Two-Sided Lossless Expanders in the Unbalanced Setting

Eshan Chattopadhyay
Cornell University, Ithaca, NY, USA

Mohit Gurumukhani
Cornell University, Ithaca, NY, USA

Noam Ringach
Cornell University, Ithaca, NY, USA

Yunya Zhao
Cornell University, Ithaca, NY, USA

Abstract

We present the first explicit construction of *two-sided* lossless expanders in the unbalanced setting (bipartite graphs that have polynomially 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. Moreover, we show that our result is tight, thus completely characterizing the graph of Kalev and Ta-Shma.

2012 ACM Subject Classification Theory of computation → Expander graphs and randomness extractors

Keywords and phrases Pseudorandomness, lossless expanders, multiplicity codes, condensers

Digital Object Identifier 10.4230/LIPIcs.APPROX/RANDOM.2026.34

Category RANDOM

Related Version *Full Version*: `https://arxiv.org/abs/2409.04549`

Funding *Eshan Chattopadhyay*: Supported by a Sloan Research Fellowship, NSF CAREER Award 2045576 and NSF Award CCF-2514586.
Mohit Gurumukhani: Supported by a Sloan Research Fellowship, NSF CAREER Award 2045576 and NSF Award CCF-2514586.
Noam Ringach: Supported by NSF GRFP grant DGE – 2139899, NSF CAREER Award 2045576, a Sloan Research Fellowship and NSF Award CCF-2514586.
Yunya Zhao: Supported by a Sloan Research Fellowship, NSF CAREER Award 2045576 and NSF Award CCF-2514586.

Acknowledgements We would like to thank Itay Kalev for helpful feedback on our paper. We are also grateful to insightful suggestions from anonymous reviewers that led to simplifying some of our proofs.

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. It is well-known that a random d-regular graph is a $(K = \gamma n, \varepsilon = 0.01)$-lossless expander with high probability, for some constant $\gamma > 0$.

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 [14].

The study of lossless expanders has paid special attention to bipartite graphs due to their connection with randomness condensers. A *one-sided lossless* expander is a bipartite graph $G = (L \sqcup R, E)$ where every "small enough" set on the left expands losslessly to the right. It is standard to view lossless condensers and one-sided bipartite lossless expanders as related objects. For this purpose, it is natural to talk about highly unbalanced bipartite graphs in which $|L| \gg |R|$, that is, 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. Current explicit constructions for unbalanced one-sided lossless expanders [21, 22, 10, 15] – with the best parameters achieved by [10, 15] [1] – have found a wide array of applications in coding theory [20], extractor constructions [21, 22, 10, 7], derandomization [5],[2] and probabilistic data structures [23, 1], with the unbalanced nature of the graph being essential.

We say a bipartite graph is a *two-sided lossless* expander if lossless expansion happens in both directions. Intuitively, in the unbalanced case where $|L| \gg |R|$, lossless expansion is hard to achieve from left to right because there is little room on the smaller side to allow for expansion from the much larger side; on the other hand, the right-to-left expansion seems to be much easier at first sight for the same reason. However, despite aforementioned constructions for one-sided lossless expanders as well as their broad applications, there has been no known explicit construction of unbalanced two-sided lossless expanders before this work. Therefore, it is an extremely intriguing direction to further the theory of lossless expanders. We are not aware of any existing applications of two-sided lossless expanders with a polynomial imbalance between the left and right – we leave this as an interesting open problem – but we believe that a deeper understanding of the structure of these objects is the first step towards making connections with other topics and finding new applications.

In this work, we try to fill the gap, namely, the lack of explicit unbalanced two-sided lossless expanders by closely studying the bipartite graph of [15] based on the multiplicity codes of [16]. [3] For simplicity, we refer to this graph as the "KT graph" (see Definition 20). As our main result, we show that the KT graph is a two-sided lossless expander. Moreover, we prove that the expansion is tight up to a constant multiplicative factor.

We note that lossless expanders have been extensively studied in the *balanced* setting as well. We discuss this in Section 1.2.

1.1 Our results

We first define a two-sided lossless expander formally:

[1] The lossless expanders of [15] have slightly better dependence on constants compared to [10].
[2] [5] instantiated Goldreich's PRG [8] with the lossless expander of [15].
[3] It is natural to consider whether the unbalanced expander from [10] is a two-sided lossless expander. It will be interesting to determine this since the GUV graph is not even right-regular – see Appendix B for details.

▶ **Definition 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 $|S_L| \leq K_L$ we have that $|\Gamma_{\rightarrow}(S_L)| \geq A_L |S_L|$ and similarly that for any subset $S_R \subseteq R$ such that $|S_R| \leq K_R$ we have that $|\Gamma_{\leftarrow}(S_R)| \geq A_R |S_R|$. 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 the above definition, we are ready to state the main theorems:

▶ **Theorem 2** (Informal version of Theorem 30, bipartite two-sided lossless expander). *For infinitely many N and all constant $0 < \delta \leq 0.99$, 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 $D_L = \text{poly}(\log N)$, $N^{1.01\delta - o(1)} \leq M \leq D_L \cdot N^{1.01\delta}$, $K_L = N^{\delta}$, and finally $K_R = \min(O(M/D_L), O(N/(MD_L)))$.*

On the other hand, for any of the explicit graphs constructed here, there exists a set $S \subseteq R$, $|S| = O(K_R)$, on the right side which has less than $(1 - \varepsilon_R/2) \cdot D_R \cdot |S|$ neighbors on the left.

▶ Remark 3. Because [15] 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 expansion constant, optimal size of sets of vertices on left side that losslessly expand, and optimal size of sets of vertices on right side that losslessly expand when $M \leq \sqrt{N}$. [4]

▶ Remark 4. When $\delta \leq 0.49$, the value of K is almost optimal (a trivial upper bound is $K \leq N/D$) since in that regime, $K = N^{\delta} \geq (N/D)^{0.99}$.

1.2 Lossless expanders in the balanced setting

A parallel line of work considers *balanced* bipartite lossless expanders, with motivations from coding theory. There have been explicit constructions of balanced one-sided lossless expanders [2, 4, 9], with which one can construct good error correcting codes [20]. There has also been progress in understanding two-sided lossless expanders in the balanced setting. Lossless expansion was shown to be feasible in high-girth regular graphs [18, 13], taking the bipartite double cover of which implies a balanced two-sided lossless expander. Chen [3] achieved balanced two-sided lossless expansion for polynomial-sized sets as one of their several results; however, their size of expanding sets is not optimal in the balanced setting. Our analysis proves optimal expanding set size in the unbalanced setting (see Remark 3).

It was shown in [17] that balanced two-sided lossless expanders with constant degree, constant imbalance, and certain algebraic properties have applications to good quantum low-density parity check (qLDPC) codes. A line of recent works [13, 11, 12] recently explicitly constructed these two-sided lossless expanders with the required algebraic property and successfully instantiated the qLDPC construction of [17]. Our work in the polynomially unbalanced setting is incomparable to the balanced setting, as it is possible to achieve constant degree in the balanced setting, while having a polynomial imbalance in left and right nodes forces the graph to have non-constant degrees.

[4] 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.

2 Proof Overview

In this section, we outline the proof of Theorem 2 – our two-sided lossless expander.

2.1 Two-sided lossless expander

We show that the bipartite graph defined in [15] based on multiplicity codes is a two-sided lossless expander. The left-to-right lossless expansion was shown in [15]. 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 5** (Informal version of Theorem 23). *For every field $\mathbb{F}_q$ and $n, s \in \mathbb{N}$ with $15 \leq (s+1) < n < char(\mathbb{F}_q)$, 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 $K_L = \Omega(q^{s+1})$, $A_L = q - n(s+2)$, $K_R = \delta q^{\min(s+1, n-(s+1))}$, $A_R = \left(1 - O\left(\delta \cdot \frac{q-1}{q}\right)\right) q^{n-(s+1)}$.*

Theorem 2 is obtained from Theorem 5 by instantiating the parameters appropriately (see Section 4.3 for more details). We now define the KT graph and then claim that it is a lossless right expander.

▶ **Definition 6** (The KT graph [15]). *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 $s + 2 \leq n$. 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 $(y, f^{(0)}(y), \ldots, f^{(s)}(y))$ where $f^{(i)}$ is the i'th iterative derivative of f.*[5]

▶ **Theorem 7** (The KT graph losslessly expands from the right). *The KT graph G is a right (K_R, A_R)-lossless expander where $K_R = \delta \min(|R|, |L|/|R|)$, $\varepsilon_R = O(\delta \cdot \frac{q-1}{q})$ 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 5 immediately follows from left expansion shown by [15] and Theorem 7. For the rest of this section, we focus on proving Theorem 7 that relies on the following two key lemmas.

▶ **Lemma 8** (Right regularity). *The KT graph G is right-regular and has right-degree $d_R = q^{n-(s+1)}$.*

▶ **Lemma 9** (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 $|\Gamma_{\leftarrow}(y_1, z_1) \cap \Gamma_{\leftarrow}(y_2, z_2)| = q^{n-(2s+2)}$ if $n \geq 2s+2$ and $|\Gamma_{\leftarrow}(y_1, z_1) \cap \Gamma_{\leftarrow}(y_2, z_2)| \leq 1$ if $n \leq 2s+2$.*

[5] Recall that the i-th iterative derivative of f is simply the the standard derivatve $\frac{\mathrm{d}}{\mathrm{d}x}$ applied i times to f.

Theorem 7 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 8 and Lemma 9. We start by making a simple but useful observation on the structure of the KT graph G.

▶ **Observation 10.** *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* [6] *must have disjoint left neighborhoods.*

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

▶ **Definition 11.** *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 12.** *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, $\psi_{y_1,y_2}(f) = (\psi_{y_1}(f), \psi_{y_2}(f))$.*

Proving the above lemmas (about the KT graph) now boils down to analyzing both ψ_y and ψ_{y_1,y_2} for all $y, y_1, y_2 \in \mathbb{F}_q$.

1. We show that ψ_y for $y \in \mathbb{F}_q$ is surjective, which along with Observation 10 implies Lemma 8: For any $w = (y, z_0, \cdots, z_s) \in R$, the set of its left neighbors is $\{f \in L \mid (y, \psi_y(f)) = w\} = \psi_y^{-1}(z_0, \cdots, z_s)$. Therefore, 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. We show ψ_{y_1,y_2} is surjective when $n \geq 2s+2$ and injective $n \leq 2s+2$, which implies Lemma 9: 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 10 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 $\left|\psi_{y_1,y_2}^{-1}(z_1, z_2)\right|$. When $n \geq 2s+2$, this map is surjective, and the number of left neighbors shared by w_1 and w_2 is $q^{n-(2s+2)}$. When $n \leq 2s+2$, this map is injective and the number of shared neighbors is at most 1.

To conclude the proof, we carry out Hermite interpolation (see Lemma 27) by applying the Chinese remainder theorem to show the surjectivity and injectivity of the maps ψ_y, ψ_{y_1} and ψ_{y_2}.

2.1.1 Tightness of right expansion

We will show that our parameters from Theorem 7 are tight. Throughout this section, we let $P_d \subseteq \mathbb{F}_q[x]$ be the polynomials of degree exactly d and $P_{<d} \subseteq \mathbb{F}_q[x]$ be the vector space over $\mathbb{F}_q$ of polynomials of degree strictly less than d. First, notice that when $|R| > |L|/|R|$, the right expansion is optimal by Remark 3. Hence, we only focus on the case when $s+1 < n < 2s+2$ and show the following:

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

▶ **Theorem 13** (Informal version of Theorem 32). *For $s+1 < n < 2s+2$ and any $0 < \delta \leq 2$, there exists $T \subseteq R$ such that $|T| = \delta q^{n-s-1}$ and $|\Gamma_{\leftarrow}(T)| = (1-\varepsilon)D_R|T|$ with $\varepsilon = \delta/4$.*

For fixed $y_1 \neq y_2 \in \mathbb{F}_q$, we will construct $T = T_1 \sqcup T_2$ satisfying the following:

- $|T_1|, |T_2| = (\delta/2)q^{n-s-1}$.
- The first coordinate of every element of T_1 is always y_1 and of T_2 is always y_2.
- For all $t_1 \in T_1$ and $t_2 \in T_2$, there exists a degree less than n polynomial f such that $\Gamma_{\rightarrow}(f, y_1) = t_1$ and $\Gamma_{\rightarrow}(f, y_2) = t_2$.

We then observe that $|\Gamma_{\leftarrow}(T)| = |\Gamma_{\leftarrow}(T_1)| + |\Gamma_{\leftarrow}(T_2)| - |T_1| \cdot |T_2|$. Since the right degree of G is q^{n-s-1}, we have that $|\Gamma_{\leftarrow}(T_1)| = |\Gamma_{\leftarrow}(T_2)| = (\delta/2)q^{2n-2s-2}$. Hence, we compute that $|\Gamma_{\leftarrow}(T)| = (\delta - \delta^2/4)q^{2n-2s-2} = (1-\delta/4)D_R|T|$, proving Theorem 13.

To construct such T_1, T_2, it suffices to construct $S_1, S_2 \subset \mathbb{F}_q^{s+1}$ with $|S_1| = |S_2| = K/2$ such that $S_1 \times S_2 \subset \psi_{y_1,y_2}(P_{<n})$ (see Lemma 35 for a formal claim). Indeed, we can let $T_1 = (y_1, S_1)$ and $T_2 = (y_2, S_2)$ and check that T_1 and T_2 have the desired properties.

Before we show how to construct such S_1 and S_2, we will need to introduce a few algebraic objects. Let $g_1(x) = (x-y_1)^{s+1}, g_2(x) = (x-y_2)^{s+1}$, and let $\varphi : \mathbb{F}_q[x] \to \mathbb{F}_q[x]/g_1 \times \mathbb{F}_q[x]/g_2$ as $\varphi(f) = (f \mod g_1, f \mod g_2)$.

We then prove a structural result regarding φ:

▶ **Lemma 14** (Informal version of Lemma 41). *For $s+1 < d < 2s+2$, we have*

$$\varphi(P_{<d}) = \bigcup_{h \in P_{<d-(s+1)}} \{(f, f+\sigma(h)) \mid f \in P_{\leq s}\}.$$

Here, $\sigma : P_{\leq n-(s+1)} \to P_{\leq s}$ is a specially chosen injective homomorphism that we define later.

To construct such S_1 and S_2, we construct $R_1 \subset \mathbb{F}_q[x]/g_1, R_2 \subset F_q[x]/g_2$ such that $R_1 \times R_2 \subset \varphi(P_{<n})$ (see Lemma 39 for formal claim). Once we have such R_1, R_2, we let $S_1 = \psi_{y_1}(R_1)$ and $S_2 = \psi_{y_2}(R_2)$. We then check that if $f \in P_{<n}$ is such that $\varphi(f) = (r_1, r_2)$, then $f(y_1) = r_1(y_1) = s_1$ and $f(y_2) = r_2(y_2) = s_2$, showing that $S_1 \times S_2 \subset \psi_{y_1,y_2}(P_{<d})$, as desired.

We now construct such R_1 and R_2. Let R_1 and R_2 be arbitrary size $K/2$ subsets of $\sigma(P_{<n-(s+1)})$. Note that since σ is injective, $\left|\sigma(P_{<n-(s+1)})\right| = q^{n-s-1} \geq K/2$ and so we can indeed pick such R_1 and R_2. We claim that for any $r_1 \in R_1, r_2 \in R_2$, it holds that $(r_1, r_2) \in \varphi(P_{<n})$. Using Lemma 14, it suffices to show that $(r_1, r_2) = (f, f+\sigma(h))$ for some $f \in P_{<n}$ and $h \in P_{n-(s+1)}$. Since $R_1, R_2 \subseteq \sigma(P_{<n-(s+1)})$, we know that $r_1 = \sigma(h_1)$ and $r_2 = \sigma(h_2)$ for some $h_1, h_2 \in P_{<n-(s+1)}$. Consequently,

$$(r_1, r_2) = (\sigma(h_1), \sigma(h_2)) = (\sigma(h_1), \sigma(h_1) + \sigma(h_2 - h_1))$$

as desired. In the last line, we used the fact that σ is a homomorphism and that $h_1, h_2 \in P_{<n-(s+1)}$.

We finally define σ:

▶ **Definition 15.** *Recall that $\sigma : P_{<n-(s+1)} \to P_{\leq s}$. To compute $\sigma(h_1)$, we let $f \in P_{<n}$ be any polynomial such that $f = h_1 g_1 + r_1$ where $r_1 \in P_{\leq s}$ is the remainder of f modulo g_1. We then write $f = h_2 g_2 + r_2$ where $r_2 \in P_{\leq s}$ is the remainder of f modulo g_2. The output of $\sigma(h_1)$ is $r_2 - r_1$.*

At first glance, it seems unclear whether σ is even a well defined function. To help show this, we define $\rho : P_{<n-(s+1)} \to P_{<n-(s+1)}$ such that $\rho(h_1) = h_2$ where h_1, h_2 are defined as above. We first show that ρ is an isomorphism. To do this, we observe that

$h_1g_1 - h_2g_2 = r_2 - r_1$ has degree at most s, and so it must be that h_1g_1 and h_2g_2 agree on all coefficients corresponding to degree $\geq s+1$. We compare these coefficients and, using linear algebra, show that we can indeed obtain a unique h_2 from h_1, showing it is indeed a function. This argument in fact directly shows that ρ is an isomorphism.

Once we have that ρ is an isomorphism, we can then define $\sigma(h_1) = h_1g_1 - \rho(h_2)g_2$. Using this, it easily follows that σ is a homomorphism. From this we obtain Lemma 14. By a further counting argument, we can show that σ is injective. For details, see Section 5.2.

2.2 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. In Section 4.3, we plug in parameters to get our two-sided lossless expander. In Section 5 we prove tightness of our right-to-left expansion analysis of the KT graph.

We prove that our constructions are explicit in Appendix A, and discuss why our techniques do not work for the [10] graph 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 16.** *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 17.** *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 16 in two ways. The first way is considering expansion with respect to the maximum number of neighbors of a set.

▶ **Definition 18.** *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 19.** *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 [15] based on multiplicity codes from [16]. We will often refer to this graph "the KT graph":

▶ **Definition 20** (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 21. In the paper [15], 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 [15].

3.4 A useful inequality

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

▷ Claim 22. 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

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

Rearranging, we infer that

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

as desired. ◁

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.

4.1 Main theorem

Putting together all of our results with the left-to-right expansion of [15] yields our main theorem.

▶ **Theorem 23.** *For all finite fields $\mathbb{F}_q$ and $n, s \in \mathbb{N}$ with $15 \le (s+1) < n < char(\mathbb{F}_q)$, 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 $A_R = \left(1 - \frac{K_R}{q^{\min(s+2,n-s)}} \cdot \frac{q-1}{2}\right) q^{n-(s+1)}$.*

Proof. The left-to-right expansion follows from Theorem 3 from [15]. The right-to-left expansion follows from Theorem 24 below. The explicitness of G follows from Claim 47. ◀

Our main achievement is showing the right-to-left expansion of the KT graph in Theorem 24 below.

▶ **Theorem 24.** *If $n \ge s+1$, then the KT graph G in Definition 6 is a right (K_{max}, ε)-lossless expander for $K_{max} = \delta q^{s+1}$ and $\varepsilon = \frac{\delta(q-1)}{2q} \cdot q^{\max(2s+2-n,0)}$ where $0 < \delta < 1$ is arbitrary.*

We prove Theorem 24 via the following properties of G:

▶ **Lemma 25.** *When $n \ge s+1$, G is right-regular and the right degree is $q^{n-(s+1)}$.*

▶ **Lemma 26.** *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*

$$|\Gamma_{\leftarrow}(y_1, z_1) \cap \Gamma_{\leftarrow}(y_2, z_2)| \le \begin{cases} q^{n-(2s+2)} & n \ge 2s+2 \\ 1 & n \le 2s+2 \end{cases}$$

We will prove both these lemmas in Section 4.2.

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 24.

Proof of Theorem 24. 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 25, the number of edges leaving T is $|T| \cdot q^{n-(s+1)} = \delta q^n$.

We now consider cases on whether $n \ge 2s+2$ or not:

Case 1. $n \geq 2s+2$.

In this case, $\varepsilon = \frac{\delta(q-1)}{2q}$. By Lemma 26, the maximum number of double-counted left vertices is

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

where for the last inequality, we used Claim 22. Applying one level of inclusion-exclusion reveals that

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

where the last equality follows because $\varepsilon = \frac{\delta(q-1)}{2q}$.

Case 2. $2s+2 \geq n \geq s+1$.

In this case, $\varepsilon = \frac{\delta(q-1)}{2q} \cdot q^{2s+2-n}$. By Lemma 26, the maximum number of double-counted left vertices is

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

where for the last inequality, we used Claim 22. We again apply one level of inclusion-exclusion to conclude that

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

where the last equality follows because $\varepsilon = \frac{\delta(q-1)}{2q} \cdot q^{2s+2-n}$. ◀

4.2 Right regularity and bounding common neighbors: Hermite interpolation

In this section, we show the $(q^{n-(s+1)})$-right-regularity of the KT graph G, and bound the number of common left neighbors shared by any pair of right vertices with different seeds. Both tasks are essentially a question of Hermite interpolation – we wish to find polynomials $f \in \mathbb{F}_q[Y]$ of degree at most $n-1$ such that when evaluating at some point $y \in \mathbb{F}_q$, the function value $f(y)$ and its first s derivatives $(f^{(0)}(y), f^{(1)}(y), \cdots, f^{(s)}(y))$ match the values given by the right vertices.

▶ **Lemma 27** (Hermite interpolation). *Let $y_1, \cdots, y_k \in \mathbb{F}_q$ be distinct, and for $i \in [k]$, let $z_{i,0}, \cdots, z_{i,s} \in \mathbb{F}_q$. Then there exists a unique polynomial $f \in \mathbb{F}_q[Y]$ with degree at most $k(s+1)$ such that $f^{(j)}(y_i) = z_{i,j}$ for $i \in [k]$ and $j \in \{0\} \cup [s]$.*

Proof. Consider the following k congruences,

$$f(Y) \equiv f_1(Y) \mod (Y-y_1)^{s+1}, \ \cdots, \ f(Y) \equiv f_k(Y) \mod (Y-y_k)^{s+1}$$

Any polynomial f that satisfies the above k congruences must also satisfy $f^{(j)}(y_i) = z_{i,j}$ for $i \in [k]$ and $j \in \{0\} \cup [s]$ – thus solving the interpolation – because $f_i(Y)$ is the order s Taylor polynomial of f at y_i.

We conclude the proof by applying the Chinese remainder theorem for univariate polynomials which asserts that there exists a *unique* polynomial $f \in \mathbb{F}_q[Y]$ of degree at most $k(s+1)$ that satisfies the above congruences. ◀

Recall the maps $\psi_{y_1} : \mathbb{F}_q^n \to \mathbb{F}_q^{s+1}$, and $\psi_{y_1,y_2} : \mathbb{F}_q^n \to \mathbb{F}_q^{2s+2}$ where we have $\psi_y(f) = (f^{(0)}(y), \ldots, f^{(s)}(y))$ and $\psi_{y_1,y_2} = (\psi_{y_1}(f), \psi_{y_2}(f))$. We will use the following fact regarding linearity of derivatives:

▶ **Fact 28** ([19]). *For all $\alpha, \beta \in \mathbb{F}_q$, $f, g \in \mathbb{F}_q[X]$ and $j \geq 0$, 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 29.** *For all $y \in \mathbb{F}_q$, ψ_y is an $\mathbb{F}_q$-linear map.*

Now we prove the right-regularity of G (Lemma 25) and bound the number of overlapping left neighbors (Lemma 26) as special cases of Lemma 27.

Proof of Lemma 25. Let $w_1 \in \mathbb{F}_q^{s+2}$ where $w_1 = (y_1, z_{1,0}, \cdots, z_{1,s})$. Take $k = 1$ in Lemma 27, we get that there exists a unique polynomial f of degree at most $s+1$ such that $f^{(j)}(y_1) = z_{1,j}$ for $j \in \{0\} \cup [s]$. This means the linear map $\psi_{y_1} : \mathbb{F}_q^n \to \mathbb{F}_q^{s+1}$ is surjective. Therefore, the number of left neighbors of any right vertex w_1 is exactly $|\psi_{y_1}^{-1}(z_{1,0}, \cdots, z_{1,s})| = q^{n-(s+1)}$. ◀

Proof of Lemma 26. Let $w_1, w_2 \in \mathbb{F}_q^{s+2}$ where $w_1 = (y_1, z_{1,0}, \cdots, z_{1,s})$ and similarly $w_2 = (y_2, z_{2,0}, \cdots, z_{2,s})$ with $y_1 \neq y_2$. Take $k = 2$ in Lemma 27, we get that there exists a unique polynomial f of degree at most $2(s+1)$ such that $f^{(j)}(y_i) = z_{i,j}$ for $i \in \{1,2\}, j \in \{0\} \cup [s]$. This means,

- When $n > 2s+2$, $\psi_{y_1,y_2} : \mathbb{F}_q^n \to \mathbb{F}_q^{2s+2}$ is surjective, the number of common neighbors shared by w_1, w_2 is exactly $|\psi_{y_1,y_2}^{-1}(z_{1,0}, \cdots, z_{1,s}, z_{2,0}, \cdots, z_{2,s})| = q^{n-2(s+1)}$.
- When $n \leq 2s+2$, $\psi_{y_1,y_2} : \mathbb{F}_q^n \to \mathbb{F}_q^{2s+2}$ is injective, w_1, w_2 share *at most* 1 common left neighbor. ◀

4.3 Plugging in the Parameters

We record our main results regarding two sided lossless expanders:

▶ **Theorem 30** (Formal version of Theorem 2). *For infinitely many N and all $0 < \delta < 0.99$, 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 $D_L \leq O(\log^{204}(N))$, $N^{1.01\cdot\delta - o(1)} \leq M \leq D_L \cdot N^{1.01\cdot\delta}$, $K_L = N^\delta$, $K_R = \frac{1}{50} \cdot (1/D_L) \cdot \min(M, N/M)$.* [7]

These will follow from the following technical lemma:

▶ **Lemma 31.** *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, $\frac{h^{1+\alpha}}{2} \leq q \leq h^{1+\alpha}$ where $h = (4nk_L/\varepsilon_L)^{1/\alpha}$ and such that both $\frac{4}{k_L}\log(2n/\varepsilon_L) \leq \alpha$ and $k_L(1+\alpha) \leq n$. Then, there exists an explicit biregular $(K_L, \varepsilon_L, K_R, \varepsilon_R)$ two-sided lossless expander $\Gamma_\to : [N] \times [D_L] \to [M]$ where $N = q^n, K_L = q^{k_L}, K_L^{1+\alpha-1/\log(h)} \leq M \leq D_L \cdot K_L^{1+\alpha}$, $D_L \leq O(\log(N)\log(K_L)/\varepsilon_L)^{1+1/\alpha+o(1)}$, $\frac{K_R}{q^{\min(s+2,n-s)}} \cdot \frac{q-1}{2} \leq \varepsilon_R$ where $s+2 = \lceil k_L/\log_q(h) \rceil$.*

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

Proof of Theorem 30. We plug in $\alpha = 0.01, \varepsilon_L = 0.01, \varepsilon_R = 0.01, k_L = \delta n$ in Lemma 31 to obtain the desired lossless expander. ◀

[7] Our theorem statement doesn't have any additional constraint on D_R since it can be uniquely inferred from N, M, D_L.

We finally prove our main technical lemma using two-sided expander from Theorem 23:

Proof of Lemma 31. As $s+2 = \lceil k_L/\log_q(h) \rceil$, we have that $h^{s+1} \leq K_L \leq h^{s+2}$. Observe that

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

So, we can apply Theorem 23 and infer that there exists a graph $\Gamma_{\rightarrow} : \mathbb{F}_q^n \times \mathbb{F}_q \rightarrow \mathbb{F}_q^{s+2}$ that is a $(\leq h^{s+2}, A_L)$ left expander and $(\leq K_R, A_R)$ right expander where $A_L = q - \frac{n(s+2)}{2} \cdot (qh^{s+2})^{1/(s+2)}$ and $A_R = \left(1 - \frac{K_R}{q^{\min(s+2,n-s)}} \cdot \frac{q-1}{2}\right) q^{n-(s+1)}$. Notice that as $K_L \leq h^{s+2}$, $\Gamma_{\rightarrow}$ is indeed a (K_L, A_L) expander.

- We first bound the left degree D_L:

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

  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:

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

  where the last inequality follows because $\frac{K_R}{q^{\min(s+2,n-s)}} \cdot \frac{q-1}{2} \leq \varepsilon_R$.
- We finally show lossless expansion from the left side: First, we note that $s+2 \leq 2k_L$. Indeed, $s+2 \leq k_L \log_q(h) + 1 = k_L \frac{\log(h)}{\log(q)} + 1 \leq k_L(1+\alpha)+1 \leq 2k_L$. Then,

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

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

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

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

$$s+2 \geq \frac{4}{\alpha}\cdot\log(2n/\varepsilon_L) \geq \frac{2}{\alpha}\cdot\log(2nk_L/\varepsilon_L) \geq 2\log(h) \geq (1+\alpha)\log(h) \geq \log(q) \quad \blacktriangleleft$$

5 Tightness of Our Construction

In this section we show that the right-to-left expansion of Theorem 24 is tight. In particular, when $n < 2s+2$ Theorem 24 gives a trade-off between the expansion parameter ε and the max size of expanding sets K_{max}. We show that this trade-off is tight up to constants, and thus fully characterize the behavior of the KT graph. Importantly, we show that in the balanced setting where $n = s + O(1)$, the KT graph is *not* a two-sided lossless expander.

Recall that when $n \geq 2s+2$ we know that our result is tight as stated in Remark 3. Consequently, our main theorem in this section deals with the regime where $s+1 < n < 2s+2$. In this setting, Theorem 24 gives us that sets $S \subseteq R$ on the right of size at most $K_{max} = \delta q^{s+1}$ expand with parameter $\varepsilon = \frac{\delta(q-1)}{2q}\cdot q^{2s+2-n}$. Equivalently, it gives us that sets of size at most $K_{max} = \delta q^{n-s-1}$ expand with parameter $\varepsilon = \frac{\delta(q-1)}{2q}$. Our main theorem in this section upper bounds this expansion.

▶ **Theorem 32.** *When $s+1 < n < 2s+2$, there exists a subset $S \subseteq R$ of the right vertices such that $|S| = K_{max} = \delta q^{n-s-1}$ and $|\Gamma_{\leftarrow}(S)| = (1-\varepsilon)D_R|S|$ with $\varepsilon = \frac{\delta}{4}$ where $\delta > 0$.*

This means that our right-to-left expansion of *Theorem* 24 is tight up to a constant factor of 1/2. The proof of our main theorem comes from the construction of two disjoint subsets of right vertices each in different buckets that have the maximum number of overlapping neighbors on the left. Recall that the y-th bucket T_y is defined as $T_y = \{(y,\alpha) : \alpha \in \mathbb{F}_q^{s+1}\}$

▶ **Lemma 33.** *Let $y_1, y_2 \in \mathbb{F}_q$ be arbitrary such that $y_1 \neq y_2$. Then there exist sets $S_1 \subseteq T_{y_1}$ and $S_2 \subseteq T_{y_2}$ such that $|S_1| = |S_2| = \frac{K_{max}}{2}$ and $|\Gamma_{\leftarrow}(S_1) \cap \Gamma_{\leftarrow}(S_2)| = |S_1|\cdot|S_2|$.*

Using this lemma, our main theorem is a result of straightforward computations.

Proof of Theorem 32. Take any $y_1, y_2 \in \mathbb{F}_q$ such that $y_1 \neq y_2$ and the S_1 and S_2 from Lemma 33. Let $S = S_1 \cup S_2$, so indeed $|S| = K_{max}$. To count $|\Gamma_{\leftarrow}(S)|$, all we need to do is to subtract the number of 2-wise overlaps of left neighbors S_1 and S_2 from the total number of possible neighbors of S_1 and S_2. The latter value is simply $|S|\cdot D_R = K_{max}\cdot D_R$, and the former is given to us by Lemma 33 as $|S_1|\cdot|S_2| = \frac{K_{max}^2}{4}$. Therefore, we can compute

$$|\Gamma_{\leftarrow}(S)| = K_{max}\cdot D_R - \frac{K_{max}^2}{4} = K_{max}\cdot D_R\left(1 - \frac{K_{max}}{4D_R}\right),$$

showing that

$$\varepsilon = \frac{K_{max}}{4D_R} = \frac{\delta q^{n-(s+1)}}{4q^{n-(s+1)}} = \frac{\delta}{4}. \quad \blacktriangleleft$$

The proof of Lemma 33 relies on choosing S_1 and S_2 to contain only the derivatives of polynomials of degree at most $n-(s+1)$. In the following proofs, we will consider vector spaces of polynomials over $\mathbb{F}_q$.

▶ **Definition 34.** *Define the set* $P_d = \{f \in \mathbb{F}_q[x] \mid \deg(f) = d\}$ *and let* $P_{<d} = \{f \in \mathbb{F}_q[x] \mid \deg(f) < d\}$ *be a vector space over* $\mathbb{F}_q$ *with addition and multiplication coming from* $\mathbb{F}_q[x]$.

5.1 Constructing sets with the smallest expansion possible

We prove Lemma 33 by restricting the KT graph to the subgraph containing the two buckets T_{y_1} and T_{y_2} and analyzing the behavior of this subgraph. Consequently, we rephrase Lemma 33 as follows.

▶ **Lemma 35** (Technical version of Lemma 33). *For any* $K \in [q^{n-(s+1)}]$ *and distinct* $y_1, y_2 \in \mathbb{F}_q$, *there exist sets* $S_1, S_2 \subseteq \mathbb{F}_q^{s+1}$ *such that* $|S_1| + |S_2| = K$ *and* $S_1 \times S_2 \in \psi_{y_1,y_2}(P_{<n})$.

To create these S_1 and S_2, we actually first create analogous sets in the image of the Chinese Remainder Theorem map, defined below.

▶ **Definition 36.** *For distinct* $y_1, y_2 \in \mathbb{F}_q$ *let* $g_1(x) = (x-y_1)^{s+1}$ *and* $g_2(x) = (x-y_2)^{s+1}$, *let* $\pi_1 : \mathbb{F}_q[x] \to \mathbb{F}_q[x]/(g_1)$ *and* $\pi_2 : \mathbb{F}_q[x] \to \mathbb{F}_q[x]/(g_2)$ *be the associated quotient maps. Then let* $\varphi : \mathbb{F}_q[x]/(g_1g_2) \to \mathbb{F}_q[x]/(g_1) \times \mathbb{F}_q[x]/(g_2)$ *be defined as* $\varphi = \pi_1 \otimes \pi_2$.

This is exactly the map that the Chinese Remainder Theorem acts on.

▷ Claim 37. The Chinese Remainder Theorem says that φ is an isomorphism of rings.[8]

▶ **Corollary 38.** *As a consequence, we may also think of* φ *as an isomorphism of* $\mathbb{F}_q$*-vector spaces* $\varphi : P_{<2s+2} \to P_{<s+1} \times P_{<s+1}$.

Whereas $\psi_{y_1,y_2}(f)$ tells us about the first s derivatives of f at y_1 and y_2, $\varphi(f)$ tells us about f quotiented by g_1 and g_2. In fact, as we will see, φ and ψ_{y_1,y_2} provide us with the same information about a particular polynomial. With this in mind, we prove a lemma similar to Lemma 35 but for φ.

▶ **Lemma 39.** *For any* $K \in [q^{n-(s+1)}]$ *and distinct* $y_1, y_2 \in \mathbb{F}_q$, *there exist sets* $S_1 \subseteq \mathbb{F}_q[x]/(g_1)$ *and* $S_2 \subseteq \mathbb{F}_q[x]/(g_2)$ *such that* $|S_1| + |S_2| = K$ *and* $S_1 \times S_2 \in \varphi(P_{<n})$.

Using this relation between φ and ψ_{y_1,y_2}, we prove Lemma 35.

Proof of Lemma 35. Use Lemma 39 to create $R_1 \subseteq \mathbb{F}_q[x]/(g_1)$ and $R_2 \subseteq \mathbb{F}_q[x]/(g_2)$ such that $|R_1| + |R_2| = K$ and $R_1 \times R_2 \in \varphi(P_{<n})$. Let $S_1 = \psi_{y_1} \circ \pi_1^{-1}(R_1)$ and $S_2 = \psi_{y_2} \circ \pi_2^{-1}(R_2)$ where π_1^{-1} and π_2^{-1} are the natural inclusions of $\mathbb{F}_q[x]/(g_1)$ and $\mathbb{F}_q[x]/(g_2)$ into $\mathbb{F}_q[x]$, respectively. We claim that $S_1 \times S_2 \in \psi_{y_1,y_2}(P_{<n})$.

Since the polynomials in the images of π_1^{-1} and π_2^{-1} are of degree strictly less than $s+1$, we have that $\psi_{y_1} \circ \pi_1^{-1}$ and $\psi_{y_2} \circ \pi_2^{-1}$ are injective, so $|S_1| + |S_2| = |R_1| + |R_2| = K$. Moreover, for a pair $(s_1, s_2) \in S_1 \times S_2$, we can take the unique $(r_1, r_2) \in R_1 \times R_2$ such that $s_1 = \psi_{y_1} \circ \pi_1^{-1}(r_1)$ and $s_2 = \psi_{y_2} \circ \pi_2^{-1}(r_2)$. Thus, $(s_1, s_2) = \psi_{y_1,y_2}(\pi_1^{-1}(r_1), \pi_2^{-1}(r_2)) \in \psi_{y_1,y_2}(P_{<n})$, as claimed. ◀

Our proof of Lemma 39 relies on a result about the structure of the image of φ which we prove in Section 5.2 but state here.

[8] For an introduction to the Chinese Remainder Theorem, see Chapter 7.6 of [6].

▶ **Definition 40.** *For any $b \in \mathbb{F}_q^{s+1}$ define the line $\ell_b = \{(f, f+b) \mid f \in \mathbb{F}_q^{s+1}\}$.*

We now show that the image of φ is actually composed of many of these lines with shifts given by the injective homomorphism $\sigma : P_{<n-(s+1)} \to P_{<s+1}$ that we introduce later in Definition 45.

▶ **Lemma 41.** *We show that:*
1. $\varphi(P_{<s+1}) = \ell_0$
2. *For $2s+2 > d \geq s+1$ we have $\varphi(P_d) = \bigcup_{h \in P_{d-(s+1)}} \ell_{\sigma(h)}$.*

Thus, we can conclude that $\varphi(P_{<n}) = \bigcup_{h \in P_{<n-(s+1)}} \ell_{\sigma(h)}$ where σ is an injective homomorphism.

This structural result on the image of φ allows us to prove Lemma 39.

Proof of Lemma 39. Let $S_1, S_2 \subseteq \sigma(P_{<n-(s+1)})$ such that $|S_1| = |S_2| = \frac{K_{max}}{2}$. Recall that σ is injective so $\left|\sigma(P_{<n-(s+1)})\right| = \left|P_{<n-(s+1)}\right| = q^{n-(s+1)}$ and we have enough elements to choose from. We claim that any such choice of S_1 and S_2 satisfies the lemma statement.

To prove this claim, we have to show that any pair $(s_1, s_2) \in S_1 \times S_2$ lies in $\varphi(P_{<n})$. By Lemma 41, this is equivalent to saying that (s_1, s_2) is of the form $(f, f + \sigma(h))$ for some $f \in P_{<s+1}$ and $h \in P_{<n-(s+1)}$. From our construction, we have that $s_1 = \sigma(h_1)$ and $s_2 = \sigma(h_2)$ for $h_1, h_2 \in P_{<n-(s+1)}$. So we are considering the point $(\sigma(h_1), \sigma(h_2))$. Using the fact that σ is a homomorphism from Claim 46, we can rewrite this point in our desired form:

$$\begin{aligned}(\sigma(h_1), \sigma(h_2)) &= (\sigma(h_1), \sigma(h_1) + \sigma(h_2) - \sigma(h_1)) \\ &= (\sigma(h_1), \sigma(h_1) + \sigma(h_2 - h_1)).\end{aligned}$$

Thus, $(s_1, s_2) \in \ell_{\sigma(h_2 - h_1)} \subseteq \varphi(P_{<n})$, as claimed. ◀

5.2 The structure of the image of φ

We end Section 5 by proving Lemma 41, that $\varphi(P_{<n}) = \bigcup_{h \in P_{<n-(s+1)}} \ell_{\sigma(h)}$. To do so we first define a new homomorphism ρ which we will use to define σ later on.

▶ **Definition 42.** *Let $\rho : P_{<n-(s+1)} \to P_{<n-(s+1)}$ be defined as follows. Given $h_1 \in P_{<n-(s+1)}$, let $f \in P_{<n}$ be such that $f = h_1 g_1 + r_1$ for some $r_1 \in P_{<s+1}$. Then let $h_2 \in P_{\deg(f)-(s+1)}$ and $r_2 \in P_{<s+1}$ be the unique polynomials such that $f = h_2 g_2 + r_2$. We define $\rho(h_1) := h_2$.*

Given this definition, the natural first question is whether ρ is even well-defined since there are q^{s+1} many choices of f that could be used. Lemma 43 shows that ρ is well-defined and that it is, in fact, just an invertible linear operator, meaning that ρ is an automorphism of $P_{<n-(s+1)}$.

▶ **Lemma 43.** *Let $f \in P_{<n}$ and take $h_1, h_2, r_1, r_2 \in \mathbb{F}_q[x]$ to be the unique polynomials such that*

$$f = h_1 g_1 + r_1$$
$$f = h_2 g_2 + r_2$$

where $\deg(h_1) = \deg(h_2) = \deg(f) - (s+1)$ and $\deg(r_1), \deg(r_2) < s+1$.

Then h_2 can be determined uniquely from h_1, g_1, and g_2. Similarly, h_1 can be determined uniquely from h_2, g_1, and g_2.

Proof of Lemma 43. Rearranging the equations in the lemma statement gives us that

$$h_1 g_1 - h_2 g_2 = r_2 - r_1.$$

Since the degrees of r_1 and r_2 are at most s, we have that $\deg(r_2 - r_1) < s+1$ as well, meaning that $\deg(h_1 g_1 - h_2 g_2) < s+1$. Consequently, the coefficients of x^k for $k \in \{s+1, \ldots, n-1\}$ of $h_1 g_1$ and $h_2 g_2$ must match, which uniquely determines h_2 from h_1.

Formally, if for $t \in \{1,2\}$ we write $h_t(x) = \sum_{k=0}^{n-1-(s+1)} \eta_k^{(t)} x^k$ for $\eta_k^{(t)} \in \mathbb{F}_q$ and expand out $g_t(x) = \sum_{k=0}^{s+1} \gamma_k^{(t)} x^k$ where $\gamma_k^{(t)} \in \mathbb{F}_q$ and $\gamma_{s+1}^{(t)} = 1$, then for each $k \in \{s+1, \ldots, n-1\}$ we have the linear equation

$$\sum_{j=k-(s+1)}^{n-1-(s+1)} \gamma_{k-j}^{(1)} \eta_j^{(1)} = \sum_{j=k-(s+1)}^{n-1-(s+1)} \gamma_{k-j}^{(2)} \eta_j^{(2)}.$$

This yields $n-s-1$ linear equations, which we can write as $M^{(1)}\eta^{(1)} = M^{(2)}\eta^{(2)}$ where for $t \in \{1,2\}$ we let $\eta^{(t)} = (\eta_0^{(t)}, \ldots, \eta_{n-s-2}^{(t)})^\intercal$ and $M^{(t)} \in \mathbb{F}_q^{(n-s-1)\times(n-s-1)}$ is the upper triangular matrix defined as

$$M_{i,j}^{(t)} = \begin{cases} \gamma_{s+1+i-j}^{(t)} & i \le j \\ 0 & i > j \end{cases}$$

Since g_t is monic, meaning that $\gamma_{s+1}^{(t)} = 1$, we clearly see that $\det(M^{(t)}) = 1$, so it is invertible and $\eta^{(2)} = \left(M^{(2)}\right)^{-1} M^{(1)} \eta^{(1)}$. Similarly, $\eta^{(1)} = \left(M^{(1)}\right)^{-1} M^{(2)} \eta^{(2)}$. ◀

▶ **Corollary 44.** *ρ is an automorphism of $P_{<n-(s+1)}$.*

Proof. Lemma 43 shows that we can equivalently define ρ as $\rho = \left(M^{(2)}\right)^{-1} M^{(1)}$, which is an invertible linear transformation. ◀

Now that we have defined ρ and shown that it is an isomorphism, we use it to build σ.

▶ **Definition 45.** *Let $\sigma : P_{<n-(s+1)} \to P_{<s+1}$ be defined as $\sigma(h) = hg_1 - \rho(h)g_2$. Note that while we consider multiplication here to occur in $\mathbb{F}_q[x]$, Lemma 43 tells us that this difference yields a polynomial in $P_{<s+1}$.*

Unsurprisingly, σ is a homomorphism of vector spaces since ρ is one.

▷ Claim 46. Since ρ is an isomorphism, σ is a homomorphism of vector spaces over $\mathbb{F}_q$.

Proof. The fact that σ is a homomorphism of vector spaces over $\mathbb{F}_q$ follows from ρ being a homomorphism and addition and multiplication commuting in $\mathbb{F}_q[x]$. ◁

Finally, we are ready to prove Lemma 41, that $\varphi(P_{<n}) = \bigcup_{h \in P_{<n-(s+1)}} \ell_{\sigma(h)}$.

Proof of Lemma 41. We can directly show the first item by the fact that that the remainder of dividing a polynomial by another of larger degree is the polynomial itself. That is, for any polynomial $f \in P_{<s+1}$, we have that $\pi_1(f) = \pi_2(f) = f$, so $\varphi(f) = (f, f)$. Consequently, going over all f of degree less than $s+1$ gives us $\varphi(P_{<s+1}) = \{(f,f) : f \in P_{<s+1}\} = \ell_0$.

Now, when considering P_d for $2s+2 > d \ge s+1$, quotienting by a degree $s+1$ polynomial does have a non-trivial effect. That is, for $f \in P_d$, there must exist unique $h_1, h_2, r_1, r_2 \in \mathbb{F}_q[x]$ such that

$$f = h_1 g_1 + r_1$$
$$f = h_2 g_2 + r_2$$

where $\deg(h_1) = \deg(h_2) = \deg(f) - (s+1)$ and $\deg(r_1), \deg(r_2) < s+1$. Recall that $g_1(x) = (x-y_1)^{s+1}$ and $g_2(x) = (x-y_2)^{s+1}$. Moreover, $\pi_1(f) = r_1$ and $\pi_2(f) = r_2$. By definition, we have that $h_2 = \rho(h_1)$, meaning that $r_2 = r_1 + h_1 g_1 - \rho(h_1) g_2 = r_1 + \sigma(h_1)$. Therefore, we have $\varphi(f) = (r_1, r_1 + \sigma(h_1))$.

With this in mind, we recall that because h_1 and r_1 uniquely identify f, we can iterate over all elements of P_d by iterating over all $h_1 \in P_{d-(s+1)}$ and $r_1 \in P_{<s+1}$. That is, $P_d = \{h_1 g_1 + r_1 : h_1 \in P_{d-(s+1)}, r_1 \in P_{<s+1}\}$. From this we can conclude that

$$\begin{aligned}
\varphi(P_d) &= \{\varphi(f) : f \in P_d\} \\
&= \{\varphi(h_1 g_1 + r_1) : h_1 \in P_{d-(s+1)}, r_1 \in P_{<s+1}\} \\
&= \{(r_1, r_1 + \sigma(h_1)) : h_1 \in P_{d-(s+1)}, r_1 \in P_{<s+1}\} \\
&= \bigcup_{h_1 \in P_{d-(s+1)}} \ell_{\sigma(h_1)},
\end{aligned}$$

as claimed.

Lastly, to see that σ is injective we recall that φ is an isomorphism and count cardinalities. For the left hand side of $\varphi(P_{<n}) = \bigcup_{h \in P_{<n-(s+1)}} \ell_{\sigma(h)}$, we have that $|\varphi(P_{<n})| = |P_{<n}| = q^n$. For the right hand side, we recall that $|\ell_b| = q^{s+1}$ for any b, so $\left|\bigcup_{h \in P_{<n-(s+1)}} \ell_{\sigma(h)}\right| = \left|\sigma(P_{<n-(s+1)})\right| \cdot q^{s+1}$. Therefore, $\left|\sigma(P_{<n-(s+1)})\right| = \frac{q^n}{q^{s+1}} = q^{n-(s+1)}$, showing that σ is injective since $\left|P_{<n-(s+1)}\right| = q^{n-(s+1)}$. ◀

References

1. H. Buhrman, P. B. Miltersen, J. Radhakrishnan, and S. Venkatesh. Are Bitvectors Optimal? *SIAM Journal on Computing*, 31(6):1723–1744, January 2002. doi:10.1137/S0097539702405292.
2. 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, pages 659–668, New York, NY, USA, May 2002. Association for Computing Machinery. doi:10.1145/509907.510003.
3. Yeyuan Chen. Unique-neighbor expanders with better expansion for polynomial-sized sets. In Yossi Azar and Debmalya Panigrahi, editors, *Proceedings of the 2025 Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2025, New Orleans, LA, USA, January 12-15, 2025*, pages 3335–3362. SIAM, 2025. doi:10.1137/1.9781611978322.108.
4. Itay Cohen, Roy Roth, and Amnon Ta-Shma. HDX Condensers. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1649–1664, November 2023. doi:10.1109/FOCS57990.2023.00100.
5. Dean Doron and Roei Tell. Derandomization with Minimal Memory Footprint. 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.
6. David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley & Sons, 3 edition, July 2003. Google-Books-ID: KJDBQgAACAAJ.
7. Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan. Extensions to the Method of Multiplicities, with Applications to Kakeya Sets and Mergers. *SIAM Journal on Computing*, 42(6):2305–2328, January 2013. doi:10.1137/100783704.
8. Oded Goldreich. In a World of P=BPP. In Oded Goldreich, editor, *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*, pages 191–232. Springer, Berlin, Heidelberg, 2011. doi:10.1007/978-3-642-22670-0_20.

9 Louis Golowich. New Explicit Constant-Degree Lossless Expanders. In *Proceedings of the 2024 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, Proceedings, pages 4963–4971. Society for Industrial and Applied Mathematics, January 2024. doi:10.1137/1.9781611977912.177.

10 Venkatesan Guruswami, Christopher Umans, and Salil Vadhan. Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes. *Journal of the ACM*, 56(4):20:1–20:34, July 2009. doi:10.1145/1538902.1538904.

11 Jun-Ting Hsieh, Ting-Chun Lin, Sidhanth Mohanty, Ryan O'Donnell, and Rachel Yun Zhang. Explicit Two-Sided Vertex Expanders beyond the Spectral Barrier. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, pages 833–842, New York, NY, USA, June 2025. Association for Computing Machinery. doi:10.1145/3717823.3718241.

12 Jun-Ting Hsieh, Alexander Lubotzky, Sidhanth Mohanty, Assaf Reiner, and Rachel Yun Zhang. Explicit Lossless Vertex Expanders. In *2025 IEEE 66th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 894–911, December 2025. ISSN: 2575-8454. doi:10.1109/FOCS63196.2025.00046.

13 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, pages 788–799, New York, NY, USA, June 2024. Association for Computing Machinery. doi:10.1145/3618260.3649705.

14 Nabil Kahale. Eigenvalues and expansion of regular graphs. *J. ACM*, 42(5):1091–1106, September 1995. doi:10.1145/210118.210136.

15 Itay Kalev and Amnon Ta-Shma. Unbalanced Expanders from Multiplicity Codes. In *In Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2022)*. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022. doi:10.4230/LIPIcs.APPROX/RANDOM.2022.12.

16 Swastik Kopparty, Shubhangi Saraf, and Sergey Yekhanin. High-rate codes with sublinear-time decoding. *J. ACM*, 61(5):28:1–28:20, September 2014. doi:10.1145/2629416.

17 Ting-Chun Lin and Min-Hsiu Hsieh. Good quantum LDPC codes with linear time decoder from lossless expanders, March 2022. arXiv:2203.03581 [quant-ph]. doi:10.48550/arXiv.2203.03581.

18 Theo McKenzie and Sidhanth Mohanty. High-girth near-ramanujan graphs with lossy vertex expansion. In Nikhil Bansal, Emanuela Merelli, and James Worrell, editors, *48th International Colloquium on Automata, Languages, and Programming, ICALP 2021, July 12-16, 2021, Glasgow, Scotland (Virtual Conference)*, volume 198 of *LIPIcs*, pages 96:1–96:15. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.ICALP.2021.96.

19 Joseph Fels Ritt. *Differential algebra*, volume 33. American Mathematical Soc., 1950.

20 M. Sipser and D.A. Spielman. Expander codes. *IEEE Transactions on Information Theory*, 42(6):1710–1722, November 1996. Conference Name: IEEE Transactions on Information Theory. doi:10.1109/18.556667.

21 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)*, pages 177–186, October 2006. doi:10.1109/FOCS.2006.18.

22 Amnon Ta-Shma, Christopher Umans, and David Zuckerman. Lossless Condensers, Unbalanced Expanders, And Extractors. *Combinatorica*, 27(2):213–240, March 2007. doi:10.1007/s00493-007-0053-2.

23 Eli Upfal and Avi Wigderson. How to share memory in a distributed system. *J. ACM*, 34(1):116–127, January 1987. doi:10.1145/7531.7926.

A Explicitness

▷ Claim 47. The KT graph G as defined in Definition 20 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 $\text{poly}(n, \log(q))$ time.

Proof. 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 $\text{poly}(n, \log(q))$ 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 Lemma 25, 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 $\text{poly}(n, \log(q))$ 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 $\text{poly}(n, \log(q))$ 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 31 sets $q = \text{poly}(n, k, 1/\varepsilon)$, so we can deterministically find such a prime q satisfying the requirements in $\text{poly}(n, 1/\varepsilon)$ time as well.

B The [10] Graph is Not Right Regular

One may naturally try to show that the predecessor to the KT graph, the [10] graph, is also a two-sided lossless expander. However, it turns out that the [10] graph is not even right regular. To see why, we give the definition of the [10] graph which is similar to the KT graph.

▶ **Definition 48** (The GUV graph, [10]). *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*

$$\Gamma_{\rightarrow}(f, y) = \left(y, f(y), (f^h \bmod z(x))(y), (f^{h^2} \bmod z(x))(y), \ldots, (f^{h^{m-1}} \bmod z(x))(y)\right).$$

Our proof of right-regularity - Lemma 25 - relied on the fact that the map $\psi_y(f) \mapsto (f^{(0)}(y), \ldots, f^{(s)}(y))$ is full rank over $\mathbb{F}_q$. The analogous GUV map defined as $\varphi_y(f) = (f(y), f^h(y), \ldots, f^{h^{m-1}}(y))$ 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`.