Near-Optimal Expanding Generator Sets for Solvable Permutation Groups

V. Arvind[1], Partha Mukhopadhyay[2], Prajakta Nimbhorkar[2], Yadu Vasudev[1]

[1] The Institute of Mathematical Sciences, Chennai, India
{arvind,yadu}@imsc.res.in
[2] Chennai Mathematical Institute, Siruseri, India
{partham,prajakta}@cmi.ac.in

Abstract. Let $G = \langle S \rangle$ be a solvable subgroup of the symmetric group S_n given as input by the generator set S. We give a deterministic polynomial-time algorithm that computes an *expanding generator set* of size $\widetilde{O}(n^2)$ for G. As a byproduct of our proof, we obtain a new explicit construction of ε-bias spaces of size $\widetilde{O}(n \operatorname{poly}(\log d))(\frac{1}{\varepsilon})^{O(1)}$ for the groups $\mathbb{Z}_d^n$.

1 Introduction

Expander graphs are of great interest and importance in theoretical computer science, especially in the study of randomness in computation; the monograph by Hoory, Linial, and Wigderson [10] is an excellent reference. A central problem is the explicit construction of expander graph families [10, 12]. By explicit it is meant that the family of graphs has efficient deterministic constructions, where the notion of efficiency depends upon the application, e.g. [14]. Explicit constructions with the best known, near optimal expansion and degree parameters (the so-called Ramanujan graphs) are Cayley expander families [12].

Alon and Roichman,in [4], show for any finite group G and $\lambda > 0$, that with high probability a multiset S of size $O(\frac{1}{\lambda^2} \log |G|)$ picked uniformly at random from G is a λ-spectral expander: I.e. the second largest eigenvalue in absolute value, of the normalized adjacency matrix of the Cayley graph is bounded by λ. If G is given by its multiplication table then there is a simple *Las Vegas* algorithm for computing S: pick a random multiset S of size $O(\frac{1}{\lambda^2} \log |G|)$ from G and check in deterministic time $|G|^{O(1)}$ that $\mathrm{Cay}(G, T)$ is a λ-spectral expander. Wigderson and Xiao give a deterministic polynomial-time algorithm for computing S by derandomizing this algorithm [17] (see [5] for a combinatorial proof).

This paper

Suppose G, a subgroup of S_n, is given as input by a *generator set* S, and not a multiplication table. Can we compute an $O(\log |G|)$ size expanding generator set for G in deterministic time polynomial in n and $|S|$? Now, it is possible to sample nearly uniformly in polynomial time from G given by a generator set (e.g. see [8]). Therefore, by the Alon-Roichman theorem we have a randomized

polynomial-time algorithm for the problem (although it is not Las Vegas since we do not know how to certify an expanding generator set in polynomial time).

This problem can be seen as a generalization of the construction of small bias spaces in $\mathbb{F}_2^n$ [3]. It is easily proved (see [10]) using properties of finite abelian groups, that ε-bias spaces are precisely the expanding generator sets for any finite abelian group. Interestingly, the best known explicit construction of ε-bias spaces is of size either $O(n^2/\varepsilon^2)$ [3] or $O(n/\varepsilon^3)$ [2], whereas the Alon-Roichman theorem guarantees the existence of ε-bias spaces of size $O(n/\varepsilon^2)$.

Subsequently, Azar, Motwani and Naor [7] gave a construction of ε-bias spaces for finite abelian groups of the form $\mathbb{Z}_d^n$ using Linnik's theorem and Weil's character sum bounds. The size of the ε-bias space they give is $O((d+n^2/\varepsilon^2)^C)$ where the current best known bound for C is $11/2$.

Let G be a finite group, and let $S = \{g_1, g_2, \ldots, g_k\}$ be a *generating* set for G. The *undirected Cayley graph* $\mathrm{Cay}(G, S \cup S^{-1})$ is an undirected multigraph with vertex set G and edges of the form $\{x, xg_i\}$ for each $x \in G$ and $g_i \in S$. Since S is a generator set for G, $\mathrm{Cay}(G, S \cup S^{-1})$ is a connected regular multigraph.

In this paper we prove a more general result. Given any solvable subgroup G of S_n (where G is given by a generator set) and $\lambda > 0$, we construct an expanding generator set T for G of size $\widetilde{O}(n^2)(\frac{1}{\lambda})^{O(1)}$ such that $\mathrm{Cay}(G, T)$ is a λ-spectral expander. The exact constant factor in the upper bound is given in Section 4.

We also note that, for a *general* permutation group $G \leq S_n$ given by a generator set, we can compute (in deterministic polynomial time) an $O(n^c)(\frac{1}{\lambda})^{O(1)}$ size generator set T such that $\mathrm{Cay}(G, T)$ is a λ-spectral expander, where c is a large constant.

Now we explain the main ingredients of our expanding generator set construction for solvable groups.

1. Let G be a finite group and N be a normal subgroup of G. Given expanding generator sets S_1 and S_2 for N and G/N respectively such that the corresponding Cayley graphs are λ-spectral expanders, we give a simple polynomial-time algorithm to construct an expanding generator set S for G such that $\mathrm{Cay}(G, S)$ is also λ-spectral expander. Moreover, $|S|$ is bounded by a constant factor of $|S_1| + |S_2|$. The analysis in this section is similar to the work of [15, 16].
2. We compute the derived series for the given solvable group $G \leq S_n$ in polynomial time using a standard algorithm [13]. This series is of $O(\log n)$ length due to Dixon's theorem. Let the derived series for G be $G = G_0 \rhd G_1 \rhd \cdots \rhd G_k = \{1\}$. Assuming that we already have an expanding generator set for each quotient group G_i/G_{i+1} (which is abelian) of size $\widetilde{O}(n^2)$, we apply the previous step repeatedly to obtain an expanding generator set for G of size $\widetilde{O}(n^2)$. We can do this because the derived series is a normal series.
3. Finally, we consider the abelian quotient groups G_i/G_{i+1} and give a polynomial time algorithm to construct expanding generator sets of size $\widetilde{O}(n^2)$ for them. This construction applies a series decomposition of abelian groups as well as makes use of the Ajtai et al construction of expanding generator sets for $\mathbb{Z}_t$ [1]. This construction is motivated by work of Alon et al. [3].

We describe the steps 1, 2 and 3 outlined above in Sections 2, 3 and 4, respectively. As a simple application of our main result, we give a new explicit construction of ε-bias spaces for the groups $\mathbb{Z}_d^n$ which we explain in Section 5. The size of our ε-bias spaces are $O(n\,\mathrm{poly}(\log n, \log d))(\frac{1}{\varepsilon})^{O(1)}$. The known construction of ε-bias space for $\mathbb{Z}_d^n$ is of size $O((d + n/\varepsilon^2))^{11/2}$ [7]. The size bound of our construction improves on the Azar-Motwani-Naor construction in the parameters d and n.

It is interesting to ask, for a finite group G given by generator sets, whether we can obtain expanding generator sets of $O(\log |G|)$ size in deterministic polynomial time. By the Alon-Roichman theorem we know that such expanding generator sets for G exist.

In this connection, we note a negative result that Lubotzky and Weiss [11] have shown about solvable groups: Let $\{G_i\}$ be any infinite family of finite solvable groups $\{G_i\}$ where each G_i has derived series length bounded by some constant ℓ. Suppose Σ_i is any generator set for G_i of size $|\Sigma_i| \leq k$ for each i and some constant k. Then the Cayley graphs $\mathrm{Cay}(G_i, \Sigma_i)$ do not form an expander family. In contrast, they also exhibit an infinite family of solvable groups in [11] that give rise to constant-degree Cayley expanders.

2 Combining Generator Sets for Normal subgroup and Quotient Group

Let G be any finite group and N be a normal subgroup of G, denoted $G \rhd N$. I.e. $g^{-1}Ng = N$ for all elements $g \in G$. Let $A \subset N$ be an expanding generator set for N and $\mathrm{Cay}(N, A)$ be a λ-spectral expander. Similarly, let $B \subset G$ such that $\widehat{B} = \{Nx \mid x \in B\}$ is an expanding generator set for the quotient group G/N and $\mathrm{Cay}(G/N, \widehat{B})$ is λ-spectral. We first show that $\mathrm{Cay}(G, A \cup B)$ is a $\frac{1+\lambda}{2}$-spectral expander.

In order to analyze the spectral expansion of the Cayley graph $\mathrm{Cay}(G, A \cup B)$ it is useful to view vectors in $\mathbb{C}^{|G|}$ as elements of the group algebra $\mathbb{C}[G]$. The group algebra $\mathbb{C}[G]$ consists of linear combinations $\sum_{g\in G} \alpha_g g$ for $\alpha_g \in \mathbb{C}$. Addition in $\mathbb{C}[G]$ is component-wise, and clearly $\mathbb{C}[G]$ is a $|G|$-dimensional vector space over $\mathbb{C}$. The product of $\sum_{g\in G} \alpha_g g$ and $\sum_{h\in G} \beta_h h$ is defined naturally as: $\sum_{g,h\in G} \alpha_g \beta_h gh$.

Let $S \subset G$ be any symmetric subset (i.e. S is closed under inverse) and let M_S denote the normalized adjacency matrix of the undirected Cayley graph $\mathrm{Cay}(G, S)$. Now, each element $a \in G$ defines the linear map $M_a : \mathbb{C}[G] \to \mathbb{C}[G]$ by $M_a(\sum_g \alpha_g g) = \sum_g \alpha_g ga$. Clearly, $M_S = \frac{1}{|S|} \sum_{a\in S} M_a$ and $M_S(\sum_g \alpha_g g) = \frac{1}{|S|} \sum_{a\in S} \sum_g \alpha_g ga$.

Let $X = \{x_1, x_2, \ldots, x_k\}$ denote a set of distinct coset representatives for the normal subgroup N in G. In order to analyze the spectral expansion of $\mathrm{Cay}(G, A \cup B)$ we consider the basis $\{xn \mid x \in X, n \in N\}$ of $\mathbb{C}[G]$. The element $u_N = \frac{1}{|N|} \sum_{n\in N} n$ of $\mathbb{C}[G]$ corresponds to the uniform distribution supported on N. It has the following important properties:

1. For all $a \in N$ $M_a(u_N) = u_N$ because $Na = N$ for each $a \in N$.
2. For any $b \in G$ consider the linear map $\sigma_b : \mathbb{C}[G] \to \mathbb{C}[G]$ defined by conjugation: $\sigma_b(\sum_g \alpha_g g) = \sum_g \alpha_g b^{-1} g b$. Since $N \lhd G$ the linear map σ_b is an automorphism of N. It follows that for all $b \in G$ $\sigma_b(u_N) = u_N$.

Now, consider the subspaces U and W of $\mathbb{C}[G]$ defined as follows:

$$U = \left\{ \left(\sum_{x \in X} \alpha_x x \right) u_N \right\}, \quad W = \left\{ \sum_{x \in X} x \left(\sum_{n \in N} \beta_{n,x} n \right) \;\middle|\; \sum_n \beta_{n,x} = 0, \ \forall x \in X \right\}$$

It is easy to see that U and W are indeed subspaces of $\mathbb{C}[G]$. Furthermore, we note that every vector in U is orthogonal to every vector in W with respect to the usual dot product, i.e. $U \perp W$. This follows easily from the fact that xu_N is orthogonal to $x \sum_{n \in N} \beta_{n,x} n$ whenever $\sum_{n \in N} \beta_{n,x} n$ is orthogonal to u_N. Note that $\sum_{n \in N} \beta_{n,x} n$ is indeed orthogonal to u_N when $\sum_{n \in N} \beta_{n,x} = 0$. We claim that $\mathbb{C}[G]$ is a direct sum of its subspaces U and W.

Proposition 1. *The group algebra $\mathbb{C}[G]$ has a direct sum decomposition $\mathbb{C}[G] = U + W$.*

We now prove the main result of this section. For a vector v, $\|v\|$ will denote its standard ℓ_2-norm.

Lemma 1. *Let G be any finite group and N be a normal subgroup of G and $\lambda < 1/2$ be any constant. Suppose A is an expanding generator set for N so that $\mathrm{Cay}(N, A)$ is a λ-spectral expander. Furthermore, suppose $B \subseteq G$ such that $\widehat{B} = \{Nx \mid x \in B\}$ is an expanding generator for the quotient group G/N and $\mathrm{Cay}(G/N, \widehat{B})$ is also a λ-spectral expander. Then $A \cup B$ is an expanding generator set for G such that $\mathrm{Cay}(G, A \cup B)$ is a $\frac{(1+\lambda)(\max\{|A|,|B|\})}{|A|+|B|}$-spectral expander.* [3]

Proof. We give the proof for the case when $|A| = |B|$ (the general case is identical). Let $v \in \mathbb{C}[G]$ be any vector such that $v \perp \mathbf{1}$ and M denote the normalized adjacency matrix of the Cayley graph $\mathrm{Cay}(G, A \cup B)$. Our goal is to show that $\|Mv\| \leq (1 + \lambda)\|v\|/2$. Notice that the adjacency matrix M can be written as $(M_A + M_B)/2$ where $M_A = \sum_{a \in A} M_a/|A|$ and $M_B = \sum_{b \in B} M_b/|B|$.[4]

Claim 1. For any two vectors $u \in U$ and $w \in W$, we have $M_A u \in U$, $M_A w \in W$, $M_B u \in U$, $M_B w \in W$, i.e. U and W are invariant under the transformations M_A and M_B.

Proof. Consider vectors of the form $u = xu_N \in U$ and $w = x \sum_{n \in N} \beta_{n,x} n \in W$, where $x \in X$ is arbitrary. By linearity, it suffices to prove for each $a \in A$

[3] Since A and B are multisets, we can ensure $|A|$ and $|B|$ are within a factor of 2 of each other by scaling up the smaller multiset. We can even ensure that A and B are of the same cardinality which is a power of 2.

[4] In the case when $|A| \neq |B|$, the adjacency matrix M will be $\frac{|A|}{|A|+|B|} M_A + \frac{|B|}{|A|+|B|} M_B$.

and $b \in B$ that $M_a u \in U$, $M_b u \in U$, $M_a w \in W$, and $M_b w \in W$. Notice that $M_a u = x u_N a = x u_N = u$ since $u_N a = u_N$. Furthermore, we can write $M_a w = x \sum_{n \in N} \beta_{n,x} na = x \sum_{n' \in N} \gamma_{n',x} n'$, where $\gamma_{n',x} = \beta_{n,x}$ and $n' = na$. Since $\sum_{n' \in N} \gamma_{n',x} = \sum_{n \in N} \beta_{n,x} = 0$ it follows that $M_a w \in W$. Now, consider $M_b u = ub$. For $x \in X$ and $b \in B$ the element xb can be *uniquely* written as $x_b n_{x,b}$, where $x_b \in X$ and $n_{x,b} \in N$. Hence, $M_b u = x u_N b = xb(b^{-1} u_N b) = x_b n_{x,b} \sigma_b(u_N) = x_b n_{x,b} u_N = x_b u_N \in U$. Finally, $M_b w = x(\sum_{n \in N} \beta_{n,x} n)b = xb(\sum_{n \in N} \beta_{n,x} b^{-1} nb) = x_b n_{x,b} \sum_{n \in N} \beta_{bnb^{-1},x} n = x_b \sum_{n \in N} \gamma_{n,x} n \in W$. Here, we note that $\gamma_{n,x} = \beta_{n',x}$ and $n' = b(n_{x,b}^{-1} n)b^{-1}$. Hence $\sum_{n \in N} \gamma_{n,x} = 0$, which puts $M_b w$ in the subspace W as claimed. □

Claim 2. Let $u \in U$ such that $u \perp \mathbf{1}$ and $w \in W$. Then $\|M_A u\| \leq \|u\|$, $\|M_B w\| \leq \|w\|$, $\|M_B u\| \leq \lambda \|u\|$, and $\|M_A w\| \leq \lambda \|w\|$.

Proof. The first two inequalities follow from the fact that M_A and M_B are the normalized adjacency matrices of the Cayley graphs $\mathrm{Cay}(G, A)$ and $\mathrm{Cay}(G, B)$ respectively.

Now we prove the third inequality. Let $u = (\sum_x \alpha_x x) u_N$ be any vector in U such that $u \perp \mathbf{1}$. Then $\sum_{x \in X} \alpha_x = 0$. Now consider the vector $\widehat{u} = \sum_{x \in X} \alpha_x Nx$ in the group algebra $\mathbb{C}[G/N]$. Notice that $\widehat{u} \perp \mathbf{1}$. Let $M_{\widehat{B}}$ denote the normalized adjacency matrix of $\mathrm{Cay}(G/N, \widehat{B})$. Since it is a λ-spectral expander it follows that $\|M_{\widehat{B}} \widehat{u}\| \leq \lambda \|\widehat{u}\|$. Writing out $M_{\widehat{B}} \widehat{u}$ we get $M_{\widehat{B}} \widehat{u} = \frac{1}{|B|} \sum_{b \in B} \sum_{x \in X} \alpha_x Nxb = \frac{1}{|B|} \sum_{b \in B} \sum_{x \in X} \alpha_x Nx_b$, because $xb = x_b n_{x,b}$ and $Nxb = Nx_b$ (as N is a normal subgroup). Hence the norm of the vector $\frac{1}{|B|} \sum_{b \in B} \sum_{x \in X} \alpha_x Nx_b$ is bounded by $\lambda \|\widehat{u}\|$. Equivalently, the norm of the vector $\frac{1}{|B|} \sum_{b \in B} \sum_{x \in X} \alpha_x x_b$ is bounded by $\lambda \|\widehat{u}\|$. On the other hand, we have

$$M_B u = \frac{1}{|B|} \sum_b \left(\sum_x \alpha_x x \right) u_N b = \frac{1}{|B|} \sum_b \left(\sum_x \alpha_x xb \right) b^{-1} u_N b$$
$$= \frac{1}{|B|} \left(\sum_b \sum_x \alpha_x x_b n_{x,b} \right) u_N = \frac{1}{|B|} \left(\sum_b \sum_x \alpha_x x_b \right) u_N.$$

For any vector $(\sum_{x \in X} \gamma_x x) u_N \in U$ it is easy to see that its norm can be written as $\| \sum_{x \in X} \gamma_x x \| \|u_N\|$. Since $\|1/|B| \sum_b \sum_x \alpha_x x_b\| \leq \lambda \| \sum_{x \in X} \alpha_x x\|$, we have $\|M_B u\| \leq \lambda \|u\|$.

We now show the fourth inequality. For each $x \in X$ it is useful to consider the following subspaces of $\mathbb{C}[G]$: $\mathbb{C}[xN] = \{x \sum_{n \in N} \theta_n n \mid \theta_n \in \mathbb{C}\}$. For any distinct $x \neq x' \in X$, since $xN \cap x'N = \emptyset$, vectors in $\mathbb{C}[xN]$ have support disjoint from vectors in $\mathbb{C}[x'N]$. Hence $\mathbb{C}[xN] \perp \mathbb{C}[x'N]$ which implies that the subspaces $\mathbb{C}[xN], x \in X$ are pairwise mutually orthogonal. Furthermore, the matrix M_A maps $\mathbb{C}[xN]$ to $\mathbb{C}[xN]$ for each $x \in X$.

Now, consider any vector $w = \sum_{x \in X} x \left(\sum_n \beta_{n,x} n \right)$ in W. Letting $w_x = x \left(\sum_{n \in N} \beta_{n,x} n \right) \in \mathbb{C}[xN]$ for each $x \in X$ we note that $M_A w_x \in \mathbb{C}[xN]$ for each $x \in X$. Hence, by Pythogoras theorem we have $\|w\|^2 = \sum_{x \in X} \|w_x\|^2$ and

$\|M_A w\|^2 = \sum_{x\in X} \|M_A w_x\|^2$. Since $M_A w_x = x M_A \left(\sum_{n\in N} \beta_{n,x} n\right)$, it follows that $\|M_A w_x\| = \|M_A \left(\sum_{n\in N} \beta_{n,x} n\right)\| \leq \lambda \| \sum_{n\in N} \beta_{n,x} n\| = \lambda \|w_x\|$. Putting it together, it follows that $\|M_A w\|^2 \leq \lambda^2 \left(\sum_{x\in X} \|w_x\|^2\right) = \lambda^2 \|w\|^2$. □

We now complete the proof of the lemma. Consider any vector $v \in \mathbb{C}[G]$ such that $v \perp \mathbf{1}$. Let $v = u + w$ where $u \in U$ and $w \in W$. Let $\langle , \rangle$ denote the inner product in $\mathbb{C}[G]$. Since $M = (M_A + M_B)/2$, we have $\|Mv\|^2 = \frac{1}{4}\langle M_A v, M_A v\rangle + \frac{1}{4}\langle M_B v, M_B v\rangle + \frac{1}{2}\langle M_A v, M_B v\rangle$. We consider each of the three summands in the above expression.

Firstly, since $v = u + w$, we can write $\langle M_A v, M_A v\rangle = \langle M_A u, M_A u\rangle + \langle M_A w, M_A w\rangle + 2\langle M_A u, M_A w\rangle$. By Claim 1 and the fact that $U \perp W$, we get $\langle M_A u, M_A w\rangle = 0$. Thus, $\langle M_A v, M_A v\rangle \leq \|u\|^2 + \lambda^2 \|w\|^2$. By an identical argument, Claim 1 and Claim 2 imply $\langle M_B v, M_B v\rangle \leq \lambda^2 \|u\|^2 + \|w\|^2$. Finally, $\langle M_A v, M_B v\rangle = \langle M_A u, M_B u\rangle + \langle M_A w, M_B w\rangle$. Now, using the Cauchy-Schwarz inequality and Claim 2, we get $\langle M_A v, M_B v\rangle \leq \lambda(\|u\|^2 + \|w\|^2)$. Combining all the inequalities, we get $\|Mv\|^2 \leq \frac{1}{4}\left(1 + 2\lambda + \lambda^2\right)\left(\|u\|^2 + \|w\|^2\right) = \frac{(1+\lambda)^2}{4}\|v\|^2$. Hence, it follows that $\|Mv\| \leq \frac{1+\lambda}{2}\|v\|$. □

The graph $\mathrm{Cay}(G, A \cup B)$ is $\frac{1+\lambda}{2}$-spectral. Using *derandomized squaring* [16], we can compute from $A \cup B$ an expanding generator set S for G of size $O(|A \cup B|)$, such that $\mathrm{Cay}(G, S)$ is λ-spectral. Details are given in the full version [6]. As a consequence, we obtain the following lemma which we will apply repeatedly. For ease of subsequent exposition, we fix $\lambda = 1/4$ in the following lemma.

Lemma 2. *Let G be a finite group and N be a normal subgroup of G such that $N = \langle A\rangle$ and $\mathrm{Cay}(N, A)$ is a 1/4-spectral expander. Further, let $B \subseteq G$ and $\widehat{B} = \{Nx \mid x \in B\}$ such that $G/N = \langle \widehat{B}\rangle$ and $\mathrm{Cay}(G/N, \widehat{B})$ is a 1/4-spectral expander. Then in time polynomial in $|A| + |B|$, we can construct an expanding generator set S for G, such that $|S| = O(|A| + |B|)$ and $\mathrm{Cay}(G, S)$ is a 1/4-spectral expander.*[5]

3 Normal Series and Solvable Permutation Groups

In section 2, we saw how to construct an expanding generator set for a group G from expanding generator sets for some normal subgroup N and the associated quotient group G/N. We apply it to the entire normal series for a *solvable* group G. More precisely, let $G \leq S_n$ such that $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = \{1\}$ is a *normal series* for G. That means G_i is a normal subgroup of G for each i, and hence G_i is also a normal subgroup of G_j for each $j < i$. Given expanding generator sets for each of the quotient groups G_i/G_{i+1}, we give an efficient construction of an expanding generator set for G.

[5] The lemma holds for any finite group G with the caveat that group operations in G are polynomial-time computable. However, we require the lemma only for quotient groups H/N where $H, N \leq S_n$, and group operations for such H/N are polynomial-time computable.

Lemma 3. *Let $G \leq S_n$ with normal series $\{G_i\}_{i=0}^r$ be as above. Further, for each i let B_i be a generator set for G_i/G_{i+1} such that $\mathrm{Cay}(G_i/G_{i+1}, B_i)$ is a $1/4$-spectral expander. Let $s = \max_i\{|B_i|\}$. Then in deterministic time polynomial in n and s we can compute a generator set B for G such that $\mathrm{Cay}(G, B)$ is a $1/4$-spectral expander and $|B| = c^{\log r}s$ for some constant $c > 0$.*

A detailed proof of this lemma is in the full version [6].

Now we apply the above lemma to solvable permutation groups. Let G be any finite solvable group. The *derived series* for G is the following chain of subgroups of G: $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_k = \{1\}$ where, for each i, G_{i+1} is the *commutator subgroup* of G_i. That is G_{i+1} is the normal subgroup of G_i generated by all elements of the form $xyx^{-1}y^{-1}$ for $x, y \in G_i$. It turns out that G_{i+1} is the minimal normal subgroup of G_i such that G_i/G_{i+1} is abelian. Furthermore, the derived series is also a *normal series*. It implies that G_i is a normal subgroup of G_j for each $j < i$.

Our algorithm will crucially exploit a property of the derived series of solvable groups $G \leq S_n$: By a theorem of Dixon [9], the length k of the derived series of a solvable subgroup of S_n is bounded by $5\log_3 n$. Thus, we get the following result as a direct application of Lemma 3:

Lemma 4. *Suppose $G \leq S_n$ is a solvable group with derived series $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_k = \{1\}$ such that for each i we have an expanding generator set B_i for the abelian quotient group G_i/G_{i+1} such that $\mathrm{Cay}(G_i/G_{i+1}, B_i)$ is a $1/4$-spectral expander. Let $s = \max_i\{|B_i|\}$. Then in deterministic time polynomial in n and s we can compute a generator set B for G such that $\mathrm{Cay}(G, B)$ is a $1/4$-spectral expander and $|B| = 2^{O(\log k)}s = (\log n)^{O(1)}s$.*

Given a solvable permutation group $G \leq S_n$ by a generator set the polynomial-time algorithm for computing an expanding generator set will proceed as follows: in deterministic polynomial time, we first compute generator sets for each subgroup $\{G_i\}_{1 \leq i \leq k}$ in the derived series for G [13]. In order to apply the above lemma it suffices to compute an expanding generator set B_i for G_i/G_{i+1} such that $\mathrm{Cay}(G_i/G_{i+1}, B_i)$ is $1/4$-spectral. We deal with this problem in the next section.

4 Abelian Quotient Groups

In Section 3, we have seen how to construct an expanding generator set for a solvable group G, from expanding generator sets for the quotient groups G_i/G_{i+1} in the normal series for G. We are now left with the problem of computing expanding generator sets for the abelian quotient groups G_i/G_{i+1}. We state a couple of easy lemmas that will allow us to further simplify the problem. For proofs of these lemmas, we refer the reader to an extended version of this paper [6].

Lemma 5. *Let H and N be subgroups of S_n such that N is a normal subgroup of H and H/N is abelian. Let $p_1 < p_2 < \ldots < p_k$ be the set of all primes bounded*

by n and $e = \lceil \log n \rceil$. Then, there is an onto homomorphism ϕ from the product group $\mathbb{Z}_{p_1^e}^n \times \mathbb{Z}_{p_2^e}^n \times \cdots \times \mathbb{Z}_{p_k^e}^n$ to the abelian quotient group H/N.

From the proof of Lemma 5, it is obvious that ϕ is computable in $\text{poly}(n)$ time. Suppose H_1 and H_2 are two finite groups such that $\phi : H_1 \to H_2$ is an onto homomorphism. In the next lemma we show that the ϕ-image of an expanding generator set for H_1, is an expanding generator set for H_2.

Lemma 6. *Suppose H_1 and H_2 are two finite groups such that $\phi : H_1 \to H_2$ is an onto homomorphism. Furthermore, suppose $\text{Cay}(H_1, S)$ is a λ-spectral expander. Then $\text{Cay}(H_2, \phi(S))$ is also a λ-spectral expander.*

Now, suppose $H, N \leq S_n$ are groups given by their generator sets, where $N \lhd H$ and H/N is abelian. By Lemmas 5 and 6, it suffices to describe a polynomial (in n) time algorithm for computing an expanding generator set of size $\widetilde{O}(n^2)$ for the product group $\mathbb{Z}_{p_1^e}^n \times \mathbb{Z}_{p_2^e}^n \times \cdots \times \mathbb{Z}_{p_k^e}^n$ such that the second largest eigenvalue of the corresponding Cayley graph is bounded by $1/4$. In the following section, we solve this problem.

4.1 Expanding generator set for the product group

In this section, we give a deterministic polynomial (in n) time construction of an $\widetilde{O}(n^2)$ size expanding generator set for the product group $\mathbb{Z}_{p_1^e}^n \times \ldots \times \mathbb{Z}_{p_k^e}^n$ such that the corresponding Cayley graph is a $1/4$-spectral expander.

Consider the following *normal series* for this product group given by the subgroups $K_i = \mathbb{Z}_{p_1^{e-i}}^n \times \ldots \times \mathbb{Z}_{p_k^{e-i}}^n$ for $0 \leq i \leq e$. Clearly, $K_0 \rhd K_1 \rhd \cdots \rhd K_e = \{1\}$. This is obviously a normal series since $K_0 = \mathbb{Z}_{p_1^e}^n \times \ldots \times \mathbb{Z}_{p_k^e}^n$ is abelian. Furthermore, $K_i/K_{i+1} = \mathbb{Z}_{p_1}^n \times \ldots \times \mathbb{Z}_{p_k}^n$. Since the length of this series is $e = \lceil \log n \rceil$ we can apply Lemma 3 to construct an expanding generator set of size $\widetilde{O}(n^2)$ for K_0 in polynomial time assuming that we can compute an expanding generator set of size $\widetilde{O}(n^2)$ for $\mathbb{Z}_{p_1}^n \times \ldots \times \mathbb{Z}_{p_k}^n$ in deterministic polynomial time. Thus, it suffices to efficiently compute an $\widetilde{O}(n^2)$-size expanding generator set for the product group $\mathbb{Z}_{p_1}^n \times \ldots \times \mathbb{Z}_{p_k}^n$.

In [1], Ajtai et al, using some number theory, gave a deterministic polynomial time expanding generator set construction for the cyclic group $\mathbb{Z}_t$, where t is given in *binary*.

Theorem 1 ([1]). *Let t be a positive integer given in binary as an input. Then there is a deterministic polynomial-time (i.e. in $\text{poly}(\log t)$ time) algorithm that computes an expanding generator set T for $\mathbb{Z}_t$ of size $O(\log^* t \log t)$, where $\log^* t$ is the least positive integer k such that a tower of k 2's bounds t from above. Furthermore, $\text{Cay}(\mathbb{Z}_t, T)$ is λ-spectral for any constant λ.*

Now, consider the group $\mathbb{Z}_{p_1 p_2 \ldots p_k}$. Since $p_1 p_2 \ldots p_k$ can be represented by $O(n \log n)$ bits in binary, we apply the above theorem (with $\lambda = 1/4$) to compute an expanding generator set of size $\widetilde{O}(n)$ for $\mathbb{Z}_{p_1 p_2 \ldots p_k}$ in $\text{poly}(n)$ time. Let $m =$

$O(\log n)$ be a positive integer to be fixed in the analysis later. Consider the product group $M_0 = \mathbb{Z}_{p_1}^m \times \mathbb{Z}_{p_2}^m \times \ldots \mathbb{Z}_{p_k}^m$ and for $1 \leq i \leq m$ let $M_i = \mathbb{Z}_{p_1}^{m-i} \times \mathbb{Z}_{p_2}^{m-i} \times \ldots \times \mathbb{Z}_{p_k}^{m-i}$. Clearly, the groups M_i form a *normal* series for M_0: $M_0 \rhd M_1 \rhd \cdots \rhd M_m = \{1\}$, and the quotient groups are $M_i/M_{i+1} = \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \ldots \times \mathbb{Z}_{p_k} = \mathbb{Z}_{p_1 p_2 \ldots p_k}$ (recall that p_i's are all distinct). Now we compute (in poly(n) time) an expanding generator set for $\mathbb{Z}_{p_1 p_2 \cdots p_k}$ of size $\widetilde{O}(n)$ using Theorem 1. Then, we apply Lemma 3 to the above normal series and compute an expanding generator set of size $\widetilde{O}(n)$ for the product group M_0 in polynomial time. The corresponding Cayley graph will be a 1/4-spectral expander. Now we are ready to describe the expanding generator set construction for $\mathbb{Z}_{p_1}^n \times \mathbb{Z}_{p_2}^n \times \ldots \times \mathbb{Z}_{p_k}^n$.

The final construction The construction is based on the technique developed in [3]. For $1 \leq i \leq k$ let m_i be the least positive integer such that $p_i^{m_i} > cn$ (where c is a suitably large constant). Thus, $p_i^{m_i} \leq cn^2$ for each i. For each i, $\mathbb{F}_{p_i^{m_i}}$ be the finite field of $p_i^{m_i}$ elements which can be deterministically constructed in polynomial time since it is polynomial sized. Let $m = \max\{m_i\}_{i=1}^k$ which is still of $O(\log n)$. Clearly, there is an onto homomorphism ψ from the group $\mathbb{Z}_{p_1}^m \times \mathbb{Z}_{p_2}^m \times \ldots \times \mathbb{Z}_{p_k}^m$ to the additive group of $\mathbb{F}_{p_1^{m_1}} \times \mathbb{F}_{p_2^{m_2}} \times \ldots \times \mathbb{F}_{p_k^{m_k}}$. Thus, if S is the expanding generator set of size $\widetilde{O}(n)$ constructed above for $\mathbb{Z}_{p_1}^m \times \mathbb{Z}_{p_2}^m \times \ldots \times \mathbb{Z}_{p_k}^m$, it follows from Lemma 6 that $\psi(S)$ is an expanding generator multiset of size $\widetilde{O}(n)$ for the additive group $\mathbb{F}_{p_1^{m_1}} \times \mathbb{F}_{p_2^{m_2}} \times \ldots \times \mathbb{F}_{p_k^{m_k}}$. Define $T \subset \mathbb{F}_{p_1^{m_1}} \times \mathbb{F}_{p_2^{m_2}} \times \ldots \times \mathbb{F}_{p_k^{m_k}}$ to be any (say, the lexicographically first) set of cn many k-tuples such that any two tuples $(x_1, x_2, \ldots, x_k)$ and $(x_1', x_2', \ldots, x_k')$ in T are distinct in all coordinates. Thus $x_j \neq x_j'$ for all $j \in [k]$. It is obvious that we can construct T by picking the first cn such tuples in lexicographic order.

We now define the expanding generator set R. Let $x = (x_1, x_2, \ldots, x_k) \in T$ and $y = (y_1, y_2, \ldots, y_k) \in \psi(S)$. Define $v_i = (\langle 1, y_i\rangle, \langle x_i, y_i\rangle, \ldots, \langle x_i^{n-1}, y_i\rangle)$ where $x_i^j \in \mathbb{F}_{p_i^{m_i}}$ and $\langle x_i^j, y_i\rangle$ is the dot product modulo p_i of the elements x_i^j and y_i seen as p_i-tuples in $\mathbb{Z}_{p_i}^{m_i}$. Hence, v_i is an n-tuple and $v_i \in \mathbb{Z}_{p_i}^n$. Now define $R = \{(v_1, v_2, \ldots, v_k) \mid x \in T, y \in \psi(S)\}$. Notice that $|R| = \widetilde{O}(n^2)$. Using ideas from [3] we can prove that R is an expanding generator set for $\mathbb{Z}_{p_1}^n \times \mathbb{Z}_{p_2}^n \times \ldots \times \mathbb{Z}_{p_k}^n$.

Claim. R is an expanding generator set for the product group $\mathbb{Z}_{p_1}^n \times \ldots \times \mathbb{Z}_{p_k}^n$.

Proof. Let $(\chi_1, \chi_2, \ldots, \chi_k)$ be a nontrivial character of the product group $\mathbb{Z}_{p_1}^n \times \mathbb{Z}_{p_2}^n \times \ldots \times \mathbb{Z}_{p_k}^n$, i.e. there is at least one j such that χ_j is nontrivial. Let ω_i be a primitive p_i^{th} root of unity. Recall that, since χ_i is a character there is a corresponding vector $\beta_i \in \mathbb{Z}_{p_i}^n$, i.e. $\chi_i : \mathbb{Z}_{p_i}^n \to \mathbb{C}$ and $\chi_i(u) = \omega_i^{\langle \beta_i, u\rangle}$ for $u \in \mathbb{Z}_{p_i}^n$ and the inner product in the exponent is a modulo p_i inner product. The character χ_i is nontrivial if and only if β_i is a nonzero element of $\mathbb{Z}_{p_i}^n$.

It is well-known that the characters $(\chi_1, \chi_2, \ldots, \chi_k)$ of the abelian group $\mathbb{Z}_{p_1}^n \times \mathbb{Z}_{p_2}^n \times \ldots \times \mathbb{Z}_{p_k}^n$ are also the eigenvectors for the adjacency matrix of the Cayley graph of the group with any generator set (see Proposition 11.7 of [10]). Thus, in order to prove that R is an expanding generator set for

$\mathbb{Z}_{p_1}^n \times \mathbb{Z}_{p_2}^n \times \ldots \times \mathbb{Z}_{p_k}^n$, it is enough to bound the following estimate for the nontrivial characters $(\chi_1, \chi_2, \ldots, \chi_k)$ since that directly bounds the second largest eigenvalue in absolute value.

$$\begin{aligned}\left|\mathbb{E}_{x\in T, y\in\psi(S)}[\chi_1(v_1)\chi_2(v_2)\ldots\chi_k(v)]\right| &= \left|\mathbb{E}_{x\in T, y\in\psi(S)}[\omega_1^{\langle\beta_1,v_1\rangle}\ldots\omega_k^{\langle\beta_k,v_k\rangle}]\right| \\ &= \left|\mathbb{E}_{x,y}[\omega_1^{\langle q_1(x_1),y_1\rangle}\ldots\omega_k^{\langle q_k(x_k),y_k\rangle}]\right| \\ &\leq \mathbb{E}_x\left|\mathbb{E}_y[\omega_1^{\langle q_1(x_1),y_1\rangle}\ldots\omega_k^{\langle q_k(x_k),y_k\rangle}]\right|,\end{aligned}$$

where $q_i(x) = \sum_{\ell=0}^{n-1}\beta_{i,\ell}x^\ell \in \mathbb{F}_{p_i}[x]$ for $\beta_i = (\beta_{i,0}, \beta_{i,1}, \ldots, \beta_{i,n-1})$. Since the character is nontrivial, suppose $\beta_j \neq 0$, then q_j is a nonzero polynomial of degree at most $n-1$. Hence the probability that $q_j(x_j) = 0$, when x is picked from T is bounded by $\frac{n}{cn}$. On the other hand, when $q_j(x_j) \neq 0$ the tuple $(q_1(x_1), \ldots, q_k(x_k))$ defines a nontrivial character of the group $\mathbb{Z}_{p_1}^m \times \ldots \times \mathbb{Z}_{p_k}^m$. Since S is an expanding generator set for the abelian group $\mathbb{Z}_{p_1}^m \times \ldots \times \mathbb{Z}_{p_k}^m$, the character defined by $(q_1(x_1), \ldots, q_k(x_k))$ is also an eigenvector for $\mathbb{Z}_{p_1}^m \times \ldots \times \mathbb{Z}_{p_k}^m$, in particular w.r.t. generator set S. Hence, $|\mathbb{E}_{y\in S}[\omega_1^{\langle q_1(x_1),y_1\rangle}\ldots\omega_k^{\langle q_k(x_k),y_k\rangle}]| \leq \varepsilon$, where the parameter ε can be fixed to an arbitrary small constant by Theorem 1. Hence the above estimate is bounded by $\frac{n}{cn} + \varepsilon = \frac{1}{c} + \varepsilon$ which can be made $\leq 1/4$ by choosing c and ϵ suitably. □

To summarize, Claim 4.1 along with Lemmas 5 and 6 directly yields the following theorem.

Theorem 2. *In deterministic polynomial (in n) time we can construct an expanding generator set of size $\widetilde{O}(n^2)$ for the product group $\mathbb{Z}_{p_1}^n \times \cdots \times \mathbb{Z}_{p_k}^n$ (where for each i, p_i is a prime number $\leq n$) that makes it a $1/4$-spectral expander. Consequently, if H and N are subgroups of S_n given by generator sets and H/N is abelian then in deterministic polynomial time we can compute an expanding generator set of size $\widetilde{O}(n^2)$ for H/N that makes it a $1/4$-spectral expander.*

Finally, we state the main theorem which follows directly from the above theorem and Lemma 4.

Theorem 3. *Let $G \leq S_n$ be a solvable permutation group given by a generating set. Then in deterministic polynomial time we can compute an expanding generator set S of size $\widetilde{O}(n^2)$ such that the Cayley graph $\mathrm{Cay}(G, S)$ is a $1/4$-spectral expander.*

On a related note, in the case of general permutation groups we have the following theorem about computing expanding generator sets. The proof, omitted here, can be found in the full version [6].

Theorem 4. *Given $G \leq S_n$ by a generator set S' and $\lambda > 0$, we can deterministically compute (in time $\mathrm{poly}(n, |S'|)$) an expanding generator set T for G such that $\mathrm{Cay}(G, T)$ is a λ-spectral expander and $|T| = O(n^{16q+10}\left(\frac{1}{\lambda}\right)^{32q})$ (where q is a large constant).*

5 Small Bias Spaces for $\mathbb{Z}_d^n$

We note that the expanding generator set construction for abelian groups in the previous section also gives a new construction of ε-bias spaces for $\mathbb{Z}_d^n$, which we now describe.

In [7] Azar, Motwani, and Naor first considered the construction of ε-bias spaces for abelian groups, specifically for the group $\mathbb{Z}_d^n$. For arbitrary d and any $\varepsilon > 0$ they construct ε-bias spaces of size $O((d + n^2/\varepsilon^2)^C)$, where C is the constant in Linnik's Theorem. The construction involves finding a suitable prime (or prime power) promised by Linnik's theorem which can take time up to $O((d+n^2)^C)$. The current best known bound for C is $\leq 11/2$ (and assuming ERH it is 2). Their construction yields a polynomial-size ε-bias space for $d = n^{O(1)}$.

It is interesting to compare this result of [7] with our results. Let d be any positive integer with prime factorization $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. So each p_i is $O(\log d)$ bit sized and each e_i is bounded by $O(\log d)$. Given d as input in unary, we can efficiently find the prime factorization of d. Using the result of Wigderson and Xiao [17], we compute an $O(\log d)$ size expanding generator set for $\mathbb{Z}_{p_1 p_2 \ldots p_k}$ in deterministic time polynomial in d. Then we construct an expanding generator set of size $O(\text{poly}(\log n) \log d)$ for $\mathbb{Z}_{p_1}^m \times \ldots \times \mathbb{Z}_{p_k}^m$ for $m = O(\log n)$ using the method described in Section 4.1. It then follows from Section 4.1 that we can construct an $O(n \,\text{poly}(\log n) \log d)$ size expanding generator set for $\mathbb{Z}_{p_1}^n \times \ldots \times \mathbb{Z}_{p_k}^n$ in deterministic polynomial time. Finally, from Section 4.1, it follows that we can construct an $O(n \,\text{poly}(\log n, \log d))$ size expanding generator set for $\mathbb{Z}_d^n$ (which is isomorphic to $\mathbb{Z}_{p_1^{e_1}}^n \times \ldots \mathbb{Z}_{p_k^{e_k}}^n$) since each e_i is bounded by $\log d$. Now for any arbitrary $\varepsilon > 0$, the explicit dependence of ε in the size of the generator set is $(1/\epsilon)^{32q}$. We summarize the discussion in the following theorem.

Theorem 5. *Let d, n be any positive integers (in unary) and $\varepsilon > 0$. Then, in deterministic $\text{poly}(n, d, \frac{1}{\varepsilon})$ time, we can construct an $O(n \,\text{poly}(\log n, \log d))(1/\varepsilon)^{32q}$ size ε-bias space for $\mathbb{Z}_d^n$.*

6 Final Remarks

The Alon-Roichman theorem guarantees the existence of $O(n \log n)$ size expanding generator sets for permutation groups $G \leq S_n$. In this paper, we construct $\widetilde{O}(n^2)$ size expanding generator sets for solvable groups. But for non-solvable permutation groups our construction is far from optimal. On the other hand, our construction of ε-bias space for $\mathbb{Z}_d^n$ is very different from the construction of [7] and improves upon it in terms of d and n, although it is worse in terms of the parameter ε. Finding efficient constructions that improve these bounds is an interesting open problem.

Acknowledgements. We are grateful to the anonymous referees for their valuable comments. We thank Shachar Lovett for pointing out the result of Ajtai et al [1]. We also thank Avi Wigderson for his comments and suggestions.

References

1. Miklós Ajtai, Henryk Iwaniec, János Komlós, János Pintz, and Endre Szemerédi. Construction of a thin set with small Fourier coeffciients. *Bull. London Math. Soc.*, 22:583–590, 1990.
2. Noga Alon, Jehoshua Bruck, Joseph Naor, Moni Naor, and Ron M. Roth. Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs. *IEEE Transactions on Information Theory*, 38(2):509–, 1992.
3. Noga Alon, Oded Goldreich, Johan Håstad, and René Peralta. Simple construction of almost k-wise independent random variables. *Random Struct. Algorithms*, 3(3):289–304, 1992.
4. Noga Alon and Yuval Roichman. Random Cayley Graphs and Expanders. *Random Struct. Algorithms*, 5(2):271–285, 1994.
5. Vikraman Arvind, Partha Mukhopadhyay, and Prajakta Nimbhorkar. Erdös-Rényi Sequences and Deterministic construction of Expanding Cayley Graphs. *Electronic Colloquium on Computational Complexity (ECCC)*, 18:81, 2011.
6. Vikraman Arvind, Partha Mukhopadhyay, Prajakta Nimbhorkar, and Yadu Vasudev. Expanding generator sets for solvable permutation groups. *Electronic Colloquium on Computational Complexity (ECCC)*, 18:140, 2011.
7. Yossi Azar, Rajeev Motwani, and Joseph Naor. Approximating Probability Distributions Using Small Sample Spaces. *Combinatorica*, 18(2):151–171, 1998.
8. László Babai. Local expansion of vertex-transitive graphs and random generation in finite groups. In *STOC*, pages 164–174, 1991.
9. John D. Dixon. The solvable length of a solvable linear group. *Mathematische Zeitschrift*, 107:151–158, 1968. 10.1007/BF01111027.
10. Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *Bull. Amer. Math. Soc.*, 43:439–561, 2006.
11. A. Lubotzky and B. Weiss. Groups and expanders. *Expanding Graphs (e. J. Friedman), DIMACS Ser. Discrete Math. Theoret. Compt. Sci.*, 10pp:95–109, 1993.
12. Alexander Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.
13. Eugene M. Luks. Permutation groups and polynomial-time computation. *DIMACS series in Discrete Mathematics and Theoretical Computer Science*, 11:139–175, 1993.
14. Omer Reingold. Undirected connectivity in log-space. *J. ACM*, 55(4):17:1–17:24, 2008.
15. Omer Reingold, Salil P. Vadhan, and Avi Wigderson. Entropy waves, the zig-zag graph product, and new constant-degree expanders and extractors. In *FOCS*, pages 3–13, 2000.
16. Eyal Rozenman and Salil P. Vadhan. Derandomized squaring of graphs. In *APPROX-RANDOM*, volume 3624 of *Lecture Notes in Computer Science*, pages 436–447. Springer, 2005.
17. Avi Wigderson and David Xiao. Derandomizing the Ahlswede-Winter matrix-valued Chernoff bound using pessimistic estimators, and applications. *Theory of Computing*, 4(1):53–76, 2008.