Electronic Colloquium on Computational Complexity, Report No. 178 (2025)

A Logspace Constructive Proof of $\mathsf{L} = \mathsf{SL}$

Sam Buss[1], Anant Dhayal[2], Valentine Kabanets[3], Antonina Kolokolova[4], and Sasank Mouli[5]

[1]Department of Mathematics, University of California, San Diego, La Jolla, CA, USA
[2]Google, Kirkland, WA, USA
[3]School of Computing Science, Simon Fraser University, Burnaby, B.C., Canada
[4]Department of Computer Science, Memorial University of Newfoundland, St. John's, NL, Canada
[5]Department of Computer Science, Indian Institute of Technology Indore, Madhya Pradesh, India

November 14, 2025

Abstract

We formalize the proof of Reingold's Theorem that $\mathsf{SL} = \mathsf{L}$ [Rei05] in the theory of bounded arithmetic VL, which corresponds to "logspace reasoning". As a consequence, we get that VL = VSL, where VSL is the theory of bounded arithmetic for "symmetric-logspace reasoning". This resolves in the affirmative an old open question from Kolokolova [Kol05] (see also Cook-Nguyen[CN10]).

Our proof relies on the Rozenman-Vadhan alternative proof of Reingold's Theorem [RV05]. To formalize this proof in VL, we need to avoid reasoning about eigenvalues and eigenvectors (common in both original proofs of $\mathsf{SL} = \mathsf{L}$). We achieve this by using some results from Buss-Kabanets-Kolokolova-Koucký [Bus+20] that allow VL to reason about graph expansion in combinatorial terms.

ISSN 1433-8092

Contents

1 Introduction

Symmetric logspace (SL) has been studied for many years as a natural complexity class, with the st-connectivity (reachability) problem (USTCON) for *undirected* graphs as a natural complete problem for SL; that is, SL can be defined as the class of problems that are many-one log-space reducible to USTCON. Nisan and Ta-Shma [NT95] showed that SL is closed under complement. Finally, Reingold proved a breakthrough result that $\mathsf{SL} = \mathsf{L}$, i.e., that symmetric logspace is equal to (deterministic) logspace [Rei05; Rei08], by showing that USTCON is in logspace. (See [Rei08] for a broader overview of prior work on SL including expander graphs and derandomization.) Rozenman and Vadhan [RV05] later gave an alternative proof that USTCON is in logspace. Both proofs of $\mathsf{SL} = \mathsf{L}$ use expander graphs and linear algebra to analyze the expansion properties of various graph operations (usually by bounding certain eigenvalues).

Our main result is that $\mathsf{SL} = \mathsf{L}$ can be proved using "logspace reasoning". We show this by formalizing a variant of the Rozenman-Vadhan proof of $\mathsf{SL} = \mathsf{L}$ in the system of bounded arithmetic VL, corresponding to logspace. This finally answers in the affirmative an old open question of [Kol05; CN10] of whether VL can prove $\mathsf{L} = \mathsf{SL}$.

Formalizing complexity results in logical theories. First-order logical theories, in particular fragments of bounded arithmetic, are known to prove a wide range of complexity results. A number of non-trivial algorithmic constructions, including Toda's theorem [BKZ15], the PCP theorem [Pic15], NC^1-constructions of expander graphs [Bus+20], the fact that $\mathsf{NL} = \mathsf{coNL}$ [CK04; CN10], constructions of hardness amplification [Jeř05], and properties of the Arthur-Merlin hierarchy [Jeř07], can be formalized and proved in various fragments of bounded arithmetic. Some circuit lower bounds can be proved in bounded arithmetic theories, including lower bounds on constant depth circuits [Kra95; MP20]. A recent unprovability result shows that a (weak) second order fragment of bounded arithmetic cannot prove $\mathsf{NEXP} \subseteq \mathsf{P/poly}$ [ABM23]. Finally, recent work has shown that several complexity constructions can be "reversed" and are actually equivalent to some of the axioms used for bounded arithmetic [CLO24]. The present paper proves a new formalization in bounded arithmetic, namely of $\mathsf{L} = \mathsf{SL}$.

Logspace reasoning in bounded arithmetic. What is the power of reasoning needed to prove that $\mathsf{SL} = \mathsf{L}$? Is "logspace reasoning" enough? More formally, we ask for the weakest theory of bounded arithmetic that can formalize the proof of $\mathsf{L} = \mathsf{SL}$. It is natural to consider theories of bounded arithmetic that "capture" logspace reasoning.

There are several theories of bounded arithmetic for L; see the related work section below. Here we will use the theory VL of Cook and Nguyen [CN10]. This theory (like all other known theories for L) can prove the existence of second-order objects encoding logspace predicates, and can prove the totality of logspace functions. Conversely, these are the only predicates that can be proved to exist as second-order objects, and the only provably total functions of VL. In other words, VL can reason using logspace properties and only logspace properties. This means, in particular, that

> the *only* way that VL can prove $\mathsf{SL} = \mathsf{L}$ is to give, at least implicitly, a constructively defined logspace algorithm for SL-predicates.

An analogous situation is the case of VNL, a theory corresponding to nondeterministic logspace (NL), that can prove $\mathsf{NL} = \mathsf{coNL}$ [CK04; CN10]. It does so by formalizing explicitly the Immerman-Szelepcsényi algorithm.

There are theories of bounded arithmetic that correspond to SL in the same way as VL corresponds to L. The first one was defined by Kolokolova [Kol05], who gave a second-order theory of bounded arithmetic, V-SymKrom that corresponds to SL. A natural question left open by [Kol05] was whether V-SymKrom = VL. Cook and Nguyen reformulated V-SymKrom by giving a theory VSL based on an axiom for undirected graph reachability (based on Zambella [Zam97]). Their Open Problem IX.7.5 [CN10] asked whether VL proves $\mathsf{L} = \mathsf{SL}$ and whether VSL = VL. The present paper answers these questions affirmatively.

The difficulty of formalizing $\mathsf{SL} = \mathsf{L}$ in VL. The difficulties arise from the fact that any VL proof can talk only about logspace properties; it cannot talk about SL properties, such as reachability in undirected graphs until *after* $\mathsf{SL} = \mathsf{L}$ is established. Any VL proof of $\mathsf{SL} = \mathsf{L}$ must be sufficiently constructive to use only concepts which are definable in logspace. It cannot, for instance, use general exponential- or polynomial-time computations; furthermore, we cannot hope to directly use concepts such as determinants or eigenvalues which are only known to be in NC^2 and are conjecturally not logspace computable.

Fortunately, the arguments of Reingold [Rei08] and of Rozenman and Vadhan [RV05], albeit somewhat complex, are fairly straightforward and constructive. Reingold's proof used iteratively graph powering and a zig-zag/replacement product to transform an arbitrary connected graph into a good expander. His methods increased the number of vertices in the graph polynomially, but kept the graph constant degree. Rozenman and Vadhan [RV05] gave an alternate construction to prove that $\mathsf{L} = \mathsf{SL}$, using derandomized squaring (denoted by "Ⓢ") to transform any connected graph into a good expander; their construction kept the number of vertices in the graph fixed but increased the degree polynomially. As we shall explain below, from our point of view, the Rozenman-Vadhan construction is easier to work with.

The apparent difficulty is that both proofs of $\mathsf{SL} = \mathsf{L}$ use expander graphs, and properties of expander graphs are often proved using properties of eigenvalues and eigenvectors. On the other hand, Gaussian elimination and the determination of eigenvectors and eigenvalues are *not* known to be computable in logspace, and thus cannot be used by VL proofs.

Recently, Buss, Kabanets, Kolokolova, and Koucký [Bus+20] proved that the theory VNC^1, which has logical complexity corresponding to alternating logtime (uniform NC^1), can prove the existence of expander graphs without needing to reason about eigenvalues and eigenvectors. Since VNC^1 is a subtheory of VL, this provided hope that VL can prove that $\mathsf{L} = \mathsf{SL}$.

Our main result. The present paper succeeds in this direction and gives a precise characterization of the logical complexity of the proof that $\mathsf{L} = \mathsf{SL}$.

Theorem 1 (Main theorem, informal)**.** VL *proves* $\mathsf{L} = \mathsf{SL}$*. In addition,* VSL = VL.

We show that a variation of the Rozenman-Vadhan proof can be carried out in the second-order bounded arithmetic theory VL. Carrying out this proof requires making the proof more explicitly constructive; namely, the VL-proof argues by contradictions proving the existence of witnesses for existential statements. The VL proof (like the Rozenman-Vadhan proof) works with mixing ratios instead of second eigenvalues. In addition, the VL proof bypasses the use of the Cheeger inequality (which is not known to be provable in VL), and instead uses a special case of the Cheeger inequality due to Mihail [Mih89] that is known to be provable in VL [Bus+20]. We provide more details next.

Our techniques. The proof by Rozenman and Vadhan [RV05] works mainly with the concept of the mixing ratio (see Definition 7 below) that measures how fast a random walk on a given undirected regular graph G converges to the uniform distribution. Even though the mixing ratio happens to be equal to the second largest eigenvalue for the adjacency matrix of the graph G, this fact is *not* used for most of the proof in [RV05].

In particular, the analysis of the derandomized squaring operation on graphs is done purely in terms of the mixing ratios of the input graphs, without using the equivalence between the mixing ratios and second largest eignevalues. As we show, the basic linear algebra that is used in the analysis of derandomized squaring is simple enough to be proved in VL.

The only place where [RV05] seems to rely on the use of eignevalues in their proof is to show that every connected graph must have a nontrivial mixing ratio (at most $1 - 1/\mathsf{poly}(n, d)$, where n is the number of vertices, and d the degree of a given graph). Such a bound on the mixing ratio of a connected graph can be easily deduced by Cheeger's Inequality that relates the mixing ratio to the edge expansion of a graph. It is elemenentary to show (also in VL) that any connected graph has nontrivial edge expansion. Thus, if VL could prove Cheeger's inequality, we could prove this step of the Rozenman-Vadhan argument in VL as well.

Unfortunately, it is not known if VL can prove Cheeger's inequality in general. However, a version of Cheeger's inequality (for undirected regular graphs with enough self-loops around each vertex) can be proved in VL! This was done in [Bus+20], based on [Mih89]; the approach in [Bus+20] was to use the concept of *edge expansion* to analyze graph operations (like replacement product, powering, and tensoring), and the results of [Mih89] were used to relate edge expansion and mixing ratio, via a version of Cheeger's inequality. This version of the Cheeger-Mihail inequality can be used to get the required bound on the mixing ratio of any given regular graph, placing this part of the Rozenman-Vadhan proof in VL.

But we are not done yet. The Rozenman-Vadhan argument also needs a sequence of explict expander graphs, of growing size and degree, to use in the successive applications of the derandomized squaring operation. We need such expanders graphs to be constructible in VL. Luckily, we can again use the results of [Bus+20] to argue that the required expander graphs can be constructed (and their expansion properties proved) in VL.

Finally, we need to show in VL how to use the Rozenman-Vadhan transformation of a given input graph G into an expander $\tilde{G}$ in order to solve the connectivity problem for G. Given a simple recursive construction of $\tilde{G}$ from G (obtained by repeatedly applying the derandomized squaring to the previous graph, using an appropriate expander as an auxiliary graph), we can show that $\tilde{G}$ is definable from G in VL. This allows us to complete the proof of $\mathsf{SL} = \mathsf{L}$ in VL.

We note that it may be possible to formalize Reingold's proof of $\mathsf{SL} = \mathsf{L}$ in VL as well, with some extra work. The original proof in [Rei05] relied on the complicated analysis of the zig-zag product from the famous paper by Reingold, Vadhan, and Wigderson [RVW02], which used eigenvalues. However, based on [RV05], Reingold, Trevisan and Vadhan [RTV06] later gave a simpler analysis of the zig-zag product in terms of the mixing ratios (without using eigenvalues), which is sufficient for Reingold's proof of $\mathsf{SL} = \mathsf{L}$. This simpler analysis appears to be formalizable in VL (as it is very similar to the Rozenman-Vadhan analysis of derandomized squaring, which we show in this paper to be formalizable in VL). The other ingredient in Reingold's proof, graph powering, can be easily analyzed in terms of mixing ratios as well. As above, we can use the Cheeger-Mihail inequality to show that any connected regular graph has a nontrivial mixing ratio, to start off Reingold's logspace transformation of a graph G into an expander G'. A somewhat tricky part in Reingold's proof is to argue that G' can be used to answer the connectivity question for G, by a *logspace* algorithm. This part seems more complicated that the corresponding part in the Rozenman-Vadhan proof of $\mathsf{SL} = \mathsf{L}$, and may be challenging to implement in VL, but probably could be. However, we do not pursue this approach in the present paper.

Related work. Several early authors discussed the undirected graph reachability problem, including [JLL76; Sch78; Ale+79], but the first systematic study of symmetric computation, including the definition of SL, was due to Lewis and Papadimitriou [LP82] in 1982. Savitch's theorem implies that SL is in $\mathsf{SPACE}(\log^2 n)$. Aleliunas et al. [Ale+79] and Borodin [Bor+89] gave *randomized* logspace algorithms for USTCON. Nisan, Szemerédi, and Wigderson [NSW92] gave a deterministic $\mathsf{SPACE}(\log^{1.5} n)$ algorithm; Armoni et al. [Arm+00] improved this to $\mathsf{SPACE}(\log^{4/3} n)$ and Trifonov [Tri08] even more dramatically to $\mathsf{SPACE}(\log n \log\log n)$.

There have been several bounded arithmetic theories proposed for logspace and symmetric logspace. Clote and Takeuti [CT92] give the first theory for logspace using a second-order theory $\mathrm{S}^{\log}$ of bounded arithmetic. Zambella [Zam97] gave a second, and more elegant, theory of bounded arithmetic, based on a second-order theory of bounded arithmetic including the Σ_0^B-rec axioms; the Σ_0^B-rec axioms state that there are second-order objects encoding polynomially long paths in directed graphs of out-degree one. Cook and Nguyen [CN10] defined an equivalent second-order theory VL for logspace computation with a reformulated version of the Σ_0^B-rec axioms.

Derandomized squaring has attracted renewed attention recently in the context of space-bounded derandomization; see, e.g., [Mur+21; Ahm+20; Ahm+23; Che+23; Coh+25].

Remainder of the paper. Section 2 introduces the needed preliminaries for directed and undirected graphs, adjacency matrices, vectors and tensors, edge expansion, and derandomized squaring. Section 3 gives the details of the Rozenman-Vadhan proof of $\mathsf{L} = \mathsf{SL}$, both in its orginal form and with a second version of the proof that will later be shown to be formalizable in VL. Sections 2 and 3 can be read independently of the rest of the paper for a self-contained exposition of the proof of $\mathsf{L} = \mathsf{SL}$ that does not require any knowledge of bounded arithmetic. Section 4 starts with preliminaries for the bounded arithmetic theory VL, and reviews the needed results of [Bus+20] about edge expanders in VNC^1, including a "Cheeger-Mihail lemma" that can be formalized in VNC^1 in lieu of the full Cheeger lemma. It then sketches how to formalize the proof of $\mathsf{L} = \mathsf{SL}$ in VL. It follows that VL and VSL are equal (Theorem 31). Section 5 proves that the Sedrakyan lemma and one direction of the Cheeger Inequality are provable in VNC^1 and thereby in VL. The former is needed for the VL proof described in Section 4.

2 Preliminaries

2.1 Graphs and expansion

A good source on expander graphs is [HLW06]. This paper will consider both directed and undirected graphs. The statement of $\mathsf{L} = \mathsf{SL}$ uses undirected graphs, and the expander graph constructions of [Bus+20] are stated in terms of undirected graphs. However, following Rozenman-Vadhan [RV05], our proofs depend on directed graphs.

An undirected graph is represented as $G = (V, E)$ where V is a set of vertices, and E is a multiset of *edges* $\{u, v\}$ with $u, v \in V$. It is allowed for G to have multiple ("parallel") edges between u and v; i.e., E may contain multiple copies of $\{u, v\}$. Self-loops are allowed; namely, it is permitted that $u = v$. The degree of a vertex $v \in G$ is the number of incident edges. (A self-loop counts as a single incident edge.) A directed graph is *k-regular* if each vertex has degree k.

A directed graph $G = (V, E)$ has E as a multiset of directed edges $\langle u, v\rangle$ where $u, v \in G$. It is again permitted that a directed graph may contain self-loops as well as multiple directed edges from u to v. A directed graph G is *k-inregular*, respectively *k-outregular*, if each vertex has indegree (resp., outdegree) equal to k. The graph is *k-regular* if it is both k-inregular and k-outregular.

An undirected graph $G = (V, E)$ can be converted into a directed graph $G' = (V, E')$ by replacing each non-self-loop edge $\{u, v\}$ with the pair of directed edges $\langle u, v\rangle$ and $\langle v, u\rangle$ and replacing each self-loop $\{u, u\}$ with a directed self-loop $\langle u, u\rangle$. If G is k-regular, then so is G'.

We define edge expansion for both undirected and directed graphs $G = (V, E)$. We say there is an edge from u to v in G provided that E contains $\{u, v\}$ if G is undirected or that E contains $\langle u, v\rangle$ if G is directed. For $U \subseteq V$, let $\overline{U}$ be $V \setminus U$. Then $E(U, \overline{U})$ is the multiset of edges from U to $\overline{U}$, namely the edges from a vertex $u \in U$ to a vertex $v \notin U$.

Definition 2 (Edge expansion)**.** Let G be a a d-regular graph on n vertices, either directed or undirected. The *edge expansion* of G is defined as:

$$\min_{\substack{\emptyset \neq U \subset V \\ |U| \leq n/2}} \frac{|E(U, \overline{U})|}{d \cdot |U|} \;=\; \min_{\emptyset \neq U \subsetneq V} \frac{|E(U, \overline{U}|)}{d \cdot \min\{|U|, |\overline{U}|\}} \tag{1}$$

Note that if an undirected graph with edge expansion ϵ is converted to a directed graph, it still has edge expansion ϵ. We often omit stating whether a graph is directed or undirected, when the results hold in both cases. A directed graph is connected provided any two vertices are connected by a directed path.

The developments in Sections 1 and 3.2 follow the treatment in [RV05] closely. We will take care to make the details of the proofs sufficiently clear in order to later show how they can be formalized in VL.

Theorem 3. *Let G be a connected d-regular graph on n vertices. Then the edge expansion of G is at least $2/(dn)$.*

Proof. This follows immediately from the definitions, since $E(U, \overline{U})$ must be nonempty. □

Let $G = (V, E)$ be a d-regular graph on $n = |V|$ many vertices. When convenient, the vertices are identified with the integers $[n] = \{1, \ldots, n\}$. The (normalized) *adjacency matrix* for G is the $n \times n$ matrix M with entries $M_{i,j}$ equal to the number of edges in E from vertex j to vertex i divided by d. All entries in M are non-negative, and since G is d-regular, each row sum and column sum of G is equal to 1. The adjacency matrix can be viewed as a transition matrix for a random walk in the graph. Namely, if a n-vector $\vec{v}$ represents a probability distribution on the vertices V, then $M\vec{v}$ gives the probability distribution obtained after one step of a random walk starting from the distribution $\vec{v}$.

We use the term "adjacency matrix" for the just-defined normalized version of the adjacency matrix. The *unnormalized adjacency matrix* for d-regular graph G is just $d \cdot M$: the (i, j) entry in the unnormalized adjacency matrix is the number of edges from j to i.

For $\vec{v} = \langle v_1, \ldots, v_n\rangle$ a vector, $\|\vec{v}\|$ denotes the 2-norm $\left(\sum_i v_i^2\right)^{1/2}$. We use $\langle \vec{v}, \vec{w}\rangle$ for the inner product of two vectors, namely $\sum_i v_i w_i$. We write $\vec{v} \perp \vec{w}$ to denote that $\vec{v}$ and $\vec{w}$ are orthogonal, i.e., that $\langle \vec{v}, \vec{w} \rangle = 0$. We call $\vec{v}$ a *(probability) distribution* if $\sum_i v_i = 1$ and each $v_i \geq 0$. The vector $\vec{1}$ is the n-vector $\langle 1/n, \ldots 1/n \rangle$ corresponding to to the uniform distribution on the vertices V. Note that $\|\vec{1}\| = 1/\sqrt{n}$. The zero vector is denoted $\vec{0}$.

The next theorem follows immediately from the fact that the adjacency matrix has non-negative entries and all of M's row and column sums equal 1.

Theorem 4. *Let M be the adjacency matrix of a regular graph.*

(a) *If $\vec{v}$ is a probability distribution, then so is $M\vec{v}$.*

(b) $M\vec{1} = \vec{1}$.

(c) *If $\vec{v} \perp \vec{1}$, then also $M\vec{v} \perp \vec{1}$.*

Lemma 5 (Sedrakyan's Lemma)**.** *Suppose $u_i, v_i \in \mathbb{R}$ and $v_i > 0$ for $1 \leq i \leq n$. Then*

$$\sum_i \frac{u_i^2}{v_i} \;\geq\; \frac{\left(\sum_i u_i\right)^2}{\sum_i v_i}.$$

Proof. This follows from the Cauchy-Schwarz inequality $\langle \vec{u}', \vec{v}' \rangle^2 \leq \|\vec{u}'\|^2 \cdot \|\vec{v}'\|^2$ for the vectors $\vec{u}'$ and $\vec{v}'$ with entries $u_i' = u_i/\sqrt{v_i}$ and $v_i' = \sqrt{v_i}$. □

The *norm* of a matrix M, denoted $\|M\|$, is the least α such that $\|M\vec{v}\| \leq \alpha\|\vec{v}\|$ for all $\vec{v}$.

Theorem 6. *Let M be the adjacency matrix of a regular graph. Then $\|M\| = 1$.*

Proof. By part (b) of Theorem 4, it suffices to prove that $\|M\vec{v}\| \leq \|\vec{v}\|$ if $\vec{v} \perp \vec{1}$. So suppose $\vec{v} \perp \vec{1}$. Then

$$\begin{aligned}
\|M\vec{v}\|^2 &= \textstyle\sum_i \left(\sum_j M_{i,j} v_j\right)^2 \\
&\leq \textstyle\sum_i \sum_{j:\, M_{i,j} \neq 0} \dfrac{(M_{i,j} v_j)^2}{M_{i,j}} && \text{(By Sedrakyan's lemma since } \textstyle\sum_j M_{i,j} = 1) \\
&= \textstyle\sum_i \sum_j M_{i,j} v_j^2 \\
&= \textstyle\sum_j \left(\sum_i M_{i,j}\right) v_j^2 \;=\; \sum_j v_j^2 \;=\; \|\vec{v}\|^2. && \square
\end{aligned}$$

Definition 7 (Mixing ratio)**.** Let G be a k-regular graph (directed or undirected) with adjacency matrix M. Let $\eta \geq 0$. The graph G has *mixing ratio* η provided that

$$\|M\vec{v}\| \;\leq \eta \cdot \|\vec{v}\|$$

holds for all $\vec{v} \perp \vec{1}$. The minimum such η is called *the mixing ratio* of G.

When we say "G has mixing ratio η", we mean that the mixing ratio of G is $\leq \eta$.

By Theorem 6, the mixing ratio η is ≤ 1. It is easy to see that the mixing ratio of G is equal to the second largest, in absolute value, eigenvalue of its adjacency matrix M. However, Definition 7 defines the mixing ratio without referring to eigenvalues or eigenvectors. This has the advantage that the bounded arithmetic theory VL can work with the concept of mixing ratio, even though VL is not known to be able to prove properties about eigenvalues and eigenvectors.

Definition 8. A graph G is a (n, d, η)-graph if it has n vertices, is d-regular, and has mixing ratio (at most) η.

We let J_n denote the $n \times n$ matrix with all entries equal to $1/n$. Note that J_n is the adjacency matrix for the complete graph on n vertices; equivalently, J_n is the transition matrix for a random walk on n vertices (on the complete graph).

Theorem 9. *Let M be the adjacency matrix of an (n, d, η)-graph with $0 < \eta \leq 1$. Then*

(a) *[RV05] M is equal to $(1-\eta)J_n + \eta C$ where $\|C\| \leq 1$.*

(b) *M is equal to $J_n + \eta D$ where $\|D\| \leq 1$ and all of the row and column sums of D are equal to zero.*

(c) $\|M\| = \|J_n\| = \|J_n + D\| = 1$.

Proof. We let $C = (M - (1-\eta)J_n)/\eta$. By Theorem 4, $M\vec{1} = J_n\vec{1} = \vec{1}$. Hence $C\vec{1} = \vec{1}$. Now suppose $\vec{v} \perp \vec{1}$, so $J_n\vec{v} = \vec{0}$ and therefore $C\vec{v} = M\vec{v}/\eta$. By hypothesis, $\|M\vec{v}\| \leq \eta\|\vec{v}\|$ and by Theorem 4, $M\vec{v} \perp \vec{1}$. It follows that $C\vec{v} \perp \vec{1}$ and $\|C\vec{v}\| \leq \|\vec{v}\|$. That proves (a).

Now let $D = (M - J_n)/\eta = C - J_n$. From the argument for part (a), we have that $D\vec{1} = \vec{0}$ and that for all $\vec{v} \perp \vec{1}$, we have $D\vec{v} \perp \vec{1}$ and $\|D\vec{v}\| \leq \|\vec{v}\|$. Parts (b) and (c) follow. □

Theorem 10. *Let G be a connected, d-regular, undirected graph on n vertices. The mixing ratio η of G is at most $1 - 2/(dn)^2$.*

Proof. By Theorem 3, the edge expansion of G is at least $2/(dn)$. The well-known Cheeger inequality, which is stated below as Theorem 24, immediately implies that $1 - \eta \geq 2/(dn)^2$. □

Theorem 11. *Let G be a connected, d-regular, directed graph on n vertices with a self-loop at each vertex. The mixing ratio η of G is at most $1 - 1/(d^4n^2)$.*

Proof. Let M be the adjacency matrix for the directed graph G. Form the undirected graph H that has adjacency matrix $M^{\mathsf{T}}M$ by letting the edges of H be pairs $\{x, y\}$ such that there is a vertex u such that (x, u) and (u, y) are (directed) edges in M. We allow multiedges and self-loops in H; the multiplicity of an edge $\{x, y\}$ in H depends on the number of pairs of edges $\langle x, u\rangle$ and $\langle u, y\rangle$ in G. In particular, H is d^2-regular. Since G has self-loops, every edge (x, y) in G gives rise to the edge $\{x, y\}$ in H. Therefore, H is connected.

Suppose $\|\vec{v}\| = 1$ and $\vec{v} \perp \vec{1}$. We wish to show $\|M\vec{v}\| \leq 1 - 1/(d^4n^2)$. By Theorem 10, H has mixing ratio $\leq 1 - 2/(d^4n^2)$. Thus, $\|M^{\mathsf{T}}M\vec{v}\| \leq 1 - 2/(d^4n^2)$. Therefore

$$\begin{aligned}
\|M\vec{v}\|^2 &= \langle M\vec{v}, M\vec{v}\rangle \\
&= \langle \vec{v}, M^{\mathsf{T}}M\vec{v}\rangle \\
&\leq \|M^{\mathsf{T}}M\vec{v}\| && \text{(by Cauchy-Schwarz)} \\
&\leq 1 - 2/(d^4n^2) \\
&\leq (1 - 1/(d^4n^2))^2.
\end{aligned}$$

Thus $\|M\vec{v}\| \leq 1 - 1/(d^4n^2)$ as desired. □

Rozenman and Vadhan [RV05] prove slightly stronger versions of Theorems 10 and 11 with $1-2/(dn)^2$ and $1-1/(d^4n^2)$ replaced with $1-1/(dn^2)$ and $1-1/(2d^2n^2)$.

Unfortunately, it is open whether the Cheeger inequality and thus Theorems 10 and 11 can be proved in the theory VL. However, there is a weaker form of the Cheeger lemma with a constructive proof by Mihail [Mih89] that can be used instead, and this Cheeger-Mihail theorem is known to be provable in VNC^1 [Bus+20]. The Cheeger-Mihail theorem states that the Cheeger inequality holds for an undirected regular graph of even degree d provided that each vertex has at least $d/2$ self-loops. The proof of Theorem 11 can thus be formalized in VNC^1 (and hence in VL) provided that the graph H has sufficiently many self-loops at each vertex. For more details, see Theorems 33 and 34, in Section 4 on formalizations in VL.

2.2 Derandomized Squaring

We now review the definition of derandomized squaring, $X \circledS G$.

Definition 12 (Proper labeling)**.** Let G be a d-regular graph. Suppose each edge in G has been assigned a member of $[d]$ as a label.

If G is undirected, this is called a *proper labeling* provided that, for each vertex of G, the d incident edges have distinct labels.

If G is directed, this is called a *proper labeling* provided that, for each vertex, the d incoming edges have distinct labels, and the d outgoing edges have distinct labels.[1]

Note that a proper labeling of an undirected d-regular graph immediately gives a proper labeling of the corresponding directed d-regular graph.

Definition 13. Suppose $G=(V,E)$ is a properly labeled d-regular (directed) graph, with edge labels taken from $[d]$. For v a vertex in V and $i \in [d]$ an edge label, we write $v[i]$ to denote the vertex w that is reached by taking a single step in G from vertex v along the outgoing edge labeled i.

Now suppose that X and G are properly labeled, regular, directed graphs and that X has N vertices and is K-regular and that G has K vertices and is D-regular. Without loss of generality, the vertex set of X is $[N]$ and the vertex set of G is $[K]$.

The squared graph X^2 is the graph on the same set of vertices $[N]$ and degree K^2. It has an edge between vertices v and u iff u can be reached from v in two steps, i.e., if there exist $1 \le i, j \le K$ such that $u = w[j]$ for $w = v[i]$. In contrast, the derandomized square of X, using an auxiliary graph G, contains an edge between vertices v and u only if u can be reached from v in two steps $1 \le i, j \le K$, where the second step j is computed from the first step i using G. Namely, vertex j must be a neighbor of vertex i in G. (If G were a complete graph on $[K]$, we would end up with the usual squared graph X^2. We get the savings, however, if G has degree $D < K$.) More formally, we have the following definition.

Definition 14 (Derandomized squaring)**.** The *derandomized squaring product* of X and G is denoted $X \circledS G$; it is a KD-regular directed graph on N vertices (it has the same set of vertices as X). The edge labels of X are taken from $[K]$. The edge labels of G are likewise taken from $[D]$. The edge labels of $X \circledS G$ will be written as pairs (i,j) where $i \in [K]$ and $j \in [D]$; in other words, i is an edge label for X and j is an edge label for G. We also view i as a vertex in G.

[1] Our "proper labeling" is the same as what Rozenman and Vadhan [RV05] call a "consistent labeling".

The edges of $X \circledS G$ are defined as follows. Let $v \in [K]$ be a vertex of $X \circledS G$ (and a vertex of X) and let (i, j) be an edge label for $X \circledS G$. Working in X, let $w = v[i]$, namely the vertex of X reached by following edge i from v. Then, working in G, let $k = i[j]$, namely the vertex in G obtained by following edge j from i. Then, working in X again, let $u = w[k]$, namely the vertex reached by following edge k from w. This u is a vertex in $X \circledS G$; by definition, $X \circledS G$ has an edge from v to u with edge label (i, j). As a shorthand notation, we can write $u = (v[i])[i[j]]$.

Theorem 15 ([RV05])**.** *Suppose X and G are properly labeled, regular, directed graphs as above. Then $X \circledS G$ is is a properly labeled, regular, directed graph.*

Proof. The proof of Theorem 15 is completely elementary. By construction, $X \circledS G$ is KD-outregular and the outgoing edges of any vertex in $X \circledS G$ have distinct labels. Conversely, consider whether a vertex u in $X \circledS G$ has an incoming edge with the label (i, j). Since X is properly labeled, there are unique vertices w and u of X such that $u = w[i[j]]$, and $w = v[i]$. Therefore, there is exactly one incoming edge to u in $X \circledS G$ with label (i, j). It follows that $X \circledS G$ is KD-inregular and properly labeled. □

2.3 Tensors

Let U and V be (real) vector spaces, of finite dimension m and n respectively. Let $\vec{u} = \langle u_1, \ldots, u_m \rangle \in U$ and $\vec{v} = \langle v_1, \ldots, v_n \rangle \in V$. We write $\vec{u} \otimes \vec{v}$ to denote the rank one tensor product of $\vec{u}$ and $\vec{v}$; this is by definition equal to the $m \times n$ outer product matrix $\vec{u}(\vec{v}^T)$. Here $\vec{v}^T$ is the transpose of $\vec{v}$: vectors are column vectors, so $\vec{v}^T$ is a row vector.

More generally, any $m \times n$ matrix represents a tensor $\mathbf{w}$. (We use boldface to represent tensors.) For $i \in [m]$ and $j \in [n]$, we let $\mathbf{w}_{i,j}$ denote the (i, j)-entry of $\mathbf{w}$. Alternately, a tensor can viewed as a mn-vector; however, usually the matrix representation is more useful. In either representation, the tensors over U and V form an mn-dimensional vector space.

A linear map on tensors can be represented by an $mn \times mn$ matrix M. The entries of M are denoted $M_{(i,j),(i',j')}$ for $i, i' \in [m]$ and $j, j' \in [n]$. Then $M\mathbf{w}$ is the tensor with entries $(M\mathbf{w})_{i,j} = \sum_{i',j'} M_{(i,j),(i',j')}\mathbf{w}_{i',j'}$. The magnitude $\|\mathbf{w}\|$ of $\mathbf{w}$ is the magnitude of the mn-vector representation of $\mathbf{w}$. It is easy to check that $\|\vec{u} \otimes \vec{v}\|$ is equal to $\|\vec{u}\| \cdot \|\vec{v}\|$. The norm $\|M\|$ of a linear map M on tensors is the same as the matrix 2-norm of M viewed as an mn-matrix. Thus $\|M\|$ equal to the least ν such that $\|M\mathbf{w}\| \le \nu\|\mathbf{w}\|$ for all $\mathbf{w}$.

Suppose now that N and N' are $m \times m$ and $n \times n$ matrices, respectively. Their tensor product $N \otimes N'$ is the tensor map with matrix representation given by M with $M_{(i,j),(i',j')} = N_{i,i'}N'_{j,j'}$. For rank one tensors N and N', straightforward computation shows that the tensor product $N \otimes N'$ acts on $\vec{u} \otimes \vec{v}$ by sending it to $N\vec{u} \otimes N'\vec{v}$. In addition, $\|N \otimes N'\|$ is equal to $\|N\| \cdot \|N'\|$.

We also work with mappings between vectors and tensors. The first is the projection operation P that projects away the second component of tensors. More precisely, $P\mathbf{w}$ is the m-vector $\vec{v}$ such that $\vec{v}_i = \sum_j \mathbf{w}_{i,j}$. The operator P can be expressed as the $m \times mn$-matrix with entries $P_{i',(i,j)} = \delta_{i,i'}$ where $\delta_{i,i'}$ equals 1 if $i = i'$ and equals 0 otherwise. (Of course, P depends on m and n, but we suppress this in the notation.) It is easy to check that $\|P\| = \sqrt{n}$.

Conversely, the lifting operation L is defined by letting $L\vec{u}$ equal the tensor product $\vec{u} \otimes \langle 1/n, \ldots, 1/n \rangle$. The lifting operation L can be presented by the $mn \times n$-matrix with all entries equal to $L_{(i,j),i'} = \delta_{i,i'}/n$. We have $\|L\| = 1/\sqrt{n}$, and in fact $\|L\vec{u}\| = \|u\|/\sqrt{n}$ for all u. The composition $P \circ L$ is the identity transformation, and of course has magnitude $\|P \circ L\| = 1$.

Recall that J_n is the matrix with all entries equal to $1/n$. It is easy to check that PJ_nL is the identity matrix. For the matrix D of Theorem 9, in which row and column sums are equal to zero, PDL is the zero matrix.

3 Expansion for $\mathsf{L} = \mathsf{SL}$

This section details the Rozenman and Vadhan proof of $\mathsf{L} = \mathsf{SL}$.

3.1 One application of derandomized squaring

The core construction of Rozenman and Vadhan's proof that $\mathsf{L} = \mathsf{SL}$ required showing bounds on the mixing ratio of derandomized squaring. Their bound is re-proved in the next theorem.

Theorem 16 ([RV05]). *Suppose X is a properly labeled, K-regular, directed graph with vertices $[N]$. Let G be a properly labeled, directed (K, D, μ)-graph. Thus $X \circledS G$ is a properly labeled, directed, KD-regular graph with vertices $[N]$. Let $0 < \lambda < 1$.*

(a) *If X has mixing ratio λ, then $X \circledS G$ has mixing ratio at most $f(\lambda, \mu)$ where*

$$f(\lambda, \mu) \;=\; \mu + (1 - \mu)\lambda^2. \tag{2}$$

(b) *In particular, let A and M be the adjacency matrices of X and $X \circledS G$, respectively, and suppose there is an N-vector $\vec{v}$ such that $\vec{v} \perp \vec{1}$ such that $\|M\vec{v}\| > f(\lambda, \mu)\|\vec{v}\|$. Then there is an N-vector $\vec{u}$ such that $\vec{u} \perp \vec{1}$ and $\|A\vec{u}\| > \lambda\|\vec{u}\|$. In fact, this will hold for at least one of $\vec{u} = \vec{v}$ or $\vec{u} = A\vec{v}$.*

Part (a) can be more succinctly stated as saying that if X is an (N, K, λ)-graph and G is a (K, D, μ)-graph, then $X \circledS G$ is an $(N, KD, f(\lambda, \mu))$-graph. The theorem is stated in a roundabout way, however, so we can better discuss its provability in the theory VL.

Proof. Part (a) follows from (b), so we prove (b). The adjacency matrix M can be viewed as computing a single random step in $X \circledS G$. We view M as acting on an N-vector $\vec{v}$ representing a probability distribution on vertices $[N]$. The ℓ-th entry $(\vec{v})_\ell$ of $\vec{v}$ gives the probability of being at vertex ℓ. Following the proof of [RV05], we shall describe M as the transition matrix for a five-step random process applied to a vertex $v \in [N]$ where v is chosen at random according to $\vec{v}$.

The five-step random process starts at a vertex v of X and ends at a vertex w of X; note that $v, w \in [N]$. As is described below, the s-th intermediate step (for $s = 1, 2, 3, 4$) of the random process transitions to a state of the form $\langle u, i\rangle$, where $u \in [N]$ and $i \in [K]$. We interpret u as a vertex of X and i as a vertex of G.

Suppose the input v to the random process is chosen according to a fixed probability distribution $\vec{v}$ on $[N]$. For $s = 1, 2, 3, 4$, let $\mathbf{w}_s$ be the tensor that gives the probability distribution on the result $\langle u, i\rangle$ of the s-th step of the random process; that is, $(\mathbf{w}_s)_{u,i}$ is the probability of being in the state $\langle u, i\rangle$ after the s-th step. Of course, $\mathbf{w}_s = M_s\vec{v}$ for some $NK \times N$ matrix M_s.

1. Choose a random vertex $v \in [N]$ of G according to the probability distribution $\vec{v}$. Choose $i \in K$ at uniformly at random and go to the state represented the pair $\langle v, i\rangle$. This corresponds to picking a random outgoing edge i of v. Note i is also a vertex of G.

   The transition matrix for this step is L; namely, this step is represented by the lifting operation $\vec{v} \mapsto L\vec{v}$, so $\mathbf{w}_1$ equals the NK-vector $L\vec{v}$.

2. Transition deterministically to the state represented by $\langle v[i], i\rangle$. This corresponds to following the edge labeled i in X.

   The transition matrix for this step is the $NK \times NK$-matrix $\tilde{A}$ defined with $\tilde{A}_{(u,i),(u',i)} = 1$ if there is an edge in X from u to u' labeled i and with all other entries of $\tilde{A}$ equal to zero. Since X is K-regular and properly labeled, $\tilde{A}$ is a permutation matrix. (This corresponds to the fact that this is a deterministic, reversible step.) In fact, when $\tilde{A}$ is viewed as acting on a NK matrix, multiplication by $\tilde{A}$ permutes entries within each column of the NK matrix. Then $\mathbf{w}_2 = \tilde{A}\mathbf{w}_1$.

3. Choose a random neighbor k of i in G, and transition to the state given by $\langle v[i], k\rangle$. In other words, choose a random $j \in [D]$ and transition to $\langle v[i], i[j]\rangle$.

   Since the index i was chosen uniformly at random, $\mathbf{w}_2$ has the form $\vec{z}\otimes\vec{1}$ for some $\vec{z}$. Therefore, the transition matrix for this step is equal to $\tilde{B} := I_N \otimes B$, where I_N is the $N \times N$ identity matrix and B is the $K \times K$ transition matrix for G. We have $\mathbf{w}_3 = \tilde{B}\mathbf{w}_2$.

4. Deterministically transition to the pair $\langle v[i][k], k\rangle$. This corresponds to following the edge in X labeled k from the vertex $v[i]$ to reach the vertex $v[i][k]$.

   The transition matrix for this step is the same matrix $\tilde{A}$ that was used for step 2. We have $\mathbf{w}_4 = \tilde{A}\mathbf{w}_3$.

5. Deterministically go to state $v[i][k]$ (discarding the second component of the state).

   The transition matrix for this step is the projection operator P. We let $\vec{w}$ be the N-vector $\vec{w} = P\mathbf{w}_4$; this makes $\vec{w}$ the probability distribution on the vertices of $[N]$ at the end of the five step random process.

Putting this all together shows that the transition matrix M for $X \circledS G$ is equal to

$$M \;=\; P\tilde{A}(I_N \otimes B)\tilde{A}L. \tag{3}$$

By Theorem 9, B is equal to $(1-\mu)J_K + \mu C$ where $\|C\| \le 1$. Thus,

$$M \;=\; (1-\mu)P\tilde{A}(I_N \otimes J_K)\tilde{A}L + \mu P\tilde{A}(I_N \otimes C)\tilde{A}L.$$

We have $I_N \otimes J_K$ is equal to LP. And $P\tilde{A}L$ is equal to A, the transition matrix for X. Therefore,

$$\begin{aligned} M &= (1-\mu)P\tilde{A}LP\tilde{A}L + \mu P\tilde{A}(I_N \otimes C)\tilde{A}L \\ &= (1-\mu)(P\tilde{A}L)^2 + \mu P\tilde{A}(I_N \otimes C)\tilde{A}L \\ &= (1-\mu)A^2 + \mu P\tilde{A}(I_N \otimes C)\tilde{A}L. \end{aligned} \tag{4}$$

Recall that $\|P\| = \sqrt{K}$, and $\|L\| = 1/\sqrt{K}$. Also, $\|I_N \otimes C\| \le 1$ since $\|C\| \le 1$. Finally, $\|\tilde{A}\| = 1$ since $\tilde{A}$ is a permutation matrix. It follows that $\|P\tilde{A}(I_N \otimes C)\tilde{A}L\| \le 1$.

We can now prove part (b) of the theorem. Suppose M has mixing ratio $> f(\mu,\lambda)$, so there is a N-vector $\vec{v}$ such that $\vec{v} \perp \vec{1}$ and

$$\|M\vec{v}\| > (\mu + (1-\mu)\lambda^2)\|\vec{v}\|.$$

Therefore, by (4) and since $\|P\tilde{A}(I_N \otimes C)\tilde{A}L\| \le 1$,

$$(1-\mu)\|A^2(\vec{v})\| + \mu\|\vec{v}\| > (\mu + (1-\mu)\lambda^2)\|\vec{v}\|, \tag{5}$$

whence $\|A^2\vec{v}\| > \lambda^2\|\vec{v}\|$. Thus $\|A\vec{u}\| > \lambda\|\vec{u}\|$ for $\vec{u}$ equal to (at least) one of $\vec{v}$ and $A\vec{v}$. In either case, $\vec{u} \perp \vec{1}$, either since $\vec{v} \perp \vec{1}$ or, if $\vec{u} = A\vec{v}$, by Theorem 4(c). □

The proof that $\mathsf{L} = \mathsf{SL}$ will iterate the construction of Theorem 16. Namely, it starts with a graph X with adjacency matrix M_X that has mixing ratio at most $\lambda_X = 1 - 2/(dn)$ and applies derandomized squaring $k = O(\log n)$ times to form a graph

$$Z \;=\; ((\cdots(X \circledS G_1) \circledS G_2)\cdots) \circledS G_k.$$

It is then argued that if the G_i's have appropriate mixing ratios, then the adjacency matrix M_Z of Z has small mixing ratio λ_Y, and hence Z has good expansion. Specifically, it is proved if there is an N-vector $v \perp \vec{1}$ so that $\|M_Z\vec{v}\| > \lambda_Z\|\vec{v}\|$, then there is an N-vector $\vec{u} \perp \vec{1}$ so that $\|M_X\vec{u}\| > \lambda_X\|\vec{u}\|$.

The proof method of Theorem 16 is sufficiently constructive that it will allow the theory VL to prove expansion properties for iterated applications of derandomized squaring. This is shown in Section 4. First, however, we give the rest of the proof that $\mathsf{L} = \mathsf{SL}$.

3.2 Iterating derandomized squaring and proving $\mathsf{L} = \mathsf{SL}$

Rozenman-Vadhan's proof that $\mathsf{L} = \mathsf{SL}$ proceeds in three stages. The first (easy) stage starts with an undirected graph Y, not necessarily regular, and produces a directed graph X which is 4-regular, has a loop at each vertex and is properly labeled, such that the reachability problem for Y is easily reducible to the reachability problem for X. The construction replaces each degree d node v in Y with d-many nodes denoted $\langle v, i\rangle$ for $0 \le i < d$. The four outgoing edges for the node $\langle v, i\rangle$ in X and their labels are:

- From $\langle v, i\rangle$ to $\langle v, i{-}1 \bmod d\rangle$ with label 0.
- From $\langle v, i\rangle$ to $\langle v, i{+}1 \bmod d\rangle$ with label 1.
- From $\langle v, i\rangle$ to $\langle w, j\rangle$ with label 2, where w is the i-th neighbor of v and v is the j-th neighbor of w.
- From $\langle v, i\rangle$ to itself (a self-loop) with label 3.

Let N be the number of vertices in X.

The second stage starts with the 4-regular directed graph X and repeatedly augments it by derandomized squaring with graphs G_i. The G_i's are defined in terms of graphs H_i which have the following properties, for some constant $Q = 4^q$:

- H_i is a consistently labeled $(Q^i, Q, 1/100)$-graph.
- The edge relation in H_i is computable uniformly in simultaneous logspace and polylogarithmic time in the size of H_i. That is, the function $(v, x) \mapsto v[x]$, for v a vertex and x an edge label is computable in simultaneous space $O(i)$ and time poly(i). (Note that $O(i)$ many bits are needed to specify v and x.)

i	Number of vertices of X_i	Degree of X_i	Number of vertices of G_i	Degree of G_i	Upper bound on $\lambda(G_i)$
1	N	$Q = 4^q$	Q	Q	1/100
2	N	Q^2	Q^2	Q	1/100
3	N	Q^3	Q^3	Q	1/100
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
m_0	N	Q^{m_0}	Q^{m_0}	Q	1/100
$m_0 + 1$	N	Q^{m_0+1}	Q^{m_0+1}	Q^2	$(1/100)^2$
$m_0 + 2$	N	Q^{m_0+3}	Q^{m_0+3}	Q^4	$(1/100)^4$
$m_0 + 3$	N	Q^{m_0+7}	Q^{m_0+7}	Q^8	$(1/100)^8$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$m_0 + \ell$	N	$Q^{m_0+2^\ell-1}$	$Q^{m_0+2^\ell-1}$	Q^{2^ℓ}	$(1/100)^{2^\ell}$

Figure 1: The number of vertices and the k-regularity degree for the graphs X_i and G_i, and the mixing ratio $\lambda(G_i)$. The process stops once $m_1 = m_0 + \ell = \log\log N + O(1)$.

It is well-known that such graphs H_i exist for some suitably large (constant) value for Q. In fact, it follows from Theorem 32 of [Bus+20] that VNC[1] proves the existence of such graphs.

Set

$$m_0 = \lceil 100 \log N \rceil.$$

For $i \le m_0$, let $G_i = H_i$. For $i > m_0$, let

$$G_i = (H_{m_0+2^{i-m_0}-1})^{2^{i-m_0}}.$$

Then define $X_1 = X^q$ so that X_1 is Q-regular (since X is 4-regular). For $i \ge 1$, let

$$X_{i+1} \;=\; X_i \circledS G_i. \tag{6}$$

Figure 1 shows the sizes and degrees of the graphs X_i and G_i up to

$$m_1 = m_0 + O(\log\log N).$$

For $i \le m_0$, G_i has constant degree Q. Above m_0, G_{m_0+i} has degree Q^{2^i}. It takes $2^i \cdot \lceil \log Q \rceil$ bits to specify an edge of Q_{m_0+i}. The edge relation for G_{m_0+i} is computable in space $O(2^i + \log m)$: namely, it is computed by traversing 2^i many edges of $H_{m_0+2^i-1}$. The edge relation of $H_{m_0+2^{i-m_0}-1}$ is computable in space $O(m_0+2^i)$ and only extra i many bits are needed to keep track of the number of edges traversed.

Suppose Y, and hence X, is connected. (Or if not, restrict attention to a connected subset of X.) Let $\lambda(X_i)$ denote the mixing ratio of X_i. We claim that $\lambda(X_{m_0}) < 3/4$ and that $\lambda(X_{m_1}) < 1/N^{1.5}$, where $m_1 = m_0 + \ell$ with $\ell = \log\log N + O(1)$. These claims will be proved by induction using:

Proposition 17. *Let $f(\lambda, \mu)$ be as defined in (2). Then, for $\mu, \lambda \in (0, 1)$,*

a. $1 - f(1-\gamma, \mu) \ge (3/2)\gamma$ *if* $\gamma \le 1/4$ *and* $\mu \le 1/100$.

b. $f(\lambda, \mu) < \lambda^2 + \mu$.

c. *$f(\lambda, \mu)$ is monotonically increasing in both λ and μ.*

The "spectral gap" of X_i is defined to equal $1 - \lambda(X_i)$. Part a. of the proposition will be used to prove that the spectral gaps of the X_i's are increasing by a factor of $3/2$ for small values of i, namely for $i < m_0$. Part b. will be used for X_i's with $i > m_0$.

Proof. For part a., from $f(\lambda, \mu) = 1 - (1 - \lambda^2)(1 - \mu)$, we have

$$1 - f(1 - \gamma, \mu) \;=\; (1 - (1 - \gamma)^2)(1 - \mu) \;=\; \gamma(2 - \gamma)(1 - \mu),$$

and

$$(2 - \gamma)(1 - \mu) > 3/2 \;\text{ if }\; \gamma \leq 1/4 \text{ and } \mu \leq 1/100.$$

Parts b. and c. are immediate from the definition of $f(\lambda, \mu)$. □

Note that the bounds in Proposition 17 are not tight.

Claim 18. *Assume X is connected. Let $\ell = 10 + \log\log N$ and $m_1 = m_0 + \ell$. Then $\lambda(X_{m_0}) < 3/4$ and $\lambda(X_{m_1}) < 1/N^2$.*

Proof. To prove the first part of claim, we have $\lambda(X_1) \leq 1 - 1/(256N^2)$ by Theorem 11 using the fact that X has degree 4 and has a self-loop at every vertex. Thus by Proposition 17,

$$1 - \lambda(X_i) \geq \max\{1/4, 1 - (3/2)^{m_0}/(256N^2)\}.$$

Since $m_0 = 100 \log N$, the first inequality follows. (The constant 100 is not optimal.)

The second part of the claim is proved (following [RV05]) by letting $\lambda_i = (64/65) \cdot (7/8)^{2^i}$ and showing that $\lambda(X_{m_0+i}) \leq \lambda_i$ by induction on i. The base case of $i = 0$ follows from the first inequality since $(64/65)(7/8) > 3/4$. Let $\mu_i = (1/100)^{2^i}$. For the induction step, we have

$$X_{m_0+i+1} = X_{m_0+i} \circledS G_{m_0+i}$$

where $\lambda(G_{m_0+i}) \leq (1/100)^{2^i}$. Thus

$$\begin{aligned}
\lambda(X_{m_0+i+1}) &\leq \lambda_i^2 + (1/100)^{2^i} \\
&\leq \lambda_i^2 \cdot \frac{65}{64} && \text{(since } (1/100)^{2^i} \leq \lambda_i^2/64\text{)} \\
&\leq \left(\frac{64}{65}\right)^2 \cdot \left(\frac{7}{8}\right)^{2^{i+1}} \cdot \frac{65}{64} && \text{(by the induction hypothesis)} \\
&= \lambda_{i+1}.
\end{aligned}$$

This proves the induction step. To finish off the claim, it suffices to show $1/N^2 > (7/8)^{2^\ell}$. Taking logarithms and by $\ell = 10 + \log\log N$, it suffices to show

$$\begin{aligned}
2\log N &< \log(8/7) \cdot 2^{10} \cdot 2^{\log\log N} \\
&= 2^{10} \cdot \log(8/7) \log N.
\end{aligned}$$

Simple computation shows this holds. □

The directed graph X_{m_1} has such nice expansion properties that it lets us solve the reachability problem for X (hence for Y) essentially trivially. Namely, two vertices x and y in X are connected if and only there is edge between from x and y in X_{m_1}. Since X_{m_1} has polynomial degree, all outgoing edges from x can be checked in logarithmic space. Therefore, to finish the proof that $\mathsf{L} = \mathsf{SL}$ we need to establish two facts: first, Theorem 19 shows that, since $\lambda(X_{m_1})$ is small enough, to determine whether y is reachable from x in X, it is sufficient to check for an edge from x to y. Second, Lemma 21 shows that there is a log space algorithm to determine the i-th edge outgoing from x.

Theorem 19. *Suppose G is a directed graph with N vertices and $\lambda(G) < 1/N^2$. Then, for every pair of vertices u and v in G, there is an edge from u to v.*

Proof. Let M be the adjacency matrix of G. Let u be a vertex of G and let e_u be the vector with a 1 in the u position and all other entries 0. That is, e_u is the probability distribution assigning probability 1 to being at vertex u. We must show that all entries of the vector Me_u are non-zero. In fact, we will show that all entries of M_{e_u} are $\geq 1/N - 1/N^2$. Let $\vec{v}$ be the vector with all entries equal to $1/N$. Note that $M\vec{v} = \vec{v}$. It suffices to show that all the entries in the vector $Me_u - \vec{v} = M(e_u - \vec{v})$ have absolute value $\leq 1/N^2$.

The squared magnitude $\|e_u - \vec{v}\|^2$ is equal to $(N-1)\cdot(1/N^2) + (1-1/N)^2 = (N-1)/N < 1$. Since $\lambda(M) \leq 1/N^{1.5}$, this means

$$\|M(e_u - \vec{v})\|^2 \leq 1/N^3.$$

Let s be the entry in $M(e_u - \vec{v})$ with maximum absolute value. We have $Ns^2 \leq \|M(e_u - \vec{v})\|^2$, whence $s^2 < 1/N^4$. Thus $|s| < 1/N^2$. This proves the theorem. □

Claim 18 and Theorem 19 imply that, in order to check whether x and y are in the same connected component of X, it suffices to check whether there is an edge from x to y in X_{m_1}. We now describe how to traverse edges in X_{m_1}.

The directed graph X_{m_1} was defined from X_1 by repeatedly applying derandomized squaring with the graphs G_i, see (6). From the definition of derandomized squaring, X_m has in-degree and out-degree as given in Figure 1. From a starting vertex in X_m, the outgoing edges are indexed by m-tuples

$$w \;=\; \langle z, a_1, a_2, \ldots, a_{m-1}, a_m \rangle, \tag{7}$$

where z is an index for an edge of X_1 and each a_i is an index for an edge of G_i. The edge index w can be viewed as being obtained by appending a_m to w', where $w' = \langle z, a_1, a_2, \ldots, a_{m-1}\rangle$ is an index for an edge in X_{m-1} and a_m is an index for an edge in G_m. The value z and the values of a_i for $i \leq m_0$ are $< Q = 4^q$ and are specified with $2q$ bits each. For $i = m_0 + j$, $a_j < Q^{2^j} = 4^{q2^j}$ and is specified with $q2^{j+1}$ many bits. Since $m_0 = O(\log N)$ and $m \leq m_1 = m_0 + \log\log N + O(1)$, the edge w is specified with $O(\log N)$ bits, in keeping with the fact that X_{m_1} has polynomial degree.

Suppose x is a vertex in X and w is an edge index in X_m as in (7), We wish to find the vertex y in X such that the w-th outgoing edge from x in X_m goes to vertex y. From the definition of derandomized squaring this is done by:

1. Letting $w' = \langle z, a_1, a_2, \ldots, a_{m-1}\rangle$ and following the w'-th outgoing edge from x in X_{m-1} to reach a vertex u in X,

2. Viewing w' as a vertex in G_m and following the a_m-th outgoing edge from w' in G_m to reach a vertex w'' in G_m, and

3. Viewing w'' as an edge index in X_{m-1} and following the w''-th outgoing edge from u to y in X_{m-1}. This is the desired vertex y reached by following the w-th outgoing edge in X_m.

Algorithm 20. This can be summarized in pseudocode as follows:

Input: x a vertex in X, and
$w = \langle z, a_1, \ldots, a_m \rangle$ an edge index for X_m.
Output: $y = x[w]$ in X_m, the vertex reached via the w-th outgoing edge in X_m.
Procedure:
Let $u = x[w']$ in X_{m-1}, where $w' = \langle z, a_1, \ldots, a_{m-1} \rangle$.
Let $w'' = w'[a_m]$ in G_m.
Let $y = u[w'']$ in X_{m-1}.

Thus an edge in X_m is traversed by traversing an edge in X_{m-1}, then an edge in G_m, and then another edge in X_{m-1}. This can be implemented as a recursive procedure. Since the value of w' can be overwritten by the value of w'', the recursive procedure uses space $O(\log N)$ for $m \leq m_1$.

This establishes:

Lemma 21 ([RV05]). *There is a logspace algorithm for traversing an edge in X_m.*

The above constructions immediately give:

Theorem 22 ([Rei05; Rei08]). $\mathsf{L} = \mathsf{SL}$.

4 Formalization in VL

4.1 Preliminaries for bounded arithmetic

For space reasons, we give only a high-level descriptions of the theories VNC^1, VL and VSL. For more information on bounded arithmetic, the reader should consult [Bus86] and Krajíček [Kra95] for a broad introduction, and Cook-Nguyen [CN10] for the definitions and full development of V^0, VNC^1, VL and VSL.

There is a long history of formalizing results about low-level computational complexity in bounded arithmetic. In fact, the original definitions of $\mathrm{I}\Delta_0$, S^i_2 and T^i_2 were all motivated by the goal of designing arithmetic theories corresponding to reasoning with low-complexity concepts [Par71; Bus86]. As discussed in the introduction, a variety of complexity upper and lower bounds have been established within bounded arithmetic theories, mostly in subtheories of T_2 (which is a theory that can reason about concepts expressible in the polynomial hierarchy). The most important such result for the present paper is that the existence of expander graphs is provable in VNC^1 [Bus+20]. The present paper works primarily in VL, but also in its subtheory VNC^1.

The theories VNC^1, VL, and VSL are extensions of V^0. The theory V^0 has logical strength that corresponds to the complexity class AC^0. It is a second-order (i.e,, a two-sorted) theory of arithmetic, with two sorts of (nonnegative natural) numbers (first-order objects) and of strings (second-order objects). Strings can be viewed either as members of $\{0,1\}^*$ or as finite sets of numbers. The notation $X(i)$, where X is a string and $i \geq 0$ is a natural number, means the Boolean value of the i^{th} entry in string X. Sometimes "$i{\in}X$" is written instead of "$X(i)$". The constants 0 and 1 are number terms, and addition and multiplication are number functions. Another term of type number is string length $|X|$, defined to equal one plus the value of the largest element in X when viewed as a set. The addition and multiplication functions map pairs of numbers to numbers. The string length function $|X|$ maps strings to numbers. The equality relation is defined both for numbers and strings. The axioms of V^0 consist of a finite set of "BASIC" open axioms defining simple properties of the constants, relation symbols, and function symbols, plus the extensionality axiom and the Σ_0^B-Comprehension axioms

$$\Sigma_0^B\text{-COMP:}\quad \exists X{\le}y\,\forall z{<}y\,(X(z)\leftrightarrow\varphi(z))$$

for any formula φ in Σ_0^B not containing X as a free variable, but possibly containing free variables other than z. A Σ_0^B formula is one in which all quantifiers are bounded and which contains no second-order quantifiers. The notation $(\exists X{\le}y)\psi$ means the same as $\exists X(|X|{\le}y\wedge\psi)$.

For connecting bounded arithmetic to computational complexity, numbers are viewed as ranging over small values, namely the lengths of strings. Strings are viewed as inputs to algorithms. A Σ_0^B-formula φ is a formula in which all quantifiers have the form $\forall x{\le}t$ or $\exists x{\le}t$; namely, all quantifiers are bounded and quantify numbers. Second-order variables are allowed in a Σ_0^B formula, but not second-order quantifiers. It is well-known that the Σ_0^B-formulas $\varphi(X)$, with only X free, can express exactly properties that are in AC^0: for this, the input X is viewed as a binary string of length $|X|$. The Σ_1^B-formulas can be defined as the smallest class of formulas containing Σ_0^B and closed under application of existential second-order (bounded) quantification. For instance, if $\varphi(X,Y)$ is a Σ_0^B-formula, then $(\exists Y{\le}t)\varphi(X,Y)$ is a Σ_1^B-formula.[2]

The logical strengths of VNC^1, VL and VSL can be characterized as follows. Let T denote one of the theories VNC^1, VL or VSL, and let $\mathcal{C}$ denote the corresponding complexity class, uniform NC^1 (alternating log time), log space L, or symmetric logspace SL. A formula $\varphi(X)$ is Δ_1^B definable w.r.t. T provided that T proves both $\varphi(X)$ and $\neg\varphi(X)$ are equivalent to Σ_1^B-formulas. Then the Δ_1^B-formulas express precisely the predicates in the complexity class $\mathcal{C}$. A string-valued function $F(X)$ is Σ_1^B-defined by T provided there is a Σ_1^B-formula $\varphi(X,Y)$ which expresses the condition $Y=F(X)$ such that T proves $\forall X\,\exists Y\,\varphi(X,Y)$. Then, the Σ_1^B-definable functions of T are precisely the functions whose bit-graphs are in the complexity class $\mathcal{C}$.

The theories VNC^1, VL and VSL are axiomatized in a way that ensures these just-stated properties hold. The definition of VNC^1 can be found in Cook-Morioka [CM05] or Cook-Nguyen [CN10]. The axioms for VL and VSL assert the existence of paths in graphs. A path can be viewed as a sequence of numbers: a sequence is encoded by a string Z with $Z(i,y)$ intended to denote that y is the i-th element of a sequence. Since the i-th element is unique, the least y such that $Z(i,y)$ is used. The notation $(Z)^i$ is used for this: specifically,

$$y=(Z)^i\ \Leftrightarrow\ (Z(i,y)\vee y=|Z|)\wedge(\forall y'{<}y)\neg Z(i,y).$$

Here $Z(i,y)$ means $Z(\langle i,y\rangle)$ for a suitable, logspace computable pairing function $\langle\cdot,\cdot\rangle$ on numbers.

A string X represents the edge relation of a directed graph on the vertices $[a{+}1]=\{0,1,\ldots,a\}$, by letting $X(y,z)$ denote that there is an edge from y to z, where $y,z\le a$.

A path of length $b+1$ in the graph starting at vertex 0 is represented by a string Z so that

$$\delta_{\mathrm{PATH}}(a,b,X,Z)\ \leftrightarrow\ (\forall i{\le}b)(\,(Z)^i\le a\,)\wedge(\forall i{<}b)X(\,(Z)^i,(Z)^{i+1}\,)\wedge(Z)^0=0.$$

[2]Since all first-order quantifiers are a bounded, it makes no essential difference for the following discussion whether the second-order quantifiers in Σ_1^B-formulas are required to be bounded.

Also, let Unique(a, X) be $(\forall x{\le}a)(\exists! y{\le}a)X(x,y)$ expressing that all vertices have a unique outgoing edge. Then, VL is axiomatized as V^0 plus the axiom

$$\mathrm{Unique}(a, X) \ \rightarrow\ (\exists Z)\delta_{\mathrm{PATH}}(a, a, X, Z).$$

This asserts the existence of a path of length a in the directed graph with edge relation X, starting from the vertex 0.[3]

The theory VSL is axiomatized in terms of connectivity and paths in *undirected* graphs. Accordingly, define

$$\mathrm{Symm}(a, X) \ \Leftrightarrow\ (\forall x{\le}a)X(a,a) \wedge (\forall x{\le}a)(\forall y{\le}a)(X(x,y) \leftrightarrow X(y,x))$$

to express that the graph with edge relation X is symmetric and has self-loops. A connectivity predicate $C(\cdot)$ is a string that identifies vertices connected to the vertex 0. It is paired with a set of paths from 0 to each vertex connected to 0. Namely, letting Z now take triples as input, define $Z^{[u]}$ to be the binary predicate so that $Z^{[u]}(i,y) \Leftrightarrow Z(u,i,y)$. In other words, the string $Z^{[u]}$ is the u-th slice of the string Z. Undirected connectivity is thus witnessed by:

$$\begin{aligned}\delta_{\mathrm{UCONN}}(a, X, C, Z) \ \Leftrightarrow&\\ &C(0) \wedge (\forall x{\le}a)(\forall y{\le}a)(C(x) \wedge X(x,y) \rightarrow C(y))\\ &\wedge (\forall x{\le}a)(C(x) \rightarrow \delta_{\mathrm{PATH}}(a,a,X,Z^{[x]}) \wedge (Z^{[0]})^a = 0 \wedge (Z^{[x]})^a = x).\end{aligned} \tag{8}$$

This expresses that the connective predicate is closed under the edge relation, and that every vertex x connected to 0 has a path from 0. The theory VSL is axiomatized by V^0 plus the axiom

$$\mathrm{Symm}(a, X) \ \rightarrow\ (\exists C)(\exists Z)\delta_{\mathrm{UCONN}}(a, X, C, Z).$$

4.2 Formalization in VNC^1 and VL

VNC^1 is a subtheory of VL, which in turn is a subtheory of VSL [CN10; Kol05]. As was discussed in [Bus+20, Sec. 6.4], VNC^1 has sufficient logic strength to:

(i) Count the number of members of polynomial size sets; that is, count the number of elements in a set coded by a string. In particular, the in-degree and out-degree of a vertex in a graph is definable, concepts such as the i-th outgoing or incoming edge are definable.

(ii) Reason about integers and rational numbers as represented by numbers or pairs of numbers.

(iii) Use strings to encode vectors of integers and vectors of rational numbers.

(iv) Define the summation of vectors of integers and vectors of rational numbers with common denominator. Prove that summations satisfy such as commutativity, associativity, and distributivity properties, and invariance under reorderings of terms.

A summation is coded by a string that lists all of its terms; thus the summation has length equal to a number (a first-order object).

[3] We follow [CN10] in including the condition Unique, but all that is really needed is that every vertex has degree at least one. There is also no loss of axiomatic strength in requiring the first two parameters of δ_{PATH} both equal to a.

(v) Prove the Cauchy-Schwarz theorem. Define the square norm $\|\vec{u}\|^2$ of a vector $\vec{u}$. Define the projection of $\vec{u}$ onto a non-zero vector $\vec{v}$ via the formula $(\langle u, v\rangle/\|v\|^2)\vec{v}$. (Still subject to the proviso that entries in vectors are rationals with a common denominator.)

(vi) Use strings to encode the edge relation of a (multi)graph, and define the rotation map of a graph. Define edge expansion (see below for more details).

(vii) Carry out straightforward operations on graphs, such as adding a self-loop to each vertex, or forming graph powering, tensor products of graphs, and replacement product of graphs.

To this list, we can also add, that the theory V^0 (and hence VNC^1 and VL) can

(viii) Define small (logarithmic) powers of constants.

Proving the last point is not entirely trivial: what it means is that, for $p \in \mathbb{N}$, the function $f_p(m) = p^{\lceil \log m \rceil}$ is definable in V^0. This is well-known for $p = 2$. By convention, the logarithm is base two, and $f_2(m)$ is the least power of 2 greater than or equal to m. This is well-known to be definable and provably total in V^0. In addition $\lceil \log m \rceil$ is equal to $|m-1|$ where $|\cdot|$ is the usual length function of bounded arithmetic. More generally, for any fixed integer $p \geq 2$, the function f_p is definable in V^0. This uses standard techniques, e.g., see Cook-Nguyen [CN10].

In view of (vii) above, it is clear that VNC^1, and hence VL, can define the derandomized squaring product of two graphs. Namely, given graphs X and G coded by strings, VNC^1 can prove the existence a string Z encoding the graph $X \circledS G$, and prove its straightforward properties; e.g., defining the rotation map of Z in terms of the rotation maps of X and G.

VNC^1 can use strings to encode matrices of integers and rationals. For a matrix M and vector $\vec{v}$ whose entries are rationals with a common denominator, VNC^1 can define the product $M\vec{v}$ as well. VNC^1 proves straightforward properties of matrix products, e.g., associativity and distributivity. VNC^1 can similarly use strings to encode tensors, and prove straightforward properties of tensors.

One place where VNC^1 has difficulties is with defining the norm $\|\vec{v}\|$ of $\vec{v}$, even if the entries of $\vec{v}$ have common denominator. This is because VNC^1 has difficulties working with square roots, as the square root of a rational number may not be a rational. However, VNC^1 *can* define $\|\vec{v}\|^2$ via summation. For instance, VNC^1 can express the property $\|\vec{v}\| = \alpha$ as $\|\vec{v}\|^2 = \alpha^2$ and the property $\|\vec{v}\| \leq \alpha$ as $\|\vec{v}\|^2 \leq \alpha^2$. In this setting, $\vec{v}$ is a vector of rational numbers—with common denominator–and is coded by a second-order object V (a set) and α is a first-order object coding a rational number. The fact that VNC^1 can express, say, $\|\vec{v}\|^2 \leq \alpha^2$ corresponds to the fact that this an alternating logtime property of v and α.

For example, VNC^1 can state and prove the Cauchy-Schwarz theorem in the form $\langle \vec{x}, \vec{y}\rangle^2 \leq \|x\|^2 \cdot \|\vec{y}\|^2$ [Bus+20].

A matrix norm $\|M\|$ is harder to express. Let a matrix M of rational numbers with common denominator be represented by a second order object, also denoted M. The statement $\|M\| \leq \alpha$ is expressed by a $\Pi^{1,b}_1$-formula

$$\forall \vec{v}\, (\|M\vec{v}\|^2 \leq \alpha^2 \|\vec{v}\|^2),$$

where it is implicit in the notation that $\vec{v}$ and M contain rational numbers with common denominators. The quantified $\vec{v}$ is encoded by a second-order object V.

Even though VNC^1 can define matrix norms only in a roundabout way, it can readily prove straightforward properties about vector and matrix norms. The next lemma has a couple simple examples that will be useful later.

Lemma 23. *Working with vectors and matrices that involve rational numbers with common denominators,* VNC^1 *can prove:*

(a) *(Triangle inequality) If* $\|\vec{u}\|^2 \le a^2$ *and* $\|\vec{v}\|^2 \le b^2$*, then* $\|\vec{u}+\vec{v}\|^2 \le (a+b)^2$.

(b) *(Matrix product norms) If* $\|M\| \le a$ *and* $\|N\| \le b$*, then* $\|MN\| \le ab$.

Proof. For (a), the following argument can be carried out in VNC^1. We have

$$\|\vec{u}+\vec{v}\|^2 \;=\; \langle \vec{u}+\vec{v}, \vec{u}+\vec{v}\rangle \;=\; \|\vec{u}\|^2 + \|\vec{v}\|^2 + 2\langle \vec{u}, \vec{v}\rangle.$$

Therefore, by the Cauchy-Schwarz inequality,

$$(\, \|\vec{u}+\vec{v}\|^2 - \|\vec{u}\|^2 - \|\vec{v}\|^2 \,)^2 \;=\; 4\langle \vec{u}, \vec{v}\rangle^2 \;\le\; 4(\|\vec{u}\|^2 \cdot \|\vec{v}\|^2).$$

Suppose that the triangle inequality fails. Then we this gives

$$((a+b)^2 - a^2 - b^2)^2 \;>\; 4a^2b^2.$$

Simplifying gives $4a^2b^2 > 4a^2b^2$, and this is a contradiction.

The proof of (b) is entirely trivial. First of all, for an arbitrary vector $\vec{v}$, the bounds on the norms give $\|M(N\vec{v})\|^2 \le a^2 \cdot b^2 \cdot \|\vec{v}\|^2$. The fact that $M(N\vec{v}) = (MN)\vec{v}$ follows immediately since VNC^1 can prove simple facts about summations including distributivity and the invariance of summations under reordering of terms. □

The property of M being the adjacency matrix for a uniform graph G is straightforward to express in VNC^1 given that rotation map (or, equivalently, the edge relation) of G is encoded by a second-order object. For such a matrix, the property of the mixing ratio being $\le \alpha$ is definable by

$$\forall \vec{v}\Big[\vec{v} \perp \vec{1} \rightarrow \|M\vec{v}\|^2 \le \alpha^2 \|\vec{v}\|^2\Big]. \tag{9}$$

Again $\vec{v}$ is a vector of rational numbers with common denominator and is encoded by a second-order object V. Let $\mathrm{MixRat}(\vec{v}, M, \alpha)$ denote the subformula of (9) enclosed in square brackets, and let the entire formula (9) be denoted $\mathrm{MixRat}(G, \alpha)$ (where we are conflating the graph G with its adjacency matrix M).

An upper bound on the edge expansion is also expressed by a $\Pi_1^{1,b}$-formula in VNC^1. Referring back to Definition 2, the property that a d-regular graph G has edge expansion $\ge \alpha$ is expressed by

$$\forall U \Big[U \subset V(G) \;\wedge\; 0 < |U| \le |V(G)|/2 \;\;\rightarrow\;\; \frac{|E(U, V(G)\setminus U)|}{d \cdot |U|} \ge \alpha\Big], \tag{10}$$

where "$V(G)$" denotes the set of vertices of G, and $|\cdot|$ denotes set cardinality. The part of the formula in square brackets is expressible by a $\Sigma_0^{1,b}$-formula and computable in alternating log time, but the second-order quantifier "$\forall U$" ranging over subsets of vertices of G makes (10) a $\Pi_1^{1,b}$-property.

Let $\mathrm{EdgeExp}(U, G, \alpha)$ respectively denote the subformula of (10) that is enclosed in square brackets. The entire formula (10), namely, $\forall U\, \mathrm{EdgeExp}(U, G, \alpha)$ is denoted $\mathrm{EdgeExp}(G, \alpha)$.

Since VNC^1 can define both mixing ratio and edge expansion, it can also *state* (a version of) the Cheeger Inequality. Unfortunately, it is an open question whether VNC^1 or VL can *prove* the Cheeger Inequality.

We will work with the following form of the Cheeger lemma (for regular, undirected graphs).

Theorem 24 (Cheeger Lemma)**.** *Let G be an undirected graph. Let ϵ be the edge expansion of G, and λ be the spectral gap of G. Then*

$$2\epsilon \;\geq\; \lambda \;\geq\; \frac{\epsilon^2}{2}.$$

The Cheeger Lemma cannot be directly stated in this form when working in the theory VNC^1. Instead, VNC^1 can work only with bounds on edge expansion and the mixing ratio, since it is not known whether the values for edge expansion ϵ and the spectral gap λ or the mixing ratio $1-\lambda$ are computable in alternating log time. We can restate the Cheeger lemma for (possible) provability in VNC^1 as follows.

Theorem 25 (Cheeger Lemma — For formalization in VNC^1; however only part (a) is known to be provable in VNC^1, see Section 5.2)**.** *Let G be a d-regular undirected graph, M be the adjacency matrix for G, and $\alpha > 0$ a (rational) number. Then, with U ranging over sets of vertices of G, and V ranging over vectors of rationals with common denominator:*

(a) *(Formalizing $\lambda \leq 2\epsilon$.)*

$$\exists U\, \neg \mathrm{EdgeExp}(U, G, \alpha) \;\rightarrow\; \exists V\, \neg \mathrm{MixRat}(V, M, 1{-}2\alpha).$$

(b) *(Formalizing $\epsilon^2/2 \leq \lambda$.)*

$$\exists V\, \neg \mathrm{MixRat}(V, M, 1{-}\alpha^2/2) \;\rightarrow\; \exists U\, \neg \mathrm{EdgeExp}(U, G, \alpha).$$

Theorem 25 makes the computational content of the Cheeger Lemma explicit by using implications between existential statements. Part (a) asserts that if there is a set U witnessing that the edge expansion of G is $< \alpha$, then there is a set V that witnesses that mixing ratio is $> 1 - 2\alpha$, which means that the spectral gap λ is $< 2\alpha$. For VNC^1 to prove (a), the mapping $U \mapsto V$ must be computable in alternating log time, with its correctness provable in VNC^1.

Part (b) similarly makes constructive the other inequality of the Cheeger Lemma. It states that if there is a vector V that shows the mixing ratio is $> 1-\alpha^2/2$ (so that the spectral gap is $< \alpha^2/2$), there is a set U witnessing that the edge expansion is $< \alpha$.

Part (a) of Theorem 25 is provable in VNC^1; its proof is postponed until Section 5.2. (Furthermore, part (a) is not used in the present paper.) It is open whether part (b) of Theorem 25 is provable in VNC^1 or VL. Fortunately, there is a weakened form of the Cheeger Theorem that applies to graphs G with sufficiently many self-loops that is known to be provable in VNC^1:

Theorem 26 (Cheeger-Mihail Lemma, formalized in VNC^1, [Mih89; Bus+20])**.** VNC^1 *can prove that if (i) d, G, M, α, U and V are as in Theorem 25 and (ii) d is even and every vertex of G has at least $d/2$ self-loops, then:*

(b') *(Formalizing $\epsilon^2/2 \leq \lambda$.)*

$$\exists V\, \neg \mathrm{MixRat}(V, M, 1{-}\alpha^2/2) \;\rightarrow\; \exists U\, \neg \mathrm{EdgeExp}(U, G, \alpha).$$

Proof. This proof is based on a construction of Mihail [Mih89] that was shown to be formalizable in VNC^1 as Lemma 12 in [Bus+20]; see Section 6.2 of [Bus+20]. This allows VNC^1 to formalize the following argument. Let $\vec{v} \perp \vec{1}$ be a vector of rationals that winesses that the mixing ratio of G is $> 1-\alpha^2/2$; i.e., that (9) fails. Let G^- be obtained from G by removing $d/2$ self-loops from each vertex. In the notation of [Bus+20], $G = \bigcirc G^-$. Applying Lemma 12 of [Bus+20],[4] there is a set U of vertices showing that the edge of expansion of G^- is $< 2\alpha$. Since self-loops do not contribute edges towards expansion and since the degree of G is twice that of G^-, the edge expansion of G^- is twice that of G. In particular, since U witnesses that the edge expansion of G^- is less than 2α, then the same U witnesses that the edge expansion of G is less than α. Part (b') of the theorem follows. □

Cheeger's lemma was used in the earlier proof that $\mathsf{L} = \mathsf{SL}$ in two places: in Theorem 10 and indirectly in Theorem 11. We shall discuss later how to use the Cheeger-Mihail Theorem 26 instead. We also need to use the Cheeger-Mihail Theorem in VL to prove the existence of $(Q^i, Q, 1/100)$-graphs H_i with good mixing ratio. These will be obtained via the constant degree expander graphs that can be proved to exist in VNC^1 [Bus+20].

4.3 Formalizing the statement $\mathsf{L} = \mathsf{SL}$ in VL

Before we talk about proving $\mathsf{L} = \mathsf{SL}$ in VL, we need to explain how to formalize the statement that $\mathsf{L} = \mathsf{SL}$ in VL. There are two natural definitions for an undirected graph to be connected.

Definition 27 ("Subset-Connected")**.** An undirected graph G is *subset-connected* provided that for every proper subset U of the vertices of G, there is an edge from U to $\overline{U}$.

In VNC^1, subset-connectedness can be expressed as a $\Pi^{1,b}_1$-formula

$$\forall U \left[U \subset V(G) \ \land\ 0 < |U| < |V(G)| \ \ \rightarrow\ \ E(U, V(G) \setminus U) \neq \emptyset \right].$$

This formula is denoted $\mathrm{SubsetConn}(G)$.

Definition 28 ("Path-Connected")**.** As undirected graph is *path-connected* provided that for every pair of vertices x and y, there is a path in G from x to y.

Path-connectedness can be expressed in VNC^1 as the statement that there is a set coding paths joining all pairs of vertices x and y. Recall that $Z(\cdot,\cdot)$ was used to denote a second-order object coding a path. We extend this notation by considering a 4-place predicate, $Z(\cdot,\cdot,\cdot,\cdot)$, coded as a set, and let $Z^{[x,y]}$ denote the 2-place predicate such that $Z^{[x,y]}(i,u)$ is equal to $Z(x,y,i,u)$. Then VNC^1 can express that G is path-connected with a $\Sigma^{1,b}_1$-formula

$$\exists Z \left[\forall x, y \in V(G) \,(\text{“}Z^{[x,y]} \text{ codes a path from } x \text{ to } y\text{”}) \right].$$

We denote this formula as $\mathrm{PathConn}(G)$.

Clearly, $\mathrm{SubsetConn}(G)$ and $\mathrm{PathConn}(G)$ both express that G is connected. In one direction VNC^1 proves

$$\mathrm{PathConn}(G) \ \rightarrow \mathrm{SubsetConn}(G)$$

[4] To apply Lemma 12 of [Bus+20], use $k = 1$ and $\pi = \vec{v}+u = \vec{v}+\vec{1}$ and $\epsilon = 2\alpha$ and $A = M$. The hypothesis that $\vec{v}$ witnesses that G has mixing ratio $> 1-\alpha^2/2$ means

$$\|M\vec{v}\|^2 > (1-\alpha^2/2)^2\|\vec{v}\|^2 > (1-\alpha^2/4)\|\vec{v}\|^2.$$

From this, Lemma 12 of [Bus+20] gives set U of vertices with edge expanson $< 2\alpha$.

with a simple proof that runs as follows: Suppose U witnesses SubsetConn(G) is false and Z witnesses that PathConn(G) is true. Letting $x \in U$ and $y \notin U$, then the path $Z[x, y]$ must have a first vertex $u \notin U$, and this gives an edge between U and $V(G) \setminus U$.

Proving the other direction is harder. In fact, if

$$\mathrm{VNC}^1 \ \vdash \ \mathrm{SubsetConn}(G) \to \mathrm{PathConn}(G) \tag{11}$$

there must be an alternating log time (i.e., uniform NC^1) algorithm for determining whether a given graph G is connected. To see this, note that if VNC^1 can prove the $\Sigma_1^{1,b}$-formula

$$\neg\mathrm{SubsetConn}(G) \vee \mathrm{PathConn}(G),$$

then by the witnessing theorem for VNC^1 (see [CN10]), there is a set-valued function, computable in alternating log time, which, provably in VNC^1, produces a pair U, Z such that either U witnesses the falsity of SubsetConn(G) or Z witnesses the truth of PathConn(G). Checking the truth or falsity of SubsetConn(G) and PathConn given U, Z is in the log time hierarchy, i.e., in uniform AC^0. It is conjectured that no such algorithm exists, and hence that VNC^1 does not prove SubsetConn(G) $\to$ PathConn(G).

On the other hand, VL does prove SubsetConn(G) $\to$ PathConn(G) as a consequence of proving $\mathsf{L} = \mathsf{SL}$, see Corollary 30. We formalize "$\mathrm{VL} \vdash \mathsf{L} = \mathsf{SL}$" as follows. Here G is set encoding an undirected graph, x is a vertex of G, H is a set encoding a subgraph of G, and Z is a set encoding paths in G.

Theorem 29. VL *proves*

$$\begin{aligned}\forall \text{graphs}\, G\ \forall x{\in}V(G)\ \exists H\, \exists Z\, [\text{“}H \text{ is a subgraph of } G\text{”} \wedge x \in V(H)\\ \wedge \forall\, u \in H\, (\text{“}Z^{[u]} \text{ encodes a path from } x \text{ to } u \text{ in } G\text{”})\\ \wedge \neg\, \exists\, \text{an edge}\, \{u, v\} \in G\, (u \in H \wedge v \notin H)].\end{aligned}$$

The condition on H expresses that H is a maximal connected subgraph containing x. Thus, G is connected precisely when H is equal to G. This gives:[5]

Corollary 30. $\mathrm{VL} \ \vdash \ \forall G\, [\mathrm{SubsetConn}(G) \leftrightarrow \mathrm{PathConn}(G)]$.

Theorem 29 and Corollary 30 are proved in the next section.

Theorem 31. *The theories* VSL *and* VL *prove the same theorems (that is,* VSL = VL*).*

To prove Theorem 31 we need to show that

$$\mathrm{VL} \vdash \mathrm{Symm}(a, X) \ \to \ (\exists C)(\exists Z)\delta_{\text{UCONN}}(a, X, C, Z),$$

as defined in (8) (on page 20). Here, C is a connected component of G containing the vertex 0, and Z is the set of paths from 0 to all elements of C. Now the statement follows from Theorem 29 by setting $x = 0$. The corresponding H will be C satisfying $\delta_{\text{UCONN}}(a, X, C, Z)$, and Z will be the set of paths from 0 to elements of C, as required.

[5] This is restated below as Theorem 36.

4.4 Formalizing the proof of $\mathsf{L} = \mathsf{SL}$ in VL

Preliminaries in VNC^1. As a preliminary, we claim that VNC^1 can formalize and prove all the results in Section 2, namely Theorems 3-9 and replacements for Theorems 10 and 11. Theorem 3 is in terms of subset-connectivity.

Theorem 32. VNC^1 *proves the following: Let G be a d-regular graph on n vertices. Then*

$$\text{SubsetConn}(G) \quad \rightarrow \quad \text{EdgeExp}(G, 2/(dn)).$$

Theorem 32 is an immediate consequence of the definitions since VNC^1 is able to reason about rational numbers.

Theorem 4 is easy to state and prove in VNC^1 since, as discussed above, VNC^1 is able to reason about summations. The proof of Sedrakyan's Lemma (Lemma 5) as given above uses square roots and thus does not seem to be easily formalizable in VNC^1. However, Section 5.1 gives an alternate proof of Sedrakyan's Lemma that does formalize directly in VNC^1. The earlier proof Theorem 6 now formalizes in VNC^1 since it proceeds by manipulating summations and invoking Sedrakyan's Lemma. Note that the proof of Theorem 6 worked by bounding $\|M\vec{v}\|^2$, so this fits exactly the way VNC^1 expresses matrix norms.

Theorem 9 and its proof also formalize directly in VNC^1 in form given in Section 2. When formalized, this theorem has the form "$\forall M\, \exists C\, \exists D(\cdots)$". Here C and D are easy to define in terms of M.

Theorem 10 about the mixing ratio of an undirected graph. To make it provable in VNC^1, we need the additional hypothesis that there are sufficiently many self-loops at each vertex so that Mihail's version of the Cheeger Inequality can be used. It becomes:

Theorem 33. VNC^1 *proves the following: Let G be a d-regular, undirected graph on n vertices. Suppose d is even, and G has at least $d/2$ self-loops at each vertex. Then*

$$\text{SubsetConn}(G) \quad \rightarrow \quad \text{MixRat}(G, 1 - 2/(dn)^2).$$

The proof of Theorem 33 in VNC^1 is immediate from the Cheeger-Mihail Theorem 26. Theorem 11 also needs to be modified so that Theorem 33 can be applied to the matrix H. It becomes:

Theorem 34. VNC^1 *proves the following: Let G be a connected, d-regular, directed graph on n vertices with a self-loop at each vertex. Let M be the adjacency matrix of G, and H be the undirected graph with adjaceny matrix $M^\mathsf{T} M$. Suppose H has at least $d^2/2$ self-loops at each vertex. Then the mixing ratio η of G is at most $1 - 1/(d^4n^2)$.*

The proof of Theorem 34 in VNC^1 follows the earlier proof of Theorem 11. The graph H has degree d^2; therefore Theorem 33 applies to H. The rest proof of Theorem 11 formalizes straightforwardly in VNC^1. The only change needed to carry out proof in VNC^1 is to talk about the squares of vector norms. The last paragraph of the proof of Theorem 11 is modified so that VNC^1 now proves

$$\|M\vec{v}\|^2 \leq (1 - 1/(d^4n^2))^2.$$

This is done by starting with

$$\|M^\mathsf{T} M\vec{v}\|^2 \leq (1 - 2/(d^4n^2))^2$$

from Theorem 33, and then proving that

$$\|M\vec{v}\|^4 \le (1 - 1/(d^4n^2))^4.$$

From that,

$$\|M\vec{v}\|^2 \le (1 - 1/(d^4n^2))^2$$

follows immediately.

One final preliminary result is that VNC^1 proves that $\|P\| = \sqrt{n}$ and $\|L\| = 1/\sqrt{n}$, as discussed at the end of Section 2. These statements involve a square root, but the square roots disappear when formalizing these in VNC^1. We let L and P have dimensions $mn \times n$ and $n \times mn$. To prove that $\|L\| = n$, VNC^1 proves

$$\|L\vec{v}\|^2 = (1/n) \cdot \|\vec{v}\|^2$$

holds for all m-vectors $\vec{v}$. This follows immediately from the fact that $\sum_{i=1}^{n}(1/n)^2 = 1/n$ and the fact that VNC^1 can prove this and reason effectively about summations of rationals. VNC^1 also proves

$$\|P\vec{v}\|^2 \le n\|\vec{v}^2\|.$$

Let $\vec{w}$ be an mn-vector with entries $w_{i,j}$; then the i-th entry of $P\vec{w}$ is $\sum_{j=1}^{n} w_{i,j}$. VNC^1 must prove that

$$\big(\sum_{j=1}^{n} w_{i,j}\big)^2 \le n \cdot \sum_{j=1}^{n} w_{i,j}^2.$$

This follows by the Cauchy-Schwarz theorem that the (squared) dot product $(\vec{v} \cdot \vec{1})^2$ is less than or equal to $\|\vec{v}\|^2 \cdot \|\vec{1}\|^2 = \|\vec{v}\|^2 n$, with $\vec{v}$ the n-vector with entries $w_{i,j}$, for $j = 1, \ldots, n$.

Main part of proof in VL. We next discuss how to formalize the proof that $\mathsf{L} = \mathsf{SL}$ in VL, following closely the exposition in Section 3.2. Many of the steps can be formalized in VNC^1 in fact, but some of the crucial steps require the use of VL. The starting input is an undirected graph Y without self-loops or multiedges. We shall conflate a graph such as Y with the string encoding the edge relation on Y.

The first step in the proof $\mathsf{L} = \mathsf{SL}$ was to transform Y into a 4-regular directed graph X. The graph X had a self-loop at each vertex. For formalization in VL, this step is modified to use a 16-regular direct graph X^* formed similarly to X but with 13 self-loops at each vertex instead of four.[6] Namely, each vertex in X^* has the same four edges of X with labels 0-3 plus 12 additional self-loops with labels 4-15.

This step is completely straightforward to formalize in VNC^1: Each vertex y in Y is replaced with d vertices to form X, where d is the degree of v. For $i < d$, the edges (y, u) incident to v in Y are ordered according to the index u of the other vertex of the edge. This is easily defined with counting, and the rest of the construction is straightforward to carry out in VNC^1. In particular, the number N of vertices in X is the sum of the degrees of the vertices in Y, and hence equal to twice the number of edges in Y. Let $E(\cdot,\cdot)$ be the edge relation for Y. For a vertex $y \in Y$, the i-th

[6] It would suffice for X^* to have seven self-loops at each vertex in order to apply Theorem 34 to X^* to bound the mixing ratio of X^*. However, later when Theorem 32 of [Bus+20] is used to construct the graphs H_i, it is convenient for the degree of X^* to be a power of 2. Hence, X^* is taken to be 16-regular. This makes little difference to the constants used in the constructions.

neighbor of y is equal the value u (if any) such that $E(y,u)$ holds and such that there are $i-1$ many values u' such that $E(y,u')$ holds. The vertex y of Y is replaced in X with the vertices $u=j+k$ where j is the sum of the degrees of the vertices $y'<y$ in Y (namely the number of pairs (u',u'') such that $E(u',u'')$ with $u'<y$) and where k is less than the degree of y in Y. Each vertex x in X^* has degree 16. Given $i<16$, it is straightforward to define, in VNC^1, the i-th neighbor of x in X.

The self-loops in X^* allow VNC^1 to apply Theorem 34 to X^*. Form the undirected graph H by letting M be the adjacency matrix of X^* and letting $M^{\mathsf{T}}M$ be the adjacency matrix of H. Then H is 256-regular. Furthermore, H has 171 self-loops at each vertex; this is because the thirteen self-loops at a vertex in X^* contribute $13^2=169$ self-loops to x in H and the four directed edges between vertices $\langle v,i\rangle$ and $\langle v,i\pm 1 \bmod d\rangle$ contribute two more self-loops to $\langle v,i\rangle$. Since $171\geq 256/2$, X^* and H satisfy the hypotheses of Theorem 34, thus X^* has mixing ratio at most $1-1/(16^4N^2)$ where N is the number of vertices of X^*. This is provable in VNC^1.

As discussed earlier, the Rozenman-Vadhan proof of $\mathsf{L}=\mathsf{SL}$ used the constant $Q=4^q$ for some constant q since X had degree 4 (see Figure 1). The VL-proof uses the 16-regular X^* instead of X. For this reason, we now redefine Q to equal 16^q instead instead of 4^q. The value of q is defined in the next paragraphs so that Theorem 32 of [Bus+20] combined with Theorem 34 above will give large Q-regular graphs H_i with good mixing ratio.[7]

The second step is to prove the existence of the graphs H_i with the desired expansion properties. For $i>0$, H_i is to be a $(Q^i,Q,1/100)$-graph. By [Bus+20, Theorem 32], VNC^1 proves that for constant p, letting $d=2^p$, there are undirected d-regular graphs of arbitrary size which have edge expansion $>1/2592$. By replacing undirected edges with pairs of directed edges, there are also d-regular directed graphs with the same properties. Let q' be the least value such that $16^{q'}=2^{4q'}\geq 4\cdot 2^p$, and let $Q'=16^{q'}$. Of course $4q'-p\in\{2,3,4,5\}$.

Fix $k>0$ a constant, to be defined in the next paragraph. Let $Q=(Q')^k$, and let $q=q'\cdot k$, so $Q=16^q$. Letting $i=O(\log N)$, we claim that VNC^1 can prove the existence of an undirected Q'-regular graph K_i on Q^i many vertices with nontrivial mixing ratio. By Theorem 32 of [Bus+20], VNC^1 can prove that there is an undirected 2^p-regular graph K_i' on Q^i many vertices with edge expansion $\geq 1/2592$. Form the Q'-regular undirected graph K_i by adding $16^{q'}-2^p$ many self-loops to each vertex in K_i'. This increases the degree of the graph by a factor $f=16^{q'}/2^p$, and $4\leq f\leq 32$. Therefore, K_i has edge expansion $\geq 1/(32\cdot 2592)$. Since at least 3/4 of the edges on any vertex on K_i are self-loops and since $(3/4)^2\geq 1/2$, Theorem 34 applies to K_i and implies that K_i has mixing ratio $\leq 1-\delta$ where $\delta=(1/(32\cdot 2592))^2/2$, still provably in VNC^1. (The value δ is an upper bound on the *spectral gap* of K_i.)

We choose k to be the smallest integer such that $(1-\delta)^k\leq 1/100$. Let $H_i=K_i^k$. Thus H_i is Q-regular (since $Q=(Q')^k$) and still has Q^i many vertices. In addition, VNC^1 can prove that the mixing ratio of H_i at most $(1-\delta)^k\leq 1/100$. This is proved in VNC^1 using the fact that, for any $\vec{v}\perp\vec{1}$, we have $(K_i\vec{v})\perp\vec{1}$ and $\|K_i\vec{v}\|\leq(1-\delta)\|\vec{v}\|$. We have established that VNC^1 can prove that H_i exists and is a $(Q^i,Q,1/100)$ graph. This completes the second step.

The second step of the proof as formalized in VNC^1 used different values for the constants q and δ than were used in Section 3. This will need to be taken into account below when showing that VL can prove the new version of Claim 18.

The third step is to define the graphs G_i and prove they have the desired expansion properties.

[7] Theorem 32 of [Bus+20] holds when $d=2^\ell$ is any sufficiently large power of 2.

For $i \le m_0$, we set $G_i = H_i$. For the remaining matrices, we set

$$G_{m_0+i} = (H_{m_0+2^i-1})^{2^i},$$

where $i = O(\log \log N)$. Of course G_{m_0+i} has $Q^{m_0+2^i-1}$ vertices and is Q^{2^i}-regular. Since $i = O(\log \log n)$ and $Q = O(1)$, these facts are readily expressed and proved by VL. In particular, the number of vertices $Q^{m_0+2^i-1}$ and the degree Q^{2^i} are both $N^{O(1)}$ and thus are numbers (first-order objects). This allows an edge index e in G_{m_0+i} to be specified by a sequence $\langle a_1, \ldots, a_{2^i} \rangle$ with each $a_i < Q$, namely as a sequence of 2^i steps in $H_{m_0+2^i-1}$. Thus VL can formalize all these concepts. Indeed, VL can define the function that takes a value $i \le m_1 - m_0$, a vertex w of G_{m_0+i}, and an edge index $e < Q^{2^i}$ and produces the vertex u of G_{m_0+i} which is the e-th neighbor of w in G_{m_0+i}.

This allows VL to define the entries in the adjacency matrix of G_{m_0+i}. Namely the (w, u)-entry of the unnormalized adjacency matrix is the number of edges from w to u in G_{m_0+i}; the same entry in the (normalized) adjacency matrix is this number divided by Q^{2^i}.

We furthermore claim that VL can prove that the mixing ratio of $M_{G_{m_0+i}}$ is $< (1/100)^{2^i}$. The idea for the VL proof is that it establishes that if $\vec{v} \perp \vec{1}$ with $\|\vec{v}\| = 1$ then

$$(M_{H_{m_0+2^i-1}})^j(\vec{v}) \perp \vec{1} \qquad \text{and} \qquad \|(M_{H_{m_0+2^i-1}})^j(\vec{v})\| < (1/100)^j \tag{12}$$

using induction with j ranging from 1 to 2^i. VL can formalize this kind of induction *provided* that it can meaningfully define the matrices M_j and vectors v_j

$$M_j \;:=\; (M_{H_{m_0+2^i-1}})^j \qquad \text{and} \qquad \vec{v}_j \;:=\; (M_{H_{m_0+2^i-1}})^j(\vec{v}).$$

These two concepts were already shown to be VL-definable in the previous two paragraphs when $j = 2^i$ for $i = O(\log \log n)$: The same argument shows that they are definable for arbitrary $j = O(\log n)$. Furthermore, VL proves that

$$M_{j+1} \;=\; M_1 \cdot M_j. \tag{13}$$

It does this by showing that the number of edges in M_{j+1} from vertex w to u is equal to

$$\sum_x \; [(\#\text{ of edges from } w \text{ to } x \text{ in } (M_{H_{m_0+2^i-1}})^j) \cdot (\#\text{ of edges from } x \text{ to } u \text{ in } M_{H_{m_0+2^i-1}})],$$

where x ranges over vertices (from $[N]$). This is just another way of stating the matrix product identity (13). Given this, VL readily proves (12) by induction on j.[8]

The fourth step is to prove the existence of the inductively defined graphs X_{m_1} based on the recurrence $X_{i+1} = X_i \circledS G_i$ of Equation (6). This is formalized in VL by using Algorithm 20 to define the edge relation of X_i. The graphs X_i all have the vertex set $[N]$. Also, X_i is directed and d_i regular, with d_i as shown in Figure 1; namely, X_i has degree $d_i := Q_i$ for $i \le m_0$; and for $i = m_0 + j$, X_i has degree $d_i := Q^{m_0+2^j-1}$. Similarly to before (but now generalized to X_i instead of X_{m_0}), an edge in X_i is represented by a tuple of length i:

$$(z, a_1, \ldots, a_i),$$

where

[8] This uses induction only to a logarithmically sized number $j = O(\log N)$. In fact, VL can use induction to an arbitrary integer. The limiting factor is the property to be proved must be $\Sigma_0^{1,b}$. This is why we need $j = O(\log N)$; namely, so that the values v_j and M_j are $\Sigma_1^{1,b}$-definable in VL.

(a) $z \in [Q]$

(b) for $j \le m_0$, $a_j \in [Q]$, and

(c) for $j = m_0 + j'$ (if there is any such $j \le i$), $a_j \in [Q^{2^j}]$.

Algorithm 20 can be directly and straightforwardly formalized as a logspace algorithm by VL. This uses the fact that the graphs H_i, and thereby the graphs G_i, can be uniformly defined in VL. Namely, VL can define the algorithm that takes as inputs $i < m_1$, a vertex $v \in [N]$ and an edge index e for H_i or G_i and produces the e-th neighbor of v in H_i or G_i (respectively). This is clear from the constructions in [Bus+20] that were formalizable in VNC^1. Hence, VL can define the algorithm that takes appropriate values i, v, e as inputs and produces the e-th neighbor of v in X_i.[9] Clearly, VL defines X_i as a directed and d_i-regular graph.

Furthermore, Algorithm 20 is recursive and computes the edge relation for X_i by a call to the edge relation for G_i plus two calls to the edge relation for X_{i-1}. From this, it is clear that $X_i = X_{i-1} \circledS G_i$; and VL proves this fact.

The fifth step is to prove a good lower bounds for the mixing ratios of the X_i's. This requires a little care to formalize in VL. The first observation is that the proof of Theorem 16 can be adequately carried out in VNC^1; specifically, the proof of part (b) of the theorem. For this, we claim that VL proves that if A and M are the adjacency matrices for X_i and X_{i+1}, then

$$\vec{u} \perp \vec{1} \ \rightarrow \ A\vec{u} \perp \vec{1} \tag{14}$$

and

$$\vec{u} \perp \vec{1} \wedge \|M\vec{u}\| > f(\lambda,\mu)\|\vec{v}\| \ \rightarrow \ (\|A\vec{u}\| > \lambda\|\vec{v}\| \vee \|A(A\vec{u})\| > \lambda\|A\vec{u}\|). \tag{15}$$

The vector $\vec{u}$ will always be expressible as a vector of rational numbers with a common denominator. The entries in the adjacency matrices X_i are also rational numbers with common denominator d_i, the degree of X_i. These denominators will be integers, i.e., first-order objects. Therefore the implication (14) can be expressed in terms of exact arithmetic on rational numbers, and the implication (14) can be proved in the theory VNC^1 using the arguments from Section 2 used to prove Theorem 4. Thus, this is also provable in VL.

Handling the implication (15) is a little more difficult because the proof of Theorem 16 reasons about mixing ratios, and thus needs to reason about vector norms. Computing a vector norm $\|\vec{v}\|$ requires a square root, and this is a little problematic since it uses a square root can of course takes us outside the domain of rational numbers. As discussed earlier, the solution is to argue about *squares of vector norms*, $\|\vec{v}\|^2$, whenever possible. That is, VNC^1 (and hence VL) will prove

$$\vec{v} \perp \vec{1} \wedge \|M\vec{v}\|^2 > f(\lambda,\mu)^2\|\vec{v}\|^2 \ \rightarrow \ (\|A\vec{v}\|^2 > \lambda^2\|\vec{v}\|^2 \vee \|A(A\vec{v})\|^2 > \lambda^2\|A\vec{v}\|^2) \tag{16}$$

instead of proving (15). In fact, (16) is provable in VNC^1.

For this, we need to show that the argument in the final paragraph of the proof of Theorem 16 can be formalized in VNC^1. That is, VNC^1 proves that if

$$\|M\vec{v}\|^2 > f(\lambda,\mu)^2$$

[9] Note that algorithm for traversing edges in X_i is formalizable in VL only, and not (known to be formalizable) in VNC^1. This is because the edge relation for X_i is logspace computable and not (known to be) in alternating log time.

then either

$$\|A\vec{v}\|^2 > \lambda^2 \|\vec{v}\|^2$$

or

$$\|A^2\vec{v}\|^2 > \lambda^2 \|A\vec{v}\|^2.$$

It is enough to show that VNC^1 proves that if $\|M\vec{v}\|^2 > f(\lambda,\mu)^2$ then $\|A^2\vec{v}\|^2 > \lambda^4$. Recall that VNC^1 can prove that $\|P\| \le \sqrt{n}$ and $\|L\| \le 1/\sqrt{n}$. Also, $\|\tilde{A}\| \le 1$ since it is a permutation matrix and $\|I_N \otimes C\| \le 1$ by Theorem 9(a). Therefore, letting

$$R = \mu P \tilde{A}(I_N \otimes C)\tilde{A} L,$$

we have $\|R\| \le \mu$ by Lemma 23(b). We will apply the triangle inequality to the vectors $\vec{x} = (1-\mu)A^2\vec{v}$ and $y = R\vec{v}$, and scalars $a = (1-\mu)\lambda^2\|\vec{v}\|$ and $b = \mu\|\vec{v}\|$. By hypothesis, $M\vec{v} = \vec{x} + \vec{y}$ and

$$\begin{aligned}\|M\vec{v}\|^2 &= \|\vec{x}+\vec{y}\|^2 \\ &> f(\lambda,\mu)^2\|\vec{v}\|^2 \\ &= (\mu + (1-\mu)\lambda^2)^2\|\vec{v}\|^2 \\ &= (a+b)^2.\end{aligned}$$

Since $\|R\|^2 \le \mu^2$, we have $\|\vec{y}\|^2 \le b^2$. Assuming (for sake of a contradiction) that $\|A^2\vec{v}\|^2 \le \lambda^4$, we have

$$\begin{aligned}\|\vec{x}\|^2 &= \|(1-\mu)A^2\vec{v}\|^2 \\ &\le a^2 \\ &= (1-\mu)^2\lambda^4\|v\|^2.\end{aligned}$$

This contradicts the triangle inequality of Lemma 23(a). Therefore, VNC^1 can prove (16).

For **the sixth step**, to finish proving lower bounds on the mixing ratios of the graphs X_i, VL must prove Proposition 17 and Claim 18. VNC^1 can carry out the proof of Proposition 17 as given above. However, the proof of Claim 18 needs to be carried out in VL instead of VNC^1 for the simple reason that VL can define and prove the existence of the graphs X_i and their expansion properties, and VNC^1 cannot (as far as we know). As already discussed, VL can define the graphs G_i and X_i, can prove $X_{i+1} = X_i \otimes G_i$, can prove Theorem 16, can define the functions $f_p(m) = p^{\lceil \log m \rceil}$, and of course reason about rational numbers. The VL-proof of the Claim 18 uses all these facts, but also needs to handle the use of logarithms. Logarithms take us outside rational numbers of course, but VL can instead get by with rough approximations to logarithms (specifically, rough approximations to $\lceil \log 3/2 \rceil$ and $\lceil \log 8/7 \rceil$) as shown by the next very simple lemma. The lemma is stated using 16^2.

Lemma 35. *Let $N > 1$.*

(a) VNC^1 *proves* $16^4 N^2 < (3/2)^{m_0}$ *where* $m_0 = 100 \cdot \lceil \log N \rceil$.

(b) VNC^1 *proves* $N^2 < (8/7)^{2^\ell}$ *where* $\ell = 10 + \lceil \log(\lceil \log N \rceil) \rceil$.

Proof. We argue informally in VNC^1. Since $(3/2)^2 > 2$, we have

$$(3/2)^{m_0} > 2^{50\lceil \log N \rceil} \geq 2^{25\lceil \log N^2 \rceil} = (2^{\lceil \log N^2 \rceil})^{25} \geq (N^2)^{25} > 16^4 N^2$$

for $N \geq 2$. That proves (a). Now, $(8/7)^8 > 2$. Thus

$$(8/7)^{2^\ell} = (8/7)^{2^{10+\lceil \log(\lceil \log N \rceil) \rceil}} \geq (8/7)^{2^{10}\lceil \log N \rceil} > 2^{2^7 \lceil \log N \rceil} \geq N^{2^7} \geq N^2,$$

proving (b).[10] □

This suffices for VL to prove Claim 18 and its bounds on mixing ratios. That is, VL proves that if $\lambda(X_1) \leq 1 - 1/(16^4 N^2)$, then $\lambda(X_{m_1})^2 < 1/N^3$. Recall that VL expresses bounds on the mixing ratios in terms of their squares, as in Equation (9).

The seventh step is to prove Theorem 19 in VNC^1. Fortunately, the proof as given earlier formalizes directly in VNC^1.

We are now ready to complete the proof that VL proves $\mathsf{L} = \mathsf{SL}$. As a first step, we have:

Theorem 36. VL *can prove the following. If G is an undirected graph, then G is subset-connected iff G is path-connected. That is,*

$$\mathrm{VL} \vdash \mathrm{PathConn}(G) \leftrightarrow \mathrm{SubsetConn}(G).$$

This is the same as Corollary 30, but now restated as a theorem since it will be used for the proof of Theorems 38 and 29.

Proof. As remarked earlier, VL can easily prove that $\mathrm{PathConn}(G)$ implies $\mathrm{SubsetConn}(G)$. For the converse, we argue informally in VL. Let $Y = G$ be an undirected graph such that $\mathrm{SubsetConn}(Y)$. Form X_1 as a 16-regular, directed graph using the construction of X^* used earlier. Clearly X_1 is also subset-connected. By Theorem 33, X_1 has mixing ratio at most $1 - 1/(16^4 N^2)$. Using the constructions above, form X_{m_1} from X_1. By the arguments in Section 4.4, which are formalizable in VL, X_{m_1} is connected, with each pair of vertices in X_{m_1} joined by at least one edge. Furthermore, unwinding Algorithm 20, each edge $\langle x, y \rangle$ in X_{m_1} corresponds to a directed path of length 2^{m_1} in X_1. By the construction of X_1 from Y, this path in X_1 yields a path in Y. Therefore Y is path-connected. □

This proof established a stronger property:

Lemma 37. *The theory* VL *proves the following. Suppose Y is an undirected graph such that* $\mathrm{SubsetConn}(Y)$*. Let X_1 and X_{m_1} be formed from Y as in the above constructions. Then, for every pair of vertices x and y in X, there is an edge from x to y in X_{m_1}.*

We further improve on this as follows:

Theorem 38. *The theory* VL *proves the following. Suppose Y is an undirected graph, and X_1 and X_{m_1} are formed from Y as in the above constructions. Then for each pair x, y of vertices of X_1, there is a directed path from x to y in X_1 if and only if there is an edge $\langle x, y \rangle$ from x to y in X_{m_1}.*

[10] It is clear from these calculations that the constants 100 and 10 are far from optimal. We have kept them unchanged from the conventions of [RV05].

The proof of the theorem will depend on the fact that Algorithm 20 implements a universal traversal procedure (see again Rozenman-Vadhan [RV05]). What this means is that, given a vertex x in a degree D directed graph X and an edge index $w \in X_m$, Algorithm 20 finds the vertex reached on the w-th outgoing edge from x in X_m, in effect, by calculating a sequence of edge indices

$$i_1,\, i_2,\, \ldots,\, i_{q2^{m_1}} \tag{17}$$

in X (so $i_j < Q$) and traversing the path in X containing the vertices $x_0, x_1, x_2, \ldots, x_{q2^{m_1}}$ where $x_0 = x$ and each $x_{j+1} = x_j[i_j]$. The extra factor of q arises because $X_1 = X^q$, so that each edge in X_1 is a sequence of q many edges in X.

It is important that the traversal sequence of edge indices (17) depends on w and the graphs G_i (and thereby depends on the degree D and size N of X); however it does *not* depend on any properties of X other than its degree and size. In fact, the graphs G_i have only a minimal dependence on the number N of vertices in X; in fact, the value of N affects the construction of the G_i's only in that is was used to pick the values m_0 and m_1. All that is required that the number of vertices of the (connected) graph X is *at most* N.

Proof of Theorem 38. From the above, it is clear that if there is an edge from x to y in X_{m_1}, then there is a path from x to y in X, and this is provable in VL. So suppose there is a path from x to y in X, we must show that there is an edge from x to y in X_m, using arguments that can be formalized in VL.

Let U be the set of vertices z that are reachable in X using a path that is implicitly traversed by an edge w of X_{m_1}. Specifically, for each edge index w, use Algorithm 20 to form the edge indices i_j in X and define $x_i[i_j]$ as above, see (17). Then U is the set of vertices of the form $x_j[i_j]$ for some edge index w of X_{m_1} and some $j \le q2^{m_1}$. It is possible that U is equal to all of X. If so, since U is clearly path-connected, it is also subset-connected. Thus, in this case, Theorem 38 follows from Lemma 37.

So, suppose instead that U is not all of X. The argument now splits into two cases depending on whether there is edge from U to $\overline{U}$, that is, depending on whether there are $z \in U$ and $z' \notin U$ joined by an edge. If there is no such edge, U induces a 4-regular subgraph of X, which is path-connected and hence subset-connected. Then $|U| < N$, so the edge indices $w = \langle z, a_1, \ldots, a_{m_1}\rangle$ form a complete traversal sequence for U, As a result, for every pair of vertices $z, z' \in U$ there is an edge in X_{m_1} from z to z'. In particular, if there is a path from x to y in X, then $y \in U$ and hence there is an edge in X_{m_1} from x to y. (This subcase is just a generalization of the case $U = X$.)

The remaining case to consider is where there is an edge from U to $\overline{U}$. We prove that this leads to a contradiction and so cannot happen. Modify the graph X to form a new graph X' that satisfies

i. X' has the same vertices of X, and X is 4-regular.

ii. Any edge in X joining two vertices in X is also in X'. Specifically, if $z, z' \in U$ and the i-outgoing edge of z is the i'-th incoming edge of z', then the same holds in X'.

iii. X' is path-connected and hence subset-connected

Form X' from X as follows. First remove all edges from X that touch a vertex not in U. This removes all edges involving vertices in $\overline{U}$. It also removes at least one outgoing edge from some vertex u_1 in U and (by 4-regularity) at least one incoming edge from some vertex u_2 in U. Then, introduce a sequence of edges that form a directed path from u_1 to u_2 through all the vertices of $\overline{U}$, say by taking the vertices in $\overline{U}$ in ascending order and using the first incoming and outgoing edges of U. This makes X' path-connected. Third, add back in edges to make X' 4-regular; e.g., take the vertices in X and their missing incoming-edges and outgoing edges in sequential (ascending) order, and join them up, sequentially. Note that the 4-regularity of X implies that there are the same number of missing incoming edges as missing outgoing edges.

Now the universal traversal sequences (17) based in edge indices w should be universal for both X and X'. Note, however, that each such traversal sequence has to lead to the same vertex in X' as in X. This is because the traversal never leaves U, and this part of X' is the same as in X. Now we obtain a contradiction: Let $z \in \overline{U}$ have an edge from u_1 in X_1. It is not reachable by any traversal (17) in X, but it must reachable in X' since X' is (subset-)connected. □

This completes the proof that $\mathsf{L} = \mathsf{SL}$ in VL. The logspace algorithm to determine whether there is a path from u to v in an undirected graph Y, acts by forming X and X_m, choosing (arbitrarily) a pair of vertices x, y in X that correspond (respectively) to u and v, and checking whether one of the polynomially many outgoing edges of x in X_{m-1} connects x to y.

5 Cheeger and Sedrakyan inequalities in VNC^1

The section proves that Sedrakyan's lemma (Lemma 5) and that part (a) the Cheeger inequality (namely, the $2\epsilon \geq \lambda$ part) is provable in VNC^1, and hence in VL. To formalize and prove these in VNC^1, vectors should be encoded as rational numbers with a common denominator.

The proof of Sedrakyan's lemma based on Cauchy-Schwarz that was given earlier used square roots, which means that VNC^1 cannot use this proof method using only rational numbers. Instead, we present a proof (based on one of the standard proofs of the Cauchy-Schwarz inequality) that can be formalized via reasoning only about rational numbers.

Our VNC^1 proof of the first half of Cheeger inequality will follow the first one of the four proofs exposited in Chung [Chu10]. We have also used the lecture notes of Sauerwald-Sub [SS11] to fill in some of the missing details in [Chu10]. For simplicity, we will give the proof only for the case of d-regular graphs. However, the proof in [Chu10] covers the more general case of part (a) of Cheeger's inequality, and is also formalizable in VNC^1.

5.1 Sedrakyan's lemma in VNC^1

Theorem 39. VNC^1 *proves Sedrakyan's Lemma for n-vectors $\vec{u}$ and $\vec{v}$ of rational numbers with a common denominator provided each component v_i of $\vec{v}$ is positive.*

Proof. The following argument is formalizable in VNC^1, where i and j range over indices for members of $\vec{u}$ and $\vec{v}$.

$$
\begin{aligned}
\sum_i \frac{u_i^2}{v_i} &\geq \frac{\left(\sum_i u_i\right)^2}{\sum_i v_i} \\
\Leftrightarrow \quad \left(\sum_i u_i\right)^2 &\leq \sum_i \frac{u_i^2}{v_i} \cdot \sum_i v_i \\
\Leftrightarrow \quad \sum_{i<j} 2u_i u_j + \sum_i u_i^2 &\leq \sum_i \sum_j \frac{u_i^2}{v_i} v_j \\
\Leftrightarrow \quad \sum_{i<j} 2u_i u_j + \sum_i u_i^2 &\leq \sum_i u_i^2 + \sum_{i \neq j} \frac{u_i^2}{v_i} v_j \\
\Leftrightarrow \quad \sum_{i<j} 2u_i u_j &\leq \sum_{i<j} \left(\frac{u_i^2}{v_i} v_j + \frac{u_j^2}{v_j} v_i\right) \\
\Leftrightarrow \quad 0 &\leq \sum_{i<j} \left(u_i^2 \frac{v_j}{v_i} + u_j^2 \frac{v_i}{v_j} - 2u_i u_j\right) \\
\Leftrightarrow \quad 0 &\leq \sum_{i<j} \left(u_i^2 v_j^2 + u_j^2 v_i^2 - 2u_i u_j v_i v_j\right) \frac{1}{v_i v_j} \\
\Leftrightarrow \quad 0 &\leq \sum_{i<j} (u_i v_j - u_j v_i)^2 \frac{1}{v_i v_j}.
\end{aligned}
$$

The last inequality is obviously true as squares are nonnegative, and since the v_i's are positive. □

5.2 Half of the Cheeger inequality in VNC^1

Theorem 40. VNC^1 *can prove part (a) of the Cheeger inequality in the form stated in Theorem 25.*

Recall that part (a) formalizes the inequality $2\epsilon \geq \lambda$ constructively.

Proof. We prove part (a) of Theorem 25, arguing informally using methods that can be formalized in VNC^1. Assume that U is a set of vertices in G that shows the edge expansion as defined by (1) in Definition 2 is $< \alpha$. Let G have vertices $[N]$ and edges E; let $i \sim j$ mean that $\{i, j\}$ is in the multiset of edges E. Let χ_U be the N-vector such that its i-th component is $(\chi_U)_i = 1$ if $i \in U$ and $(\chi_U)_i = 0$ for $i \notin U$. Let $\vec{v}$ be the component of $\vec{u}$ that is perpendicular to $\vec{1}$; namely, $\vec{v} = \chi_U - (\langle \chi_U, \vec{1}\rangle / N^2)\vec{1}$. More explicitly,

$$
\vec{v}_i = \begin{cases} 1 - \frac{|U|}{N} & \text{if } i \in U \\ -\frac{|U|}{N} & \text{if } i \notin U. \end{cases}
$$

Our goal is to prove $\|M\vec{v}\|^2 \geq (1 - 2\alpha)^2 \|\vec{v}\|^2$ and thereby prove part (a). Using the assumption of edge expansion assumption, we get

$$
\sum_{i \sim j} ((v)_i - (v)_j)^2 = \sum_{i \sim j} ((\chi_U)_i - (\chi_U)_j)^2 < \alpha \cdot d \cdot |U|. \tag{18}
$$

We have[11]

$$
\begin{aligned}
\|\vec{v}\|^2 &= |U|\left(1 - \frac{|U|}{N}\right)^2 + (N - |U|)\left(\frac{U}{N}\right)^2 \\
&= |U|\left(1 - \frac{|U|}{N}\right).
\end{aligned}
$$

[11] We work with $\|\vec{v}\|^2$ instead of $\|\vec{v}\|$ since VNC^1 needs to talk about square norms, not norms.

Consequently, $\|v\|^2 \geq |U|/2$ since w.lo.g., $|U| \leq N/2$.

The following holds for an arbitrary vector $\vec{v}$:

Lemma 41. *Let M be the (normalized) adjacency matrix for a d-regular undirected graph G. Then*

$$\sum_{i\sim j}((v)_i - (v)_j)^2 \ = \ d \cdot (\|\vec{v}\|^2 - \langle \vec{v}, M\vec{v}\rangle).$$

Proof. (of the lemma). The lemma is proved by:

$$\begin{aligned}\sum_{i\sim j}((v)_i - (v)_j)^2 = \ &\sum_{i\sim j}(v_i^2 + v_j^2 - 2v_iv_j) \ = \ \sum_i d\cdot v_i^2 - 2\sum_{i\sim j} v_iv_j \\ = \ & d\cdot\|\vec{v}\|^2 - \sum_i \big(v_i \cdot \sum_{j:i\sim j} v_j\big) \\ = \ & d\cdot\|\vec{v}\|^2 - \sum_i \big(v_i \cdot d \cdot (M\vec{v})_i\big) \\ = \ & d\cdot\|\vec{v}\|^2 - d\cdot\langle \vec{v}, M\vec{v}\rangle.\end{aligned}$$

□

The lemma and (18) imply $\langle \vec{v}, M\vec{v}\rangle \leq \|\vec{v}\|^2 - \alpha\cdot|U|$, whence

$$\begin{aligned}\frac{\langle \vec{v}, M\vec{v}\rangle}{\|\vec{v}\|^2} &\geq 1 - \frac{U}{\|\vec{v}\|}^2 \\ &\geq 1 - 2\alpha,\end{aligned}$$

since $|U|/2 \leq \|\vec{v}\|^2$. Since $\langle \vec{v}, M\vec{v}\rangle\vec{v}/\|\vec{v}\|^2$ is the projection of $M\vec{v}$ onto $\vec{v}$, we have

$$\begin{aligned}\|M\vec{v}\|^2 &\geq \frac{\|(\langle \vec{v}, M\vec{v}\rangle\vec{v})\|^2}{\|\vec{v}\|^4} \\ &= \frac{\langle \vec{v}, M\vec{v}\rangle^2}{\|\vec{v}\|^2}.\end{aligned}$$

Hence $\|M\vec{v}\|^2 \geq (1-2\alpha)^2\|\vec{v}\|^2$. This establishes part (a) of Theorem 25 since the second-order V can be the set encoding the vector V. □

References

[ABM23] Albert Atserias, Sam Buss, and Moritz Müller. "On the Consistency of Circuit Lower Bounds for Non-Deterministic Time". In: *Proc. 55th ACM Symposium on the Theory of Computing (STOC)*. 2023, pp. 1257–1270.

[Ahm+20] AmirMahdi Ahmadinejad, Jonathan A. Kelner, Jack Murtagh, John Peebles, Aaron Sidford, and Salil P. Vadhan. "High-precision Estimation of Random Walks in Small Space". In: *61st IEEE Annual Symposium on Foundations of Computer Science, FOCS 2020, Durham, NC, USA, November 16-19, 2020*. Ed. by Sandy Irani. IEEE, 2020, pp. 1295–1306. DOI: 10.1109/FOCS46700.2020.00123.

[Ahm+23] AmirMahdi Ahmadinejad, John Peebles, Edward Pyne, Aaron Sidford, and Salil P. Vadhan. “Singular Value Approximation and Sparsifying Random Walks on Directed Graphs”. In: *64th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2023, Santa Cruz, CA, USA, November 6-9, 2023*. IEEE, 2023, pp. 846–854. DOI: 10.1109/FOCS57990.2023.00054.

[Ale+79] Romas Aleliunas, Richard M. Karp, Richard J. Lipton, László Lovász, and Charles Rackoff. “Random Walks, Universal Traversal Sequences, and the Complexity of Maze Problems”. In: *Proc. 20th Symp. on Foundations of Computer Science (FOCS)*. 1979, pp. 218–223.

[Arm+00] Roy Armoni, Amnon Ta-Shma, Avi Wigderson, and Shiyu Zhou. “An $O(\log(n)^{4/3})$ Space Algorithm for Connectivity in Undirected Graphs”. In: *Journal of the ACM* 47.2 (2000), pp. 294–311.

[BKZ15] Samuel R. Buss, Leszek Aleksander Kołodziejczyk, and Konrad Zdanowski. “Collapsing Modular Counting in Bounded Arithmetic and Constant Depth Propositional Proofs”. In: *Transactions of the AMS* 367 (2015), pp. 7517–7563.

[Bor+89] Allan Borodin, Stephen Cook, Patrick W. Dymond, and Walter L. Ruzzon. “Two Applications of Inductive Counting for the Complementation Problem”. In: *SIAM Journal of Computing* 18.3 (1989), pp. 559–578.

[Bus+20] Sam Buss, Valentine Kabanets, Antonina Kolokolova, and Michal Koucký. “Expander construction in VNC^1”. In: *Ann. Pure Appl. Log.* 171.7 (2020), p. 102796. DOI: 10.1016/J.APAL.2020.102796.

[Bus86] Samuel R. Buss. *Bounded Arithmetic*. Revision of 1985 Princeton University Ph.D. thesis. Naples, Italy: Bibliopolis, 1986.

[Che+23] Lijie Chen, William M. Hoza, Xin Lyu, Avishay Tal, and Hongxun Wu. “Weighted Pseudorandom Generators via Inverse Analysis of Random Walks and Shortcutting”. In: *64th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2023, Santa Cruz, CA, USA, November 6-9, 2023*. IEEE, 2023, pp. 1224–1239. DOI: 10.1109/FOCS57990.2023.00072.

[Chu10] Fan Chung. “Four Proofs of the Cheeger Inequality and Graph Partition Algorithms”. In: *Proc. Fourth International Congress of Chinese Mathematicians (ICCM, 2007)*. American Mathematical Society and International Press of Boston, 2010, pp. 331–349.

[CK04] Stephen A. Cook and Antonina Kolokolova. “A Second-Order Theory for NL”. In: *Proc. 19th IEEE Symp. on Logic in Computer Science (LICS’04)*. 2004, pp. 398–407.

[CLO24] Lijie Chen, Jiatu Li, and Igor C. Oliviera. “Reverse Mathematics of Complexity Lower Bounds”. In: *Proc. 65th Symp. on Foundations of Computer Science (FOCS)*. IEEE, 2024, pp. 505–527. DOI: 10.1109/FOCS61266.2024.00040.

[CM05] Stephen A. Cook and Tsuyoshi Morioka. “Quantified Propositional Calculus and A Second-Order Theory for NC^1”. In: *Archive for Mathematical Logic* 44 (2005), pp. 711–749.

[CN10] Stephen A. Cook and Phuong Nguyen. *Foundations of Proof Complexity: Bounded Arithmetic and Propositional Translations*. 496 pages. ASL and Cambridge University Press, 2010.

[Coh+25] Gil Cohen, Itay Cohen, Gal Maor, and Yuval Peled. "Derandomized Squaring: An Analytical Insight into Its True Behavior". In: *16th Innovations in Theoretical Computer Science Conference, ITCS 2025, January 7-10, 2025, Columbia University, New York, NY, USA*. Ed. by Raghu Meka. Vol. 325. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2025, 40:1–40:24. DOI: 10.4230/LIPICS.ITCS.2025.40.

[CT92] Peter Clote and Gaisi Takeuti. "Bounded Arithmetics for NC, ALOGTIME, L and NL". In: *Annals of Pure and Applied Logic* 56 (1992), pp. 73–117.

[HLW06] Shlomo Hoory, Nathan Linial, and Avi Wigderson. "Expander Graphs and Their Applications". In: *Bull. Amer. Math. Soc.* 43.04 (Aug. 2006), pp. 439–562. DOI: 10.1090/s0273-0979-06-01126-8.

[Jeř05] Emil Jeřábek. "Weak Pigeonhole Principle, and Randomized Computation". PhD thesis. Charles University, Prague, 2005.

[Jeř07] Emil Jeřábek. "Approximate counting in bounded arithmetic". In: *Journal of Symbolic Logic* 72.3 (2007), pp. 959–993.

[JLL76] Neil D. Jones, Y. Edmund Lien, and William T. Laaser. "New Problems Complete for Nondeterministic Log Space". In: *Mathematical Systems Theory* 10 (1976), pp. 1–17.

[Kol05] Antonina Kolokolova. "Systems of Bounded Arithmetic from Descriptive Complexity". PhD thesis. Department of Computer Science, University of Toronto, 2005.

[Kra95] Jan Krajíček. *Bounded Arithmetic, Propositional Calculus and Complexity Theory*. Heidelberg: Cambridge University Press, 1995.

[LP82] Harry R. Lewis and Christos H. Papadimitriou. "Symmetric Space-Bounded Computation". In: *Theoretical Computer Science* 19 (1982), pp. 161–187.

[Mih89] Milena Mihail. "Conductance and Convergence of Markov Chains". In: *Proc. 13th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 1989, pp. 526–531.

[MP20] Moritz Müller and Jan Pich. "Feasibly Constructive Proofs of Succinct Weak Circuit Lower Bounds". In: *Annals of Pure and Applied Logic* 172.2 (2020), p. 102735.

[Mur+21] Jack Murtagh, Omer Reingold, Aaron Sidford, and Salil Vadhan. "Derandomization beyond Connectivity: Undirected Laplacian Systems in Nearly Logarithmic Space". In: *SIAM Journal on Computing* 50.6 (2021), pp. 1892–1922. DOI: 10.1137/20M134109X. eprint: https://doi.org/10.1137/20M134109X.

[NSW92] Noam Nisan, Endre Szemerédi, and Avi Wigderson. "Undirected Connectivity in $O(\log^{1.5} n)$ Space". In: *33rd Annual Symposium on Foundations of Computer Science, Pittsburgh, Pennsylvania, USA, 24-27 October 1992*. IEEE Computer Society, 1992, pp. 24–29. DOI: 10.1109/SFCS.1992.267822.

[NT95] Noah Nisan and Amnon Ta-Shma. "Symmetric Logspace is Closed Under Complement". In: *Chicago Journal of Theoretical Computer Science* (1995), Article 1.

[Par71] Rohit J. Parikh. "Existence and Feasibility in Arithmetic". In: *Journal of Symbolic Logic* 36 (1971), pp. 494–508.

[Pic15] Jan Pich. "Logical Strength of Complexity Theory and a Formalization of the PCP Theorem in Bounded Arithmetic". In: *Logical Methods in Computer Science* 11.2:8 (2015), pp. 1–38.

[Rei05] Omer Reingold. "Undirected ST-connectivity in log-space". In: *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*. Ed. by Harold N. Gabow and Ronald Fagin. ACM, 2005, pp. 376–385. DOI: 10.1145/1060590.1060647.

[Rei08] Omer Reingold. "Undirected connectivity in log-space". In: *J. ACM* 55.4 (2008), 17:1–17:24. DOI: 10.1145/1391289.1391291.

[RTV06] Omer Reingold, Luca Trevisan, and Salil P. Vadhan. "Pseudorandom walks on regular digraphs and the RL vs. L problem". In: *Proceedings of the 38th Annual ACM Symposium on Theory of Computing, Seattle, WA, USA, May 21-23, 2006*. Ed. by Jon M. Kleinberg. ACM, 2006, pp. 457–466. DOI: 10.1145/1132516.1132583.

[RV05] Eyal Rozenman and Salil P. Vadhan. "Derandomized Squaring of Graphs". In: *Approximation, Randomization and Combinatorial Optimization, Algorithms and Techniques, 8th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems, APPROX 2005 and 9th InternationalWorkshop on Randomization and Computation, RANDOM 2005, Berkeley, CA, USA, August 22-24, 2005, Proceedings*. Ed. by Chandra Chekuri, Klaus Jansen, José D. P. Rolim, and Luca Trevisan. Vol. 3624. Lecture Notes in Computer Science. Springer, 2005, pp. 436–447. DOI: 10.1007/11538462_37.

[RVW02] Omer Reingold, Salil P Vadhan, and Avi Wigderson. "Entropy Waves, The Zig-Zag Graph Product, and New Constant-Degree Expanders and Extractors". In: *Annals of Mathematics, Second Series* 155.1 (2002), pp. 157–187.

[Sch78] Thomas J. Schaefer. "The Complexity of Satisfiability Problems". In: *Proc. 10th ACM Symposium on Theory of Computing (STOC)*. 1978, pp. 216–226.

[SS11] Thomas Sauerwald and He Sun. "Cheeger's Inequality". Lecture 4 of a course on Spectral Graph Theory at the Max Planck Institut Informatik, https://resources.mpi-inf.mpg.de/departments/d1/teaching/ws11/SGT/. 2011.

[Tri08] Vladimir Trifonov. "An $O(\log n \log\log n)$ Space Algorithm for Undirected st-Connectivity". In: *SIAM Journal on Computing* 38.2 (2008), pp. 449–483.

[Zam97] Domenico Zambella. "End Extensions of Models of Linearly Bounded Arithmetic". In: *Annals of Pure and Applied Logic* 88 (1997), pp. 263–277.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il