Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 152 (2016)

# Deconstructing 1-local expanders

Oded Goldreich
Department of Computer Science
Weizmann Institute of Science, Rehovot, Israel.
oded.goldreich@weizmann.ac.il

April 17, 2018

**Abstract**

Contemplating the recently announced 1-local expanders of Viola and Wigderson (*ECCC*, TR16-129, 2016), one may observe that weaker constructs are well known. For example, one may easily obtain a 4-regular $N$-vertex 1-local graph with spectral gap that is $\Omega(1/\log^2 N)$, and similarly a $O(1)$-regular $N$-vertex 1-local graph with spectral gap $1/\widetilde{O}(\log N)$. Starting from a generic candidate for a 1-local expander, we formulate a natural problem regarding "coordinated random walks" (CRW) on the corresponding "relocation" graph (which has size that is logarithmic in the size of the candidate 1-local graph), and observe that

1. any solution to the CRW problem yields 1-local expanders, and
2. any constant-size expanding set of generators for the symmetric group yields a solution to the CRW problem.

This yields an alternative construction and different analysis than the one used by Viola and Wigderson. Furthermore, we show that solving the CRW problem is equivalent to constructing 1-local expanders.

## Contents



ISSN 1433-8092

# 1 Introduction and preliminaries

A function $f : \{0,1\}^n \to \{0,1\}^n$ is called $t$-local if each bit in its output depends on at most $t$ bits in its input. We study the following recent result of Viola and Wigderson [6], where (throughout this text) we view $n$ as varying.

**Theorem 1** (a construction of 1-local expanders [6]): *There exists a constant $d$ and a set of $d$ explicit 1-local bijections, $\{f_1, ..., f_d : \{0,1\}^n \to \{0,1\}^n\}_{n\in\mathbb{N}}$, such that the $2d$-regular $2^n$-vertex graph that consists of the vertex set $\{0,1\}^n$ and the edge multiset $\cup_{i\in[d]}\{\{x, f_i(x)\} : x \in \{0,1\}^n\}$ is an expander.*

Since $f_i$ is a 1-local bijection, each bit of $f_i(x)$ is a bit of $x$ offset by a fixed bit, and different bits of $f_i(x)$ must depend on different bits in $x$. Hence, each $f_i$ is determined by a permutation on the bit locations $\pi^{(i)} : [n] \to [n]$, called the relocation, and an offset $s^{(i)} \in \{0,1\}^n$ such that $f_i(x) = x_{\pi^{(i)}} \oplus s^{(i)}$, where $x_{\pi^{(i)}} = x_{\pi^{(i)}(1)} \cdots x_{\pi^{(i)}(n)}$; that is, $f_i(x)$ is the string obtained by relocating the bits of $x$ according to $\pi^{(i)}$ and offsetting the result by $s^{(i)}$. Indeed, by association, we refer to a $2d$-regular graph with an edge multi-set that is described by 1-local bijections by the term 1-local.

We shall deconstruct the construction of 1-local expanders presented by Viola and Wigderson [6], which relies on the construction of an expanding set of generators for the symmetric group (of $n$-elements), provided by Kassabov [4]. In particular, the relocation permutations in the 1-local expander are the permutations in the generating set constructed by Kassabov [4]. (Indeed, the level of explicitness of the construction of the 1-local expanders is dominated by the level of explicitness of the construction of the said generating set.) We shall show that an expanding set of generators for the symmetric group (of $n$ elements) yields a 1-local $2^n$-vertex expander by passing through an intermediate problem that refers to "correlated random walks" on $n$-vertex graphs.

Recall that the (normalized) second eigenvalue of a regular graph represents the rate at which a random walk on the graph converges to the uniform distribution (hereafter called the convergence rate). In an expander this rate is a constant smaller than 1, whereas in a general (regular and non-$k$-partite) $N$-vertex graph the rate is upper-bounded by $1 - \frac{1}{\mathrm{poly}(N)}$. When trying to estimate the convergence rate, denoted $\lambda$, of an $N$-vertex regular graph it is useful to recall the following facts, where $\Delta_t^{(p)}$ denotes the distance (in norm $L_p$) of the uniform distribution from the distribution of the final vertex in a $t$-step random walk that starts at the worst possible vertex:[1]

1. $\Delta_t^{(1)} \leq \sqrt{N} \cdot \Delta_t^{(2)} \leq \sqrt{N} \cdot \lambda^t$.
2. $N^{-1} \cdot \lambda^t \leq \Delta_t^{(2)} \leq \Delta_t^{(1)}$.

Hence, for sufficiently large $t$, it holds that $\lambda \approx (\Delta_t^{(1)})^{1/t}$. In particular, for any functions $f, g : \mathbb{N} \to \mathbb{N}$, if $\Delta_t^{(1)} \leq \exp(-(t/f(n)) + g(n))$, for sufficiently large $t$, then $\lambda \leq 1 - \Omega(1/f(n))$.

[1] The first inequality is well-known and captures the fact that the corresponding linear operator shrinks each vector that is orthogonal to the uniform one. The second inequality can be proved by considering a random walk that starts in a probability distribution that is described by the vector $u + v_2$, where $u = (1/N, ..., 1/N)$ is the uniform distribution and $v_2$ is a vector in the direction of the second eigenvector (such that no coordinate has value lower than $-1/N$).

## 2 Initial observations

Obtaining a 1-local expander requires using *both* the offsets (i.e., $s^{(i)}$'s) and the relocation permutations, because without the offsets the $f_i$'s maintain the Hamming weight of the vertex (and so the $2^n$-vertex graph is not even connected), whereas without the permutations the $2^n$-vertex graph decomposes into even smaller connected components (i.e., each of size at most $2^d$). On the other hand, using both offsets and relocations, it is quite easy to obtain 1-local 4-regular graphs with polylogarithmic mixing time (equiv., the rate of convergence is bounded away from 1 by the reciprocal of a polylogarithmic function in the size of the graph).

**Observation 2** (the "shuffle exchange" graph is a 1-local weak expander):[2] *Let* $f_1(x) = \mathtt{sh}(x)$ *and* $f_2(x) = x \oplus 0^{n-1}1$ (or, alternatively, $f_2(x) = \mathtt{sh}(x) \oplus 0^{n-1}1$), *where* $\mathtt{sh}(x_1 \cdots x_n) = (x_2 \cdots x_n x_1)$ *is a cyclic shift that corresponds to the relocation permutation* $\pi(i) = (i \bmod n)+1$. *Then, the* 4*-regular* $2^n$*-vertex graph that consists of the vertex set* $\{0,1\}^n$ *and the edge* multiset $\cup_{i\in[2]}\{\{x, f_i(x)\} : x \in \{0,1\}^n\}$ *has second eigenvalue* $1 - \Theta(1/n^2)$.

(Indeed, in this graph, $x$ is connected to $x \oplus 0^{n-1}1$ by two parallel edges (i.e., $\{x, x \oplus 0^{n-1}1\}$ and $\{x \oplus 0^{n-1}1, (x \oplus 0^{n-1}1) \oplus 0^{n-1}1\}$), and the the other pairs of edges (i.e., $\{x, \mathtt{sh}(x)\}$ and $\{\mathtt{sh}^{-1}(x), x\}$ for each $x$) may also be non-distinct.)

**Proof:** We claim that taking a random walk of length $t = O(t' \cdot n^2)$ on this graph yields a distribution that is $2^{-t'}$-close to uniform. The claim is proved by observing that during such a walk, with probability at least $1 - 2^{-t'}$, each position in the original string appeared at the rightmost position at some time during the walk (and that at the next step the corresponding value is randomized, since at that step $f_2$ is applied with probability one half).[3] ■

The foregoing argument refers implicitly to a random walk on the $n$-vertex cycle, which represents the shift relocation permutation used in the 1-local $2^n$-vertex graph that consists of the relocation permutation $\mathtt{sh}$ and the offset $0^{n-1}1$. In general, we shall be discussing two graphs: The $2^n$-vertex graph with transitions that are 1-local, and an $n$-vertex graph that describes the relocation permutations used in the 1-local graph.

**Definition 3** (a generic 1-local graph and the corresponding relocation graph): *Let* $\pi^{(1)}, ..., \pi^{(d)} : [n] \to [n]$ *be* $d$ *permutations and* $s^{(1)}, ..., s^{(d)} \in \{0,1\}^n$.

1. *The* 1-local graph associated with $\pi^{(1)}, ..., \pi^{(d)}$ and $s^{(1)}, ..., s^{(d)}$ *is the* $2d$*-regular* $2^n$*-vertex graph that consists of the vertex set* $\{0,1\}^n$ *and the edge multi-set* $\cup_{i\in[d]}\{\{x, x_{\pi^{(i)}} \oplus s^{(i)}\} : x \in \{0,1\}^n\}$, *where* $x_\pi = x_{\pi(1)} \cdots x_{\pi(n)}$.

[2] Note that when taking an $n$-step random walk on the 2-regular directed graph in which edges are directed from each vertex $x$ to the vertices $\mathtt{sh}(x)$ and $\mathtt{sh}(x) \oplus 0^{n-1}1$ the final vertex is uniformly distributed (regardless of the start vertex). However, there is a fundamental difference between random walks on directed graphs and random walks on the underlying undirected graphs.

[3] The location of the $j^{\text{th}}$ bit in the original string after $i$ steps is determined by $j + \sum_{k\in[i]} X_k \bmod n$, where the $X_k$'s are the $\{0, \pm 1\}$-indicators of the chosen transitions (i.e., $X_k = 1$ (resp. $X_k = -1$) if the transition $\mathtt{sh}$ (resp., $\mathtt{sh}^{-1}$) was taken in the $k^{\text{th}}$ step and $X_k = 0$ otherwise (i.e., if the offset $0^{n-1}1$ was applied)). Note that each block of $O(n^2)$ symbols has absolute value of at least $2n$ with probability at least $1/2$. Hence, looking at $t'$ partial sums that correspond to $t'$ such disjoint blocks, we observe that the probability that all these partial sums are in the interval $[-n, n]$ is at most $2^{-t'}$. Finally, note that if any of these partials sums has value outside $[-n, n]$, then at the corresponding $O(n^2)$ steps each original bit position appeared in the rightmost location.

2. *The* relocation graph associated with $\pi^{(1)}, ..., \pi^{(d)}$ *is the* $2d$*-regular* $n$*-vertex graph that consists of the vertex set* $[n]$ *and the edge multi-set* $\cup_{i\in[d]}\{\{j, \pi^{(i)}(j)\} : j \in [n]\}$.

*The mapping* $x \mapsto x_{\pi^{(i)}} \oplus s^{(i)}$ (resp., $j \mapsto \pi^{(i)}(j)$) *is called a* forward transition*, whereas the reverse mapping* $y \mapsto (y \oplus s^{(i)})_{\pi^{(-i)}}$ (resp., $k \mapsto \pi^{(-i)}(k)$) *is called a* reverse transition*, where* $\pi^{(-i)}$ *denotes the inverse of* $\pi^{(i)}$.

Wishing to use shorter random walks in the rate-convergence analysis, consider the case that the $n$-vertex relocation graph is a $O(1)$-regular expander graph.[4] In this case, a random walk of length $t = O(t' \cdot n \log n)$ on the $n$-vertex graph visits all vertices with probability at least $1 - 2^{-t'}$ (since its cover time is $O(n \log n)$ and we have $t'$ "covering attempts").[5] It follows that the corresponding 1-local $2^n$-vertex graph (in which half of the edges use the corresponding relocation permutations and the other half use the offset $0^{n-1}1$) has second eigenvalue $1 - \Omega(1/n \log n)$. This is the case because taking a random walk of length $O(t' \cdot n \log n)$ on the 1-local graph yields a distribution that is $2^{-t'}$-close to uniform, since (with probability $1 - 2^{-t'}$) each position in the original $n$-bit string is mapped to the rightmost position at some time, and at the next step the corresponding value is "randomized" (since the offset is applied with probability 1/2).

We observe that the foregoing analysis is essentially tight for any $n$-vertex relocation graph. This is the case because the probability that a walk of length $t$ on any regular $n$-vertex graph misses a specific vertex is at least $(1 - O(1/n))^t = \exp(-\Omega(t/n))$.[6] In that case, there exists a position in the original $n$-bit string (i.e., in the label of the vertex of the 1-local $2^n$-vertex graph) that is not moved to the active location where it may be randomized, where the active location refer to the 1-entry in the offset. This suggests using an offset that has many 1-entries (rather than one); in fact, we shall use an offset with a linear number of 1-entries. Before doing so, we observe that there is no hope of obtaining a constant-degree $2^n$-vertex expander when using only offsets of Hamming weight $o(n)$.

**Observation 4** (using only light offsets can not yield an expander): *Consider a* $2d$*-regular* $2^n$*-vertex graph as in Definition 3, and suppose that* $|s^{(i)}| = o(n)$ *for all* $i \in [d]$*. Then, this 1-local* $2^n$*-vertex graph is not an expander.*

**Proof:** For starters, consider an auxiliary $4d$-regular $2^n$-vertex graph in which, for each $i \in [d]$, the $i^{\text{th}}$ relocation permutation (i.e., $\pi^{(i)}$) is coupled both with the offset $s^{(i)}$ and with the all-zero offset. Now, for a $t$-step random walk (on this $2^n$-vertex graph) that starts at the vertex $0^n$, consider the event this walk does not randomize position $j \in [n]$ (in the initial $n$-bit string); that is, the corresponding walk on the $n$-vertex graph that starts at vertex $j \in [n]$ does not go through any vertex in the set $\cup_{i\in[d]}\{k : s^{(i)}_k = 1\}$. This event occurs with probability at least $\eta = \exp(-o(t))/n$, since a $t$-step random walk that starts at the uniform probability misses the said set with probability at least $(1 - o(1))^t = \exp(-o(t))$.[7]

[4] We assume that the edges of this $2d$-regular expander can be represented by $d$ permutations, as in the foregoing definition of a relocation graph.

[5] The cover time bound was established in [1, 2, 5].

[6] Note that here we seek a lower bound on the probability of missing a specific vertex, whereas the common focus is on good upper bounds (which exists when the graph is an expander). This can be proved as in Footnote 7, which deals with the more general case of missing a set of vertices.

[7] Note that here we seek a lower bound on the probability of missing the set $S$ (equiv., staying in $\overline{S} = [n] \setminus S$), whereas the common focus is on good upper bounds (which exists when the graph is an expander). Letting $d$ denote

Note that randomized bit positions are reset to 1 with probability exactly 1/2 (by virtue of the auxiliary construction performed upfront), whereas non-randomized positions maintain the value 0. Considering the expected number of ones in the label of the final vertex of a $t$-step random walk (on the $2^n$-vertex graph), observe that if some bit is not randomized with probability $\eta$, then the expected number of ones is at most $(1-\eta)\cdot 0.5n + \eta\cdot 0.5(n-1) = (n-\eta)/2$. It follows that the distribution of the final vertex is $\eta/2n$-far from uniform[8], which implies that the convergence rate is not bounded away from 1 (since $(\sqrt{2^{-n}}\cdot\eta/2n)^{1/t} \approx \exp(-o(1)-O(n/t)) = \exp(-o(1))$ for sufficiently large $t$).[9] Finally, since the auxiliary $4d$-regular graph is not an expander, the $2d$-regular original graph (which is a subgraph of it) is also not an expander. ■

We note that using offsets of Hamming weight $n-o(n)$ does not help, since this is equivalent to adding the all-ones offset, which merely complements the vertex label in the $2^n$-vertex graph.[10] In view of the above, we must use at least one offset that has Hamming weight in $[\Omega(n), n-\Omega(n)]$.

## 3 A sufficient condition

We now identify a property of 1-local $2^n$-vertex $O(1)$-regular graphs that suffices for showing that they are expanders. Let $\pi^{(1)},...,\pi^{(d)}:[n]\to[n]$ and $s^{(1)},...,s^{(d)}\in\{0,1\}^n$ be as in Definiton 3 and consider a $t$-step random walk on the 1-local graph associated with them. Such a random walk is determined by a starting vertex $x\in\{0,1\}^n$ and a sequence of $t$ steps associated with the sequence $((\sigma_1,\tau_1),...,(\sigma_t,\tau_t))\in([d]\times\{\pm1\})^t$ such that $\sigma_i\in[d]$ indicates a choice of a bijection (associated with the pair $(\pi^{(\sigma_i)},s^{(\sigma_i)})$) and $\tau_i=1$ (resp., $\tau_1=-1$) indicates a forward (resp., backward) transition. For simplicity, let us assume that $\tau_i=1$ for all $i\in[t]$. In such a case, letting $\pi^{(\sigma_i,...,\sigma_j)}$ denote $\pi^{(\sigma_i)}\circ\cdots\circ\pi^{(\sigma_j)}$, we observe that the vertex reached at the end of the walk is

$$\begin{aligned}
&(\cdots((x_{\pi^{(\sigma_1)}}\oplus s^{(\sigma_1)})_{\pi^{(\sigma_2)}}\oplus s^{(\sigma_2)})_{\pi^{(\sigma_3)}}\oplus s^{(\sigma_3)}\cdots)_{\pi^{(\sigma_t)}}\oplus s^{(\sigma_t)}\\
&= x_{\pi^{(\sigma_t,...,\sigma_1)}}\oplus(s^{(\sigma_1)})_{\pi^{(\sigma_t,...,\sigma_2)}}\oplus(s^{(\sigma_2)})_{\pi^{(\sigma_t,...,\sigma_3)}}\oplus(s^{(\sigma_3)})_{\pi^{(\sigma_t,...,\sigma_4)}}\oplus\cdots\oplus s^{(\sigma_t)}\\
&= \left(x\oplus\bigoplus_{i\in[t]}(s^{(\sigma_i)})_{(\pi^{(\sigma_i,...,\sigma_1)})^{-1}}\right)_{\pi^{(\sigma_t,...,\sigma_1)}}
\end{aligned}$$

Recalling that we wish the end-vertex of the ($t$-step) random walk to be almost uniformly distributed, regardless of the start vertex, we need to show that, when $\sigma_1,...,\sigma_t\in[d]$ are uni-

---

the degree of the $n$-vertex graph, we observe that there are at most $d\cdot|S|$ edges incident at $S$, and the worst case is that their other endpoints are distributed evenly among the vertices in $\overline{S}$ (because otherwise, conditioning on not leaving $\overline{S}$ biases the distribution towards vertices that have more neighbors in $\overline{S}$ (equiv., less neighbors in $S$)). Hence, the probability that the random walk never leaves $\overline{S}$ is at least $(1-\frac{d|S|}{d\cdot|\overline{S}|})^t$, whereas in our case $|\overline{S}|=(1-o(1))\cdot n$.

[8] We use the fact that if $\mathrm{E}[X]<\mathrm{E}[Y]-\epsilon$ and $X,Y\in[0,1]$, then there exists a set of values $S$ such that $\Pr[X\in S]<\Pr[Y\in S]-\epsilon$. This can be proved by taking $S=\{v:\Pr[X=v]<\Pr[Y=v]\}\subseteq[0,1]$ and using

$$\Pr[Y\in S]-\Pr[X\in S] \;=\; \sum_{v\in S}(\Pr[Y=v]-\Pr[X=v]) \;\geq\; \sum_{v\in[0,1]}(\Pr[Y=v]-\Pr[X=v])\cdot v \;=\; \mathrm{E}[Y]-\mathrm{E}[X] \;>\; \epsilon.$$

[9] Since the convergence rate $\lambda$ must satisfy $\sqrt{2^n}\cdot\lambda^t\geq\eta/2n$.

[10] In that case, with similar probability, there are two positions in the original string that are not moved through an active location (which implies that their final values are identical). To see this, follow the argument in Footnote 7, while noting that the probability that one of the two coordinated random walks does not stay in $\overline{S}$ is only doubled (wrt to what it is in Footnote 7). The argument is completed by considering the expected number of pairs of positions that hold the same value.

formly distributed, it holds that $\bigoplus_{i\in[t]}(s^{(\sigma_i)})_{(\pi^{(\sigma_i,...,\sigma_1)})^{-1}}$ is almost uniformly distributed. Note that $(s^{(\sigma_i)})_{(\pi^{(\sigma_i,...,\sigma_1)})^{-1}}$ represents the offset applied in the $i^{\text{th}}$ step when viewed as applied to the initial bit positions; actually, in the $i^{\text{th}}$ step the offset $s^{(\sigma_i)}$ is applied to a label whose bits were permuted under $\pi^{(\sigma_i,...,\sigma_1)}$. Now, assume that $\pi^{(\sigma)} = \pi^{(2\lceil\sigma/2\rceil)}$ and that $s^{(\sigma)}$ is determined by the least significant bit of $\sigma$ such that $s^{(\sigma)} = s$ if $\sigma$ is odd and $s^{(\sigma)} = 0^n$ otherwise. In this case, we have

$$\bigoplus_{i\in[t]}(s^{(\sigma_i)})_{(\pi^{(\sigma_i,...,\sigma_1)})^{-1}} = \bigoplus_{i\in[t]:\sigma_1\equiv 1 \pmod 2} s_{(\pi^{(\sigma_i,...,\sigma_1)})^{-1}}$$

which means that, for fixed values of $\lceil\sigma_1/2\rceil, ..., \lceil\sigma_t/2\rceil \in [d/2]$, random values of the least significant bits of $\sigma_1, ..., \sigma_t$ yield an offset that is a random linear combination of the $s_{(\pi^{(2\lceil\sigma_i/2\rceil,...,2\lceil\sigma_1/2\rceil)})^{-1}}$'s. Hence, this offset is uniformly distributed in $\{0,1\}^n$ if and only if these $s_{(\pi^{(2\lceil\sigma_i/2\rceil,...,2\lceil\sigma_1/2\rceil)})^{-1}}$'s span $\{0,1\}^n$. Lastly, fixing $s$ (e.g., $s = 1^{n/2}0^{n/2}$), the latter event depends only on the corresponding relocation permutations (i.e., the $\pi^{(2\lceil\sigma_i/2\rceil,...,2\lceil\sigma_1/2\rceil)}$'s), which in turn can be stated as a condition that refers to the correponding walk on the associated relocation graph. Details follow.

We now identify a property of $n$-vertex relocation graph that suffices for showing that coupled with adequate offsets it yields a 1-local $2^n$-vertex expander. As hinted above, for simplicity, we consider the case of using a single non-zero offset $s \in \{0,1\}^n$ (along with the offsets that are derived from it when considering also the reverse transitions). Actually, for each relocation permutation $\pi : [n] \to [n]$, we consider the four transitions $x \mapsto (x \oplus s^b)_\pi \oplus s^c$, where $b, c \in \{0,1\}$ and $s^0 = 0^n$ (and $s^1 = s$). (Note that such a generic transition can be viewed as $x \mapsto x_\pi \oplus (s_\pi)^b \oplus s^c$, and that the reverse transition has the form $y \mapsto (y \oplus s^c)_{\pi^{-1}} \oplus s^b = y_{\pi^{-1}} \oplus (s_{\pi^{-1}})^c \oplus s^b$.)[11] In other words, referring to Definition 3 and assuming that $d$ is a multiple of 4, we postulate that for some $s \in \{0,1\}^n \setminus \{0^n\}$ and every $\sigma \in [d/4]$ and $b, c \in \{0,1\}$ it holds that $\pi^{(4\sigma-2b-c)} = \pi^{(4\sigma)}$ and $s^{(4\sigma-2b-c)} = (s_{\pi^{(4\sigma)}})^b \oplus s^c$. Note that in this case, for every $\sigma$, taking at random one of the four corresponding (forward) transitions has the effect of randomizing the vertex label by the offset $s$ (by virtue of the random value of $c \in \{0,1\}$), and the same holds when taking the reverse transition (by virtue of the random value of $b \in \{0,1\}$). When taking a random walk on this 1-local graph, we consider only the randomizing effect of this offset (i.e., of the choice of $c$ in a forward move, and the choice of $b$ in a reverse move).[12]

To clarify the above and motivate the following property, suppose that we take $t = \Omega(n)$ random steps on the 1-local graph, and consider the $t$-by-$n$ Boolean matrix describing the activity status of the location to which each of the initial positions is moved during the $t \geq n$ steps, where an initial position is said to be active if it currently reside in location in $\{k : s_k = 1\}$. That is, the $(i,j)^{\text{th}}$ entry in the matrix indicates whether or not, in the $i^{\text{th}}$ step of the fixed random walk being considered, the $j^{\text{th}}$ initial location is mapped to an active location (i.e., a 1-entry in the offset $s$ being used).[13] Using an $n$-vertex expander and $s$ of weight approximately $n/2$, we observe that (w.v.h.p.) approximately half of the entries in each ($t$-long) column (in this random matrix) hold

[11] In contrast, if we were only to use the transitions $x \mapsto x_\pi \oplus s^c$, then the reverse transitions would have had the form $y \mapsto (y \oplus s^c)_{\pi^{-1}} = y_{\pi^{-1}} \oplus (s_{\pi^{-1}})^c$, which would have hindered the argument that follows.

[12] If we are currently at vertex $x$ and take the forward transition associated with $(\pi, b, c)$, then we move to vertex $x_\pi \oplus (s_\pi)^b \oplus s^c$, and the foregoing randomization effect refers to the addition of the offset $s$ (to $(x \oplus s^b)_\pi$), which occurs if and only if $c = 1$. Likewise, if we are currently at vertex $y$ and take the reverse transition associated with $(\pi, b, c)$, then we move to vertex $(y \oplus s^c)_{\pi^{-1}} \oplus s^b$, and the foregoing randomization effect refers to the addition of the offset $s$ (to $(y \oplus s^c)_{\pi^{-1}}$), which occurs if and only if $b = 1$.

[13] To further clarify the analysis, suppose that we place tokens in the $n$ vertices and suppose that these tokens are moved according to the fixed (random) walk. Consider an auxiliary $t$-by-$n$ matrix such that the $(i,j)^{\text{th}}$ entry

the value 1 (i.e., the colomn has approximately $t/2$ 1-entries), but as we shall see what we need is that (w.v.h.p.) this matrix has full rank.

Note that the foregoing Boolean matrix, which is defined based on a random walk on the 1-local $2^n$-vertex graph (of degree $2d$), describes $n$ coordinated walks on the $n$-vertex relocation graph, each starting at a different vertex of the graph and all proceeding according to the same sequence of (random) choices. (Recall that steps on the 1-local $2^n$-vertex graph are associated with tuples $(\sigma, \tau, b, c)$, where $\sigma \in [d/4]$ is the index of a permutation (of $[n]$) and $\tau \in \{\pm 1\}$ indicate the of the transition (i.e., forward or backward), whereas a step on the $n$-vertex relocation graph only determines $(\sigma, \tau)$, leaving the choice of the corresponding bits $b$ and $c$ unspecified.) For $t \geq n$, when the foregoing $t$-by-$n$ matrix has full rank, the $t$ random choices of whether to apply the offset $s$ correspond to a random linear combination of the $t$ rows of the matrix, which yields a uniformly distributed $n$-bit long string, since the linear space of the rows of the matrix equals $\{0,1\}^n$. In this case, the corresponding random walk on the $2^n$-vertex graph yields a uniform distribution (since the latter $n$-bit string is added to the name/label of the initial vertex in the walk).[14] This motivates the definition of the following property.

**Definition 5** (a property of coordinated random walks):[15] *For $d = O(1)$, consider a $d$-regular $n$-vertex graph such that for every $\sigma \in [d]$ the function $g_\sigma : [n] \to [n]$ that maps each vertex to its $\sigma^{\text{th}}$ neighbor is a bijection. For a set $T \subseteq [n]$ and an integer $t \geq n$, consider a random sequence $\overline{\sigma} = (\sigma_1, ..., \sigma_t) \in [d]^t$ and the $n$ corresponding* coordinate random walks (CRW) *such that the $j^{\text{th}}$ walk starts at vertex $j$ and moves in the $i^{\text{th}}$ step to the $\sigma_i^{\text{th}}$ neighbor of the current vertex, and consider a $t$-by-$n$ Boolean matrix $B^{(\overline{\sigma})}$ such that its $(i,j)^{\text{th}}$ entry indicates whether the $j^{\text{th}}$ walk passed in $T$ in its $i^{\text{th}}$ step; that is, the $(i,j)^{\text{th}}$ is 1 if and only if $g_{\sigma_i}(\cdots(g_{\sigma_1}(j)\cdots)) \in T$. The desired* CRW property *is that, for some $t \geq n$, with probability at least $1 - \exp(-n - \Omega(t))$ over the choice of $\overline{\sigma} \in [d]^t$, the matrix $B^{(\overline{\sigma})}$ has full rank* (over GF(2)).

We have already observed that for the CRW property to hold, the set $T$ must have size in $[\Omega(n), n - \Omega(n)]$. We now observe that using an *arbitrary* expander graph and an arbitrary set $T$ of any predetermined size (e.g., $|T| \approx n/2$) *will not do*: For example, consider an $n$-vertex expander that consists of two $n/2$-vertex expanders that are connected by a matching, and let $T$ be the set of vertices in one of these two expanders. Then, coordinated walks on this graph (w.r.t this $T$) always yields a Boolean matrix of rank at most two, since the coordinated walks that start at vertices in $T$ (resp., in $[n] \setminus T$) always move together to $T$ or to $[n] \setminus T$. Hence, the question we consider is the following.

---

records the location of $j^{\text{th}}$ token is time $i$, assuming that initially the $j^{\text{th}}$ token was located at vertex $j$. Then, the $(i,j)^{\text{th}}$ entry of the Boolean matrix is 1 if and only if the $(i,j)^{\text{th}}$ entry of the auxiliary matrix holds a value in the set $\{k : s_k = 1\}$..

[14] That is, fixing a random walk on the $n$-vertex relocation graph, we observe that if the matrix that corresponds to this walk has full rank, then the final vertex in the corresponding random walk on the 1-local $2^n$-vertex graph is uniformly distributed in $\{0,1\}^n$, since it is the sum of the initial vertex (adequately permuted) and a random linear linear combination of the rows of the matrix, which correspond to the adequately permuted offsets. We stress that the said permutations are fixed, since they correspond to the fixed walk on the relocation graph. Hence, our analysis does not use the randomness of the walk on the relocation graph beyond the hypothesis that (w.v.h.p.) such a walk corresponds to a full rank matrix.

[15] An alternative way of defining the matrix $B^{(\overline{\sigma})}$ consists of considering a sequence of permutations over $[n]$, denoted $\pi_0, \pi_1, ..., \pi_t$, such that $\pi_0$ is the identity permutation, and $\pi_i(j) = g_{\sigma_i}(\pi_{i-1}(j))$. The $i^{\text{th}}$ row of $B^{(\overline{\sigma})}$ is then defined as the $T$-indicator of $\pi_i$; that is, the $(i,j)^{\text{th}}$ entry in the matrix is 1 if and only if $\pi_i(j) \in T$.

**Problem 6** (the CRW problem): *For which graphs and which sets $T$'s does the property in Definition 5 hold?*

As outlined above, any $2d$-regular relocation graph that satisfies this property yields an $8d$-regular 1-local $2^n$-vertex expander.

**Theorem 7** (solutions to the CRW problem yield 1-local expanders): *Let $\pi^{(1)},...,\pi^{(d)} : [n] \to [n]$ be $d$ permutations and $s \in \{0,1\}^n$. If the $2d$-regular $n$-vertex graph with the edge multi-set $\cup_{i\in[d]}\{\{j,\pi^{(i)}(j)\} : j \in [n]\}$ along with the set $\{j \in [n] : s_j = 1\}$ satisfies the CRW property, then the $8d$-regular $2^n$-vertex graph with the edge multi-set*

$$\cup_{i\in[d],b,c\in\{0,1\}}\{\{x,(x \oplus s^b)_{\pi^{(i)}} \oplus s^c\} : x \in \{0,1\}^n\}$$

*is an expander.*

Note that the foregoing ($2{\cdot}4d$-regular) $2^n$-vertex graph is associated with the permutations $\pi^{(1,00)},...,\pi^{(d,11)} : [n] \to [n]$ and the offsets $s^{(1,00)},...,s^{(d,11)} \in \{0,1\}^n$ such that, for every $(i,bc) \in [n] \times \{0,1\}^2$, it holds that $\pi^{(i,bc)} = \pi^{(i)}$ and $s^{(i,bc)} = (s^b)_{\pi^{(i)}} \oplus s^c$.

**Proof:** By the hypothesis, for some $t \geq n$, the relevant $t$-by-$n$ matrix has full rank with probability at least $1 - \exp(-n - \Omega(t))$. Fixing an arbitrary walk $\overline{\sigma} = (\sigma_1,...,\sigma_t) \in [2d]^t$ on the $n$-vertex relocation graph such that $B^{(\overline{\sigma})}$ has full rank, we consider a corresponding random walk on the $2^n$-vertex graph. Specifically, having fixed $\overline{\sigma}$, we consider the remaining random choices of $b_i, c_i \in \{0,1\}$ for each $i \in [t]$, and the corresponding walk $(\sigma_1 b_1 c_1,...,\sigma_t b_t c_t) \in ([2d] \times \{0,1\}^2)^t$ on the $2^n$-vertex graph. Actually, we consider a random process that selects these $2t$ bits uniformly, in two steps.

- In the first step, for every $i \in [t]$, if the $i^{\text{th}}$ transition is in the forward direction, then we select $b_i$ at random, otherwise we select $c_i$ at random.
- In the second step, we make the remaining choices; that is, for every $i \in [t]$, if the $i^{\text{th}}$ transition is in the forward direction, then we select $c_i$ at random, otherwise we select $b_i$ at random.

Fixing any sequence of choices for the first step, the label of the final vertex is a random variable that depends only on the random choices made in the second step, but such random choices have the effect of randomizing the vertex label by adding to it a corresponding linear combination of the rows of the matrix $B^{(\overline{\sigma})}$. Specifically, row $i$ is taken to this linear combination if and only if the relevant $c_i$ or $b_i$ equals 1 (where for a forward direction $c_i$ determines whether the current label is offset by $s$, and for the reverse direction this choice is determined by $b_i$).[16] Recalling that the rows of the matrix $B^{(\overline{\sigma})}$ span $\{0,1\}^n$, it follows that the corresponding random walk on the $2^n$-vertex graph yields a uniform distribution (regardless of the start vertex). Thus, the distribution of the label of the final

[16] Formally, denoting the initial vertex in the walk on the 1-local graph by $v_0$, the $i^{\text{th}}$ vertex in the walk, denoted $v_i$, satisfies $v_i = (v_{i-1} \oplus s^{b_i})_\pi \oplus s^{c_i}$ (resp., $v_i = (v_{i-1} \oplus s^{c_i})_{\pi^{-1}} \oplus s^{b_i}$) if $\sigma_i$ indicates a forward (resp., reverse) transition according to $\pi$. Denoting by $\pi_i$ the relocation permutation applied in the $i^{\text{th}}$ step of the walk (i.e., $\pi_i = \pi$ (resp., $\pi_i = \pi^{-1}$) if $\sigma_i$ indicates a forward (resp., reverse) transition according to $\pi$), note that $v_i = (v_{i-1})_{\pi_i} \oplus (s_{\pi_i})^{x_i} \oplus s^{y_i}$, where $(x_i,y_i) = (b_i,c_i)$ if the $i^{\text{th}}$ step takes a forward transition and $(x_i,y_i) = (c_i,b_i)$ otherwise. In both cases, the $i^{\text{th}}$ row in the matrix, denoted $r_i$, equals $s_{(\pi_i \circ \cdots \circ \pi_1)^{-1}}$, where $\pi_i \circ \cdots \circ \pi_1$ is the composition of the relocation permutations applied in the $i$ first steps. Hence, $v_i = (v_{i-1})_{\pi_i} \oplus (s_{\pi_i})^{x_i} \oplus ((r_i)_{\pi_i \circ \cdots \circ \pi_1})^{y_i}$, which implies $(v_i)_{(\pi_i \circ \cdots \circ \pi_1)^{-1}} = (v_{i-1})_{(\pi_{i-1} \circ \cdots \circ \pi_1)^{-1}} \oplus (s_{(\pi_{i-1} \circ \cdots \circ \pi_1)^{-1}})^{x_i} \oplus r_i^{y_i}$. It follows that $(v_t)_{(\pi_t \circ \cdots \circ \pi_1)^{-1}} = v_0 \oplus \overline{s} \oplus \bigoplus_{i\in[t]} r_i^{y_i}$, where $\overline{s} = \bigoplus_{i\in[t]} (s_{(\pi_{i-1} \circ \cdots \circ \pi_1)^{-1}})^{x_i}$.

vertex is $\exp(-n-\Omega(t))$-close to the uniform distribution, which implies that the convergence rate of the $2^n$-vertex graph is bounded away from 1 (i.e., this 1-local graph is an expander), since the convergence rate of this $2^n$-vertex graph is upper-bounded by $(2^n \cdot \exp(-n-\Omega(t)))^{1/t} = \exp(-\Omega(1))$. ■

# 4 Known constructions that satisfy the CRW property

Recall that Kassabov's result [4], which is used in [6], asserts that the symmetric group (over $[n]$) has an explicit generating set that is expanding and of constant size.[17] We shall show that using this set of permutations (i.e., as our set of relocating permutations) and letting $T = [n']$ such that $n' \approx n/2$ is odd (e.g., odd $n' \in \{\lfloor n/2 \rfloor, \lfloor n/2 \rfloor + 1\}$) yields an $n$-vertex graph (along with a set $T$) that satisfies the coordinated random walks property (of Definition 5). Combined with Theorem 7, this yields an alternative proof of Theorem 1.

**Theorem 8** (a positive answer to Problem 6): *Let $\Pi = \{\pi^{(i)} : i \in [d]\}$ be a generating set of the symmetric group of $n$ elements and suppose that $\Pi$ is expanding.*[18] *Then, the $n$-vertex graph that consists of the vertex set $[n]$ and the edge multi-set $\cup_{i\in[d]}\{\{j, \pi^{(i)}(j)\} : j \in [n]\}$ combined with any set of odd size $n' \approx n/2$ satisfies the coordinated random walks property of Definition 5.*

(As observed by Irit Dinur and Roei Tell, the hypothesis of Theorem 8 directly implies a 1-local expander with vertex set consisting of all $n$-bit long strings of fixed Hamming weight, say $n/2$, and edges connecting $x$ to $x_{\pi^{(i)}}$ for every $i \in [d]$.)[19]

**Proof:** For a sufficiently large $t$, consider a random $t$-by-$n$ Boolean matrix that corresponds to coordinated random walks (from all possible start vertices) on the $n$-vertex graph (wrt the foregoing set $T$ of size $n'$). We shall show that, for every non-empty set $J \subseteq [n]$, with probability at least $1 - \exp(-\Omega(t) + O(n \log n))$, the sum of columns in positions $J$ is non-zero. (Picking a sufficiently large $t = \Omega(n \log n)$, this establishes CRW property.)[20] The probability (lower) bound on the foregoing event is proved by observing that this event occurs if and only if the sequence of permutations that describes the corresponding coordinated random walks on the $n$-vertex graph does not hit the set of permuations $\pi$ such that $\{j \in J : \pi(j) \in T\}$ has odd cardinality.[21]

[17] Indeed, Kassabov's result refers to a third graph, which is the corresponding Cayley graph with $n!$ vertices (i.e., the vertices are all the possible permutations over $[n]$).

[18] That is, letting $\mathtt{Sym}_n$ denote the symmetric group of $n$ elements, we consider the Cayley graph consisting of the vertex set $\mathtt{Sym}_n$ and the edge multi-set $\cup_{i\in[d]}\{\{\pi, \pi^{(i)} \circ \pi\} : \pi \in \mathtt{Sym}_n\}$, where $\circ$ denote composition of pemutations. The hypothesis postulates that this Cayley graph is an expander.

[19] Specifically, for any $w \in [n]$, let $S_w$ denote the set of all $n$-bit long strings of Hamming weight $w$. Then, the $2d$-regular graph that consists of the vertex set $S_w$ and the edge multi-set $\cup_{i\in[d]}\{\{x, x_{\pi^{(i)}}\} : x \in S_w\}$ is an expander. This is the case since a $t$-step random on this graph corresponds to a random sequence of permutations (and their inverses) selected from the generating set, whereas such a sequence yields a permutation that is $\exp(-\Omega(t))$-close to a random one. (Note that, for any fixed $x \in S_w$ and a random permuation $\pi \in \mathtt{Sym}_n$, the string $x_\pi$ is uniformly distributed in $S_w$.)

[20] We comment that the CRW property can be established by using any sufficiently large $t = \Omega(n)$; this requires using Claim 8.2 instead of Claim 8.1.

[21] Specifically, we consider the auxiliary matrix that describes these coordinated random walks (see Footnote 13), and observe that the foregoing event (reagrding the Boolean matrix) occurs if and only if each row in the auxiliary matrix records a permutation in the set $\bar{W} = \{pi : |\{j \in J : \pi(j) \in T\}| \equiv 0 \pmod 2\}$. We then observe that $\bar{W}$ has density approximately one half, and the probability that a sequence of $t$ permutations generated in this way (i.e., rows of the auxiliary matrix) misses a set of constant density is at most $\exp(-\Omega(t) + O(n \log n))$.

Claim **8.1** (the distribution of a specific linear combination of the columns): *For every non-empty set $J \subseteq [n]$, with probability at least $1-\exp(-\Omega(t)+O(n\log n))$ over the $t$-step random walk on the $n$-vertex graph, the sum* (mod 2) *of the columns in positions $J$ in the corresponding $t$-by-$n$ Boolean matrix is non-zero.*

Proof: For $J = [n]$ this follows from the fact that $n'$ is odd. Otherwise (i.e., for $J \subset [n]$), we shall prove the claim by using the correspondence between (coordinated) random walks on the $n$-vertex graph and random walks on the set of all permutations where in a random step the current permutation is composed with the selected generator.[22] That is, selecting the $\sigma^{\text{th}}$ neighbor in the random walk on the $n$-vertex graph, a choice that determines a transition (i.e., $\lceil \sigma/2 \rceil \in [d]$) as well as the direction (i.e., forward or reverse) in which the transition is applied, corresponds to selecting the $\lceil \sigma/2 \rceil^{\text{th}}$ generating permutation and moving by composing it or its inverse (according to the value of $\sigma$ mod 2).

In our argument, we shall refer to a set of permutations over $[n]$, denoted $\mathtt{Sym}_n$, and consider the set of permutations, denoted $W$, consisting of permutations having an $J$-image that contains an odd number of elements of $T$; that is, $\pi \in W$ if and only if $|\{j \in J : \pi(j) \in T\}|$ is odd. The claim will follow by showing that (1) $|W| \approx |\mathtt{Sym}_n|/2$, and (2) a random walk on $\mathtt{Sym}_n$ does not visit $W$ if and only if the corresponding (random) walk on the $n$-vertex graph corresponds to a matrix with columns in positions $J$ summing up to the all-zero vector.

We first show that $W$ has density approximately half within the set of all $n!$ permutations over $[n]$. This can be shown by considering, w.l.o.g., the case of $|J| \leq n/2$ (or else consider $[n] \setminus J$). To estimate the probability that a random permutation is in $W$, consider the process of selecting uniformly $\pi \in \mathtt{Sym}_n$ by randomly assigning distinct elements to the location in $J$, and ignore the residual (random) assignment of (distinct) elements to $[n] \setminus J$. Now, focus on the last assignment in that process (i.e., the assignment of the $|J|^{\text{th}}$ element). Using the hypothesis that $|T| = n' \approx n/2$, with probability $1-o(1)$, before this last assignment, the previous $|J|-1 < n/2 \approx n'$ locations were assigned approximately an equal number of elements from $T$ and from $[n] \setminus T$, which means that $n' - (1 \pm o(1)) \cdot |J|/2 = (1 \pm o(1)) \cdot (n - |J|)/2$ elements of each type remain for the last assignment, where $n - |J| = \Omega(n)$. This implies that the parity of elements from $T$ is flipped at the last step with probability $(1 \pm o(1))/2 \approx 1/2$.

The key observation is that the coordinated random walks on the $n$-vertex graph yield a Boolean matrix such that the sum of columns in positions $J$ is zero (mod 2) if and only if the corresponding walk on the set of $n!$ permutations does not pass through states in $W$, where the latter walk starts at the identity permutation. (To see this, consider the sequence, denoted $\pi_1, ..., \pi_t$, of permutations that are selected during the random walk (as determined by the sequence $\overline{\sigma} \in [2d]^t$). Then, in the $i^{\text{th}}$ step of the coordinated walks, the $j^{\text{th}}$ walk visits vertex $k = \pi_i(\cdots(\pi_1(j)\cdots))$, whereas the $(i,j)^{\text{th}}$ entry in the matrix is 1 if and only if $\pi_i(\cdots(\pi_1(j)\cdots)) \in T$ (i.e., if and only if $k \in T$). Hence, the sum of the entries in row $i$ and columns in $J$ is one (mod 2) if and only if $\pi_i \circ \cdots \circ \pi_1 \in W$.)

Finally, consider a $t$-step random walk on the set of permutations that starts at the identity permutation. By the expansion property of the generating set for the symmetric group, the probability that this walk does not pass through a fixed set of constant density is at most $\exp(-\Omega(t - O(n\log n)))$, where the first $O(n\log n)$ steps are taken for convergence to the uniform distribution and the remaining steps are used for hitting attempts (and are analyzed using the "expander hitting lemma"). ■

[22] That is, we use the correspondence between (coordinated) random walks on the $n$-vertex graph and random walks on the $n!$-vertex Cayley graph.

Using a union bound (over all non-empty sets $J$), we conclude that, with probability at least $1-(2^n-1)\cdot\exp(-\Omega(t)+O(n\log n))$, the corresponding $t$-by-$n$ Boolean matrix has full rank. Picking a sufficiently large $t=\Omega(n\log n)$, the theorem follows (since in this case $1-(2^n-1)\cdot\exp(-\Omega(t)+O(n\log n))\geq 1-\exp(-n-\Omega(t))$, which establishes the CRW property). ■

**Conclusion:** Indeed, as stated upfront, applying Theorem 7 to the $n$-vertex graph (and set) analyzed in Theorem 8 (and using [4]) yields an alternative proof of Theorem 1.

**For sake of elegancy:** As noted in Footnote 20, the bound of Claim 8.1 can be tightened. This improvement is immaterial for proving Theorem 8, because, for any function $g:\mathbb{N}\to\mathbb{N}$, a probability (lower) bound of $1-\exp(-\Omega(t)+g(n))$, for a sufficiently large $t\geq n$ (i.e., $t$ such that $\Omega(t)>g(n)+2n$), establishes the CRW property.

Claim **8.2** (the distribution of linear combinations of the columns, revisited): *For every non-empty set $J\subseteq[n]$, with probability at least $1-\exp(-\Omega(t)+O(n))$ over the $t$-step random walk on the $n$-vertex graph, the sum* (mod 2) *of the columns in positions $J$ in the corresponding $t$-by-$n$ Boolean matrix is non-zero.*

Proof: We proceed as in the proof of Claim 8.1, but consider random walks (on the set of all permutations) that start at a state that is uniformly distributed in a specific set $S$ (rather than start at the identity permutation). The set $S$ is the set of all permutations such that each location in $T$ holds an element of $T$; that is, $\pi\in S$ if and only if $\{i\in T:\pi(i)\}=T$. Using $|T|=n'\approx n/2\approx n-|T|$, observe that $S$ has density $\frac{n'!\cdot(n-n')!}{n!}=2^{(1-o(1))\cdot n}$.

Note that the Boolean matrix that represents a random walk on the $n$-vertex graph equals (up to a permutation of its columns) the matrix that represents the same walk on any isomorphic copy of that graph that leaves $T$ invariant (i.e., rather than walking on an $n$-vertex graph $G=([n],E)$, we walk on its isomorphic copy $\phi(G)=([n],\{\{\phi(i),\phi(j)\}:\{i,j\}\in E\})$, where $\phi:[n]\to[n]$ is a permutation such that $\phi(j)\in T$ for every $j\in T$). That is, if the matrix $M$ represents a random walk on the original graph and $\phi:[n]\to[n]$ is a permutation that leaves $T$ invariant, then the matrix obtained by permuting the columns of $M$ according to $\phi$ represents a random walk on the isomorphic copy of the original graph obtained by relabeling its vertices according to $\phi$. (This is the case because the $j^{\text{th}}$ column in $M$ indicates whether the walk on $G$ that starts at vertex $j$ hits $T$ in each of the $t$ steps, but this column also indicates whether the same walk on $\phi(G)$ that starts at $\phi(j)$ hits $\phi(T)=T$ in each of the $t$ steps.) Now, since $M$ is full rank if and only if permuting its columns yields a full rank matrix, we may consider random walks on such random isomorphic copies of the original graph (i.e., copies obtained by relabeling it using a random permutation that leaves $T$ invariant). Hence, we may analyze the corresponding walk (on the set of $n!$ permutations) that starts at a state that is uniformly distributed in $S$ (rather than starting at the identity permutation).

Now, fixing any non-empty $J\subset[n]$, we consider the corresponding set $W$ (as defined in the proof of Claim 8.1). By the expansion property of the generating set for the symmetric group, we have that a $t$-step random walk that starts in uniformly distributed state in $S$ passes through $W$ with probability at least $1-\exp(-\Omega(t-O(n)))$, where the first $O(n)$ steps are taken for convergence to the uniform distribution and the remaining steps are used for hitting $W$. (The crucial point is that here we start the walk from a vertex that is uniformly distributed in a set of density $\exp(-O(n))$, whereas in the proof of Claim 8.1 the walk starts at an arbitrary vertex (which may be viewed as a set of density $1/n!=\exp(-\Theta(n\log n))$).) ■

**The CRW property does not imply that the set of relocations is an expanding set of generators for $\mathtt{Sym}_n$.** Interpreted in terms of sets of permutations over $[n]$, the CRW property asserts that a random walk on the corresponding Cayley graph passes a specific statistical test (which is specified by the corresponding set $T$). Theorem 8 asserts that if this Cayley graph is an expander, then the CRW property is satisfies for any set $T$ of odd size $n' \approx n/2$. (One may observe that this holds for any odd $n' \in [\Omega(n), n - \Omega(n)]$.) This implies that if this Cayley graph is an expander, then the CRW property is satisfies for some set $T$. Here we show that the converse of the latter conditional statement does not hold.[23]

**Theorem 9** (the converse of Theorem 8 fails): *There exists a set of permutations, $\{\pi^{(i)} : i \in [3d]\}$, over $[2n]$ that does not generate the symmetric group of $2n$ elements* (let alone in an expanding manner) *such that the $2n$-vertex graph consisting of the vertex set $[2n]$ and the edge multi-set $\cup_{i\in[3d]}\{\{j, \pi^{(i)}(j)\} : j \in [2n]\}$ combined with some set of odd size $n' \approx n/2$ satisfies the coordinated random walks property of Definition 5.*

Indeed, $n'$ is approximately one fourth of the size of the vertex set, but (as noted above) Theorem 8 holds also in that case.

**Proof Sketch:** We start with a set of permutations $\Pi = \{\pi^{(i)} : i \in [d]\}$ that generates the symmetric group of $n$ elements and is expanding. We first extend each $\pi^{(i)} \in \Pi$ to the domain $[2n]$ such that $\pi^{(i)}(n + j) = n + \pi^{(i)}(j)$ for every $j \in [n]$ (and $i \in [d]$). Next we add $d$ copies of the identity permutation and $d$ copies of the permutation that switches $[n]$ and $[2n] \setminus [n]$; that is, for every $i \in [d]$, we have $\pi^{(d+i)}(b \cdot n + j) = b \cdot n + j$ and $\pi^{(2d+i)}(b \cdot n + j) = (1 - b) \cdot n + j$ for every $j \in [n]$ and $b \in \{0, 1\}$. The $2n$-vertex $6d$-regular relocation graph $G'$ that corresponds to the augmented set of permutations $\Pi'$ consists of two copies of the $2d$-regular $n$-vertex graph $G$ that corresponds to $\Pi$ augmented by $d$ self-loops on each vertex (where each self-loop contributing two units to the vertex's degree) and $2d$ copies of a perfect matching that matches the two copies of each original vertex.

Note that $\Pi'$ (i.e., the new set of permutations over $[2n]$) does not generate the symmetric group of $2n$ elements; it rather generates a group of $2 \cdot (n!) \ll (2n)!$ permutations. Nevertheless, we shall show that the ($2n$-vertex) relocation graph $G'$ satisfies the CRW property (with any set $T \subset [n]$ of odd size $n' \approx n/2$).[24] This will be shown by relating random walks on $G'$ to random walks on $G$, and the theorem will follow.

When analyzing (coordinated) random walks on $G'$, we distinguish steps in which one of the first $d$ permutations is employed from steps in which one of the last $2d$ permutations is employed, calling the latter steps semi-idle, since they either map each vertex to itself or map each vertex to its sibling (i.e., the other copy). The key observation is that a $t$-step random walk has the following two properties:

1. With probability at least $1 - \exp(-\Omega(t))$, at least $t/2$ of the steps in the walk are semi-idle, since at each time a semi-idle step is selected with probability $2/3$. Furthermore, *for every*

[23] Indeed, we leave open the possibility that the converse of Theorem 8 holds. We believe that even if the CRW property is satisfies for any set $T$ of odd size $n' \approx n/2$, then it does not necessarily hold that the foregoing Cayley graph is an expander.

[24] We stress that $T$ is an arbitrary subset of size $n'$ of $[n]$, whereas the vertex set is $[2n]$. Indeed, picking $T$ of size $n'$ arbitrarily in $[2n]$ will fail (e.g., if $T = T' \cup (n + T') \cup \{n\}$, for any $T' \subseteq [n - 1]$, then, for every non-empty $J' \subseteq [n]$, the sum of matrix's columns with indices in $J' \cup (n + J')$ is exactly as in the case of $T = \{n\}$, since the contributions of $T'$ and $n + T'$ cancel out).

*constant $c$, with probability at least $1-\exp(-\Omega(t))$, there are at most $t/c^2$ time-intervals of the form $[i-c,i-1]$ that do not contain a semi-idle step.*

2. Fixing a (non-empty) set $J \subseteq [n]$ and a random walk on $G'$, we call a walk good (for $J$) if the sum of the columns $J \cup \{n+j : j \in J\}$ in the matrix that corresponds to the random walk yields a vector that has at least $\Omega(t)$ ones in rows that correspond to steps that are not semi-idle. Each of these rows will be called good for $J$. (Recall that the $(i,j)^{\text{th}}$ entry in this matrix indicates whether the $j^{\text{th}}$ walk hits $T$ in its $i^{\text{th}}$ step, and that we consider here the parity of the entries in the columns $J \cup \{n+j : j \in J\}$ restricted to rows that are not semi-idle.) The observation is that *every non-empty set $J \subseteq [n]$, with probability at least $1-\exp(-\Omega(t-O(n\log n)))$ over the random walks on $G'$, it holds that the walk is good for $J$.*

   The foregoing property of the walk on (the $2n$-vertex graph) $G'$ is proven by considering an analogous lazy walk on (the $n$-vertex) graph $G$ such that the walk on $G$ takes an idle step (i.e., stays in place) if and only if the walk on $G'$ takes a semi-idle step. First note that each row of the foregoing matrix (which corresponds to a walk on $G'$) has 1-entries either in columns in $[n]$ or in columns in $[2n] \setminus [n]$; hence the sum of the entries in columns $J \cup \{n+j : j \in J\}$ (in this row) is either due to $J$ or to $n+J \stackrel{\text{def}}{=} \{n+j : j \in J\}$. Recall that Claim 8.1 asserts that, with probability at least $1-\exp(-\Omega(t-O(n\log n)))$, at least one row in the matrix that corresponds to a non-lazy walk on $G$ has an odd sum of the entries in columns $J$, but the argument extends to the matrix that corresponds to a lazy random walk (on $G$) and to rows that do not correspond to idle steps.[25] Hence, with probability at least $1-\exp(-\Omega(t-O(n\log n)))$, at least one of the rows in a matrix that corresponds to a randomn walk on $G'$ is good (for $J$). Furthermore, the same argument extends to showing that the number of good (for $J$) rows is $\Omega(t)$, by using a "Chernoff bound" for random walks on expanders.[26]

   (Note that we use the correspondence between columns $J \cup (n+J)$ in the matrix $B'$ that describes a random walk on $G'$ and columns $J$ in the matrix $B$ that describes a corresponding lazy random walk on $G$. The hypothesis was used to analyze the random walks on $G$, and the inference to $G'$ holds because each row in $B$ appears either in the first $n$ entries of the corresponding row in $B'$ or in its last $n$ entries (while the other $n$ entries of this row are all zero).)

Hence, a random walk on $G'$ satisfies both the foregoing properties with probability at least $1-\exp(-\Omega(t-O(n\log n)))$. Fixing such a walk on $G'$, note that satisfying these properties is independent of the choices made in the semi-idle steps of this walk (i.e., whether to stay idle or move to the sibling vertex). This fact will allow us to re-randomize these choices later.

By the choice of this walk, the corresponding matrix has $t' = \Omega(t)$ good rows. Letting $c = 2t/t'$, we infer that for at most $c \cdot t/c^2 = 0.5t'$ of the good rows $i$ there is no semi-idle step in the time-interval $[i-c,i-1]$. Hence, there are at least $t'' = 0.5t'/c = \Omega(t)$ good (for $J$) rows that are at distance $c$ apart from one another such that each such row $i$ is preceded by a semi-idle step in the

[25] This can be seen by mapping the lazy random walk to a non-lazy random walk.

[26] Alternatively, we may just start with a graph $G$ that satisfies a strong CRW property with respect to $T$, where this strong property asserts that *for sufficiently large $t$, with probability at least $1-\exp(\Omega(t))$, a $t$-step random walk yields a matrix with columns that span an $n$-dimensional linear code of distance $\Omega(t)$* (whereas the CRW property only asserts that the columns of this matrix span an $n$-dimensional linear space).

time-interval $[i-c, i-1]$. Calling these rows very good (for $J$), note that we can match each very good row $i$ to a semi-idle step (in $[i-c, i-1]$) that precedes row $i$ but does not precede any very good row that precedes $i$. Now, if we re-randomize the choices made in all the semi-idle steps, then with probability at least $1-2^{-t''}$ one of the rows that is (very) good for $J$ has all its ($|T|$) ones in the columns $[n]$. In this case, the sum of the columns in $J \subseteq [n]$ yields a non-zero vector. The same argument applies to $n+J$.

Recall that in order to argue that the matrix has full rank we have to show that for every non-empty $J' \cup J''$ such that $J' \subseteq [n]$ and $J'' \subset [2n] \setminus [n]$ it holds that the sum of the columns in $J' \cup J''$ yields a non-zero vector. Assuming, w.l.o.g., that $J'$ is non-empty, we have already established that, with probability at least $1-\exp(-\Omega(t-O(n\log n)))$, the sum of the columns in $J'$ yields a non-zero vector. But the sum of the columns in $J''$ cannot cancel non-zero entries of that vector, since each row of the matrix has 1-entries either in columns $[n]$ or in columns $[2n] \setminus [n]$. Hence, with probability at least $1-(2^{2n}-1)\cdot\exp(-\Omega(t-O(n\log n)))$, the matrix has full rank. ■

# 5 A sufficient and necessary condition

Turning back to the relation between the CRW property (of Definition 5) and 1-local expander, we shall show that the following generalization of Definition 5 suffices and is necessary for obtaining a 1-local expander (with $2^n$ vertices).

**Definition 10** (a relaxed property of coordinated random walks): *For $d, d' = O(1)$, consider a $d$-regular $n$-vertex graph as in Definition 5, and $d'$ sets $T_1, ..., T_{d'} \subseteq [n]$. As in Definition 5, for $t \geq n$, consider a random sequence $\overline{\sigma} = (\sigma_1, ..., \sigma_t) \in [d]^t$ and the $n$ corresponding* coordinate random walks *such that the $j^{\text{th}}$ walk starts at vertex $j$ and moves in the $i^{\text{th}}$ step to the $\sigma_i^{\text{th}}$ neighbor of the current vertex. Now, fixing the random sequence $\overline{\sigma}$, consider an arbitrary sequence $\overline{\tau} = (\tau_1, ..., \tau_t) \in [d']^t$, and let $B^{(\overline{\sigma},\overline{\tau})}$ be the $t$-by-$n$ Boolean matrix such that its $(i,j)^{\text{th}}$ entry indicates whether the $j^{\text{th}}$ walk passed in $T_{\tau_i}$ in its $i^{\text{th}}$ step. The* relaxed CRW property *asserts that, for some $t \geq n$, with probability at least $1-\exp(-n-\Omega(t))$ over the choice of $\overline{\sigma} \in [d]^t$, there exists $\overline{\tau} \in [d']^t$ such that the Boolean matrix $B^{(\overline{\sigma},\overline{\tau})}$ has full rank.*

(Indeed, Definition 5 corresponds to the special case of $d' = 1$.)

**Theorem 11** (constructing 1-local expanders is equivalent to constructing relocation graphs along with sets that satisfy Definition 10): *Let $\pi^{(1)}, ..., \pi^{(d)} : [n] \to [n]$ be permutations.*

1. *If the 1-local $2d$-regular $2^n$-vertex graph associated with $\pi^{(1)}, ..., \pi^{(d)}$ and $s^{(1)}, ..., s^{(d)} \in \{0,1\}^n$ is an expander, then the corresponding $2d$-regular $n$-vertex relocation graph along with the sets $T_1, ..., T_{2d}$ such that $T_{2i} = \{j \in [n] : s^{(i)}_j = 1\}$ and $T_{2i-1} = \{\pi^{(i)}(j) : s^{(i)}_j = 1\}$ satisfies Definition 10.*

2. *Suppose that the $2d$-regular $n$-vertex relocation graph associated with $\pi^{(1)}, ..., \pi^{(d)}$ along with the sets $T_1, ..., T_{d'}$ satisfies Definition 10, and for every $\alpha \in \{0,1\}^{d'}$ let $s^{(\alpha)} \in \{0,1\}^n$ denote the indicator string of the set $\bigoplus_{i:\alpha_i=1} T_i \subseteq [n]$; that is, the $j^{\text{th}}$ bit of $s^{(\alpha)}$ is 1 if and only if $|\{i \in [d'] : \alpha_i = 1 \ \&j \in T_i\}|$ is odd. Then, the $2^{2d'+1} \cdot d$-regular $2^n$-vertex graph with the edge multi-set $\cup_{i\in[d],\beta,\gamma\in\{0,1\}^{d'}} \{\{x, (x \oplus s^{(\beta)})_{\pi^{(i)}} \oplus s^{(\gamma)}\} : x \in \{0,1\}^n\}$ is an expander.*

**Proof:** We start with the proof of Part 2, which generalizes the proof of Theorem 7. Specifically, let $\overline{\sigma} = (\sigma_1, ..., \sigma_t) \in [2d]^t$ be a random walk on the relocation graph such that an even $\sigma_i$ (resp., an odd $\sigma_i$) indicates a forward (resp., reverse) transition using $\pi^{(\lceil \sigma_i/2 \rceil)}$. Then, by the hypothesis, with probability at least $1 - \exp(-\Omega(t))$ over the choice of $\overline{\sigma}$, there exists $\overline{\tau} = (\tau_1, ..., \tau_t)$ such that $B^{(\overline{\sigma},\overline{\tau})}$ is full rank. When analyzing a corresponding random walk on the 1-local graph, consider the following process of determining the sequence of auxiliary random choices of $\beta_1, ..., \beta_t \in \{0,1\}^{d'}$ and $\gamma_1, ..., \gamma_t \in \{0,1\}^{d'}$.

1. For every $i$ such that the $i^{\text{th}}$ step is a forward (resp., reverse) transition,
   (a) select $\beta_i$ (resp., $\gamma_i$) uniformly in $\{0,1\}^{d'}$, and,
   (b) for every $k \in [d'] \setminus \{\tau_i\}$, select the bit $\gamma_{i,k}$ (resp., $\beta_{i,k}$) uniformly in $\{0,1\}$.
2. For every $i$ such that the $i^{\text{th}}$ step is a forward (resp., reverse) transition, select $\gamma_{i,\tau_i}$ (resp., $\beta_{i,\tau_i}$) uniformly in $\{0,1\}$.

Fixing a good $\overline{\sigma}$ and a corresponding good $\overline{\tau}$ (i.e., choices such that $B^{(\sigma,\tau)}$ is full rank), consider an arbitrary fixing of the choices in Step 1. Then, the label of the final vertex in the corresponding random walk on the 1-local graph is a fixed string that is offset by a random linear combination of the rows of $B^{(\overline{\sigma},\overline{\tau})}$, where the random linear combination is determined in Step 2. (Specifically, if the $i^{\text{th}}$ step is a forward (resp., reverse) transition, then the $i^{\text{th}}$ row is included in this offset if and only if $\gamma_{i,\tau_i} = 1$ (resp., $\beta_{i,\tau_i} = 1$).) Thus, when $B^{(\overline{\sigma},\overline{\tau})}$ has full rank, the label of the final vertex is uniformly distributed in $\{0,1\}^n$, and Part 2 follows.

Turning to the proof of Part 1, we start by considering the $4d$-regular $2^n$-vertex 1-local expander obtained from the given $2d$-regular 1-local expander by augmenting each transition of the form $x \mapsto x_\pi \oplus s$ with the transition $x \mapsto x_\pi$. (The auxiliary graph is an expander because it conatins an expander as a subgraph.) Hence, a step on this auxiliary graph is specified by a pair $(\sigma, b) \in [2d] \times \{0,1\}$, where $\sigma$ specifies a step on the original 1-local graph and $b$ specifies whether the original offset is applied (i.e., we shall refer to the edge multi-set $\cup_{i \in [d], b \in \{0,1\}} \{\{x, x_{\pi^{(i)}} \oplus (s^{(i)})^b\} : x \in \{0,1\}^n\}$). Cosequently, a $t$-step random walk on the $4d$-regular expander corresponds to a sequence $(\sigma_1, b_1), ..., (\sigma_t, b_t) \in ([2d] \times \{0,1\})^t$, and the sequence $\sigma_1, ..., \sigma_t$ corresponds to a walk on the $n$-vertex relocation graph. Determining the $\tau_i$'s based on the $\sigma_i$'s yields a matrix as in Definition 10, Specificallty, we shall determine the $\tau_i$'s so that the fit the $\sigma_i$'s transition, while recalling that $\sigma_i$ determines both the edge used and the direction in which it is tranversed. (Suppose, again, without loss of generality, that an even $\sigma_i$ (resp., an odd $\sigma_i$) indicates a forward (resp., reverse) transition using $\pi^{(\lceil \sigma_i/2 \rceil)}$. Then, we let $\tau_i = \sigma_i$.)[27]

Now, we claim that if a $t$-step random walk on the $4d$-regular 1-local graph yields a distribution that is $\exp(-\Omega(t))$-close to uniform (and $t = \Omega(n)$ is large enough), then the matrix $B^{(\overline{\sigma},\overline{\sigma})}$ must have full rank with probability at least $1 - \exp(-\Omega(t))$. This claim is shown as follows.

Let $\eta$ denote the probability (over the choice of $\overline{\sigma} \in [2d]^t$) that the matrix $B^{(\overline{\sigma},\overline{\sigma})}$ does not have full rank. Such a choice of $\overline{\sigma}$ determines both the permutation $\pi_{\overline{\sigma}}$ that relates the original locations to the final ones (i.e., $\pi_{\overline{\sigma}} = \pi^{((-1)^{\sigma_t} \cdot \lceil \sigma_t/2 \rceil)} \circ \cdots \circ \pi^{((-1)^{\sigma_1} \cdot \lceil \sigma_1/2 \rceil)}$) and a non-trivial linear combination $J_{\overline{\sigma}}$ of the columns of the matrix that witnesses that the matrix is not full rank. Hence,

[27] Note that if $\sigma_i = 2k$ (resp., $\sigma = 2k-1$), then the $i^{\text{th}}$ step applied the forward (resp., reverse) transition $x \mapsto x_{\pi^{(k)}} \oplus s^{(k)}$ (resp., $y \mapsto (y \oplus s^{(k)})_{\pi^{(-k)}}$, where $\pi^{(-k)}$ denotes the inverse of $\pi^{(k)}$). Recall that $T_{2k} = \{j \in [n] : s^{(k)}_j = 1\}$ and $T_{2k-1} = \{\pi^{(k)}(j) : s^{(k)}_j = 1\} = \{j : s^{(k)}_{\pi^{(-k)}(j)} = 1\}$.

with probability $\eta' \geq \eta/(2^n-1)$ over the choice of $\overline{\sigma}$, there exists a non-empty set $J \subseteq [n]$ such that the sum of the columns indexed by $\pi_{\overline{\sigma}}^{-1}(J)$ (in the matrix $B^{(\overline{\sigma},\overline{\sigma})}$) equals the all-zero vector, whereas in the remaining choices (of $\overline{\sigma}$) this sum does not equals the all-zero vector.[28] Looking at the label of the final vertex $v_{\overline{\sigma}}$ in a random walk $\overline{\sigma}$ on the 1-local $2^n$-vertex graph that starts at the vertex $0^n$, we observe that $v_{\overline{\sigma}}$ equals a random linear combination of the rows of $B^{(\overline{\sigma},\overline{\sigma})}$ permuted by $\pi_{\overline{\sigma}}$ (i.e., $(v_{\overline{\sigma}})_{\pi_{\overline{\sigma}}^{-1}}$ equals a random linear combination of the rows of $B^{(\overline{\sigma},\overline{\sigma})}$, where this random linear combination is determined by the sequence $(b_1,...,b_t)$).[29] It follows that the sum of $v_{\overline{\sigma}}$'s bits in locations $J$ is zero with probability exactly $\eta' + (1-\eta') \cdot 0.5 = 0.5 + 0.5\eta'$, since this sum is 0 if the sum of the corresponding columns in $B^{(\overline{\sigma},\overline{\sigma})}$ is the all-zero vector (and is uniformly distributed in $\{0,1\}$ otherwise). Hence, the distribution of the final vertex is $0.5\eta'$-far from the uniform distribution. The claim follows, since $\eta' \leq \exp(-\Omega(t))$ by the hypothesis, whereas this implies $\eta \leq 2^n \cdot \exp(-\Omega(t)) = \exp(-\Omega(t))$ for sufficiently large $t = \Omega(n)$. ■

**Problem 12** (the CRW problem, revised): *For which graphs and which sequences of sets $(T_1,...,T_{d'})$'s does the random matrix considered in Definition 10 have full rank with probability at least $1-\exp(-\Omega(t))$?*

An appealing conjecture of Benny Applebaum is that every $n$-vertex expander graph yield a positive answer to Problem 12 (i.e., there exists $d' = O(1)$ sets $T_1,...,T_{d'} \subset [n]$ such that this $n$-vertex graph combined with these sets satisfies the relaxed CRW property of Definition 10).

# 6 An afterthought: Generalization to non-binary alphabets

We generalize the basic definitions to an arbitrary alphabet of prime size, which is identified with the field $\mathrm{GF}(p)$. A function $f : \mathrm{GF}(p)^n \to \mathrm{GF}(p)^n$ is called $t$-local if each symbol in its output depends on at most $t$ symbol in its input. This yields to a generalized notion of a 1-local expander.

**Definition 13** (1-local expanders, generalized): *For a fixed $d \in \mathbb{N}$ and a fixed prime $p$, let $\{f_1,...,f_d : \mathrm{GF}(p)^n \to \mathrm{GF}(p)^n\}_{n\in\mathbb{N}}$ be 1-local bijections. Then, the corresponding $2d$-regular $p^n$-vertex graph consists of the vertex set $\mathrm{GF}(p)^n$ and the edge multiset $\cup_{i\in[d]}\{\{x, f_i(x)\} : x \in \mathrm{GF}(p)^n\}$.*

Note that each $f_i$ is determined by a permutation on the bit locations $\pi^{(i)} : [n] \to [n]$, called the relocation, and $n$ bijections denoted $h_1^{(i)},...,h_n^{(i)} : \mathrm{GF}(p) \to \mathrm{GF}(p)$. Unlike in the binary case, where each $h_j^{(i)} : \mathrm{GF}(2) \to \mathrm{GF}(2)$ is linear (i.e., has the form $h_j^{(i)}(z) = z \oplus s_j^{(i)}$), here these bijections are not necesarily linear functions. Still, we shall focus on the case that they are linear. Generalizing Theorems 7 and 8, we obtain.

[28] The issue here is as follows: We know that for $\eta$ fraction of the $\overline{\sigma}$'s, there exists a $J_{\overline{\sigma}}$ such that the sum of these columns is the all-zero vector. However, these columns corresponds to locations in the (label of the) initial vertex, whereas we want to analyze locations in the end vertex. Still, there exists a non-empty $J$ (representing locations in final label) such that the sum of the columns in $\pi_{\overline{\sigma}}^{-1}(J)$ (representing locations in initial label) equals the all-zero vector with probability $\eta' > \eta/(2^n-1)$. Needless to say, for the rest of this probability space (of $\overline{\sigma} \in [2d]^t$), the sum is not the all-zero vector.

[29] This is the case since the $i^{\text{th}}$ row permuted by $\pi^{((-1)^{\sigma_i}\cdot\lceil\sigma_i/2\rceil)} \circ \cdots \circ \pi^{((-1)^{\sigma_1}\cdot\lceil\sigma_1/2\rceil)}$ is the offset that is potentially added in the $i^{\text{th}}$ step of the walk, whereas this offset is added if and only if $b_i = 1$.

**Theorem 14** (a construction of generalized 1-local expanders): *For every constant prime $p$, there exists a set of $d = O(p^2)$ explicit 1-local bijections, $\{f_1, ..., f_d : \mathrm{GF}(p)^n \to \mathrm{GF}(p)^n\}_{n\in\mathbb{N}}$, such that the $2d$-regular $p^n$-vertex graph that consists of the vertex set $\mathrm{GF}(p)^n$ and the edge multiset $\cup_{i\in[d]}\{\{x, f_i(x)\} : x \in \mathrm{GF}(p)^n\}$ is an expander. Furthermore, the $f_i$'s are linear mappings.*

**Proof:** The overall plan is to use a straightforward generalization of the CRW property for rank defined over $\mathrm{GF}(p)$, show that any generating set for the symmetric group of $n$ elements that is expanding (along with any set of size $n' \approx n/2$ such that $n' \not\equiv 0 \pmod p$) satisfies this property, and that this yields a 1-local $p^n$-vertex expander.

Definition **14.1** (a property of coordinated random walks, generalized): *For a $d$-regular $n$-vertex graph as in Definition 5, a set $T \subseteq [n]$ and $t \geq n$, consider coordinated random walks and Boolean matrices just as in Definition 5. The* generalized CRW property *postulates that, with probability at least $1-\exp(-\Omega(t)-n\log p)$, such a random matrix has full rank* when the arithmetics is in $\mathrm{GF}(p)$.

We stress that although these random matrices have entries in $\{0,1\}$, we consider their rank over $\mathrm{GF}(p)$. Also, the probability bound for the bad event (i.e., the matrix not being full rank) is set lower so to account for the size of the 1-local graph (i.e., $p^n$).

Claim **14.2** (Theorem 7, generalized): *Let $\pi^{(1)}, ..., \pi^{(d)} : [n] \to [n]$ be $d$ permutations and $s = (s_1, ..., s_n) \in \{0,1\}^n \subseteq \mathrm{GF}(p)^n$. If the $2d$-regular $n$-vertex graph with the edge multi-set $\cup_{i\in[d]}\{\{j, \pi^{(i)}(j)\} : j \in [n]\}$ along with the set $\{j \in [n] : s_j = 1\}$ satisfies the generalized CRW property* (of Definition 14.1)*, then the $2p^2d$-regular $p^n$-vertex graph with the edge multi-set $\cup_{i\in[d],b,c\in\mathrm{GF}(p)}\{\{x, (x - b\cdot s)_{\pi^{(i)}} + c\cdot s\} : x \in \mathrm{GF}(p)^n\}$ is an expander, where $b\cdot(s_1, ..., s_n) = (bs_1, ..., bs_n)$.*

**Proof Sketch:** We mimic the proof of Theorem 7, while noting that in the $i^{\text{th}}$ step the vertex's label is randomized by an offset that is a random $\mathrm{GF}(p)$-multiple of the $i^{\text{th}}$ row in the corresponding matrix. Hence, if the matrix has full rank over $\mathrm{GF}(p)$, then the label of the final vertex is uniformly distributed in $\mathrm{GF}(p)^n$ (since it is randomized by a random linear combination of the rows of the matrix). ■

Claim **14.3** (Theorem 8, generalized): *Let $\Pi = \{\pi^{(i)} : i \in [d]\}$ be a generating set of the symmetric group of $n$ elements and suppose that $\Pi$ is expanding. Then, the $n$-vertex graph that consists of the vertex set $[n]$ and the edge multi-set $\cup_{i\in[d]}\{\{j, \pi^{(i)}(j)\} : j \in [n]\}$ combined with any set of size $n' \approx n/2$ such that $n' \not\equiv 0 \pmod p$ satisfies the generalized CRW property of Definition 14.1.*

**Proof Sketch:** Here we mimic the proof of Theorem 8. Specifically, we consider all (non-zero) linear combinations $L : [n] \to \mathrm{GF}(n)$ of the columns of a random matrix, and upper bound the probability that each such linear combination yields the all-zero vector. That is, fixing an set $T$ of size $n'$, for every such linear combination $L$, we consider the set $W_L$ of permutations $\pi \in \mathtt{Sym}_n$ such that $\sum_{i\in[n]:\pi(i)\in T} L(i) \not\equiv 0 \pmod p$. Once we show that each $W_L$ has constant density, the claim follows as in the binary case (where here we use a union bound on all $L$'s).

The case of constant function $L : [n] \to \mathrm{GF}(p)$ is handled by the hypothesis that $n' \not\equiv 0 \pmod p$ (which implies that $W_L = \mathtt{Sym}_n$), and so we focus on non-constant functions $L$. We shall show that, for every value $v \in \mathrm{GF}(p)$, the fraction of permutations $\pi$ such that $\sum_{i\in[n]:\pi(i)\in T} L(i) \equiv v \pmod p$ is at most $0.5 + o(1)$, and infer that $W_L$ has density at least $0.5 - o(1)$ (by upper-bounding the density of $\mathtt{Sym}_n \setminus W_L$, which refers to the case of $v = 0$).

We first reduce the general case to the case that $L$ has at least $n/p$ zero entries (i.e., $|\{j \in [n] : L'(j) = 0\}| \geq n/p$): Given an arbitrary (non-constant) $L' : [n] \to \mathrm{GF}(p)$, let $w \in \mathrm{GF}(p)$ be an element that appears at least $n/p$ times in $L$ (i.e., $|\{j \in [n] : L'(j) = w\}| \geq n/p$), and consider the (non-zero) function $L(j) = L'(j) - w$. Next, letting $J = \{i \in [n] : L(i) \neq 0\}$, suppose that we generate a random permutation $\pi$ by first assigning elements to $J$, and consider the situation before the last assignment (i.e., after assigning $|J|-1$ elements). Using the hypothesis that $|T| = n' \approx n/2$, w.v.h.p., before this last assignment, these $|J| - 1 < n - n/p$ locations were assigned approximately an equal number of elements from $T$ and from $[n] \setminus T$, which means that $n' - (1 \pm o(1)) \cdot |J|/2 = (1 \pm o(1)) \cdot (n - |J|)/2$ elements from each type remain for the last assignment, where $n - |J| \geq n/p = \Omega(n)$. This means that the value of $\sum_{i \in [n]:\pi(i) \in T} L(i) \bmod p$ changes at the last assignment with probability $(1 \pm o(1))/2 \approx 1/2$ (i.e., if $i_{|J|}$ is the last element in $J$ being assigned an element, then $L(i_{|J|})$ is added to the current sum with probability $\approx 1/2$). The claim follows (since if the partial sum was $v$ before the last assignment then it changes with probability at least $0.5 - \epsilon$, whereas if the partial sum was not $v$ then it becomes $v$ with probability at most $0.5 + o(1)$).

Having shown that $W_L$ has constant density and using the hypothesis (regarding $\Pi$), we infer that, with probability at least $1 - (p^n - p) \cdot \exp(-\Omega(t) + O(n \log n))$ over the $t$-step random walk on the $n$-vertex graph, the corresponding $t$-by-$n$ Boolean matrix has full rank over $\mathrm{GF}(p)$. Picking a sufficiently large $t = \Omega(n \log n)$, the claim follows. ■

Combining Claims 14.3 and 14.2, we get.

**Corollary 14.4** (obtaining generalized 1-local expanders): *Let $\Pi = \{\pi^{(i)} : i \in [d]\}$ be a generating set of the symmetric group of $n$ elements and suppose that $\Pi$ is expanding. Then, for any $n' \approx n/2$ such that $n' \not\equiv 0 \pmod p$, the $2p^2d$-regular $p^n$-vertex graph with the edge multi-set $\cup_{i \in [d], b, c \in \mathrm{GF}(p)} \{\{x, (x - b^{n'}0^{n-n'})_{\pi^{(i)}} + c^{n'}0^{n-n'}\} : x \in \mathrm{GF}(p)^n\}$ is an expander.*

Using Kassabov's result [4] (which asserts that the symmetric group has an explicit generating set that is expanding and of constant size), the theorem follows. ■

**Comment:** The foregoing generalizes to any finite field; that is, $p$ may be a prime power. For $p = q^e$, where $q$ is prime, we select $n' \approx n/2$ such that $n' \not\equiv 0 \pmod q$, and proceed as above (while noting that in the proof of Claim 14.3 the reductions mod $p$ actually refer to doing the arithmetics in $\mathrm{GF}(p)$).

## Acknowledgments

I wish to thank Benny Applebaum for helpful discussions and for permission to include his conjecture in this text. I am also extremely grateful to Roei Tell for commenting on several drafts of this text.

This work was partially supported by the Minerva Foundation with funds from the Federal German Ministry for Education and Research.

## References


[1] A. Broder and A. Karlin. Bounds on the cover time. *J. of Theoretical Probability*, Vol. 2 (1), pages 101–120, 1989.

[2] A.K. Chandra, P. Raghavan, W.L. Ruzzo, R. Smolensky, and P. Tiwari. The electrical resistance of a graph, and its applications to random walks. In *21st STOC*, 1989.

[3] S. Horry, N. Linial, and A. Wigderson. Expander graphs and their applications. *Bull.* (new series) *of the AMS*, Vol. 43 (4), pages 439–561, 2006.

[4] M. Kassabov. Symmetric groups and expander graphs. *Invent. Math.*, Vol. 170 (2), pages 327–354, 2007.

[5] R. Rubinfeld. The cover time of a regular expander is $O(n \log n)$. *IPL*, Vol. 35, pages 49–51, 1990).

[6] E. Viola and A. Wigderson. Local Expanders. *ECCC*, TR16-129, 2016.




ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il