The Computational Complexity Column

by

V. Arvind

Institute of Mathematical Sciences, CIT Campus, Taramani
Chennai 600113, India
arvind@imsc.res.in
http://www.imsc.res.in/~arvind

Expander graphs are of much importance in theoretical computer science, and the construction of expander graphs involves different areas of mathematics. It has attracted mathematicians and theoretical computer scientists alike and continues to be a flourishing area of research [14].

In this essay we discuss the Alon-Roichman theorem which states that for any finite group G, if S is a randomly picked multiset of $O(\log |G|)$ elements then the symmetric Cayley graph $\mathrm{Cay}(G, S)$ is a spectral expander with high probability. We explain a proof of this theorem based on Erdős-Rényi sequences, which are interesting in their own right, and also outline a $|G|^{O(1)}$ time derandomized construction of the set S.

We also discuss faster, $(\log |G|)^{O(1)}$ time, derandomizations of the Alon-Roichman theorem for finite groups given by small generating sets as input and raise some open questions.

The Alon-Roichman Theorem

V. Arvind
Institute of Mathematical Sciences, Chennai, India
arvind@imsc.res.in

1 Introduction

A primary research goal in the study of expander graphs is the construction of *explicit* expander graph families. Namely, we want to construct a family of graphs $\{G_n\}_{n\in\mathbb{N}}$, where G_n is typically an n vertex graph of small degree d (preferably constant) and the second largest eigenvalue of its normalized adjacency matrix A_G is bounded by a constant $\lambda < 1$. The graph G_n is said to be an (n, d, λ) spectral expander. It turns out that this spectral condition guarantees "high connectivity" for G_n as a result of which G_n has small diameter and, moreover, random walks on G_n converge "rapidly" to the uniform distribution. An excellent source for basic material, a wide range of applications as well as current research is the monograph on expander graphs by Hoory, Linial and Wigderson [14].

The usual source for explicit constructions of expanders is finite groups. Let G be a finite group and let $S = \{g_1, g_2, \ldots, g_k\}$ be a generator set for G. We form the symmetric Cayley graph $\mathrm{Cay}(G, S \cup S^{-1})$ whose vertex set is G and an unordered pair (x, y) is an edge in the graph if and only if $x^{-1}y \in S \cup S^{-1}$. Clearly, $\mathrm{Cay}(G, S \cup S^{-1})$ is a $2k$-regular multigraph. Suppose the group G has an explicit description (i.e. the elements of G have small encodings, are efficiently recognizable and the group operations can be efficiently performed). Furthermore, suppose the generating set S is explicit and of small size then the Cayley graph $\mathrm{Cay}(G, S \cup S^{-1})$ is explicit and has small degree. The best known explicit constructions of expander graphs are Cayley graphs of a subgroup of 2×2 matrices over a finite field $\mathbb{F}_p$. These expander graph families, known as Ramanujan graphs, have constant degree d and $\lambda = \Theta(1/\sqrt{d})$, which is optimal to a constant factor, and matches the λ for random d-regular multigraphs [17].

A general aspect in constructing such expander families lies, of course, in understanding which families of finite groups G_n have small size expanding generating sets S so that $\mathrm{Cay}(G, S \cup S^{-1})$ is a λ-spectral expander.

For any finite group G we know that it has a generating set of size $\log |G|$. Indeed, given G as a multiplication table we can compute a $\log |G|$ size generating set in $|G|^{O(1)}$ time. It is a simple greedy algorithm: having picked i elements $g_1, g_2, \ldots, g_i$ from G into the generating set we list out the elements of the subgroup H generated by the set $\{g_1, g_2, \ldots, g_i\}$. If $H \neq G$ we pick any $g_{i+1} \in G \setminus H$ as the next element in the generating set. The new subgroup $\langle g_1, g_2, \ldots, g_{i+1}\rangle$ obtained contains H properly and its size is at least $2|H|$ by Lagrange's theorem (which states that the size of a finite group is divisible by the size of any subgroup of it). Hence, $\log|G|$ elements suffice to generate G. It turns out that $\log|G|$ is also optimal for certain finite groups. E.g. if G is the additive group $\mathbb{F}_2^n$ then a generating set for it is also a spanning set for the vector space $\mathbb{F}_2^n$ and hence has to have at least $n = \log|G|$ elements in it as $\mathbb{F}_2^n$ is n-dimensional over $\mathbb{F}_2$.

In general, for a finite group G, a natural question that arises is whether G also has an expanding generating set of size $\log|G|$ or at least $O(\log|G|)$. Alon and Roichman in [3] prove the following beautiful result which answers this question in the affirmative.

Theorem 1 (Alon-Roichman Theorem). *[3] Let $\lambda > 0$ and G be any finite group. Then a random multiset $S \subset G$ of size $c\log|G|$ makes the symmetric Cayley graph $\mathrm{Cay}(G, S \cup S^{-1})$ a λ-spectral expander with high probability.*

The theorem suggests a simple efficient Las Vegas algorithm for the problem of computing an $O(\log|G|)$ size expanding generating set for G, where G is given as input by its multiplication table: we sample $c\log|G|$ many elements from G uniformly at random with replacement to obtain the multiset S. We can check in $|G|^{O(1)}$ time if $\mathrm{Cay}(G, S \cup S^{-1})$ is a λ-spectral expander by estimating its second largest eigenvalue and checking that it is bounded in magnitude by λ.

A natural question is whether we can compute such an expanding generating set in deterministic $|G|^{O(1)}$ time. This is along the lines of constructing explicit expander families, and it was answered in the affirmative by Wigderson and Xiao [25] who gave an efficient derandomization of the Alon-Roichman theorem using a representation-theoretic approach. More precisely, in [25] they use Chernoff bounds for matrix-valued random variables (due to Ahlswede and Winter [1]) combined with the application of the method of conditional probabilities [21]. This representation-theoretic approach to the Alon-Roichman theorem is based on alternative proofs of the theorem due to [15, 16]. The original proof of Alon and Roichman [3] is combinatorial in flavour. Igor Pak [20] gives another combinatorial proof for the Alon-Roichman theorem based on Erdős-Rényi sequences [12]. In this essay we give a somewhat different account of Pak's proof which is amenable to a derandomized construction [6]. This actually yields a $|G|^{O(1)}$ time combinatorial derandomization of Alon-Roichman, which is quite different from the previously mentioned one [25]. In the second part of this article we consider finite groups G given by small generating sets as input and address the question of $(\log|G|)^{O(1)}$ time derandomization of the Alon-Roichman theorem for some interesting classes of groups.

2 Randomized construction

We now discuss a version of Pak's proof which is amenable to derandomization [6]. The connection between mixing times of random walks on a graph and its spectral expansion is well studied. For undirected graphs we have the following.

Theorem 2. [22, Theorem 1] *Let A be the normalized adjacency matrix of an undirected graph. For every initial distribution, suppose the distribution obtained after t steps of the random walk following A is ϵ-close to the uniform distribution in the L_1 norm. Then the spectral gap $(1 - |\lambda_1|)$ of A is $\Omega(\frac{1}{t}\log\left(\frac{1}{\epsilon}\right))$.*

Even for directed graphs a connection between mixing times of random walks and the spectral properties of the underlying Markov chain is known.

Theorem 3. [19, Theorem 5.9] *Let λ_{max} denote the second largest magnitude (complex valued) eigenvalue of the normalized adjacency matrix P of a strongly connected aperiodic Markov Chain. Then the mixing time is lower bounded by $\tau(\epsilon) \geq \frac{\log(1/2\epsilon)}{\log(1/|\lambda_{max}|)}$, where ϵ is the difference between the resulting distribution and the uniform distribution in the L_1 norm.*

In [20], Pak uses this connection to prove an analogue of the Alon-Roichman theorem for *directed* Cayley graphs.

Let D_1 and D_2 be probability distributions on the set $\{1, 2, \ldots, n\}$. We use the L_2 norm $\|D_1 - D_2\|_2 = \left[\sum_{x\in[n]} |D_1(x) - D_2(x)|^2\right]^{\frac{1}{2}}$ to measure the distance between them.

We say that a distribution D is δ-close to the uniform distribution U, if $\|D - U\|_2 \leq \delta$. The *collision probability* of a distribution D is $\mathrm{Coll}(D) = \sum_{i\in[n]} D(i)^2$. It is easily seen that $\mathrm{Coll}(D) \leq 1/n + \delta$ if and only if $\|D - U\|_2^2 \leq \delta$ and $\mathrm{Coll}(D)$ attains its minimum value $1/n$ if and only if $D = U$.

Let G be an n-element group. For a sequence of group elements $J = \langle g_1, \ldots, g_k\rangle$ in G, consider the directed Cayley graph $\mathrm{Cay}(G, J)$, which is a multigraph with in-degrees and out-degrees of all vertices equal to k. Let A denote the adjacency matrix of $\mathrm{Cay}(G, J)$. Consider the "lazy" random walk defined by the probability transition matrix $(A + I)/2$ where I is the identity matrix. That is to say, with probability $1/2$ the random walk stays at the same vertex and with probability $1/2$ it moves to one of its k out-neighbors (each destination with probability $1/2k$).

Let Q_J be the probability distribution after m steps of the lazy random walk. Strictly speaking, Q_J depends on the initial distribution. However, we wish to bound the worst-case distance $\|Q_J - U\|_2$ of Q_J from the uniform. Hence the initial distribution does not matter. Pak [20] has analyzed Q_J and shown that for a random J of $O(\log n)$ size and $m = O(\log n)$, Q_J is $1/n^{O(1)}$-close to the uniform distribution. Pak works with the L_∞ norm. Since our aim is to give a derandomization of this construction, the L_2 norm and the collision probability are the right objects to work with since we can compute these quantities exactly as we fix elements of J one by one in the derandomization.

Pak's randomized construction is based on *Erdős-Rényi sequences* for finite groups introduced by Erdős and Rényi in [12].

Definition 4. *Let G be a finite group and $J = \langle g_1, \ldots, g_k \rangle$ be a sequence of elements in G. For $\delta > 0$, J is an* Erdős-Rényi sequence *for G with* closeness parameter δ, *if the probability distribution D_J on G given by $g_1^{\epsilon_1} \ldots g_k^{\epsilon_k}$, where the $\epsilon_i \in \{0, 1\}$ are independent unbiased random bits, is δ-close to the uniform distribution in the L_2-norm.*

Erdős and Rényi proved the following theorem.

Theorem 5 (Erdős Rényi)**.** *([12]) Let G be a finite group and U be the uniform distribution on G. Let $J = \langle g_1, \ldots, g_k \rangle$ denote a sequence of k elements of G picked independently and uniformly at random. Then the expected value*

$$\mathbb{E}_J \|D_J - U\|_2^2 \ = \ 1/2^k(1 - 1/n).$$

In particular, it implies that a random sequence J of $O(\log n)$ elements is an *Erdős-Rényi sequence* for G with *closeness parameter* $1/n^{O(1)}$.

Consider any m-length sequence $I = \langle i_1, \ldots, i_m \rangle \in [k]^m$, where i_j's are indices that refer to elements in the sequence J. Let R_I^J be the following probability distribution on G. For $g \in G$: $R_I^J(g) = \mathsf{Pr}_{\bar{\epsilon}}[g_{i_1}^{\epsilon_1} \cdot \ldots \cdot g_{i_m}^{\epsilon_m} = g]$, where $\bar{\epsilon} = (\epsilon_1, \ldots, \epsilon_m)$ and the $\epsilon_i \in \{0, 1\}$ are independent and uniformly random. For each $g \in G$ we have: $Q_J(g) = \frac{1}{k^m} \sum_{I \in [k]^m} R_I^J(g)$.

Each R_I^J is the distribution defined by the Erdős-Rényi sequence $\langle g_{i_1}, g_{i_2}, \ldots, g_{i_m} \rangle$. Hence, the above equation implies that the distribution Q_J is the average of R_I^J over $I \in [k]^m$.

The indices in $I \in [k]^m$ need not be distinct. Let $L(I)$ denote the subsequence of distinct indices in the order of their *first occurrence* in I, from left to right. We refer to $L(I)$ as the L-subsequence of I. The L-subsequence $L(I)$ also defines a probability distribution $R_{L(I)}^J$ on the group G.

For analyzing the random walk and the distribution G_J, it is more convenient to deal with $R_{L(I)}^J$ rather than R_I^J. Fortunately, we can show that the two are tied together pretty closely. More precisely, suppose the elements of J are picked from G independently and uniformly at random. Then we can show for each $I \in [k]^m$ that, in expectation, if $R_{L(I)}^J$ is δ-close to uniform distribution (in L_2 norm) then so is R_I^J. We state this in terms of collision probabilities.

Lemma 6. *For a fixed I, If $\mathbb{E}_J[\text{Coll}(R_{L(I)}^J)] = \mathbb{E}_J[\sum_{g \in G} R_{L(I)}^J(g)^2] \leq 1/n + \delta$ then $\mathbb{E}_J[\text{Coll}(R_I^J)] = \mathbb{E}_J[\sum_{g \in G} R_I^J(g)^2] \leq 1/n + \delta$.*

Pak actually proves a similar lemma for the L_∞ norm [20]. When elements of J are picked uniformly and independently from G, by Theorem 5,

$$\mathbb{E}_J[\mathrm{Coll}(R^J_{L(I)})] = \mathbb{E}_J[\sum_{g\in G} R^J_{L(I)}(g)^2] = \frac{1}{n} + \frac{1}{2^\ell}(1-\frac{1}{n}),$$

where ℓ is the length of the L-subsequence. Thus the expectation is small provided ℓ is large enough. It turns out, with an easy counting argument, that most $I \in [k]^m$ have sufficiently long L-subsequences (Lemma 7 below).

Lemma 7. [20] *For any k, ℓ, the probability that a sequence of length m over $[k]$ does not have an L-subsequence of length ℓ is at most $\frac{(ae)^{\frac{k}{a}}}{a^m}$ where $a = \frac{k}{\ell-1}$.*

To ensure the above probability is bounded by $\frac{1}{2^m}$, it suffices to choose $m = \lceil \frac{(k/a)\log(ae)}{\log(a/2)} \rceil$. Here a is a constant so that both m and ℓ are $\Theta(k)$.

Lemma 8. $\mathbb{E}_J[\mathrm{Coll}(Q_J)] \leq \frac{1}{n} + \frac{1}{2^{\Theta(m)}}$.

Proof. We call $I \in [k]^m$ *good* if it has an L-subsequence of length at least ℓ, else we call it *bad.*

$$\begin{aligned}
\mathbb{E}_J[\mathrm{Coll}(Q_J)] &= \mathbb{E}_J[\sum_{g\in G} Q_J^2(g)] \\
&= \mathbb{E}_J[\sum_{g\in G}(\mathbb{E}_I(R_I(g))^2] \\
&\leq \mathbb{E}_J[\sum_{g\in G} \mathbb{E}_I(R_I^2(g))] \text{ By Cauchy-Schwartz inequality} \quad (1) \\
&= \mathbb{E}_I[\mathbb{E}_J[\mathrm{Coll}(R_I)]] \\
&\leq \frac{1}{k^m}\mathbb{E}_J[\sum_{\substack{I\in[k]^m \\ I \text{ is good}}} \sum_{g\in G}(R^J_L(g))^2 + \sum_{\substack{I\in[k]^m \\ I \text{ is bad}}} 1] \\
&\leq \mathsf{Pr}_I[I \text{ is good}]\left(\frac{1}{n}+\frac{1}{2^\ell}\right) + \mathsf{Pr}_I[I \text{ is bad}] \quad (2)
\end{aligned}$$

The last step follows from Lemma 6 and Theorem 5. Fix m in Lemma 7 to $O(\log n)$ such that $\mathsf{Pr}_I[I \text{ is bad}] \leq \frac{1}{2^m}$ and let $\ell = \Theta(m)$ to yield $\mathbb{E}_J[\mathrm{Coll}(Q_J)] \leq \frac{1}{n} + \frac{1}{2^{\Theta(m)}}$. In particular, m is chosen so that $\mathsf{Pr}_I[I \text{ is bad}] \leq \frac{1}{2^m}$. □

Clearly, $\frac{1}{2^{\Theta(m)}} < \frac{1}{n^c}$ for a given $c > 0$, by choosing $m = O(\log n)$. We also choose $\ell = \Theta(m)$ in the proof of Lemma 8. Then, from the relation that $m = \lceil \frac{(k/a)\log(ae)}{\log(a/2)} \rceil$, we fix k to be $O(\log n)$ suitably. Since random walks on $\mathrm{Cay}(G, J)$ mix well, as a consequence of Theorem 3 we obtain the following.

Theorem 9. [20] *Let $\lambda > 0$ and G be any finite group. Then, with high probability, a random multiset $J \subset G$ of size $c \log |G|$ makes the directed Cayley graph $\mathrm{Cay}(G, J)$ a spectral expander (i.e. its second largest eigenvalue in absolute value is bounded by ϵ).*

2.1 Derandomizing the construction

We outline a derandomization [6] of the randomized Cayley expanders $\mathrm{Cay}(G, J)$ given by Theorem 9.

Given a group G with n elements, we need to compute in deterministic $|G|^{O(1)}$ time, a multiset J of k group elements of G such that:

$$\mathrm{Coll}(Q_J) = \sum_{g \in G} Q_J(g)^2 \ \leq \ 1/n + 1/n^c, \tag{3}$$

where $c > 0$ is a given constant and both k and m are $O(\log n)$. By Theorem 9 a random set J satisfies this with high probability. For each J observe, by the Cauchy-Schwartz inequality, that

$$\mathrm{Coll}(Q_J) = \sum_{g \in G} Q_J(g)^2 \leq \sum_{g \in G} \frac{1}{k^m} \sum_{I \in [k]^m} R_I^J(g)^2 = \frac{1}{k^m} \sum_{I \in [k]^m} \mathrm{Coll}(R_I^J). \tag{4}$$

Thus, it suffices to compute a multiset J of group elements such that the average collision probability $\frac{1}{k^m} \sum_{I \in [k]^m} \mathrm{Coll}(R_I^J) \leq 1/n + 1/n^c$.

We start with $J = \{X_1, \ldots, X_k\}$ where each X_i is an independent random variable uniformly distributed in G. By Theorem 9 (in particular from Equation 3), for a given $c > 1$ there are k and m, both $O(\log n)$ such that:

$$\mathbb{E}_J[\mathrm{Coll}(Q_J)] = \mathbb{E}_J[\mathbb{E}_{I \in [k]^m} \mathrm{Coll}(R_I^J)] \leq \frac{1}{n} \ + \ \frac{1}{n^c}. \tag{5}$$

The algorithm is based on the method of conditional probabilities. It fixes elements in J one by one. Suppose at the j^{th} stage, for $j < k$, $J = J_j = \{x_1, x_2, \ldots, x_j, X_{j+1}, \ldots, X_k\}$, where x_r $(1 \leq r \leq j)$ are fixed elements of G and the remaining $X_s, s = j+1, \ldots, k$ are still random variables such that $\mathbb{E}[\mathbb{E}_{I \in [k]^m} \mathrm{Coll}(R_I^J)] \leq 1/n + 1/n^c$, where the outer expectation is over these X_s.

It suffices to give a polynomial-time procedure that fixes X_{j+1} to an $x_{j+1} \in G$ such that $\mathbb{E}[\mathbb{E}_{I \in [k]^m} \mathrm{Coll}(R_I^J)] \leq 1/n + 1/n^c$. Given $J = J_j = \{x_1, \ldots, x_j, X_{j+1}, \ldots, X_k\}$ with j fixed elements and $k - j$ random elements, we partition $[k]^m$ into subsets $S_{r,\ell}$ where $I \in S_{r,\ell}$ if and only if there are exactly r indices in I from $\{1, \ldots, j\}$, and of the remaining $m - r$ indices of I there are exactly ℓ distinct indices.

An (r,ℓ)-*normal sequence* for J is a sequence $\langle n_1, n_2, \ldots, n_r, \ldots, n_{r+\ell}\rangle \in [k]^{r+\ell}$ such that $n_s, 1 \leq s \leq r$ are in $\{1, 2, \ldots, j\}$ and the $n_s, s > r$ are *all distinct* and in $\{j+1, \ldots, k\}$. In other words, the first r indices (possibly with repetition) are from the fixed part of J and the last ℓ are all distinct indices from the random part of J.

It turns out that a sequence $I \in [k]^m$ can be transformed, by group conjugation, into (r,ℓ)-normal form such that the expected collision probability of the distribution generated by the (r,ℓ)-normal form gives an upper bound on $\mathbb{E}[\mathrm{Coll}(R_I^J]$. This upper bound plays the role of a pessimistic estimator in the derandomization.

In order to transform a sequence in $S_{r,\ell}$ into (r,ℓ)-normal form we will make repeated use of the fact that if $y \in G$ is picked uniformly at random and $x \in G$ be any element independent of y, then the distribution of xyx^{-1}, namely the x-conjugate of y, is uniform in G.

Let $I = \langle i_1, \ldots, i_m\rangle \in S_{r,\ell}$ be a sequence. Let $F = \langle i_{f_1}, \ldots, i_{f_r}\rangle$ be the index subsequence whose corresponding elements are from the fixed part $\{x_1, x_2, \ldots, x_j\}$ of J. Let $R = \langle i_{s_1}, \ldots, i_{s_{m-r}}\rangle$ be the index subsequence for the random part of J. Let $L = \langle i_{e_1}, \ldots, i_{e_\ell}\rangle$ be the L-subsequence in R. More precisely, notice that R is a sequence in $\{j+1, \ldots, k\}^{m-r}$ and L is the L-subsequence for R. The (r,ℓ)-normal sequence $\widehat{I}$ of $I \in S_{r,\ell}$ is $\langle i_{f_1}, \ldots, i_{f_r}, i_{e_1}, \ldots, i_{e_\ell}\rangle$.

Denote the elements of J by $g_t, 1 \leq t \leq k$, where $g_t = x_t$ for $t \leq j$ and $g_t = X_t$ for $t > j$. Consider the distribution R_I^J consisting of the products $g_{i_1}^{\epsilon_1} \ldots g_{i_m}^{\epsilon_m}$ where $\epsilon_i \in \{0,1\}$ are independent and uniformly picked at random. Then, using repeated conjugation of the group elements to move the fixed part to the left, we can write

$$g_{i_1}^{\epsilon_1} \ldots g_{i_m}^{\epsilon_m} = g_{i_{f_1}}^{\epsilon_{f_1}} \ldots g_{i_{f_r}}^{\epsilon_{f_r}} h_{e_1}^{\epsilon_{e_1}} \ldots h_{e_\ell}^{\epsilon_{e_\ell}} y(\bar{\epsilon}),$$

where $y(\bar{\epsilon})$ is an element in G that depends on J, I and $\bar{\epsilon}$, where $\bar{\epsilon}$ consists of all the ϵ_j for $i_j \in I \setminus (F \cup L)$. Here, $(h_{e_1}, h_{e_2}, \ldots, h_{e_\ell})$ is the sequence of all *independent* random elements in the above product $\prod_{a=1}^{m-r} h_{s_a}^{\epsilon_{s_a}}$ consisting of conjugates of the original L-subsequence in J.

Let J_I denote the multiset of group elements obtained from J by replacing the subset $\{g_{i_{e_1}}, g_{i_{e_2}}, \ldots, g_{i_{e_\ell}}\}$ in J with $\{h_{e_1}, h_{e_2}, \ldots, h_{e_\ell}\}$. Note that, in this substitution, we are replacing a uniformly distributed random variable $g_{i_{e_j}}$ over G with another uniformly distributed random variable h_{e_j} over G, where the later is obtained from the former by a conjugacy transformation. Clearly, J_I also has j fixed elements $x_1, x_2, \ldots, x_j$ and $k-j$ uniformly distributed independent random elements. Recall that $\widehat{I} = \langle i_{f_1}, i_{f_2}, \ldots, i_{f_r}, i_{e_1}, i_{e_2}, \ldots, i_{e_\ell}\rangle$ is the (r,ℓ)-normal sequence for I. The probability distributions R_I^J and $R_{\widehat{I}}^{J_I}$ are compared in the following lemma.

Lemma 10. *For each $j \leq k$ and $J = \{x_1, \ldots, x_j, X_{j+1}, \ldots, X_k\}$ (where $x_1, \ldots, x_j \in G$ are fixed elements and $X_{j+1}, \ldots, X_k$ are independent uniformly distributed in G), and for each $I \in [k]^m$, $\mathbb{E}[\mathrm{Coll}(R_I^J)] \leq \mathbb{E}[\mathrm{Coll}(R_{\hat{I}}^{J_I})]$, where $\mathbb{E}[\mathrm{Coll}(R_I^J)]$ is computed over random elements in J and $\mathbb{E}[\mathrm{Coll}(R_{\hat{I}}^{J_I})]$ over random elements in J_I.*

It follows that $\mathbb{E}_J[\mathrm{Coll}(Q_J)] \leq \mathbb{E}_{J_I}\mathbb{E}_{I\in[k]^m}[\mathrm{Coll}(R_{\hat{I}}^{J_I})]$. Furthermore, it turns out that given $J = \{x_1, \ldots, x_j, X_{j+1}, \ldots, X_k\}$ we can compute $\mathbb{E}_{J_I}\mathbb{E}_{I\in[k]^m}[\mathrm{Coll}(R_{\hat{I}}^{J_I})]$ in deterministic polynomial (in n) time by reducing it to the problem of counting directed s-t paths in a weighted directed acyclic graph. This completes the proof outline of the following.

Theorem 11. [6] *Let G be a group with n elements, given as its multiplication table. For any constant $c > 1$, there is a deterministic* $\mathrm{poly}(n)$ *time algorithm that computes a generating set J of size $O(\log n)$ for the given group G, such that for any initial distribution on G the lazy random walk of $O(\log n)$ steps on the directed Cayley graph* $\mathrm{Cay}(G, J)$ *yields a distribution that is $\frac{1}{n^c}$-close (in L_2 norm) to the uniform distribution.*

Together with Theorem 3 this yields the following corollary.

Corollary 12. [6] *Given a finite group G and any $\epsilon > 0$, there is a deterministic polynomial-time algorithm to construct an $O(\log n)$ size generating set J such that* $\mathrm{Cay}(G, J)$ *is a spectral expander (i.e. its second largest eigenvalue in absolute value is bounded by ϵ).*

Undirected Cayley graphs

This approach can be adapted for undirected Cayley graphs as well [6]. The key point is a suitable generalization of Erdős-Rényi sequences. We consider the distribution on G defined by $g_1^{\epsilon_1} \ldots g_k^{\epsilon_k}$ where $\epsilon_i \in_R \{-1, 0, 1\}$. Using these generalized Erdős-Rényi sequences we can analyze lazy random walks on the *undirected* Cayley graph $\mathrm{Cay}(G, J \cup J^{-1})$ for a random multiset J of $O(\log |G|)$ size. More precisely, we consider the lazy random walk described by the symmetric transition matrix $A_J = \frac{1}{3}I + \frac{1}{3k}(P_J + P_{J^{-1}})$ where P_J and $P_{J^{-1}}$ are the adjacency matrices of the directed Cayley graphs $\mathrm{Cay}(G, J)$ and $\mathrm{Cay}(G, J^{-1})$ respectively. We obtain the following results.

Theorem 13. [6] *Let G be a finite group of order n and $c > 1$ be any constant. There is a deterministic* $\mathrm{poly}(n)$ *time algorithm that computes a generating set J of size $O(\log n)$ for G, such that an $O(\log n)$ step lazy random walk on G, governed by the transition matrix A_J described above, is $\frac{1}{n^c}$-close to the uniform distribution, for any given initial distribution on G.*

Theorem 13 and the connection between mixing time and spectral expansion for undirected graphs given by Theorem 2 yields an alternative proof of the following [6].

Corollary 14. [25] *Given a finite group G by its multiplication table, there is a deterministic polynomial (in $|G|$) time algorithm to construct a generating set J such that* $\mathrm{Cay}(G, J \cup J^{-1})$ *is a spectral expander.*

3 Faster derandomizations

We now explore the question of computing expanding generating sets for finite groups G in time polynomial in $\log |G|$. Since every finite group G has a generating set of size $\log |G|$, we can assume that $G = \langle S \rangle$ is given as input by a small generating set S and the goal is to compute an expanding generating set for G in time polynomial in $\log |G|$ and $|S|$.

For example, let G be any subgroup of the group S_n. Then G has a generating set $S \subset S_n$ of size at most $n \log n$. Furthermore, the group operation is permutation composition, and for two given permutations $\pi, \pi' \in S_n$ we can compute $\pi\pi'$ in time polynomial in n.

Another example: consider subgroups $G = \langle S \rangle$ of the group of invertible $n \times n$ matrices over a finite field $\mathbb{F}_q$ under matrix product. Matrix product can be performed in time polynomial in n and $\log q$ and every such group has a generating set of size $n^2 \log q$ (as there are at most q^{n^2} many invertible $n \times n$ matrices).

An algorithmic framework for finite groups input by their generating sets is the notion of *black-box groups* due to Babai and Szemerédi [10]. The elements of a finite black-box group G are assumed to be uniformly encoded as binary strings of some length m (where m would typically be polynomial in $\log |G|$). Each group operation is performed by a black-box in time polynomial in m. The group G is given by a generating set S.

In a general result about finite black-box groups Babai has shown [9] that it is possible to sample nearly uniformly in polynomial time from $G = \langle S \rangle$, where S is an arbitrary generating set. Interestingly, Babai's sampling algorithm is based on Erdős-Rényi sequences. The randomized algorithm computes with high probability an Erdős-Rényi sequence $\{g_1, g_2, \ldots, g_k\}$ for G with closeness parameter $2^{-O(m)}$, where k is polynomial in m. Once we have an Erdős-Rényi sequence the sampling algorithm simply outputs $\prod_{i=1}^{k} g_i^{\varepsilon_i}$ where each $\varepsilon_i \in \{0, 1\}$ is independently and uniformly picked at random. We can summarize this result as follows.

Theorem 15 (Babai)**.** [9] *Let $G = \langle S \rangle$ be a finite black-box group whose elements uniformly encoded as binary strings length m. Then there is a randomized*

$\mathrm{poly}(m, |S|)$ *time algorithm that outputs with high probability an Erdős-Rényi sequence with closeness parameter* $2^{-O(m)}$. *As a consequence, there is a randomized* $\mathrm{poly}(m, |S|)$ *time algorithm for sampling almost uniformly at random from* G.

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). More precisely, we have the following consequence of Alon-Roichman for general black-box groups.

Proposition 16. *Given* $\lambda > 0$ *and a finite black-box group* $G = \langle S \rangle$ *whose elements uniformly encoded as binary strings length* m. *There is a randomized* $\mathrm{poly}(m, |S|, 1/\lambda)$ *time Monte-Carlo algorithm that outputs with high probability an expanding generating set* T *of size* $(O(\log |G|/\lambda^2)$ *for* G *such that* $\mathrm{Cay}(G, T \cup T^{-1})$ *is a* λ*-spectral expander.*

The algorithmic question we now address is to obtain a *deterministic* polynomial (in $\log |G|$ and $|S|$) time algorithm for computing small expanding generating sets for G. A precise formulation of the problem is as follows:

Problem 17. *Given a finite group* $G = \langle S \rangle$ *by a small generating set* S *and a* $\lambda > 0$ *the problem is to compute, in deterministic time polynomial in* $|S|$, $\log |G|$, *and* $\nVdash/\lambda$, *a generating set* T *for* G *such that* $|T| = O(\log |G|/\lambda^2)$ *and* $\mathrm{Cay}(G, T \cup T^{-1})$ *is a* λ*-spectral expander.*

In Problem 17, the real challenge seems to be computing an expanding generating set T of the size $O(\log |G|/\lambda^2)$ promised by the Alon-Roichman theorem. We will discuss deterministic polynomial time algorithms that compute somewhat larger generating sets.

3.1 Small bias spaces

We will first consider the additive group $\mathbb{F}_2^n$ which is the simplest of groups. Its elements are the 2^n binary vectors and the group operation is coordinate-wise addition modulo 2. The group is abelian and each nonzero element has order 2. By the Alon-Roichman theorem, for any $\epsilon > 0$ the group $\mathbb{F}_2^n$ has an expanding generating set T of size $O(n/\epsilon^2)$ that makes the Cayley graph ϵ-spectral.

Although we do not know any polynomial-time deterministic construction of size $O(n/\epsilon^2)$, it turns out that we can compute T of size $O(n^2/\epsilon^2)$ or of size $O(n/\epsilon^{O(1)})$. This is because expanding generating sets for $\mathbb{F}_2^n$ are precisely ϵ-bias spaces in $\mathbb{F}_2^n$ whose constructions are well studied in the context of almost k-wise independent sample spaces [5, 2].

We explain this connection between small bias spaces in $\mathbb{F}_2^n$ and expanding generating sets for $\mathbb{F}_2^n$. We will require some elementary group representation theory. A *character* χ of the group $\mathbb{F}_2^n$ is a *group homomorphism* from $\mathbb{F}_2^n$ to the multiplicative group of complex numbers $\mathbb{C}^*$. As all elements of $\mathbb{F}_2^n$ are or order either 1 or 2, and χ is a group homomorphism, it follows that $\chi(a) \in \{-1, 1\}$ for each $a \in \mathbb{F}_2^n$. The *trivial* character χ_0 maps all elements to 1. Each vector $b \in \mathbb{F}_2^n$ defines a character

$$\chi_b(a) = (-1)^{a.b},$$

where $a.b = \sum_i a_i b_i \bmod 2$.

The set of all functions $f : \mathbb{F}_2^n \to \mathbb{C}$ forms a 2^n-dimensional vector space over $\mathbb{C}$ and it turns out that the set of characters $\{\chi_b \mid b \in \mathbb{F}_2^n\}$ spans the vector space. This is a consequence of the fact that these 2^n characters $\chi_b, b \in \mathbb{F}_2^n$ are mutually orthogonal under the inner product $\langle f, g\rangle = \frac{1}{2^n}\sum_{a \in \mathbb{F}_2^n} f(a)\overline{g(a)}$.

Now, consider a generating set $S \subset \mathbb{F}_2^n$ for the group $\mathbb{F}_2^n$ and the resulting symmetric Cayley graph $\mathrm{Cay}(\mathbb{F}_2^n, S)$. Note that any subset S is already symmetric as $S = S^{-1}$. Let A_S denote its normalized adjacency matrix. The following nice fact about its eigenvectors suitably generalizes to the setting of all abelian groups.

Claim 18. *The vectors $\{\chi_b \mid b \in \mathbb{F}_2^n\}$ are the eigenvectors of the symmetric matrix A_S.*

Indeed, an easy calculation shows that the vector $A_S\chi_b = (1/|S|\sum_{s \in S}\chi_b(s))\chi_b$. Thus the eigenvalues of A_S are $\frac{1}{|S|}\sum_{s \in S}\chi_b(s)$ for $b \in \mathbb{F}_2^n$. The trivial character χ_0 is the eigenvector for eigenvalue 1. We can summarize the discussion in the following.

Proposition 19 (folklore)**.** *The Cayley graph $\mathrm{Cay}(\mathbb{F}_2^n, S)$ is an ϵ-spectral expander if and only if for all nontrivial characters χ_b*

$$\frac{1}{|S|}|\sum_{s \in S}\chi_b(s)| \leq \epsilon.$$

The latter condition is precisely the definition of an ϵ-bias space. The known deterministic efficient constructions of Alon et al [4] of size $O(n^2/\epsilon^2)$ and [5] of size $O(n/\epsilon^{O(1)})$ fall short of constructing $O(n/\epsilon^2)$ size ϵ-bias spaces promised by the Alon-Roichman theorem.

3.2 General case: Divide and Conquer Constructions

We now consider deterministic construction of expanding generating sets for more general groups. Let $G = \langle g_1, g_2, \ldots, g_k\rangle$ be a finite group given by generators g_i. We will now outline a divide and conquer strategy [7] for the problem of computing expanding generating sets that works quite well for a large class of finite groups. The idea is to decompose G into smaller groups, compute expanding generating sets for the smaller groups and put these generating sets together suitably for G.

Exploiting normal subgroups

Let G be a finite group and N be a *normal* subgroup of G. I.e. N is a subgroup such that $g^{-1}Ng = N$ for all $g \in G$. Suppose $A \subset N$ is an expanding generating set for N so that $\mathrm{Cay}(N, A \cup A^{-1})$ is a λ-spectral expander. Similarly, consider the quotient group G/N (which is well defined by virtue of N's normality). Suppose $B \subset G$ such that $\hat{B} = \{Nx \mid x \in B\}$ is an expanding generating set for the quotient group G/N and the corresponding Cayley graph $\mathrm{Cay}(G/N, \hat{B} \cup \hat{B}^{-1})$ is also λ-spectral. Then we can prove the following.

Lemma 20. [7] *Suppose both* $\mathrm{Cay}(N, A \cup A^{-1})$ *and* $\mathrm{Cay}(G/N, \hat{B} \cup \hat{B}^{-1})$ *are* λ*-spectral and let* $C = A \cup B$*. Then* $\mathrm{Cay}(G, C \cup C^{-1})$ *is a* $(1 + \lambda)/2$*-spectral expander.*

See [7] for proof details. The overall idea is similar in spirit to the analysis of the zig-zag product construction [24]. There are some additional issues in this construction that makes $C \cup C^{-1}$ an expanding generating set for G which are taken care of because N is a normal subgroup of G. This theorem provides us a divide-and-conquer tool in the following sense. Suppose G is a finite group with a *normal series*

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\},$$

where each G_i is a normal subgroup of G. I.e. $G \rhd G_i$ for each i. Suppose we are given expanding generating sets for each quotient group G_i/G_{i+1}. Using the above theorem we can put them together efficiently to construct an expanding generator set for G.

Lemma 21. [7] *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* $c > 0$*.*

The proof of this lemma is essentially based on repeated application of Lemma 20.

The case of solvable permutation groups

In order to actually apply Lemma 21 we need to compute a normal series for $G = \langle S \rangle$ efficiently. Moreover, we will also need to compute expanding generating sets for the quotient groups G_i/G_{i+1}. A large class of groups for which this approach works well is solvable permutation groups. First we recall some definitions.

Let G be a finite group. The *commutator subgroup* of G is the subgroup G' generated by elements $xyx^{-1}y^{-1}$ where $x, y \in G$. The commutator subgroup G'

is the minimal normal subgroup of G such that the quotient G/G' is abelian. The *derived series* for G is the following chain of subgroups of G:

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_k$$

where, for each i, G_{i+1} is the *commutator subgroup* of G_i.

The group G is said to be *solvable* if the derived series terminates in $G_k = \{1\}$ for some k, where k is the *length* of the derived series for G. We note that the derived series for G is a normal series.

A group G is *non-solvable* if the derived series does not terminate at $\{1\}$. For instance, the group $G = A_5$, consisting of all even permutations on five elements, is non-solvable because $G_1 = G$.

A *permutation group* is a subgroup $G = \langle S \rangle$ of the group S_n of all permutations on $[n]$. Given a permutation group $G = \langle S \rangle$ by a generating set we can compute its derived series in deterministic polynomial time [18]. Dixon [11] has shown that derived series of solvable subgroups of S_n have length bounded by $5 \log_3 n$. The above observations combined with Theorem 21 yields the following consequence.

Lemma 22. *Suppose $G \leq S_n$ is a solvable group with derived series*

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_k = \{1\},$$

and we have $B_i \subset G_i/G_{i+1}$ such that $\mathrm{Cay}(G_i/G_{i+1}, B_i \cup B_i^{-1})$ is a 1/4-spectral expander. Let $s = \max_i\{|B_i|\}$. Then in deterministic $\mathrm{poly}(n, s)$ time we can compute a subset B of G such that $\mathrm{Cay}(G, B \cup B^{-1})$ is a 1/4-spectral expander and $|B| = 2^{O(\log k)} s = (\log n)^{O(1)} s$.

In order to compute an expanding generating set for a solvable subgroup G of S_n we first need to compute an expanding generating set B_i for G_i/G_{i+1} such that $\mathrm{Cay}(G_i/G_{i+1}, B_i)$ is 1/4-spectral and then apply the above lemma.

Abelian quotient groups

We now explain the computation of expanding generating sets for the abelian quotient groups G_i/G_{i+1}, where $G_{i+1} \lhd G_i \leq S_n$. Let $p_1 < p_2 < \ldots < p_k$ be the list of all primes bounded by n. Let $e = \lceil \log n \rceil$. As G_i/G_{i+1} is abelian, there is an onto group 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 G_i/G_{i+1}. Moreover, this homomorphism is easily computable. It suffices to compute an expanding generating set for $\mathbb{Z}_{p_1^e}^n \times \mathbb{Z}_{p_2^e}^n \times \cdots \times \mathbb{Z}_{p_k^e}^n$ because its ϕ-image will be an expanding generating set for G_i/G_{i+1}.

It turns out that we can compute an expanding generating set for $\mathbb{Z}_{p_1^e}^n \times \mathbb{Z}_{p_2^e}^n \times \cdots \times \mathbb{Z}_{p_k^e}^n$ of size $\tilde{O}(n^2)$ in polynomial time [7]. This construction is again a careful application of Lemma 20 combined with a result of Ajtai et al [2] of expanding generating sets for cyclic groups Z_N.

Theorem 23. [7] *Let $G = \langle S \rangle$ be a solvable subgroup of S_n. In deterministic polynomial time we can compute an expanding generating set of size $\tilde{O}(n^2)$ such that the Cayley graph* $\mathrm{Cay}(G, S \cup S^{-1})$ *is a 1/4-spectral expander.*

For general permutation groups we have the following theorem based on derandomized squaring [23] about computing expanding generator sets. Details are given in [7].

Theorem 24. *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 constant.*

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

In conclusion, we note that the expanding generating set construction for abelian groups $\mathbb{Z}^n_{p_1^e} \times \mathbb{Z}^n_{p_2^e} \times \cdots \times \mathbb{Z}^n_{p_k^e}$ mentioned above also gives a new construction of ε-bias spaces for $\mathbb{Z}_d^n$, which we now describe.

In [8] 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 $\epsilon > 0$ they construct ϵ-bias spaces of size $O((d+n^2/\epsilon^2)^C)$, 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 [8] with the construction described above. Let d have prime factorization $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Each p_i is $O(\log d)$ bit sized and each e_i is bounded by $O(\log d)$. Given d in unary, we can efficiently find the prime factorization of d. Using the result of Wigderson and Xiao [25], 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 $O((\log n)^{O(1)} \log d)$ for $\mathbb{Z}^m_{p_1} \times \ldots \times \mathbb{Z}^m_{p_k}$ for $m = O(\log n)$ based on Lemma 22. It then follows that we can construct an $O(n(\log n)^{O(1)} \log d)$ size expanding generator set for $\mathbb{Z}^n_{p_1} \times \ldots \times \mathbb{Z}^n_{p_k}$ in deterministic polynomial time. Finally, it follows that we can construct an $O(n(\log n \log d)^{O(1)})$ size expanding generator set for $\mathbb{Z}_d^n$ (which is isomorphic to $\mathbb{Z}^n_{p_1^{e_1}} \times \ldots \mathbb{Z}^n_{p_k^{e_k}}$) since each e_i is bounded by $\log d$. Given $\epsilon > 0$, the dependence of ϵ in the size of the generating set that makes the Cayley graph λ-spectral is $(1/\epsilon)^{32q}$.

Theorem 25. *Let d, n be any positive integers (in unary) and $\varepsilon > 0$. Then, in deterministic* $\mathrm{poly}(n, d, \frac{1}{\epsilon})$ *time, we can construct an* $O(n\mathrm{poly}(\log n, \log d))(1/\varepsilon)^{32q}$ *size ϵ-bias space for $\mathbb{Z}_d^n$.*

References

[1] R. Ahlswede and A. Winter. Strong Converse for Identification via Quantum Channels. *IEEE Transactions on Information Theory,* 48(3): 569âĂŞ579, 2003.

[2] Miklós Ajtai, Henryk Iwaniec, János Komlós, János Pintz, and Endre Szemerédi. . Construction of a thin set with small Fourier coefficients. *Bull. London Math. Soc.* 22:583-590, 1990.

[3] Noga Alon and Yuval Roichman. Random Cayley Graphs and Expanders. *Random Struct. Algorithms*, 5(2):271–285, 1994.

[4] 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.

[5] 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), 1992.

[6] Vikraman Arvind, Partha Mukhopadhyay, and Prajakta Nimbhorkar. Erdős-Rényi Sequences and Deterministic Construction of Expanding Cayley Graphs. *Electronic Colloquium on Computational Complexity (ECCC)*, 18:81, 2011 and *Proc. of LATIN 2012,* Springer.

[7] 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 and *Proc of MFCS 2012,* Springer.

[8] Yossi Azar, Rajeev Motwani, and Joseph Naor. Approximating Probability Distributions Using Small Sample Spaces. *Combinatorica,* 18(2):151–171, 1998.

[9] László Babai. Local expansion of vertex-transitive graphs and random generation in finite groups. *Proc. 23rd Annual ACM Symp. on Theory of computing,* 164-174, 1991.

[10] Laszlo Babai, Endre Szemerédi. On the Complexity of Matrix Group Problems I. *Proc. of the 25th IEEE FOCS Conference,* 229-240.

[11] John D. Dixon. The solvable length of a solvable linear group. *Mathematische Zeitschrift,* 107: 151-158, 1968.

[12] Paul Erdős and Alfréd Rényi. Probabilistic methods in group theory. *Journal D'analyse Mathematique*, 14(1):127–138, 1965.

[13] Martin Hildebrand. A survey of results on random random walks on finite groups. *Probability Surveys*, 2:33–63, 2005.

[14] Shlomo Hoory, Nati Linial, and Avi Wigderson. Expander graphs and their applications. *Bull. AMS*, 43(4):439–561, 2006.

[15] Zeph Landau, Alexander Russell. Random Cayley Graphs are Expanders: a Simple Proof of the Alon-Roichman Theorem. *Electr. J. Comb.* 11(1) (2004).

[16] Po-Shen Loh, Leonard J. Schulman: Improved Expansion of Random Cayley Graphs. *Discrete Mathematics & Theoretical Computer Science* 6(2): 523-528, 2004.

[17] Alexander Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica,* 8(3): 261–277, 1988.

[18] Eugene M. Luks, *Permutation groups and polynomial-time computation*, DIMACS series in Discrete Mathematics and Theoretical Computer Science **11** (1993), 139–175.

[19] Ravi Montenegro and Prasad Tetali. Mathematical Aspects of Mixing Times in Markov Chains. *Foundations and Trends in Theoretical Computer Science*, 1(3), 2005.

[20] Igor Pak. Random Cayley Graphs with $O(\log[g])$ Generators Are Expanders. In *Proceedings of the 7th Annual European Symposium on Algorithms*, ESA '99, pages 521–526. Springer-Verlag, 1999.

[21] P. Raghavan. Probabilistic construction of deterministic algorithms: approximating packing integer programs. *Journal of Computer and System Sciences,* 37(2):130Âą V143, 1988.

[22] Dana Randall. Rapidly Mixing Markov Chains with Applications in Computer Science and Physics. *Computing in Science and Engg.*, 8(2):30–41, 2006.

[23] Eyal Rozenman and Salil P. Vadhan. Derandomized squaring of graphs. *Proc. APPROX-RANDOM 2005,* LNCS vol. 3624: 436-447, 2005, Springer.

[24] Omer Reingold, Salil Vadhan and Avi Wigderson. Entropy Waves, The Zig-Zag Graph Product, and New Constant-Degree Expanders and Extractors. *Annals of Mathematics,* 155, 157-187, 2002.

[25] 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.