Expanding Generator Sets for Solvable Permutation Groups

V. Arvind† Partha Mukhopadhyay* Prajakta Nimbhorkar *
Yadu Vasudev †

October 31, 2011

Abstract

Let \( G = \langle S \rangle \) be a solvable permutation group given as input by the generating set \( S \). I.e. \( G \) is a solvable subgroup of the symmetric group \( S_n \). We give a deterministic polynomial-time algorithm that computes an expanding generator set \( T \) of size \( \tilde{O}(n^2) \) such that the undirected Cayley graph \( \mathrm{Cay}(G,T) \) is a \( \lambda \)-spectral expander, where the \( \tilde{O} \) notation suppresses \( \log^{O(1)} n \) factors. In particular, this construction yields \( \varepsilon \)-bias spaces with improved size bounds for the groups \( \mathbb{Z}_d^n \) for any constant \( \varepsilon > 0 \).

1 Introduction

Let \( G \) be a finite group, and let \( S = \langle g_1, g_2, \ldots, g_k \rangle \) 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 generating set for \( G \), \( \mathrm{Cay}(G, S \cup S^{-1}) \) is a connected regular multigraph.

For a regular undirected graph \( X = (V, E) \) of degree \( D \) on \( n \) vertices, its normalized adjacency matrix \( A_X \) is a symmetric matrix with largest eigenvalue 1. For \( 0 < \lambda < 1 \), the graph \( X \) is an \( (n, D, \lambda) \)-spectral expander if the second largest eigenvalue of \( A_X \), in absolute value, is bounded by \( \lambda \).

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 [HLW06] is an excellent reference. A central problem is the explicit construction of expander graph families [HLW06, LPS88]. By explicit it is meant that the family of graphs has efficient deterministic constructions, where the notion of efficiency depends upon the application at hand, e.g. [Rei08]. Explicit constructions with the best known and

*Chennai Mathematical Institute, Siruseri, India. Emails: {partham,prajakta}@cmi.ac.in
†The Institute of Mathematical Sciences, Chennai, India. Emails: {arvind,yadu}@imsc.res.in
near optimal expansion and degree parameters (the so-called Ramanujan graphs) are Cayley expander families [LPS88].

Alon and Roichman, in [AR94], show that every finite group has a logarithmic size expanding generator set using the probabilistic method. For any finite group $G$ and $\lambda > 0$, they show that with high probability a random multiset $S$ of size $O(\log |G|)$ picked uniformly at random from $G$ is a $\lambda$-spectral expander. Algorithmically, if $G$ is given as input by its multiplication table there is a randomized *Las Vegas* algorithm for computing $S$: we pick the multiset $S$ of $O(\log |G|)$ many elements from $G$ and check in deterministic time $|G|^{O(1)}$ that $\text{Cay}(G, T)$ is a $\lambda$-spectral expander.

Wigderson and Xiao gave a derandomization of this algorithm in [WX08] (also see [AMN11] for an alternative proof of [WX08]). Given $\lambda > 0$ and a finite group $G$ by a multiplication table, they show that in deterministic time $|G|^{O(1)}$ a multiset $S$ of size $O(\log |G|)$ can be computed such that $\text{Cay}(G, T)$ is a $\lambda$-spectral expander.

This paper

Suppose the finite group $G$ is a subgroup of the symmetric group $S_n$ or the matrix group $\text{GL}_n(\mathbb{F}_p)$ and $G$ is given as input by a generating set $S$, and not explicitly by a multiplication table. The question we address is whether we can compute an $O(\log |G|)$ size expanding generator set for $G$ in deterministic polynomial time. Notice that if we can randomly (or nearly randomly) sample from the group $G$ in polynomial time, then the Alon Roichman theorem implies that an $O(\log |G|)$ size sample will be an expanding generator set with high probability (though we do not know how to certify this in polynomial time).

This problem can be seen as a generalization of the construction of small bias spaces in, say $\mathbb{F}_2^n$ [AGHP92]. It is easily proved (see e.g. [HLW06]), using some character theory of finite abelian groups, that $\varepsilon$-bias spaces are precisely expanding generator sets for $\mathbb{F}_2^n$ (and this holds for any finite abelian group). Interestingly, the best known explicit construction of $\varepsilon$-bias spaces is of size $O(n^2/\varepsilon)$, whereas the Alon-Roichman theorem guarantees the existence of $\varepsilon$-bias spaces of size $O(n)$.

Subsequently, Azar, Motwani and Naor [AMN98] gave a construction of $\varepsilon$-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 $\varepsilon$-bias space they give is $O((d + n^2)^C)$ where the constant $C$ comes from Linnik’s theorem and the current best known bound for $C$ is 11/2.

In this paper we prove a more general result. Given any solvable subgroup $G$ of $S_n$, where $G$ is given by a generating set, we construct an expanding generator set $T$ for $G$ such that $\text{Cay}(G, T)$ is a $\lambda$-spectral expander for constant $\lambda$. Furthermore, $|T|$ is $\widetilde{O}(n^2)$ which is close to some of the best known $\varepsilon$-bias space construction for $\mathbb{F}_2^n$ [AGHP92, ABN+92].

An interesting question is whether we can find smaller expanding generator sets for a solvable group $G \leq S_n$. For an upper bound, by the Alon-Roichman theorem we know that there exist expanding generator sets for any $G$ of size $O(\log |G|)$ which is bounded by $O(n \log n) = \widetilde{O}(n)$. In general, given $G$ an algorithmic question is to ask for a minimum size expanding generator set for $G$ that makes the Cayley graph $\lambda$-spectral.
In this connection, it is interesting to note the following negative result that Lubotzky and Weiss in [LW93] have shown about solvable groups as expanders: Let \( \{ G_i \} \) be any infinite family of finite solvable groups \( \{ G_i \} \) such that each \( G_i \) has derived series of length bounded by some constant \( \ell \). Further, suppose that \( \Sigma_i \) is an arbitrary generating set for \( G_i \) such that its size \( |\Sigma_i| \leq k \) for each \( i \) and some constant \( k \). Then the Cayley graphs \( \text{Cay}(G_i, \Sigma_i) \) do not form a family of expanders. In contrast, they also exhibit an infinite family of solvable groups in [LW93] that give rise to constant-degree Cayley expanders.

Coming back to our present paper, the main ingredients of our construction are the following:

- 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 \( \lambda \)-spectral expanders, we give a simple polynomial-time algorithm to construct an expanding generator set \( S \) for \( G \) such that \( \text{Cay}(G, S) \) is also \( \lambda \)-spectral. Moreover, \( |S| \) is bounded by a constant factor of \( |S_1| + |S_2| \).

- We compute the derived series for the given solvable group \( G \) in polynomial time using a standard algorithm [Luk93]. This series is of \( O(\log n) \) length due to Dixon’s theorem. Let the derived series for \( G \) be

\[
G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_k = \{1\}.
\]

Assuming that we already have an expanding generator set for each quotient group \( G_i/G_{i+1} \) (which is abelian) of size \( \tilde{O}(n^2) \), we apply the previous step repeatedly to obtain an expanding generator set for \( G \) of size \( \tilde{O}(n^2) \). We can do this because the derived series is a normal series.

- Finally, we consider the abelian quotient groups \( G_i/G_{i+1} \) and give a polynomial time algorithm to construct an expanding generator set for it of size \( \tilde{O}(n^2) \). 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 \( \mathbb{Z}_t \) [AIK+90]. In particular, we note that our construction improves the Azar-Motwani-Naor construction of \( \varepsilon \)-bias spaces for \( \mathbb{Z}_d^n \) for any constant \( \varepsilon > 0 \) [AMN98].

We present the above three steps of the construction in the next three sections.

2 Combining Expanders for \( N \) and \( G/N \)

Let \( G \) be any finite group and \( N \) be a normal subgroup of \( G \) (i.e. \( g^{-1}Ng = N \) for all \( g \in G \)). We denote this by \( G \triangleright N \triangleright \{1\} \). Let \( A \subset N \) be an expanding generator set for \( N \) and \( \text{Cay}(N, A) \) be a \( \lambda \)-spectral expander. Similarly, suppose \( B \subset G \) such that \( \hat{B} = \{Nx \mid x \in B\} \) is an expanding generator set for the quotient group \( G/N \) and \( \text{Cay}(G/N, \hat{B}) \) is also a \( \lambda \)-spectral expander. Let \( X = \{x_1, x_2, \ldots, x_k\} \) denote a set of distinct coset representatives for
the normal subgroup $N$ in $G$. In this section we show that $A \cup B$ is an expanding generator set for $G$. More precisely, we will show that $\text{Cay}(G, A \cup B)$ is a $\frac{1+\lambda}{2}$-spectral expander.

In order to analyze the spectral expansion of the Cayley graph $\text{Cay}(G, A \cup B)$ 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 and let $M_S$ denote the normalized adjacency matrix of the undirected Cayley graph $\text{Cay}(G, S)$. Now, each element $a \in G$ defines the linear map $M_a : \mathbb{C}[G] \rightarrow \mathbb{C}[G]$ 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 $M_S(\sum_g \alpha_g g) = \frac{1}{|S|} \sum_{a \in S} \sum_g \alpha_g ga$.

In order to analyze the spectral expansion of $\text{Cay}(G, A \cup B)$ 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 $\sigma_b : \mathbb{C}[G] \rightarrow \mathbb{C}[G]$ defined by conjugation: $\sigma_b(\sum_g \alpha_g g) = \sum_g \alpha_g b^{-1}gb$. Since $N < G$ the linear map $\sigma_b$ 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:

$$U = \left\{ \left( \sum_{x \in X} \alpha_x x \right) u_N \right\}$$

$$W = \left\{ \sum_{x \in X} x \left( \sum_{n \in N} \beta_{n,x} n \right) \mid \sum_n \beta_{n,x} = 0, \forall x \in X \right\}$$

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 $W$, 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 2.1.** The group algebra $\mathbb{C}[G]$ has a direct sum decomposition $\mathbb{C}[G] = U + W$.

**Proof.** Since $U \perp W$, it suffices to check that $\dim(U) + \dim(W) = |G|$. The set $\{xu_N \mid x \in X\}$ forms an orthogonal basis for $U$ since for any $x \neq y \in X$, $xu_N$ is orthogonal to $yu_N$. The cardinality of this basis is $|X|$.

Let $z_1, \ldots, z_{|N|-1}$ be the $|N|-1$ vectors orthogonal to the uniform distribution $u_N$ in the eigenbasis for the Cayley graph $\text{Cay}(N, A)$. It is easy to see that the set $\{xz_j \mid x \in X, 1 \leq j \leq |N|-1\}$ of size $|X|(|N|-1)$ forms a basis for $W$.

\[\square\]
We will now prove the main result of this section.

**Lemma 2.2.** 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 $\text{Cay}(N, A)$ is a $\lambda$-spectral expander. Furthermore, suppose $B \subseteq G$ such that $\hat{B} = \{Nx \mid x \in B\}$ is an expanding generator for the quotient group $G/N$ and $\text{Cay}(G/N, \hat{B})$ is also a $\lambda$-spectral expander. Then $A \cup B$ is an expanding generator set for $G$ such that $\text{Cay}(G, A \cup B)$ is a $\frac{1+\lambda}{2}$-spectral expander. In particular, if $|A| = |B|$ then $\text{Cay}(G, A \cup B)$ is a $\frac{1+\lambda}{2}$-spectral expander.$^1$

**Proof.** We will give the proof only for the case when $|A| = |B|$ (the general case is identical).

Let $v \in \mathbb{C}[G]$ be any vector such that $v \perp 1$ and $M$ denote the adjacency matrix of the Cayley graph $\text{Cay}(G, A \cup B)$. Our goal is to show that $\|Mv\| \leq \frac{1+\lambda}{2}\|v\|$. Notice that the adjacency matrix $M$ can be written as $\frac{1}{|A|} \sum_{a \in A} M_a$ and $M_B = \frac{1}{|B|} \sum_{b \in B} M_b$.$^2$

**Claim.** For any two vectors $u \in U$ and $w \in W$, we have $M_Au \in U$, $M_Aw \in W$, $M_Bu \in U$, $M_Bw \in W$, 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 $w = x \sum_{n \in N} \beta_{n,x} n$, where $x \in X$ is arbitrary. By linearity, it suffices to prove for each $a \in A$ 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 $M_a u = xu_Na = xu_N = u$ since $u_Na = u_N$. 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 $xb \sum_{n \in N} x,b \in N$, where $x,b \in X$ and $n_{x,b} \in N$.

\[
M_b u = xu_N b = xb(b^{-1}u_N b) = x_{b} n_{x,b} \sigma_{b}(u_N) = x_{b} n_{x,b} u_N = x_{b} u_N \in U.
\]

Finally,

\[
M_b w = x \left( \sum_{n \in N} \beta_{n,x} n \right) b = xb \left( \sum_{n \in N} \beta_{n,x} b^{-1}nb \right) = x_{b} n_{x,b} \sum_{n \in N} \beta_{n\beta_{b^{-1}},x} n = x_{b} \sum_{n \in N} \gamma_{n,x} n \in W.
\]

$^1$The sizes of $A$ and $B$ is not a serious issue for us. Since we consider multisets as expanding generator sets, notice that we always ensure $|A|$ and $|B|$ are within a factor of 2 of each other by scaling the smaller multiset appropriately. Indeed, in our construction we can even ensure when we apply this lemma that the multisets $A$ and $B$ are of the same cardinality which is a power of 2.

$^2$In the case when $|A| \neq |B|$, the adjacency matrix $M$ will be $\frac{|A|}{|A|+|B|} M_A + \frac{|B|}{|A|+|B|} M_B$. 

5
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 $M_bw$ in the subspace $W$ as claimed.

\[\square\]

**Claim.** Let $u \in U$ such that $u \perp 1$ and $w \in W$. Then:

1. $\|M_Au\| \leq \|u\|$.
2. $\|M_Bw\| \leq \|w\|$.
3. $\|M_Bu\| \leq \lambda \|u\|$.
4. $\|M_Aw\| \leq \lambda \|w\|$.

**Proof.** Since $M_A$ is the normalized adjacency matrix of the Cayley graph $\text{Cay}(G, A)$ and $M_B$ is the normalized adjacency matrix of the Cayley graph $\text{Cay}(G, B)$, it follows that for any vectors $u$ and $w$ we have the bounds $\|M_Au\| \leq \|u\|$ and $\|M_Bw\| \leq \|w\|$.

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

$$M_Bu = \frac{1}{|B|} \sum_b \left( \sum_x \alpha_x x \right) u_N b = \frac{1}{|B|} \sum_b \left( \sum_x \alpha_x x b \right) b^{-1} u_N b$$

$$= \frac{1}{|B|} \left( \sum_b \sum_x \alpha_x x b n_{x,b} \right) u_N = \frac{1}{|B|} \left( \sum_b \sum_x \alpha_x x b \right) u_N$$

For any vector $(\sum_{x \in X} \gamma_x x)u_N \in U$ it is easy to see that the norm $\|(\sum_{x \in X} \gamma_x x)u_N\| = \|\sum_{x \in X} \gamma_x x\| \|u_N\|$. Therefore,

$$\|M_Bu\| = \|\frac{1}{|B|} \sum_b \sum_x \alpha_x x b \| \|u_N\|$$

$$\leq \lambda \|\sum_{x \in X} \alpha_x x \| \|u_N\|$$

$$= \lambda \|u\|.$$

We now show the fourth part. 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 \( w = \sum_{x \in X} x (\sum_{n \in N} \beta_{n,x} n) \) in \( W \). Letting \( w_x = x (\sum_{n \in N} \beta_{n,x} n) \in \mathbb{C}[xN] \) 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 \( M_A w_x = x M_A (\sum_{n \in N} \beta_{n,x} n) \), it follows that \( \|M_A w_x\| = \|M_A (\sum_{n \in N} \beta_{n,x} n)\| \leq \lambda \|\sum_{n \in N} \beta_{n,x} n\| = \lambda \|w_x\| \).

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 \( v \perp 1 \). Let \( v = u + w \) where \( u \in U \) and \( w \in W \). Let \( \langle , \rangle \) denote the inner product in \( \mathbb{C}[G] \). Then we have

\[
\|Mv\|^2 = \frac{1}{4} \|(M_A + M_B)v\|^2
= \frac{1}{4} \langle (M_A + M_B)v, (M_A + M_B)v \rangle
= \frac{1}{4} \langle M_Av, M_Av \rangle + \frac{1}{4} \langle M_Bv, M_Bv \rangle + \frac{1}{2} \langle M_Av, M_Bv \rangle
\]

We consider each of the three summands in the above expression.

\[
\langle M_Av, M_Av \rangle = \langle M_A(u + w), M_A(u + w) \rangle
= \langle M_Au, M_Au \rangle + \langle M_Aw, M_Aw \rangle + 2 \langle M_Au, M_Aw \rangle.
\]

By Claim \(^2\) and the fact that \( U \perp W \), \( \langle M_Au, M_Aw \rangle = 0 \). Thus we get

\[
\langle M_Av, M_Av \rangle \leq \|u\|^2 + \lambda^2 \|w\|^2, \text{ from Claim } \(^2\)
\]

By an identical argument Claims \(^2\) and \(^2\) imply \( \langle M_Bv, M_Bv \rangle \leq \lambda^2 \|u\|^2 + \|w\|^2 \). Finally

\[
\langle M_Av, M_Bv \rangle = \langle M_A(u + w), M_B(u + w) \rangle
= \langle M_Au, M_Bu \rangle + \langle M_Aw, M_Bw \rangle + \langle M_Au, M_Bw \rangle + \langle M_Aw, M_Bu \rangle
= \langle M_Au, M_Bu \rangle + \langle M_Aw, M_Bw \rangle
\leq \|M_Au\| \|M_Bu\| + \|M_Aw\| \|M_Bw\| \text{ (by Cauchy-Schwarz inequality)}
\leq \lambda \|u\|^2 + \lambda \|w\|^2, \text{ which follows from Claim } \(^2\)
\]

Combining all the inequalities, we get

\[
\|Mv\|^2 \leq \frac{1}{4} \left( 1 + 2\lambda + \lambda^2 \right) (\|u\|^2 + \|w\|^2) = \frac{(1 + \lambda)^2}{4} \|v\|^2.
\]

Hence, it follows that \( \|Mv\| \leq \frac{1 + \lambda}{2} \|v\| \).

\( \square \)
2.1 A Derandomized Squaring Step

Notice that $\text{Cay}(G,A \cup B)$ is only a $\frac{1+\lambda}{2}$-spectral expander. We can compute another expanding generator set $S$ for $G$ from $A \cup B$, using derandomized squaring \cite{RV05}, such that $\text{Cay}(G,S)$ is a $\lambda$-spectral expander. We recall a result in \cite{RV05} Observation 4.3,Theorem 4.4] about derandomized squaring applied to Cayley graphs which we recall in some detail.

Theorem 2.3 (\cite{RV05}). Let $G$ be a finite group and $U$ be an expanding generator set such that $\text{Cay}(G,U)$ is a $\lambda'$-spectral expander and $H$ be a consistently labeled $d$-regular graph with vertex set $\{1,2,\ldots,|U|\}$ for a constant $d$ such that $H$ is a $\mu$-spectral expander. Then $\text{Cay}(G,U) \circlearrowleft H$ is a directed Cayley graph for the same group $G$ and with generator set $S = \{u_iu_j \mid (i,j) \in E(H)\}$. Furthermore, if $A$ is the normalized adjacency matrix for $\text{Cay}(G,U) \circlearrowleft H$ then for any vector $v \in \mathbb{C}^{|G|}$ such that $v \perp 1$:

$$\|Av\| \leq (\lambda'^2 + \mu)\|v\|.$$ 

Observe that in the definition of the directed Cayley graph $\text{Cay}(G,U) \circlearrowleft H$ (in the statement above) there is an identification of the vertex set $\{1,2,\ldots,|U|\}$ of $H$ with the generator multiset $U$ indexed as $U = \{u_1,u_2,\ldots,u_{|U|}\}$.

Alternatively, we can also identify the vertex set $\{1,2,\ldots,|U|\}$ of $H$ with the generator multiset $U$ indexed as $U = \{u_1^{-1},u_2^{-1},\ldots,u_{|U|}^{-1}\}$, since $U$ is closed under inverses and, as a multiset, we assume for each $u \in U$ both $u$ and $u^{-1}$ occur with same multiplicity. Let us denote this directed Cayley graph by $\text{Cay}(G,U^{-1}) \circlearrowleft H$. Clearly, by the above result of \cite{RV05} the graph $\text{Cay}(G,U^{-1}) \circlearrowleft H$ also has the same expansion property. I.e. if $A'$ denotes its normalized adjacency matrix for $\text{Cay}(G,U^{-1}) \circlearrowleft H$ then for any vector $v \in \mathbb{C}^{|G|}$ such that $v \perp 1$:

$$\|A'v\| \leq (\lambda'^2 + \mu)\|v\|.$$ 

We summarize the above discussion in the following lemma.

Lemma 2.4. Let $G$ be a finite group and $U$ be a generator multiset for $G$ such that for each $u \in U$ both $u$ and $u^{-1}$ occur with the same multiplicity (i.e. $U$ is symmetric and preserves multiplicities). Suppose $\text{Cay}(G,U)$ is a $\lambda'$-spectral expander. Let $H$ be a consistently labeled $d$-regular graph with vertex set $\{1,2,\ldots,|U|\}$ for a constant $d$ such that $H$ is a $\mu$-spectral expander. Then $\text{Cay}(G,S)$ is an undirected Cayley graph for the same group $G$ and with generator set $S = \{u_iu_j \mid (i,j) \in E(H)\} \cup \{u_i^{-1}u_j^{-1} \mid (i,j) \in E(H)\}$. Furthermore, $\text{Cay}(G,S)$ is a $(\lambda'^2 + \mu)$-spectral expander of degree $2d|U|$.

We can, for instance, use the graphs given by the following lemma for $H$ in the above construction.

Lemma 2.5 (\cite{RV05}). For some constant $Q = 4^q$, there exists a sequence of consistently labelled $Q$-regular graphs on $Q^m$ vertices whose second largest eigenvalue is bounded by 1/100 such that given a vertex $v \in [Q^m]$ and an edge label $x \in [Q]$, we can compute the $x^{th}$ neighbor of $v$ in time polynomial in $m$. 

8
Suppose Cay\((G, U)\) is a 3/4-spectral expander and we take \(H\) given by the above lemma for derandomized squaring, then it is easy to see that with a constant number of squaring operations we will obtain a generator set \(S\) for \(G\) such that \(|S| = O(|U|)\) and Cay\((G, S)\) is a 1/4-spectral expander. Putting this together with Lemma 2.2 we obtain the following consequence which we will use repeatedly in the rest of the paper.

Lemma 2.6. Let \(G\) be a finite group and \(N\) be a normal subgroup of \(G\) such that \(N = \langle A \rangle\) and Cay\((N, A)\) is a 1/4-spectral expander. Further, let \(B \subseteq G\) and \(\hat{B} = \{Nx \mid x \in B\}\) such that \(G/N = \langle \hat{B} \rangle\) and Cay\((G/N, \hat{B})\) 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 Cay\((G, S)\) is a 1/4-spectral expander.

3 Normal Series and Solvable Permutation Groups

Let \(G \leq S_n\) such that
\[
G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = \{1\}
\]
is a normal series for \(G\). I.e. \(G_i\) is a normal subgroup of \(G\) for each \(i\) and hence \(G_i\) is a normal subgroup of \(G_j\) for each \(j < i\).

Lemma 3.1. Let \(G \leq S_n\) with normal series \(\{G_i\}_{i=0}^r\) as above. Further, for each \(i\) let \(B_i\) be a generator set for \(G_i/G_{i+1}\) such that Cay\((G_i/G_{i+1}, B_i)\) is a 1/4-spectral expander. Let \(s = r \cdot \max\{|B_i|\}\). Then in deterministic time polynomial in \(n\) and \(s\) we can compute a generating set \(B\) for \(G\) such that Cay\((G, B)\) is a 1/4-spectral expander and \(|B| = c \log r s\) for some constant \(c > 0\).

Proof. The proof is an easy application of Lemma 2.6. First suppose we have three indices \(k, \ell, m\) such that \(G_k \triangleright G_\ell \triangleright G_m\) and Cay\((G_k/G_\ell, S)\) and Cay\((G_\ell/G_m, T)\) both are 1/4-spectral expanders. Then notice that we have the groups \(G_k/G_m \triangleright G_\ell/G_m \triangleright \{1\}\) and the group \(G/K\) is isomorphic to \(G_k/G_m\) via a natural isomorphism. Hence Cay\((\hat{G}_k/G_m, \hat{S})\) is also a 1/4-spectral expander, where \(\hat{S}\) is the image of \(S\) under the said natural isomorphism. Therefore, we can apply Lemma 2.6 by setting \(G_k\) to \(G_k/G_m\) and \(N\) to \(G_\ell/G_m\) to get a generator set \(U\) for \(G_k/G_m\) such that Cay\((G_k/G_m, U)\) is 1/4-spectral and \(|U| \leq c(|S| + |T|)\).

To apply this inductively to the entire normal series, assume wlog its length \(r = 2^t\). Inductively assume that in the normal series \(G = G_0 \triangleright G_{2^t} \triangleright G_{2^t} \triangleright G_{2^t} \cdots \triangleright G_r = \{1\}\),

for each quotient group \(G_{2^t}/G_{(t+1)2^t}\) we have an expanding generator set of size \(c\)'s that makes \(G_{2^t}/G_{(t+1)2^t}\) 1/4-spectral. Now, consider the three groups \(G_{(2j)2^t} \triangleright G_{(2j+1)2^t} \triangleright G_{(2j+2)2^t}\)

\(^3\)Though the lemma holds for any finite group \(G\), the caveat is that the group operations in \(G\) should be polynomial-time computable. Since we focus on permutation groups in this paper we will require it only for quotient groups \(G = H/N\) where \(H\) and \(N\) are subgroups of \(S_n\).
and setting \( k = 2j2^i \), \( \ell = (2j + 1)2^i \) and \( m = (2j + 2)2^i \) in the above argument we get expanding generator sets for \( G_{2j2^i}/G_{(2j+2)2^i} \) of size \( c^{i+1}s \) that makes it 1/4-spectral. The lemma follows by induction.

### 3.1 Solvable permutation groups

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 \( G_i \). I.e. \( G_{i+1} \) 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. I.e. each \( G_i \) is in fact a normal subgroup of \( G \) itself. It also 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 \( G \leq S_n \). This is a theorem of Dixon \cite{Dix68} which states that the length \( k \) of the derived series of a solvable subgroup of \( S_n \) is bounded by \( 5\log_3 n \).

**Lemma 3.2.** 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 \( \text{Cay}(G_i/G_{i+1}, B_i) \) 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 generating set \( B \) for \( G \) such that \( \text{Cay}(G, B) \) is a 1/4-spectral expander and \( |B| = 2^{O(\log k)}s = (\log n)^{O(1)}s \).

**Proof.** Follows by a direct application of Lemma 3.1.

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 \cite{Luk93} generator sets for each subgroup \( \{G_i\}_{1 \leq i \leq k} \) in the derived series for \( G \). 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 \( \text{Cay}(G_i/G_{i+1}, B_i) \) is 1/4-spectral. We deal with this problem in the next section.

### 4 Abelian Quotient Groups

As explained above we are now left with the problem of computing expanding generator sets for the abelian quotient groups \( G_i/G_{i+1} \). We prove a couple of easy lemmas that will allow us to further simplify the problem.
Lemma 4.1. 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 $e = \lceil \log n \rceil$. There is an onto homomorphism $\phi$ from the product group $\mathbb{Z}_{p_1^n} \times \mathbb{Z}_{p_2^n} \times \cdots \times \mathbb{Z}_{p_k^n}$ onto the abelian quotient group $H/N$.

Proof. Since $H$ is a subgroup of $S_n$ it has a generator set of size at most $n - 1$. Let \{x_1, x_2, \ldots, x_n\} be a generator (multi)set for $H$. Each permutation $x_i$ can be written as a product of disjoint cycles and the order, $r_i$, of $x_i$ is the lcm of the lengths of these disjoint cycles. Thus we can write for each $i$

$$r_i = p_1^{e_{i1}} p_2^{e_{i2}} \cdots p_k^{e_{ik}},$$

where the key point to note is that $p_j^{e_{ij}} \leq n$ for each $i$ and $j$ because $r_i$ is the lcm of the disjoint cycles of permutation $x_i$. Clearly, $e_{ij} \leq \lceil \log n \rceil$.

Now, define the elements $y_{ij} = x_i^{r_i!/p_j^{e_{ij}}}$. Notice that the order, $o(y_{ij})$, of $y_{ij}$ is $p_j^{e_{ij}}$.

Let $(a_{11}, a_{n1}, \ldots, a_{1k}, \ldots, a_{nk})$ be an element of the product group $\mathbb{Z}_{p_1^n} \times \mathbb{Z}_{p_2^n} \times \cdots \times \mathbb{Z}_{p_k^n}$, where for each $i$ we have $(a_{i1}, \ldots, a_{in}) \in \mathbb{Z}_{p_i^n}$. Let $b_{ij} = p_j^{e_{ij}} a_{ij}$ for each $i$ and $j$. Now define the mapping $\phi$ as

$$\phi(a_{11}, \ldots, a_{n1}, \ldots, a_{1k}, \ldots, a_{nk}) = N(\prod_{j=1}^{k} \prod_{i=1}^{n} y_{ij}^{a_{ij}}).$$

Since $H/N$ is abelian, it is easy to see that $\phi$ is a homomorphism. To see that $\phi$ is onto, consider $N x_1^{f_1} \ldots x_t^{f_t} \in H/N$. Clearly, the cyclic subgroup generated by $x_i$ is the direct product of its $p_j$-Sylow subgroups generated by $y_{ij}$ for $1 \leq j \leq k$. Hence $x_i^{f_i} = y_{i1}^{a_{i1}} \cdots y_{ik}^{a_{ik}}$ for some $(a_{i1}, \ldots, a_{ik}) \in \mathbb{Z}_{p_{i1}^{e_{i1}}} \times \cdots \times \mathbb{Z}_{p_{ik}^{e_{ik}}}$. This vector $(a_{11}, \ldots, a_{nk})$ is a preimage of $N x_1^{f_1} \ldots x_t^{f_t}$, implying that $\phi$ is onto.

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 $\phi$-image of an expanding generator set for $H_1$, is an expanding generator set for $H_2$.

Lemma 4.2. 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 $\lambda$-spectral expander. Then $\text{Cay}(H_2, \phi(S))$ is also a $\lambda$-spectral expander.

Proof. Let $N = \text{Ker}(\phi)$ be the kernel of the onto homomorphism $\phi$. Then $H_1/N$ is isomorphic to $H_2$ and the lemma is equivalent to the claim that $\text{Cay}(H_1/N, \widehat{S})$ is a $\lambda$-spectral expander, where $\widehat{S} = \{Ns \mid s \in S\}$ is the corresponding generator set for $H_1/N$. We can check by a direct calculation that all eigenvalues of the normalized adjacency matrix of $\text{Cay}(H_1/N, \widehat{S})$ are also eigenvalues of $\text{Cay}(H_1, S)$. This claim also follows from well-known results in the “expanders monograph” [HLW06, Lemma 11.15, Proposition 11.17]. In order to apply these results we note that $H_1$ naturally defines a permutation action on the quotient
group $H_1/N$ by $h : Nx \mapsto Nhx$ for each $h \in H_1$ and $Nx \in H_1/N$. Then the Cayley graph $\text{Cay}(H_1/N, \hat{S})$ is just the Schreier graph for this action and the generator set $S$ of $H_1$ and, by [HLW06, Proposition 11.17], all eigenvalues of $\text{Cay}(H_1/N, \hat{S})$ are eigenvalues of $\text{Cay}(H_1, S)$ and the lemma follows.

Now, suppose $H, N \leq S_n$ are groups given by generator sets where $N < H$ and $H/N$ is abelian. By Lemmas 4.1 and 4.2, it suffices to describe a polynomial (in $n$) time algorithm for computing an expanding generator set of size $\tilde{O}(n^2)$ for the product group $\mathbb{Z}_{p_1^n} \times \mathbb{Z}_{p_2^n} \times \ldots \times \mathbb{Z}_{p_k^n}$. In the following section we solve this problem. Our solution improves the Azar-Motwani-Naor construction of $\varepsilon$-bias spaces for $\mathbb{Z}_d^n$ [AMN98] for constant $\varepsilon > 0$, that we describe in Section 5.

### 4.1 Improved small-bias spaces for abelian groups

In this section we give a deterministic polynomial (in $n$) time construction of an $\tilde{O}(n^2)$ size expanding generator set for the product group $\mathbb{Z}_{p_1^n} \times \mathbb{Z}_{p_2^n} \times \ldots \times \mathbb{Z}_{p_k^n}$.

Consider the following normal series for this product group given by the subgroups $\mathcal{K}_i = \mathbb{Z}_{p_1}^{m - i} \times \mathbb{Z}_{p_2}^{m - i} \times \ldots \times \mathbb{Z}_{p_k}^{m - i}$ for $0 \leq i \leq e$. Clearly,

$$\mathcal{K}_0 \supset \mathcal{K}_1 \supset \cdots \supset \mathcal{K}_e = \{\emptyset\}$$

This is obviously a normal series since $\mathcal{K}_0 = \mathbb{Z}_{p_1}^{m} \times \mathbb{Z}_{p_2}^{m} \times \ldots \times \mathbb{Z}_{p_k}^{m}$ is abelian. Furthermore, $\mathcal{K}_i/\mathcal{K}_{i+1} = \mathbb{Z}_{p_1}^{m - i} \times \mathbb{Z}_{p_2}^{m - i} \times \ldots \times \mathbb{Z}_{p_k}^{m - i}$.

Since the length of this series is $e = \lceil \log n \rceil$ we can apply Lemma 3.1 to construct an expanding generator set of size $\tilde{O}(n^2)$ for $\mathcal{K}_0$ in polynomial time assuming that we can compute an expanding generator set of size $\tilde{O}(n^2)$ for $\mathbb{Z}_{p_1}^{m} \times \mathbb{Z}_{p_2}^{m} \times \ldots \times \mathbb{Z}_{p_k}^{m}$ in deterministic polynomial time.

Thus, it suffices to efficiently compute an $\tilde{O}(n^2)$-size expanding generator set for the product group $\mathbb{Z}_{p_1}^{m} \times \mathbb{Z}_{p_2}^{m} \times \ldots \times \mathbb{Z}_{p_k}^{m}$.

In [AIK+90], 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 4.3.** 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 generating set $T$ for $\mathbb{Z}_t$ of size $O(\log^* t \log t)$, where $\log^* t$ is the least positive integer such that a tower of $k$ 2’s bounds $t$. Furthermore, $\text{Cay}(\mathbb{Z}_t, T)$ is $\lambda$-spectral for each constant $\lambda$.

Now, consider the group $\mathbb{Z}_{p_1 p_2 \cdots p_k}$. Since $p_1 p_2 \cdots p_k$ can be represented by $O(n \log n)$ bits in binary, we apply the above theorem to compute an expanding generating set of size $\tilde{O}(n)$ for $\mathbb{Z}_{p_1 p_2 \cdots p_k}$ in poly$(n)$ time. Let $m = O(\log n)$ be a positive integer to be fixed in the analysis later. Consider the product group $M_0 = \mathbb{Z}_{p_1}^m \times \mathbb{Z}_{p_2}^m \times \ldots \times \mathbb{Z}_{p_k}^m$ 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 $M_0$: $M_0 \supset M_1 \supset \cdots \supset M_m = \{\emptyset\}$. 

12
and the quotient groups are $M_i/M_{i+1} = \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \ldots \times \mathbb{Z}_{p_k} = \mathbb{Z}_{p_1 \cdot p_2 \cdot \ldots \cdot p_k}$. Since we can compute in $\text{poly}(n)$ time an expanding generating set for $\mathbb{Z}_{p_1 \cdot p_2 \cdot \ldots \cdot p_k}$ of size $\tilde{O}(n)$ by Theorem 4.3, we can again apply Lemma 3.1 to this normal series and, given $\lambda > 0$, compute in polynomial time an expanding generator set of size $\tilde{O}(n)$ for the product group $M_0$ such that the corresponding Cayley graph is $\lambda$-spectral.

Now we are ready to describe the expanding generator set construction for $\mathbb{Z}_{p_1}^n \times \mathbb{Z}_{p_2}^n \times \ldots \times \mathbb{Z}_{p_k}^n$.

4.1.1 The final construction

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. Clearly, there is an onto homomorphism $\psi$ 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 $\tilde{O}(n)$ constructed above for $\mathbb{Z}_{p_1}^m \times \mathbb{Z}_{p_2}^m \times \ldots \times \mathbb{Z}_{p_k}^m$ it follows that $\psi(S)$ is an expanding generator multiset of size $\tilde{O}(n)$ 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 for 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. I.e. $x_j \neq x_j'$ for all $j \in [k]$. It is obvious that we can construct $T$ by picking the first $cn$ such tuples in lexicographic order.

Now we will 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 $v_i = (y_i, \langle x_i, y_i \rangle, \langle x_i^2, y_i \rangle, \ldots, \langle x_i^{n-1}, y_i \rangle)$ where $x_i^j \in \mathbb{F}_{p_i^{m_i}}$ and $\langle x_i^j, y_i \rangle$ is the inner product modulo $p_i$ of the elements $x_i^j$ and $y_i$ seen as $p_i$-tuples in $\mathbb{Z}_{p_i}^{m_i} \cong \mathbb{F}_{p_i^{m_i}}$. 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 $|R| = \tilde{O}(n^2)$. We claim that $R$ is an expanding generator set for the product group $\mathbb{Z}_{p_1}^n \times \mathbb{Z}_{p_2}^n \times \ldots \times \mathbb{Z}_{p_k}^n$. 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 $\chi_j$ is nontrivial. Let $\omega_i$ be a primitive $p_i^{th}$ root of unity. Recall that, since $\chi_i$ 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 $\chi_i$ is nontrivial if and only if $\beta_i$ is a nonzero element of $\mathbb{Z}_{p_i}^n$.

Since 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 group (for any generator set for it). In particular, for the set $R$ as well the characters are the eigenvectors, and the nontrivial characters are orthogonal to 1. Thus, in order to prove that $R$ is an expanding generating 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 exponential sum estimate for the nontrivial characters $(\chi_1, \chi_2, \ldots, \chi_k)$ since that directly bounds the second largest eigenvalue in absolute value.
In fact when which can take time up to \(O\) construction involves finding a suitable prime (or prime power) promised by Linnik’s theorem \(\varepsilon\).

Abelian groups, specifically for the group \(\mathbb{Z}\) and \(\mathbb{Z}_S\), generator set \(\lambda \neq 0\) makes it spectral. 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 \(\tilde{O}(n^2)\) for \(H/N\) that makes it \(\lambda\) spectral.

Finally, we state the main theorem which follows directly from the above theorem and Lemma 3.2.

**Theorem 4.5.** Let \(G \leq S_n\) be a solvable permutation group given by a generator set and \(\lambda > 0\) any constant. Then in deterministic polynomial time we can compute an expanding generator set \(S\) of size \(\tilde{O}(n^2)\) such that the Cayley graph \(\text{Cay}(G,S)\) is a \(\lambda\)-spectral expander.

### 5 Comparison with known results

In [AMN98] Azar, Motwani, and Naor first considered the construction of \(\varepsilon\)-bias spaces for abelian groups, specifically for the group \(\mathbb{Z}_d^n\). For arbitrary \(d\) and any \(\varepsilon > 0\) they construct \(\varepsilon\)-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 \(\varepsilon\)-bias space for \(d = n^{O(1)}\). In fact when \(d = O(\log n)^{O(1)}\), their construction is of size \(O(n^2)\).
It is interesting to compare with our results in Section 4.1. Let \( d \) be any positive integer with prime factorization \( p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \) such that each \( p_i \) is \( \widetilde{O}(\log n) \) bit sized and each \( e_i \) is bounded by \( O(\log n) \). Then note that we can efficiently find the prime factorization of \( d \). Now, it follows from the construction described in Section 4.1 that in polynomial time we can compute an \( \widetilde{O}(n^2) \) size \( \varepsilon \)-bias space for \( \mathbb{Z}_n^d \) for any constant \( \varepsilon > 0 \). Notice that for constant \( \varepsilon \) this is a significant improvement upon the construction in [AMN98] for such \( d \), in particular for \( d = n^{O(1)} \). Also, we note that for \( d = O(\log n)^{O(1)} \) and constant \( \varepsilon \), our construction yields an \( \widetilde{O}(n) \) size \( \varepsilon \)-bias space. The reason is that we get an \( O(\log^* n \log \log n) \) size expanding generating set for \( \mathbb{Z}_{p_1 p_2 \cdots p_k} \) (where \( p_1, p_2, \ldots, p_k \) are the distinct prime factors of \( d \)) using [AIK+90].

Acknowledgements. We thank Shachar Lovett for pointing out to us the result of Ajtai et al [AIK+90]. We also thank Avi Wigderson for his comments and suggestions.

References


