L = \mathbb{F}_q^n, R = \mathbb{F}_q^{s+2}$, left degree equal to q and right degree $q^{n-(s+1)}$ such that G is a two-sided (K_L, A_L, K_R, A_R) expander with $A_L = q - \frac{n(s+2)}{2} \cdot (qK_L)^{1/(s+2)}$ and $A_R = \left(1 - \frac{K_R}{q^{s+2}} \cdot \frac{q-1}{2}\right) q^{n-(s+1)}$.*

Proof. The left-to-right expansion follows from Theorem 3 from [KT22]. The right-to-left expansion follows from Theorem 4.2 below. The explicitness of G follows from Claim A.1. □

Our main achievement is showing the right-to-left expansion of the KT graph in Theorem 4.2 below.

Theorem 4.2. *If $n > 2s + 2$, then the KT graph G in Definition 2.2 is a right (K_{max}, ε)-lossless expander for $K_{max} = \delta q^{s+1}$ and $\varepsilon = \frac{\delta(q-1)}{2q}$ where $0 < \delta < 1$ is arbitrary.*

We prove Theorem 4.2 via the following two theorems regarding properties of G.

Lemma 4.3. *G is right-regular and the right degree is $q^{n-(s+1)}$.*

Lemma 4.4. *For any pair of right-vertices w_1, w_2 such that $w_1 = (y_1, z_1), w_2 = (y_2, z_2) \in \mathbb{F}_q^{s+2}$ where $y_1 \ne y_2 \in \mathbb{F}_q$ and $z_1, z_2 \in \mathbb{F}_q^{s+1}$, we have $|\Gamma_{\leftarrow}(y_1, z_1) \cap \Gamma_{\leftarrow}(y_2, z_2)| = q^{n-(2s+2)}$.*

With the exact right-regularity of G and the number of common left-neighbors shared by any pair of right-vertices generated by different seeds, we are ready to prove Theorem 4.2.

Proof of Theorem 4.2. Our goal is to show that any right subset $T \subseteq \mathbb{F}_q^{s+2}$ of size at most δq^{s+1} has a neighborhood of size at least $(1-\varepsilon)q^{n-(s+1)}\,|T|$ on the left.

To do this, we consider T as the disjoint union $T = \bigsqcup_{y\in\mathbb{F}_q} T_y$ of buckets $T_y = \{(y,\alpha) : \alpha \in \mathbb{F}_q^{s+1}\}$ where $|T_y| = t_y = \delta_y q^{s+1}$. Let $\delta = \sum_{y\in\mathbb{F}_q} \delta_y$. So, $|T| = \delta q^{s+1}$. By Lemma 4.3, the number of edges leaving T is $|T| \cdot q^{n-(s+1)} = \delta q^n$.

Moreover, by Lemma 4.4, the maximum number of double-counted left vertices is

$$\sum_{\substack{i,j\in[q]\\ i<j}} t_i t_j q^{n-2(s+1)} = \sum_{\substack{i,j\in[q]\\ i<j}} \delta_i q^{s+1}\cdot \delta_j q^{s+1} \cdot q^{n-2(s+1)} = q^n \sum_{\substack{i,j\in[q]\\ i<j}} \delta_i\delta_j \le q^n \cdot \frac{q-1}{2q}\cdot \delta^2$$

where for the last inequality, we used Claim 3.7. Applying one level of inclusion-exclusion reveals that

$$|\Gamma_{\leftarrow}(T)| \ge \delta q^n - q^n \cdot \frac{q-1}{2q}\cdot\delta^2 = \left(1 - \frac{\delta(q-1)}{2q}\right)\delta q^n = (1-\varepsilon)\, q^{n-(s+1)}|T|$$

where $\varepsilon = \frac{\delta(q-1)}{2q}$. ☐

We prove Lemma 4.3 in Section 4.2, and Lemma 4.4 in Section 4.3

4.2 Right-regularity

In this subsection, we will show that the KT graph G is right-regular, and that the right-degree is $q^{n-(s+1)}$. For $f \in \mathbb{F}_q^n$ and seed $y \in \mathbb{F}_q$, recall the linear map $\psi_y(f) = (f^{(0)}(y), \ldots, f^{(s)}(y))$ where $f^{(i)}$ is the i'th iterative derivative of $f \in \mathbb{F}_q[X]$ interpreted as a degree $\le (n-1)$ polynomial.

We will use the following fact regarding linearity of derivatives:

Fact 4.5 ([Rit50])**.** *For all $\alpha, \beta \in \mathbb{F}_q$, $f, g \in \mathbb{F}_q[X]$ and $j \ge 0$, it holds that $(\alpha f + \beta g)^{(j)} = \alpha f^{(j)} + \beta g^{(j)}$.*

From this fact, we directly obtain that ψ_y is a linear map:

Corollary 4.6. *For all $y \in \mathbb{F}_q$, ψ_y is an $\mathbb{F}_q$-linear map.*

Therefore, to show right regularity we show that for all $y \in \mathbb{F}_q$, ψ_y always has full rank.

Claim 4.7. *For $y \in \mathbb{F}_q$, ψ_y is a full rank $\mathbb{F}_q$-linear map.*

Proof. First, $\mathbb{F}_q$-linearity of ψ_y follows from Corollary 4.6. Fix the monomial basis $b_0, \ldots, b_{n-1} \in \mathbb{F}_q[X]$ for degree $\le n-1$ polynomials over $\mathbb{F}_q[X]$ where $b_0 = x^0, b_1 = x^1, b_2 = x^2, \ldots, b_{n-1} = x^{n-1}$. Now, for any $y \in \mathbb{F}_q$, consider the matrix $M_y \in \mathbb{F}_q^{n\times(s+1)}$ where for $0 \le i \le n-1$ and $0 \le j \le s$ entry (i,j) is given by $b_i^{(j)}(y)$. We claim that M_y has full rank, i.e., $\mathrm{rank}(M_y) = \min(s+1, n)$.

This suffices to prove the overall claim as $\psi_y(f) = v_f M_y$ where $v_f \in \mathbb{F}_q^{1\times n}$ is the unique vector of coefficients expressing f as $\mathbb{F}_q$-linear combination of the basis vectors $(b_0, \ldots, b_{n-1})$.

Let N_y be the matrix induced by taking the first $s+1$ rows of M_y. So, $N_y \in \mathbb{F}_q^{(s+1)\times(s+1)}$. We will show that N_y has full rank by showing $\det(N_y) \ne 0$.

We first observe that N_y is lower triangular: For i, j s.t. $j > i$, entry (i,j) of N_y is $b_i^{(j)}(y)$. As b_i is a degree i polynomial, $b_i^{(j)} \equiv 0$ and hence, $b_i^{(j)}(y) = 0$. Moreover, as entry (i,i) in N_y is $b_i^{(i)}(y)$ and $b_i = x^i$, we compute that $b_i^{(i)} \equiv (i)!$. Hence, the entry (i,i) in N_y equals $(i)!$. So, $\det(N_y) = \prod_{i=0}^{s}(i)!$ as determinant of a triangular matrix is the product of its diagonal entries. As characteristic of the field $\mathbb{F}_q$ is greater than $n > s$, $\det(N_y)$ is indeed non-zero. ☐

We are now ready to prove Lemma 4.3.

Proof of Lemma 4.3. Let $w \in \mathbb{F}_q^{s+2}$ be arbitrary. Let $w = (y, z_0, \ldots, z_s)$ where $y, z_0, \ldots, z_s \in \mathbb{F}_q$. For every vertex $f \in \mathbb{F}_q^n$ with $w \in \Gamma_{\rightarrow}(f)$, w must be the y'th neighbor of f. As $\Gamma_{\rightarrow}(f, y) = (y, \psi_y(f))$, the number of such f is exactly $\left|\psi_y^{-1}(z_0, \ldots, z_s)\right|$. By Claim 4.7, ψ_y is full rank and so the number of such f is $q^{n-(s+1)}$ as desired. ☐

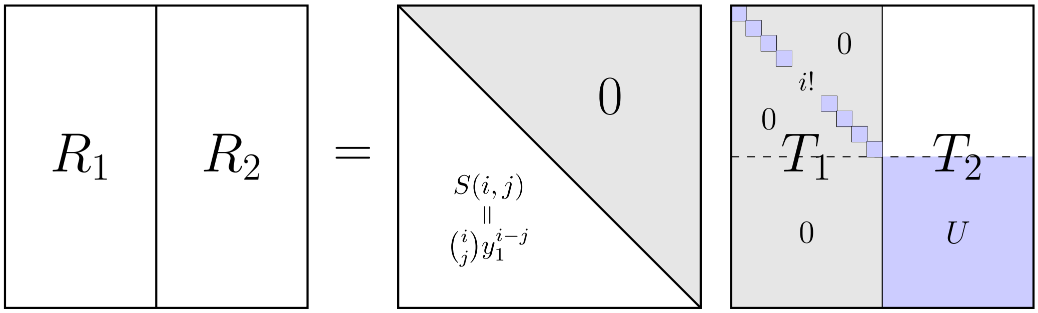

Figure 1: Factoring $R = ST$

4.3 All pairs of seeds have full rank

In this section, we bound the number of common left neighbors shared by any pair of right vertices with different seeds. We do this in a similar fashion as how we proved right-regularity in Section 4.2, namely, we need the main technical lemma of this section:

Lemma 4.8. *For all $y_1, y_2 \in \mathbb{F}_q$ with $y_1 \neq y_2$, the linear map $\psi_{y_1,y_2} = (\psi_{y_1}(f), \psi_{y_2}(f))$ has full rank.*

Using this main lemma, Lemma 4.4 directly follows:

Proof of Lemma 4.4. For all $f \in \mathbb{F}_q^n$ with $w_1, w_2 \in \Gamma_{\rightarrow}(f)$, w_1 must be the y_1'th neighbor of f and w_2 must be the y_2'th neighbor of f. Observe that $\Gamma_{\rightarrow}(f, y_1) = (y_1, \psi_{y_1}(f))$ and $\Gamma_{\rightarrow}(f, y_2) = (y_2, \psi_{y_2}(f))$. So, the number of such f is exactly $\left|\psi_{y_1,y_2}^{-1}(z_1, z_2)\right|$. As ψ_{y_1,y_2} has full rank, the number of such f is $q^{n-(2s+2)}$ as desired. $\square$

Now to prove Lemma 4.8, we again associate with ψ_{y_1,y_2} a matrix and show that it has full rank or, equivalently, non-zero determinant. More specifically, for $z \in \{1, 2\}$ define the matrix $R_z \in \mathbb{F}_q^{(2s+2)\times(s+1)}$ where for $0 \leq i \leq 2s+1$ and $0 \leq j \leq s$ entry $R_z(i,j) = b_i^{(j)}(y_z)$ where $b_i = x^i$.

Lemma 4.9 (Lemma 1 restated)**.** *For all y_1, y_2, let $R = (R_1, R_2) \in \mathbb{F}_q^{(2s+2)\times(2s+2)}$ be the matrix associated with the map ψ_{y_1,y_2}, then* $\det(R) \neq 0$*.*

We now focus on computing the determinant of R. To do this, we will factorize $R = ST$ as in Figure 1 and then compute $\det(R) = \det(S) \cdot \det(T)$ through the following series of claims.

Claim 4.10. *$R = ST = S(T_1, T_2)$ with $S, T \in \mathbb{F}_q^{(2s+2)\times(2s+2)}$, where*

$$S(i,j) = \binom{i}{j} y_1^{i-j} = \frac{1}{(j!)} \cdot b_i^{(j)}(y_1)$$

$$T(i,j) = \begin{cases} T_1(i,j) & 0 \leq j \leq s \\ T_2(i, j-s-1) & s+1 \leq j \leq 2s+1 \end{cases}$$

and matrices $T_1, T_2 \in \mathbb{F}_q^{(2s+2)\times(s+1)}$ are defined as follows:

$$T_1(i,j) = \begin{cases} i! & i = j \\ 0 & \textit{otherwise} \end{cases}$$

$$T_2(i,j) = b_i^{(j)}(y_2 - y_1)$$

.

Observe that S is a lower triangular matrix with every diagonal entry equal to 1, so $\det(S) = 1$.

Corollary 4.11. $\det(R) = \det(S) \cdot \det(T) = \det(T)$

Claim 4.12. $\det(T) = \prod_{i=0}^{s}(i!) \cdot \det(U)$, *where* $U \in \mathbb{F}_q^{(s+1)\times(s+1)}$ *is the last* $(s+1)$ *rows of* T_2.

Claim 4.13. $\det(U) = (y_2 - y_1)^{(s+1)^2} \cdot \det(V)$, *where* $V \in \mathbb{F}_q^{(s+1)\times(s+1)}$ *is defined as follows:*

$$V(i,j) = \binom{(s+1)+i}{j} \cdot (j!) = (s+1+i)^{\underline{j}}$$

Claim 4.14. $\det(V) = \prod_{0 \le i < j \le s}(j-i)$

We now prove Lemma 4.9.

Proof of Lemma 4.9. By Claim 4.10, Claim 4.12, Corollary 4.11, Claim 4.13, Claim 4.14, and since $y_1 \neq y_2$, we have

$$\det(R) = \prod_{0 \le i \le s}(i!) \cdot (y_2 - y_1)^{(s+1)^2} \cdot \prod_{0 \le i < j \le s}(j-i) \neq 0$$

□

It remains to prove the series of claims we made above. We do that here one by one, utilizing various properties of the determinant.

Proof of Claim 4.10. We want to show that $R = ST = (ST_1, ST_2)$. For $0 \le i \le 2s+1$ and $0 \le s \le j$, we indeed have that $ST_1(i,j) = \binom{i}{j} \cdot (j!) \cdot y_1^{i-j} = b_i^{(j)}(y_1) = R(i,j)$. For $0 \le i \le 2s+1$ and $0 \le s \le j$, we have that

$$\begin{aligned}
ST_2(i,j) &= \sum_{k=0}^{2s+1} \binom{i}{k} y_1^{i-k} b_k^{(j)}(y_2 - y_1) \\
&= \sum_{k=0}^{2s+1} \binom{i}{k} y_1^{i-k} \cdot \binom{k}{j} \cdot j! \cdot (y_2 - y_1)^{k-j} \\
&= \sum_{k=j}^{i} \binom{i}{k} \cdot \binom{k}{j} \cdot (j!) \cdot y_1^{i-k} \cdot (y_2 - y_1)^{k-j} \\
&= \binom{i}{j} \cdot (j!) \cdot y_2^{i-j} \\
&= b_i^{(j)}(y_2) \\
&= R(i, (s+1)+j)
\end{aligned}$$

where the third last equality follows by differentiating both sides of the binomial theorem j times. Hence, indeed $R = ST$ as claimed. □

Proof of Claim 4.12. Observe that the matrix T is in fact a 2×2 block matrix with the lower left block being 0, therefore $\det(T)$ is the product of the determinants of the upper left and lower right blocks. Moreover, the upper left block is a diagonal matrix. As a result, $\det(T) = \prod_{i=0}^{s}(i!) \cdot \det(U)$. □

Proof of Claim 4.13. By definition, for $0 \le i,j \le s$, $U(i,j) = T(s+1+i, s+1+j) = \binom{s+1+i}{j}(j!)(y_2 - y_1)^{s+1+i-j}$, and $V(i,j) = \binom{s+1+i}{j}(j!)$. In other words, V can be obtained by factoring out $(y_2 - y_1)^{s+1-j}$ from each column, and then factoring out $(y_2 - y_1)^i$ from each row. According to the property of the determinant, this means

$$\det(U) = \prod_{0 \le j \le s}(y_2 - y_1)^{s+1-j} \cdot \prod_{0 \le i \le s}(y_2 - y_1)^i \cdot \det(V) = (y_2 - y_1)^{(s+1)^2} \cdot \det(V)$$

as claimed. ☐

Proof of Claim 4.14. V is a Vandermonde matrix in disguise, (to be precise, it is exactly the Vandermonde matrix over the falling factorial basis from Fact 3.9). Thus, by the change of basis from Fact 3.12 we have that $V\mathcal{S} = \tilde{V}$ where $\tilde{V}$ is defined as $\tilde{V}(i,j) = (s+1+i)^j$ and is a Vandermonde matrix in the standard monomial basis. Furthermore, since $\det(\mathcal{S}) = 1$ by Fact 3.12, we have that $\det(V) = \det(\tilde{V}) \cdot \det(\mathcal{S}) = \det(\tilde{V}) \cdot 1 = \det(\tilde{V})$. Thus, we finish by recalling the standard equation for the determinant of a Vandermonde matrix and computing

$$\begin{aligned}\det(V) &= \det(\tilde{V})\\ &= \prod_{0\le i<j\le s} ((s+1+j) - (s+1+i))\\ &= \prod_{0\le i<j\le s} (j-i),\end{aligned}$$

giving us our claimed result. ☐

5 Plugging in the Parameters

We record our main result regarding two sided lossless expanders:

Theorem 5.1 (Formal version of Theorem 1)**.** *For infinitely many N and all $0 < \delta \le 0.49$, there exists an explicit biregular two-sided $(K_L, \varepsilon_L = 0.01, K_R, \varepsilon_R = 0.01)$ lossless expander $\Gamma_\rightarrow : [N] \times [D_L] \to [M]$ where $D_L \le O(\log^{204}(N))$, $N^{1.01\cdot\delta - o(1)} \le M \le D_L \cdot N^{1.01\cdot\delta}$, $K_L = N^\delta$, $K_R = \frac{1}{50} \cdot (M/D_L)$.*

This will follow from the following technical lemma:

Lemma 5.2. *Let $\alpha, \varepsilon_L, \varepsilon_R \in (0,1)$ and $K_R, n, k_L, q \in \mathbb{N}$ be such that q is a prime number, $\frac{h^{1+\alpha}}{2} \le q \le h^{1+\alpha}$ where $h = (4nk_L/\varepsilon_L)^{1/\alpha}$ and such that both $\frac{4}{k_L}\log(2n/\varepsilon_L) \le \alpha$ and $2k_L(1+\alpha) \le n$. Then, there exists an explicit biregular $(K_L, \varepsilon_L, K_R, \varepsilon_R)$ two-sided lossless expander $\Gamma_\rightarrow : [N] \times [D_L] \to [M]$ where $N = q^n, K_L = q^{k_L}, K_L^{1+\alpha-1/\log(h)} \le M \le D_L \cdot K_L^{1+\alpha}$, $D_L \le O(\log(N)\log(K_L)/\varepsilon_L)^{1+1/\alpha+o(1)}$, $\frac{K_R}{q^{s+2}} \cdot \frac{q-1}{2} \le \varepsilon_R$.*

We will instantiate this lemma using simple parameters to obtain our main theorem:

Proof of Theorem 5.1. We plug in $\alpha = 0.01, \varepsilon_L = 0.01, \varepsilon_R = 0.01, k = \delta n$ in Lemma 5.2 to obtain the desired lossless expander. ☐

We finally prove our main technical lemma using two-sided expander from Theorem 4.1:

Proof of Lemma 5.2. Set $s + 2 = \lceil k_L/\log_q(h)\rceil$ so that $h^{s+1} \le K_L \le h^{s+2}$. Observe that

$$2s + 2 < \frac{2k_L \log(q)}{\log(h)} \le 2k_L(1+\alpha) \le n$$

So, we can apply Theorem 4.1 and infer that there exists a graph $\Gamma_\rightarrow : \mathbb{F}_q^n \times \mathbb{F}_q \to \mathbb{F}_q^{s+2}$ that is a $(\le h^{s+2}, A_L)$ left expander and $(\le \delta q^{s+2}, A_R)$ right expander where $A_L = q - \frac{n(s+2)}{2} \cdot (qh^{s+2})^{1/(s+2)}$ and $A_R = \left(1 - \frac{K_R}{q^{s+2}} \cdot \frac{q-1}{2}\right) q^{n-(s+1)} K_R$. Notice that as $K_L \le h^{s+2}$, $\Gamma_\rightarrow$ is indeed a (K_L, A_L) expander.

- We first bound the left degree D_L:

$$\begin{aligned}D_L = q \le h^{1+\alpha} &= (4nk_L/\varepsilon_L)^{1+1/\alpha} = (4\log(N)\log(K_L)/\log^2(q)\varepsilon_L)^{1+1/\alpha}\\ &= (4\log(N)\log(K_L)/\varepsilon_L)^{1+1/\alpha} \cdot \log^{2+2/\alpha}(q)\end{aligned}$$

This implies that

$$D_L = q \leq (4\log(N)\log(K_L)/\varepsilon_L)^{1+1/\alpha}\left(\log\left(8\log(N)\log(K_L)/\varepsilon_L\right)\right)^{2+2/\alpha}$$

Then indeed, $D_L \leq O(\log(N)\log(K_L)/\varepsilon_L)^{1+1/\alpha+o(1)}$.

- We now bound the number of right vertices M:

$$M = q^{s+2} \leq q \cdot h^{(1+\alpha)(s+1)} \leq q \cdot K_L^{1+\alpha}$$

Additionally,

$$M = q^{s+2} \geq q^{K_L \log(q)/\log(h)} \geq q^{K_L((1+\alpha)(\log h)-1)/\log(h)} = q^{K_L(1+\alpha)-K_L/\log(h)}$$

- We now show lossless expansion from the right side:

$$A_R = \left(1 - \frac{K_R}{q^{s+2}} \cdot \frac{q-1}{2}\right) q^{n-(s+1)} K_R \geq (1-\varepsilon_R) D_R K_R$$

where the last inequality follows because $\frac{K_R}{q^{s+2}} \cdot \frac{q-1}{2} \leq \varepsilon_R$.

- We finally show lossless expansion from the left side: First, we note that $s+2 \leq 2k$. Indeed, $s+2 \leq k\log_q(h)+1 = k\frac{\log(h)}{\log(q)}+1 \leq k(1+\alpha)+1 \leq 2k$. Then,

$$\begin{aligned}
A_L &= q - \frac{n(s+2)}{2} \cdot (qh^{s+2})^{1/(s+2)} \\
&= q - \frac{n(s+2)h}{2} \cdot (q)^{1/(s+2)} \\
&\geq q - nkh \cdot (q)^{1/(s+2)} && \text{(since } s+2 \leq 2k\text{)} \\
&= q - \frac{\varepsilon_L \cdot h^\alpha}{4} \cdot h \cdot (q)^{1/(s+2)} && \text{(since } nk = (\varepsilon_L \cdot h^\alpha)/4\text{)} \\
&= q - \varepsilon_L \cdot \frac{h^{1+\alpha}}{4} \cdot (q)^{1/(s+2)} \\
&\geq q - \frac{\varepsilon_L}{2} \cdot q \cdot (q)^{1/(s+2)} && \text{(since } h^{1+\alpha}/2 \leq q\text{)} \\
&= q\left(1 - \varepsilon_L \cdot \frac{(q)^{1/(s+2)}}{2}\right) \\
&\geq q(1-\varepsilon_L)
\end{aligned}$$

The last inequality $(q)^{1/(s+2)} \leq 2$ follows because we claim that $s+2 \geq \log(q)$. This suffices to prove the last inequality since then $(q)^{1/(s+2)} \leq q^{1/\log(q)} \leq 2$. We indeed compute that

$$s+2 \geq \frac{k}{\log_q(h)} \geq \frac{k((1+\alpha)\log(h)-1))}{\log(h)} \geq k$$

Moreover, as $\alpha \geq \frac{4}{k_L}\log(2n/\varepsilon_L)$, we infer that $k \geq \frac{4}{\alpha} \cdot \log(2n/\varepsilon)$. Hence indeed,

$$s+2 \geq \frac{4}{\alpha} \cdot \log(2n/\varepsilon) \geq \frac{2}{\alpha} \cdot \log(2nk/\varepsilon) \geq 2\log(h) \geq (1+\alpha)\log(h) \geq \log(q)$$

□

6 Non-Bipartite Lossless Expander

Here, we show how to transform a two-sided lossless expander into an undirected graph (that is not necessarily bipartite) while retaining lossless expansion. We then apply this transformation to the KT graph to obtain our second main theorem.

Theorem 6.1 (Formal version of Theorem 2)**.** *For infinitely many N and all $0 < \delta \leq 0.49$, there exists an explicit $(K, \varepsilon = 0.01)$ lossless expander $G = (V, E)$ where $|V| = N$, each node has degree in range $[0.999D, D]$ where $N^{1-1.01\delta} \leq D \leq N^{1-1.01\delta+o(1)}$ and $K = N^{\delta}$. Moreover, G is endowed with a free group action from $\mathbb{F}_q$, where $q = \text{poly}(\log N)$.*

6.1 Expansion from the bipartite half

Given a two-sided lossless expander, we show how to obtain a (not necessarily bipartite) graph that is also a losslesss expander while inheriting the expansion of this graph. We use the bipartite half transformation defined as follows.

Definition 6.2 (Bipartite half)**.** *Let $G = (L \sqcup R, E)$ be a (D_L, D_R)-regular bipartite graph. Then the* bipartite half *$G^2[L] = (L, E^2[L])$ is defined as $E^2[L] = \{(v, w) \in L \times L \mid w \in \Gamma_{\leftarrow}(\Gamma_{\rightarrow}(v))\}$.*

Next, we show how this transformation retains lossless expansion. For the sake of clarity, we will use $\Gamma_{\rightarrow}$ and $\Gamma_{\leftarrow}$ for the left-to-right and right-to-left neighborhood functions of G and Γ as the neighborhood function of $G^2[L]$.

Lemma 6.3. *Let $G = (L \sqcup R, E)$ be a (D_L, D_R)-regular (K_L, A_L, K_R, A_R)-two-sided lossless expander with $D_L \leq K_R$. Then $G^2[L]$ is a max-degree (K, A)-expander where each node has a degree in $[D_L A_R, D_L D_R]$ and with $K = \min(K_L, K_R/D_L)$ and $A = A_L A_R$.*

Remark 6.4. *While $G^2[L]$ may not be exactly regular, since $A_L = (1 - \varepsilon_L)D_L$ and $A_R = (1 - \varepsilon_R)D_R$, we see that $A = A_L A_R = (1 - \varepsilon_L)(1 - \varepsilon_R)D_L D_R$, meaning that our expansion is with respect to the highest possible degree $D_L D_R$ of any individual vertex.*

Proof of Lemma 6.3. We begin by showing that each node $v \in L$ of $G^2[L]$ has degree in $[D_L A_R, D_L D_R]$. By assumption, we have that $|\Gamma_{\rightarrow}(v)| = D_L \leq K_R$. Thus, by the right-to-left expansion of G, we have that $|\Gamma_{\leftarrow}(\Gamma_{\rightarrow}(v))| \geq D_L A_R$. The upper bound is immediate given that the right degree is D_R so $|\Gamma_{\leftarrow}(\Gamma_{\rightarrow}(v))| \leq D_R |\Gamma_{\rightarrow}(v)| = D_R D_L$.

Next, we prove expansion. Let $S \subseteq L$ be a set of size at most K. Then, because $K \leq K_L$, the left-to-right expansion of G gives us that $|\Gamma_{\rightarrow}(S)| \geq A_L |S|$. To expand a second time, we recall that $K \leq K_R/D_L$, so $|\Gamma_{\rightarrow}(S)| \leq D_L |S| \leq D_L K \leq K_R$, meaning that we can apply the right-to-left expansion of G. This yields $|\Gamma_{\leftarrow}(\Gamma_{\rightarrow}(S))| \geq A_R |\Gamma_{\rightarrow}(S)| \geq A_R A_L |S|$, as claimed. ☐

6.2 Free group action on the bipartite half

Now that we have shown that the bipartite half generally preserves lossless expansion, we will consider it instantiated with the KT graph and show that multiplication by elements of $\mathbb{F}_q$ constitutes a free group action on this resulting graph (with one node removed).

We begin with the following observation.

Remark 6.5. *The bipartite half of the KT graph G from Definition 3.5 has a succinct representation as $G^2[L] = (L, E^2[L])$ where $E^2[L] = \{(f, g) \mid \exists y \in \mathbb{F}_q,\ \psi_y(f) = \psi_y(g)\}$.*

Our action of $\mathbb{F}_q$ on the bipartite half of the KT graph is directly by multiplication in $\mathbb{F}_q$.

Definition 6.6. *Let $G = (L \sqcup R, E)$ be the KT graph and $G^2[L]$ be its bipartite half. We define the action of $\mathbb{F}_q$ on $G^2[L]$ as follows: for any $\alpha, y \in \mathbb{F}_q$ we have $(\alpha \cdot f)(y) = \alpha(f(y))$ where the latter multiplication is in $\mathbb{F}_q$.*

We now show that $G^2[L]$ without the zero polynomial is $\mathbb{F}_q$-invariant and that this is a free group action.

Lemma 6.7. *Let $G = (L \sqcup R, E)$ be the KT graph and $H = G^2[L] \setminus \{0\}$ be its bipartite half without the zero polynomial. Consider the action of $\mathbb{F}_q$ on $G^2[L]$ as defined in Definition 6.6. Then $G^2[L]$ is $\mathbb{F}_q$-invariant and this action is free.*

Proof. To show that H is $\mathbb{F}_q$-invariant, we must prove that for any $(f, g) \in E^2[L]$ and $\alpha \in \mathbb{F}_q$ we have $(\alpha \cdot f, \alpha \cdot g) \in E^2[L]$. From Remark 6.5 we know that $E^2[L] = \{(f, g) \mid \exists y \in \mathbb{F}_q,\ \psi_y(f) = \psi_y(g)\}$. Thus, we must equivalently show that if $\psi_y(f) = \psi_y(g)$ for some $y \in \mathbb{F}_q$, then $\psi_y(\alpha \cdot f) = \psi_y(\alpha \cdot g)$. This is immediate by Corollary 4.6 because ψ_y being $\mathbb{F}_q$-linear allows us to compute

$$\psi_y(\alpha \cdot f) = \alpha\psi_y(f) = \alpha\psi_y(g) = \psi_y(\alpha \cdot g),$$

showing that $(\alpha \cdot f, \alpha \cdot g) \in E^2[L]$.

Next, we will show that this is a free group action. Consider any f in the vertices of H and $\alpha \in \mathbb{F}_q$. Since H does not contain the zero polynomial, we know that f is not identically zero. Thus, if $\alpha \cdot f = f$, it must be that $\alpha = 1$, showing that the action is indeed free. □

6.3 Plugging in parameters

Finally, we plug in our two-sided lossless expander result from the KT graph to get Theorem 6.1.

Proof of Theorem 6.1. We invoke Lemma 5.2 with $\alpha = 0.01, \varepsilon_L = 0.001, \varepsilon_R = 0.001$ to obtain a (D_L, D_R)-biregular two-sided $(K_L = N^\delta, \varepsilon_L = 0.001, K_R = 0.002 \cdot (M/D_L), \varepsilon_R = 0.001)$ lossless expander $\Gamma_\rightarrow : [N] \times [D_L] \to [M]$ where $D_L \le O(\log^{204}(N))$ and $N^{1.01\delta - o(1)} \le M \le D_L \cdot N^{1.01\delta}$. We then apply Lemma 6.3 to conclude the claim about expansion. The claim about the free $\mathbb{F}_q$ action comes from Lemma 6.7 by removing the vertex corresponding to the zero polynomial from the bipartite half of the KT graph. Observe that removing the zero polynomial still preserves expansion properties of $G^2[L]$. Indeed, the resultant graph is still a $(K, A - 1)$ expander where $A = (1 - \varepsilon)D$. As $\varepsilon \cdot D = \omega(1)$, the expansion is not affected. Moreover, the degree of a vertices in the resultant graph can decrease by one which doesn't change our degree range guarantee of $[0.999D, D]$ either, as $0.999D = \omega(1)$. Explicitness of this graph follows from Claim A.2. □

7 Open Questions

We list some open questions that are natural next steps.

1. It would be interesting to see if any of the techniques here can be pushed more towards the balanced setting—where the number of left vertices is a lot less than quadratic of the number of right vertices—with degree smaller than what we achieve in our work.

2. We are unable to show that the one-sided lossless expander constructed in [GUV09] is also a two-sided lossless. However, the graph in [GUV09] is not right-regular (see Appendix B), but can it be modified to be so in a way such that it attains lossless expansion from the right as well?

3. Expander graphs have found important uses in constructions of error-correcting codes. Thus, we wonder if there are applications of our results to coding theory.

References

[AA07] Martin Aigner and S Axler. *A course in enumeration*. Vol. 238. Springer, 2007 (cit. on p. 7).

[BMRV02] H. Buhrman, P. B. Miltersen, J. Radhakrishnan, and S. Venkatesh. “Are Bitvectors Optimal?” In: *SIAM Journal on Computing* 31.6 (Jan. 2002). Publisher: Society for Industrial and Applied Mathematics, pp. 1723–1744. ISSN: 0097-5397. DOI: 10.1137/S0097539702405292 (cit. on p. 2).

[CRVW02] Michael Capalbo, Omer Reingold, Salil Vadhan, and Avi Wigderson. "Randomness conductors and constant-degree lossless expanders". In: *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing*. STOC '02. New York, NY, USA: Association for Computing Machinery, May 2002, pp. 659–668. ISBN: 978-1-58113-495-7. DOI: 10.1145/509907.510003 (cit. on p. 1).

[CRT23] Itay Cohen, Roy Roth, and Amnon Ta-Shma. "HDX Condensers". In: *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*. ISSN: 2575-8454. Nov. 2023, pp. 1649–1664. DOI: 10.1109/FOCS57990.2023.00100 (cit. on p. 1).

[DHLV23] Irit Dinur, Min-Hsiu Hsieh, Ting-Chun Lin, and Thomas Vidick. "Good Quantum LDPC Codes with Linear Time Decoders". In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*. STOC 2023. New York, NY, USA: Association for Computing Machinery, June 2023, pp. 905–918. ISBN: 978-1-4503-9913-5. DOI: 10.1145/3564246.3585101 (cit. on p. 1).

[DT23] Dean Doron and Roei Tell. "Derandomization with Minimal Memory Footprint". en. In: *DROPS-IDN/v2/document/10.4230/LIPIcs.CCC.2023.11*. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023. DOI: 10.4230/LIPIcs.CCC.2023.11 (cit. on p. 2).

[DKSS13] Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan. "Extensions to the Method of Multiplicities, with Applications to Kakeya Sets and Mergers". In: *SIAM Journal on Computing* 42.6 (Jan. 2013). Publisher: Society for Industrial and Applied Mathematics, pp. 2305–2328. ISSN: 0097-5397. DOI: 10.1137/100783704 (cit. on p. 2).

[Gol11] Oded Goldreich. "In a World of P=BPP". en. In: *Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation: In Collaboration with Lidor Avigad, Mihir Bellare, Zvika Brakerski, Shafi Goldwasser, Shai Halevi, Tali Kaufman, Leonid Levin, Noam Nisan, Dana Ron, Madhu Sudan, Luca Trevisan, Salil Vadhan, Avi Wigderson, David Zuckerman*. Ed. by Oded Goldreich. Berlin, Heidelberg: Springer, 2011, pp. 191–232. ISBN: 978-3-642-22670-0. DOI: 10.1007/978-3-642-22670-0_20 (cit. on p. 2).

[Gol24] Louis Golowich. "New Explicit Constant-Degree Lossless Expanders". In: *Proceedings of the 2024 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*. Proceedings. Society for Industrial and Applied Mathematics, Jan. 2024, pp. 4963–4971. DOI: 10.1137/1.9781611977912.177 (cit. on p. 1).

[GUV09] Venkatesan Guruswami, Christopher Umans, and Salil Vadhan. "Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes". In: *Journal of the ACM* 56.4 (July 2009), 20:1–20:34. ISSN: 0004-5411. DOI: 10.1145/1538902.1538904 (cit. on pp. 2, 5, 15, 18).

[HMMP24] Jun-Ting Hsieh, Theo McKenzie, Sidhanth Mohanty, and Pedro Paredes. "Explicit Two-Sided Unique-Neighbor Expanders". In: *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*. STOC 2024. New York, NY, USA: Association for Computing Machinery, June 2024, pp. 788–799. DOI: 10.1145/3618260.3649705 (cit. on p. 2).

[Kah95] Nabil Kahale. "Eigenvalues and expansion of regular graphs". In: *J. ACM* 42.5 (Sept. 1995), pp. 1091–1106. ISSN: 0004-5411. DOI: 10.1145/210118.210136 (cit. on p. 1).

[KT22] Itay Kalev and Amnon Ta-Shma. "Unbalanced Expanders from Multiplicity Codes". en. In: *DROPS-IDN/v2/document/10.4230/LIPIcs.APPROX/RANDOM.2022.12*. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022. DOI: 10.4230/LIPIcs.APPROX/RANDOM.2022.12 (cit. on pp. 2, 3, 6, 8).

[KSY14] Swastik Kopparty, Shubhangi Saraf, and Sergey Yekhanin. "High-rate codes with sublinear-time decoding". In: *J. ACM* 61.5 (Sept. 2014), 28:1–28:20. ISSN: 0004-5411. DOI: 10.1145/2629416 (cit. on pp. 2, 6).

[LH22] Ting-Chun Lin and Min-Hsiu Hsieh. *Good quantum LDPC codes with linear time decoder from lossless expanders*. arXiv:2203.03581 [quant-ph]. Mar. 2022. DOI: 10.48550/arXiv.2203.03581 (cit. on p. 1).

[PK22] Pavel Panteleev and Gleb Kalachev. "Asymptotically good Quantum and locally testable classical LDPC codes". In: *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*. STOC 2022. New York, NY, USA: Association for Computing Machinery, June 2022, pp. 375–388. ISBN: 978-1-4503-9264-8. DOI: 10.1145/3519935.3520017 (cit. on p. 1).

[Rit50] Joseph Fels Ritt. *Differential algebra*. Vol. 33. American Mathematical Soc., 1950 (cit. on p. 9).

[TU06] Amnon Ta-Shma and Christopher Umans. "Better lossless condensers through derandomized curve samplers". In: *2006 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06)*. ISSN: 0272-5428. Oct. 2006, pp. 177–186. DOI: 10.1109/FOCS.2006.18 (cit. on p. 2).

[TUZ07] Amnon Ta-Shma, Christopher Umans, and David Zuckerman. "Lossless Condensers, Unbalanced Expanders, And Extractors". en. In: *Combinatorica* 27.2 (Mar. 2007), pp. 213–240. ISSN: 1439-6912. DOI: 10.1007/s00493-007-0053-2 (cit. on p. 2).

[SS96] M. Sipser and D.A. Spielman. "Expander codes". In: *IEEE Transactions on Information Theory* 42.6 (Nov. 1996). Conference Name: IEEE Transactions on Information Theory, pp. 1710–1722. ISSN: 1557-9654. DOI: 10.1109/18.556667 (cit. on p. 2).

[Ter19] Terence Tao. *Conversions between standard polynomial bases*. https://terrytao.wordpress.com/2019/04/07/conversions-between-standard-polynomial-bases/. Accessed: 08-30-2024. 2019 (cit. on p. 7).

[UW87] Eli Upfal and Avi Wigderson. "How to share memory in a distributed system". In: *J. ACM* 34.1 (Jan. 1987), pp. 116–127. ISSN: 0004-5411. DOI: 10.1145/7531.7926 (cit. on p. 2).

[Vad12] Salil P. Vadhan. "Pseudorandomness". English. In: *Foundations and Trends® in Theoretical Computer Science* 7.1–3 (Dec. 2012). Publisher: Now Publishers, Inc., pp. 1–336. ISSN: 1551-305X, 1551-3068. DOI: 10.1561/0400000010 (cit. on p. 1).

A Explicitness

Claim A.1. *The KT graph G as defined in Definition 3.5 is explicit, i.e., the left neighborhood function $\Gamma_{\rightarrow} : \mathbb{F}_q^n \times \mathbb{F}_q \to \mathbb{F}_q^{s+2}$ and right neighborhood function $\Gamma_{\leftarrow} : \mathbb{F}_q^{s+2} \times \mathbb{F}_q^{n-(s+1)} \to \mathbb{F}_q^n$ can be computed in $\mathrm{poly}(\log(q^n))$ time.*

Proof. Recall that for the graph G, we have $char(\mathbb{F}_q) \geq n$ and so, $q \geq n$. Hence, $\mathrm{poly}(\log(q^n)) = \mathrm{poly}(n, q)$ and this is the time our algorithm can afford to take. To compute $\Gamma_{\rightarrow}(f, y)$, we treat f as an element of $\mathbb{F}_q[X]$ of degree at most $n-1$, and map it to $(y, f^{(0)}(y), \ldots, f^{(s)}(y))$. We can compute derivatives of f and evaluate it at y in time $\mathrm{poly}(n, q)$ and hence explicitly compute $\Gamma_{\rightarrow}(f, y)$.

To compute $\Gamma_{\leftarrow}(z, t)$, we proceed as follows. Let $z = (y, w)$ where $y \in \mathbb{F}_q$ and $w \in \mathbb{F}_q^{s+1}$. Then, we need to find f such that $\Gamma_{\rightarrow}(f, y) = z$. Define $\psi_y : \mathbb{F}_q^n \to \mathbb{F}_q^{s+1}$ as $\psi_y(f) = (f^{(0)}(y), \ldots, f^{(s)}(y))$. By Claim 4.7, ψ_y is a full rank $\mathbb{F}_q$-linear map. As $n > s+1$, kernel of ψ_y has dimension $n - (s+1) > 0$. By considering the matrix associated with ψ_y and using standard linear algebra algorithms, we construct an injective linear map $K_y : \mathbb{F}_q^{n-(s+1)} \to \mathbb{F}_q^n$ in $\mathrm{poly}(n, q)$ time such that the image of K_y is exactly the kernel of ψ_y. Furthermore, using Gaussian elimination on the matrix associated with ψ_y, we can, in $\mathrm{poly}(n, q)$ time, find some $g \in \mathbb{F}_q^n$ such that $\psi_y(g) = w$. Finally, we let $\Gamma_{\leftarrow}(z, t) = K_y(t) + g$. By linearity of ψ_y, we have that $\psi_y(K_y(t) + g) = \psi_y(g) = w$. As K_y is injective, for a fixed z, our computed function maps different t to different outputs as desired. □

Note that given any $n, k, \varepsilon, \alpha$, Lemma 5.2 sets $q = \mathrm{poly}(n, k, 1/\varepsilon)$, so we can deterministically find such a prime q satisfying the requirements in $\mathrm{poly}(n, 1/\varepsilon)$ time as well.

Explicitness of the KT graph also implies explicitness of our non-bipartite lossless expander obtained by taking the bipartite half of the KT graph (and removing the zero vertex):

Claim A.2. *The non-bipartite graph $H = G^2[L \setminus \{0\}]$ as constructed in Theorem 6.1 is explicit. I.e., the neighborhood function $\Gamma : (\mathbb{F}_q^n \setminus \{0\}) \times (\mathbb{F}_q \times \mathbb{F}_q^{n-(s+1)}) \to \mathbb{F}_q^n$ can be computed in $\mathrm{poly}(\log(q^n))$ time.*

Proof. Note that since G is not necessarily regular, Γ may sometimes output $\perp$. The guarantee that we will have is that for all $f, g \in \mathbb{F}_q^n$ that are neighbors in H, there will exist unique $y, t \in \mathbb{F}_q \times \mathbb{F}_q^{n-(s+1)}$ such that $\Gamma(f, y, t) = g$.

Let $\Gamma_\to, \Gamma_\leftarrow$ be the explicit left and right neighborhood functions of the KT graph as defined in Claim A.1. To compute $\Gamma(f, y, t)$, we first compute $g = \Gamma_\leftarrow(\Gamma_\to(f, y), t)$. If $g = 0$, then we output $\perp$. Then, for all $y' < y$, we check whether $\Gamma_\to(f, y') = \Gamma_\to(g, y')$. If they are equal for any such y', we output $\perp$. Otherwise, we output g. This last check is done so that we only output g once as a neighbor of f and otherwise output $\perp$. Explicitness of Γ follows because of explicitness of $\Gamma_\to, \Gamma_\leftarrow$ and because the last check has to be done $O(q)$ times. □

B The [GUV09] Graph is Not Right Regular

One may naturally try to show that the predecessor to the KT graph, the [GUV09] graph, is also a two-sided lossless expander. However, it turns out that the [GUV09] graph is not even right regular. To see why, we give the definition of the [GUV09] graph which is similar to the KT graph.

Definition B.1 (The GUV graph, [GUV09])**.** *Let $q, n, m, h \in \mathbb{N}$ be such that q is a prime power greater than h, characteristic of the finite field $\mathbb{F}_q \geq n$ and $m < n$. We define $G = (L \sqcup R, E)$ where $L = \mathbb{F}_q^n \cong \mathbb{F}_q[x]/(z(x))$ for some irreducible polynomial $z(x) \in \mathbb{F}_q(x)$ of degree n and $R = \mathbb{F}_q^{m+1}$. The left degree is q and for any $f \in \mathbb{F}_q[x]/(z(x))$ and $y \in \mathbb{F}_q$, the y'th neighbor of f is defined as $\Gamma_\to(f, y) = \Big(y, f(y), (f^h \mod z(x))(y), (f^{h^2} \mod z(x))(y), \ldots, (f^{h^{m-1}} \mod z(x))(y)\Big)$.*

Our proof of right-regularity for Lemma 4.3 relied on the fact that the map $\psi_y(f) \mapsto (f^{(0)}(y), \ldots, f^{(s)}(y))$ is full rank over $\mathbb{F}_q$, as shown in Claim 4.7. The analogous GUV map $\varphi_y(f) = (f(y), f^h(y), \ldots, f^{h^{m-1}}(y))$ does not have this property because of two issues. First, it is not necessarily linear over $\mathbb{F}_q$, although it can be made linear over $\mathbb{F}_2$ when q is a power of 2. Second, even over $\mathbb{F}_2$, it does not necessarily have full rank, meaning we cannot guarantee right regularity.

Simulations bear this out. The GUV graph with $q = 2^4$, $n = 4$, $m = 2$, and $h = 2$ has 3072 right vertices with degree 256, 64 with degree 4096, and 960 isolated vertices. For more examples of parameter settings where the GUV graph is not right-regular, we invite the reader to run simulations with our code at `https://github.com/mjguru/GUV-Expander`.

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il