HAMILTONIAN PATHS IN CAYLEY GRAPHS

Igor Pak, Radoš Radoičić

Department of Mathematics, MIT
Cambridge, MA 02139
pak@math.mit.edu, rados@math.mit.edu

August 13, 2004

Abstract. The classical Lovász conjecture says that every connected Cayley graph is Hamiltonian. We present a short survey of various results in that direction and make some additional observations. In particular, we prove that every finite group G has a generating set of size at most $\log_2 |G|$, such that the corresponding Cayley graph contains a Hamiltonian cycle. We also present an explicit construction of 3-regular Hamiltonian expanders.

Introduction

Finding Hamiltonian cycles in graphs is a difficult problem, of interest in combinatorics, computer science, and applications. It is one of the classical **NP**-complete problems, and thus not expected to have a simple solution [GJ]. In 1969 Lovász conjectured that every vertex-transitive graph has a Hamiltonian path [Lo1]. Despite a significant effort [CG,WG], there has been very little progress towards resolving this conjecture in full generality. Further, some authors strongly disbelieve the conjecture and see little hope in proving it (see section 4 for references and details). In this paper we survey several little known results that until now were scattered in literature. We prove these results in modern language, as well several new results. In particular, we present a rare positive result for *all* finite groups:

Theorem 1. *Every finite group G of size $|G| \geq 3$ has a generating set S of size $|S| \leq \log_2 |G|$, such that the corresponding Cayley graph $\Gamma(G,S)$ contains a Hamiltonian cycle.*

The result is optimal in a sense that the size of the smallest generating set of group G, denoted $d(G)$, is equal to $\log_2 |G|$ for $G = \mathbb{Z}_2^m$. Of course, for other groups $d(G)$ is much smaller. For example, $d(G) = 2$ for all finite simple groups [Go]. We obtain optimal results in this case as well (see section 1).

Key words and phrases. Hamiltonian cycles and paths, simple groups, expander graphs, explicit constructions.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Note that we cannot prove that all, or even most, Cayley graphs of a finite group (with a fixed number of, say, $d(G)$ generators) are Hamiltonian.[1] Even for simple groups, or for symmetric groups S_n (generated by two elements), Lovász conjecture remains infeasible. Instead, Theorem 1 shows that every finite group G has a Hamiltonian Cayley graph with a generating set of small size. The proof relies on an explicit combinatorial construction and a consequence from the Classification of Finite Simple Groups (CFSG).

Our second result is an explicit construction of 3-regular Hamiltonian expanders. Expanders are highly connected graphs of bounded degree. They have a number of useful graph theoretic properties, and have applications in a number of problems in computer science, ranging from parallel computation to complexity theory, from cryptography to coding theory, and, most recently, computational group theory (see e.g. [AKS,G+,LP,SS,V,WZ].) It is well known that random d-regular graphs are expanders with high probability, for $d \geq 3$ [JLR]. However, finding *explicit constructions* of expanders is an important problem of interest in Combinatorics and Computer Science. The first such constructions were found in [M1,M2,LPS] (see also [Lu1,RVW].)

In this paper we present a construction of Hamiltonian 3-regular Cayley graphs, and prove that these are expanders. We should emphasize that the existence of such expanders has been known for years since random d-regular graphs are Hamiltonian for all $d \geq 3$ (see e.g. [RW]). Our construction is related to involutions of Nuzhin [N4] and the expansion is proved by reduction to expanders of Lubotzky-Phillips-Sarnak [LPS].

This paper is written in a mixture of research and survey styles. We start with definitions and main results in section 1. Then, in section 2, we present proofs of three interrelated combinatorial lemmas, two of which are known in the literature. This is the heart of the paper. We prove theorems by technical arguments in section 3. At this point point we switch to a survey style and in an extensive section 4 we elaborate on the history behind this problem, connections to problems in graph theory, probabilistic and geometric group theory, etc. We also include a number of references and promising research venues.

Let us mention here the previous survey articles [CG,WG] which have virtually no overlap with results in this paper. We really hope the reader enjoys this subject as much as we do, and are looking forward to future progress in this direction.

1. Main Results

Let G be a finite group and let S be a generating set. A *Cayley graph* $\Gamma = \Gamma(G, S)$ is defined to be a graph with vertices $g \in G$, and edges (g, gs), $(g, gs^{-1}) \in G^2$, where $s \in S$. We shall ignore labels and orientation of edges and treat Γ as a simple graph on $|G|$ vertices. Clearly, Γ is d-regular, where $d = |S|$. From this point on, we consider only Cayley graphs.

A *Hamiltonian path* is a path in Γ which goes though all vertices exactly once. A *Hamiltonian cycle* is a closed Hamiltonian path. *Lovász conjecture* claims that every connected Cayley graph contains a Hamiltonian path.

---

[1] We refer to a graph as Hamiltonian, if it contains Hamiltonian cycle or Hamiltonian path, depending on a context. We hope this will not lead to a confusion, as there is little difference between these two notions.

Let G be a finite group, and let $\ell(G)$ be the number of composition factors of G. Denote by $r(G)$ and $m(G)$ the number of abelian and nonabelian composition factors, respectively. Clearly, $\ell(G) = r(G) + m(G)$.

Theorem 2. *Let G be a finite group, and let $r(G)$ and $m(G)$ be as above. Then there exists a generating set S, $\langle S\rangle = G$, with $|S| \le r(G) + 2m(G)$, such that the corresponding Cayley graph $\Gamma(G,S)$ contains a Hamiltonian path.*

Since the smallest nonabelian simple group has order $|A_5| = 60$, one can show that Theorem 2 implies Theorem 1 (see section 3).

For every subset of vertices $X \subset G$ define ∂X to be the set of vertices $v \in G - X$, which are connected to X by an edge. We say that a graph is *ε-expander* if for every $|X| \le |G|/2$, we have $|\partial X| > \varepsilon |X|$, for some fixed $\varepsilon > 0$.

Let p be a prime, $p \equiv 1 \mod 4$. Let $\mathbb{F}_p$ be a finite field with p elements, and $a \in \mathbb{F}_p$ such that $a^2 = -1$. Consider a group $\mathrm{SL}(2,p)$ of two by two matrices over $\mathbb{F}_p$ with determinant one. Let $G = \mathrm{PSL}(2,p)$ be a quotient of $\mathrm{SL}(2,p)$ by the subgroup of diagonal matrices $\{\pm 1\}$. By abuse of notation, we use matrices to denote elements of $\mathrm{PSL}(2,p)$.

Consider three elements $\alpha, \beta, \gamma \in \mathrm{PSL}(2,p)$, given by the matrices

$$\alpha = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}, \ \beta = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ \gamma = \begin{pmatrix} a & 0 \\ a & -a \end{pmatrix}.$$

These particular generators were introduced by Nuzhin in [N4]. One can easily check that $\alpha^2 = \beta^2 = \gamma^2 = 1$ (see section 3). Now consider Cayley graphs

$$\Gamma_p = \Gamma\big(\mathrm{PSL}(2,p), \{\alpha, \beta, \gamma\}\big).$$

Theorem 3. *Cayley graphs Γ_p defined as above contain Hamiltonian cycles and are ε-expanders, for some $\varepsilon > 0$, independent of prime $p \equiv 1 \mod 4$.*

Note that one cannot hope to obtain a sharper result since connected 2-regular graphs are simple cycles. Proof of Theorems 2 and 3 are based on combinatorial lemmas of independent interest. We present these lemmas in the following section.

2. Combinatorial Conditions for Hamiltonicity

Let G be a finite group with a generating set S, and $|S| \le 3$. In this section we consider simple relations on generators which suffice to prove that the Cayley graph $\Gamma(G,S)$ contains a Hamiltonian cycle.

An element $\alpha \in G$ is called an *involution*, if $\alpha^2 = 1$.

Lemma 1. (Rapaport-Strasser) *Let G be a finite group, generated by three involutions α, β, γ. Suppose $\alpha\beta = \beta\alpha$. Then the Cayley graph $\Gamma = \Gamma(G, \{\alpha, \beta, \gamma\})$ contains a Hamiltonian cycle.*

Proof. For every $z \in G$ and every $X \subset G$, denote

$$\partial_z(X) = \{g \in G - X \,:\, g = x\,z,\, x \in X\}.$$

Denote by $H = \langle \beta, \gamma \rangle$ a subgroup of G of order $|H| = 2m$. Let $X_1 = H$. Since H is a dihedral group, X_1 contains a Hamiltonian cycle:

$$(*) \qquad 1 \to \beta \to \beta\gamma \to \beta\gamma\beta \to \cdots \to (\beta\gamma)^{m-1}\beta \to (\beta\gamma)^m = 1.$$

We shall construct a Hamiltonian cycle in Γ by induction. At step i we obtain a cycle which spans set $X_i \subset G$. Further, each X_i will satisfy the condition $\partial_\beta(X_i) = \partial_\gamma(X_i) = \emptyset$. This is equivalent to saying that each X_i is a union of left cosets of H. By definition, $\partial_\beta(X_1) = \partial_\gamma(X_1) = \emptyset$. This establishes the base of induction.

Now suppose X_i is as above. Either $\partial_\alpha(X_i) = \emptyset$, in which case the spanning cycle in X_i is a Hamiltonian cycle. Otherwise, there exists $y \in \partial_\alpha(X_i) \subset G - X_i$. Observe that $y\,H \cap X_i = \emptyset$, since otherwise $y \cdot h = x \in X_i$, for some $h \in H$. This implies that $y = x \cdot h^{-1} \in X_i$, since $h \in \langle \beta, \gamma \rangle$ and $z\beta, z\gamma \in X$ for all $z \in X$.

Let $X_{i+1} = X_i \cup y\,H$. Clearly, $\partial_\beta(X_{i+1}) = \partial_\gamma(X_{i+1}) = \emptyset$. By inductive assumption, $x = y\alpha \in X_i$ lies on a cycle which spans X_i. Then x must be connected to $x\beta$ and $x\gamma$, as $x\alpha = y \notin X_i$. Consider a cycle in $y \cdot H$, obtained by multiplying cycle in $(*)$ by y. Recall that $\alpha\beta = \beta\alpha$. This implies $x\beta\alpha = y\beta$. Remove edges $(x, x\beta)$ and $(y, y\beta)$ from cycles in X_i and $y\,H$, and add (x, y), $(x\beta, y\beta)$. This gives a cycle which spans X_{i+1}, and completes the step of induction. □

Example 1. Consider $G = S_{2n+1}$ and three involutions $\alpha = (1\,2)$, $\beta = (1\,2)(3\,4)\cdots(2n-1\,2n)$, $\gamma = (2\,3)(4\,5)\cdots(2n\,2n+1)$ (we use cycle notation here.) Observe that

$$\beta\gamma = (1\,3\,5\,\ldots\,2n-1\,2n+1\,2n\,2n-2\,\ldots\,4\,2),$$

so $\langle \alpha, \beta, \gamma \rangle = S_{2n+1}$. Note also that $\alpha\beta = \beta\alpha$. Then Lemma 1 implies that the Cayley graph $\Gamma(S_n, \{\alpha, \beta, \gamma\})$ contains a Hamiltonian cycle. This result goes back to [RS] (cf. section 4).

The following result is not formally needed to prove Theorem 2, but is of independent interest. It also gives new interesting examples and helps to smooth the transition from the proof of Lemma 1 to the proof of Lemma 3.

Lemma 2. *Let G be a finite group, generated by an involution β and an element α. Let $\gamma = \beta^\alpha := \alpha^{-1}\beta\alpha$. Then the Cayley graph $\Gamma = \Gamma(G, \{\alpha, \beta, \gamma\})$ contains a Hamiltonian cycle.*

Proof. We use the same induction assumption as in the proof of Lemma 1, but the induction step requires more cases to consider. As before, let $H = \langle \beta, \gamma \rangle \subset G$. Let $X_1 = H$. We assume that Γ restricted to X_i contains a Hamiltonian cycle C_i, and that $\partial_\beta(X_i) = \partial_\gamma(X_i) = \emptyset$. Further, we assume that in the sequence of labels of the *oriented* Hamiltonian cycle C_i no label α^{-1} precedes label β or succeeds label γ.[2] Similarly, assume that in C_i no label α precedes label γ or succeeds label β (other possibilities are allowed). We shall call these *label conditions* on the cycle.

For the step of induction, recall that α is no longer an involution. Either $\partial_\alpha(X_i) = \partial_{\alpha^{-1}}(X_i) = \emptyset$, in which case $X_i = G$ and we are done, or at least one of these subsets is nonempty. Suppose there exists $y = x\alpha \in \partial_\alpha(X_i) \subset G - X_i$,

---

[2] We are using the terms *precedes* and *succeeds* as a shorthand for "occurs right before" and "occurs right after", respectively.

where $x \in X_i$. Let $X_{i+1} = X_i \sqcup yH$, as in the proof of Lemma 1. It remains to show that X_{i+1} contains a Hamiltonian cycle C_{i+1} in this case, satisfying conditions as above.

Observe that of the three remaining possibilities (α^{-1}, β, and γ) at least one of the two edges adjacent to x in a Hamiltonian cycle C_i in X_i must be an involution β or γ. In the first case, the cycles C_i in X_i and R in yH are connected by a square:

$$x \to y = x\alpha \to y\gamma = x\alpha\gamma \to x\alpha\gamma\alpha^{-1} \to x\alpha\gamma\alpha^{-1}\beta = x,$$

so we can join the two cycles. Formally, remove edges $(x, x\beta)$ and $(y, y\gamma)$ from the union of two cycles $C_i \cup R$, and add edges (x, y), $(x\beta, y\gamma)$. Clearly, the resulting graph C_{i+1} is a Hamiltonian cycle in X_{i+1} indeed. We should note that C_{i+1} inherits orientation from C_i, due to the fact that labels of R are all involutions β and γ, and can be oriented accordingly. A simple check shows that the label conditions for C_{i+1} with respect to such orientation are all satisfied.

Now suppose neither of the two edges adjacent to x in C_i is β. By the label conditions, label α cannot precede γ and thus must succeed it. Similarly, label α^{-1} cannot succeed γ and thus must precede it. But in both of these label arrangements this contradicts the fact that an edge leaving x in C_i must have label α^{-1} (in the direction of the cycle, opposite direction). Therefore we can discard these possibilities, which finalizes the case $y = x\alpha$.

Now, suppose $y = x\alpha^{-1} \in \partial_{\alpha^{-1}}(X_i) \subset G - X_i$. Since $\beta = \alpha\gamma\alpha^{-1}$, we can proceed as before, with the roles of β and γ, α and α^{-1} interchanged. Note that the label conditions are invariant under this transformation. This completes the step of induction. □

Example 2. Let $G = S_n$, and let $\alpha = (1\,2\,\ldots\,n)$, $\beta = (1\,2)$, $\gamma = (2\,3)$. Observe that $\gamma = \alpha^{-1}\beta\alpha$. Then Lemma 2 implies that the Cayley graph $\Gamma(S_n, \{\alpha, \beta, \gamma\})$ contains a Hamiltonian cycle. In fact, a subgraph $\Gamma(S_n, \{\alpha, \beta\})$ is already Hamiltonian [CW] (cf. section 4).

Lemma 3. (Rankin) *Let G be a finite group, generated by two elements α and β, such that $(\alpha\beta)^2 = 1$. Then the Cayley graph $\Gamma = \Gamma(G, \{\alpha, \beta\})$ contains a Hamiltonian cycle.*

Proof. Again, we use an inductive assumption with a new simple label condition. Let $H = \langle\beta\rangle$, $X_1 = H$, and assume that $\partial_\alpha(X_i) = \partial_{\alpha^{-1}}(X_i) = \emptyset$. We also assume, by induction, that restriction of Γ to X_i contains an oriented Hamiltonian cycle C_i, which contains only labels β and α^{-1}. We call these the label conditions.

The base of induction is obvious. For the step of induction, consider $y = x\alpha \in \partial_\alpha X_i - X_i$. Note that the edge oriented towards $x \in X_i$ in C_i cannot have label α^{-1} (otherwise it is (y, x), whereas $y \notin X_i$) nor labels α, or β^{-1} (by the label conditions). Therefore this edge has the only remaining label β, and $(x\beta^{-1}, x) \in C_i$. Now consider a cycle R on yH with labels β on all edges, and observe that

$$x \to x\alpha = y \to x\alpha\beta = y\beta \to x\beta^{-1} = x\alpha\beta\alpha \to x$$

is a square which connects R and C_i. Formally, let

$$C_{i+1} = C_i \cup R + (x, y) + (y\beta, x\beta^{-1}) - (x\beta^{-1}, x) - (y, y\beta),$$

and observe that C_i is a Hamiltonian cycle on $X_{i+1} = X_i \cup yH$. Let C_{i+1} inherit the orientation from C_i, and check that now C_{i+1} satisfies the label conditions with respect to this orientation.

In case when $y = x\alpha^{-1} \notin X_i$, we consider the edge leaving $x \in X_i$, and proceed verbatim. If $\partial_\alpha X_i = \partial_\alpha^{-1} X_i = \emptyset$, we have $X_i = G$, which completes the proof. $\square$

Example 3. Let $G = S_n$, $\alpha = (1\,2\,\ldots\,n)$, $\beta = (2\,3\,\ldots\,n)$. Then $\alpha\beta^{-1} = (1\,n)$ is an involution, and by Lemma 3 the Cayley graph $\Gamma(S_n, \{\alpha, \beta\})$ contains a Hamiltonian cycle. Incidentally, this Cayley graph is conjectured to have the longest diameter and the largest mixing time of all Cayley graphs of S_n [B,D].

3. Proof of Theorems.

Proof of Theorem 1. We deduce it from Theorem 2. Fix a composition series of G. Let $r = r(G)$ and $m = m(G)$. Denote by $K_1, \ldots, K_r$ and $L_1, \ldots, L_m$ the of abelian and nonabelian composition factors of G, respectively. Recall that $|L_j| \geq 60 > 4$. We have:

$$2^{r+2m} = 2^r \cdot 4^m \leq \prod_{i=1}^{r} |K_i| \cdot \prod_{j=1}^{m} |L_j| = |G|.$$

Therefore, $r(G) + 2m(G) \leq \log_2 |G|$, with the equality attained only for $G \simeq \mathbb{Z}_2^n$. In the latter case, when $n \geq 2$, an elementary inductive argument (or a Gray code [WG,Kn]) gives a Hamiltonian cycle. In other cases, one can add to a generating set one extra group element, which connects the endpoints of a Hamiltonian path. This gives the desired Hamiltonian cycle and completes the proof. $\square$

Proof of Theorem 2. It is a well known consequence of CFSG that every nonabelian finite simple group can be generated by two elements, one of which is an involution. Therefore Lemma 3 is applicable, and for every nonabelian finite simple group produces a generating set S, with $|S| = 2$, such that the corresponding Cayley graph contains a Hamiltonian cycle. If the group G is cyclic ($G = \mathbb{Z}_p$), a single generator suffices, of course. We need the following simple "reduction lemma":

Lemma 4 *Let G be a finite group, a let $H \triangleleft G$ be a normal subgroup. Suppose $S = S_1 \sqcup S_2$ is a generating set of G, such that $S_1 \subset H$, $\langle S_1 \rangle = H$, and projection S_2' of S_2 onto G/H generates G/H. Suppose both $\Gamma_1 = \Gamma(H, S_1)$ and $\Gamma_2 = \Gamma(G/H, S_2')$ contain Hamiltonian paths. Then $\Gamma = \Gamma(G, S)$ also contains a Hamiltonian path.*

We postpone the proof of lemma until after we finish the proof of the theorem. Observe that in notation of Lemma 4, any generating set $\langle S_2' \rangle = G/H$ can be lifted to $S_2 \subset G$, so that $S = S_1 \sqcup S_2$ is a generating set of G. Therefore, if H and G/H have generating sets of size k_1 and k_2, respectively, so that the corresponding Cayley graphs contain Hamiltonian paths, then G contains such a generating set of size $k_1 + k_2$.

Now fix any composition series of a finite group G. By Lemma 4, we can construct a generating set S of size $r(G) + 2m(G)$, so that the corresponding Cayley graph $\Gamma(G, S)$ has a Hamiltonian path. This completes the proof of Theorem 2. $\square$

Proof of Lemma 4. We start with the following elementary observation. Let $\Gamma = \Gamma(G,S)$ be a Cayley graph which contains a Hamiltonian path. By vertex-transitivity of Γ one can arrange this path to start at any vertex $g \in G$.

Let $k = [G:H] = |G/H|$, and let $g_1 = 1 \in G$. Consider a Hamiltonian path in the Cayley graph $\Gamma(G/H, S_2')$:

$$H = Hg_1 \to Hg_2 \to Hg_3 \to \cdots \to Hg_k\,.$$

Now proceed by induction in a manner similar to that in the proof of Lemma 1. Fix a Hamiltonian path in the coset Hg_1, so that $1 \in G$ is its starting point. Suppose h_1g_1 is its end point. Add an edge $(h_1g_1, h_1g_2) \in \Gamma$. Consider a Hamiltonian path path in the coset Hg_2 starting at h_1g_2. Suppose h_2g_2 is its end point. Repeat until the resulting path ends at h_kg_k. This completes the construction and proves the Lemma. $\square$

Proof of Theorem 3. We write $A = \pm B$ for matrices $A, B \in \mathrm{SL}(2,p)$, to indicate that these elements map onto the same element in $\mathrm{PSL}(2,p)$.

For matrices α, β, γ as in section 1, note that:

$$\alpha^2 = \gamma^2 = \begin{pmatrix} a^2 & 0 \\ 0 & a^2 \end{pmatrix} = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \beta^2 = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\alpha\,\beta = \begin{pmatrix} 0 & a \\ a & 0 \end{pmatrix}, \quad \beta\,\alpha = \begin{pmatrix} 0 & -a \\ -a & 0 \end{pmatrix} = \pm \alpha\,\beta,$$

$$\gamma\,\alpha = \begin{pmatrix} a^2 & 0 \\ a^2 & a^2 \end{pmatrix} = \pm \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \beta\,\gamma\,\alpha\,\beta = \pm \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

The first line shows that α, β, γ are indeed involutions in $\mathrm{PSL}(2,p)$. The second line shows that α and β commute in $\mathrm{PSL}(2,p)$. Therefore, Lemma 1 implies that the Cayley graphs $\Gamma_p = \Gamma(\mathrm{PSL}(2,p), \{\alpha, \beta, \gamma\})$ contain a Hamiltonian cycle.

Finally, the third line implies that elementary transvections

$$E = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad E^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \quad F = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad F^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$

can be obtained as words of length at most 4 in α, β, γ. The celebrated result in [LPS] (see also [Lu1], Theorem 4.4.3) shows that the Cayley graphs

$$\widetilde{\Gamma}_p = \Gamma\bigl(\mathrm{PSL}(2,p), \{E, F\}\bigr)$$

are ε-expanders for some universal $\varepsilon > 1/100$. It is well known and easy to see (see e.g. [Lu1]) that if a set $\Gamma(G,S)$ is an expander with some $\varepsilon > 0$, and if elements of S are the words of length at most C in generators S', then $\Gamma(G,S')$ is an expander with $\varepsilon' > 0$ depending only on ε and C. Taking $C = 4$, this implies the result. $\square$

4. Historical remarks, connections and applications

1) It seems that the problem of finding Hamiltonian cycles in Cayley graphs was suggested for the first time by Rapaport-Strasser [RS]. She was motivated by bell ringing (cf. [Kn]) and "chess problem of the knight", popular in recreational literature.

As stated in [CG], versions of Lovász conjecture (for Cayley graphs, digraphs, etc.) were proposed by "many people". Lovász himself originally conceived it as a special case of another then–problem of Gallai [Ga] in graph theory, which asked whether all longest self-avoiding paths in simple connected graphs must have a common vertex [Lo3]. In a special case of vertex-transitive graphs this would imply that all such longest paths must have *every* vertex in common, and thus are Hamiltonian. Gallai's problem was later shown to have a negative answer [Wa].

Despite a very positive tone in [CG], there seems to be no consensus in the field as to whether one should believe in Lovász conjecture. As opposed to conventional wisdom, the original conjecture of Lovász puts it in the negative. Here is a full and precise quote from [Lo1], stating it as a research problem: "*Let us construct a finite, connected undirected graph, which is symmetric and has no simple path containing all the vertices. A graph is symmetric, if for any two vertices x and y, it has an automorphism mapping x onto y.*" Traditionally, however, the conjecture is stated in the positive, as in the present paper.

In a survey article [B, §3.3], Babai is sharply critical of the Lovász conjecture: "*In my view these beliefs only reflect that Hamiltonicity obstacles are not well understood; and indeed, vertex-transitive graphs may provide a testing ground for the power of such obstacles. We conjecture that for some $c > 0$, there exist infinitely many connected vertex-transitive graphs (even Cayley graphs) without cycles of length $\geq (1 - c)n$.*"

To avoid the controversy, we will not render our opinion on the matter.

2) Hamiltonian cycles in several classical vertex-transitive and Cayley graphs play an important role in Combinatorics and applications. The story starts with *Gray codes* which are Hamiltonian cycles in the hypercube $\mathbb{Z}_2^n$ (patented by F. Gray in 1953). The recent treatise by Knuth [Kn] on the Hamiltonian cycles in Johnson's graph (on k-subsets of an n-set) and other graphs is a great source of references and results.[3]

The case of Cayley graphs of the symmetric group is of particular interest. A number of results are known for particular sets of generators, such as certain involutions [RS], transpositions [KoL], or a transposition and a long cycle [CW]. The ad hoc argument in the latter paper proves the result in Example 2. Example 1 was resolved in the early paper [RS], and was further investigated in [Kn]. We should mention that the arguments in [CW,Kn] prove much more than a mere existence of a Hamiltonian cycle, but also present algorithms for their construction with linear space requirements. Note that our generic approach is inherently exponential (we keep all elements of G in the memory.) We refer to survey papers [B,CG,Kn,WG] for further references and generalizations.

3) The most general classes of finite groups for which Lovász conjecture was proved include abelian groups, p-groups, dihedral groups, and certain extensions (see e.g. [Lo2,Wi].) We refer to [B,CG,WG] for further references.

---

[3] See also a related concept of "universal cycles" in [CDG].

4) If one ignores a tight bound and an explicit construction of the Cayley graphs in Theorem 1, this result can be viewed as a corollary from the following natural conjecture:

Conjecture 1. *There exists a constant $c \geq 1$, such that for every finite group G, and every $k \geq c \log_2 |G|$, the probability $P(G,k)$ that the Cayley graph $\Gamma = \Gamma(G,S)$ with a random generating set S of size $|S| = k$ contains a Hamiltonian cycle, satisfies:*

$$P(G,k) \to 1 \quad as \quad |G| \to \infty.$$

While, of course, Conjecture 1 is much weaker than the Lovász conjecture, it may prove to be more feasible. It also does not contradict Babai's conjecture (see above). Until recently, the best known bound in this direction was in [MH], where $k \geq |G|/3$ bound was established. A recent work [KS], using sharp results of an earlier paper [AR], reduces this bound down to $k \geq c \log^5 |G|$. Interestingly enough, papers [AR,KS] use no group theory to obtain the results. This suggests that there might be an elementary, classification-free, proof of Theorem 1.

5) Following the paper of Pósa [Pó] (see also [Lo2]), the connection between expansion and Hamiltonicity is well known, although yet to be fully understood (see [KS,Pa]). In particular, all expanders on n vertices contain a self-avoiding path of length $> (1-c)n$, where $c = c(\varepsilon)$ is independent of n. It is easy to see that the inverse is false. Whether expansion implies Hamiltonicity is yet to be seen, as a weaker *toughness condition* of Chvátal (known to be true for all connected Cayley graphs [B]) is conjectured to imply Hamiltonicity [Ch].

It is known that Cayley graphs with $k > C \log_2 |G|$ are expanders w.h.p. [AR], for a universal constant $C > 1$. This implies that they also have self-avoiding paths of length $(1-c)n$. This view gives an extra support in favor of Conjecture 1.

6) Both Theorems 2 and 3 require some delicacy in understanding. We present here few arguments and counterarguments which explain why neither theorem follows from known results.

We start with Theorem 2, which is somewhat more straightforward. In the case of simple groups, for example, pairs of generators are well known. Can one, perhaps, simply check whether the corresponding Cayley graphs contain Hamiltonian cycles? The answer may be affirmative for sporadic group, even for the Monster (although the size is prohibitively large), but for the series this is not so clear. As demonstrated by papers [CW,GY,Sc], even for $G = S_n$ or $\mathrm{SL}(2,p)$, proving Hamiltonicity requires a substantial amount of work with no common approach in sight.

The same argument goes in defense of Theorem 3. Indeed, Lovász conjecture states that Cayley graphs $\widetilde{\Gamma}_p$ (see section 3) must contain Hamiltonian cycles, which should imply the result. Unfortunately we do not know if graphs $\widetilde{\Gamma}_p$ are Hamiltonian. Even if they are, it is not easy to construct an explicit Hamiltonian cycle in this case and we know of no fast algorithm which would do this in polynomial time. On the other hand, an algorithm for constructing a Hamiltonian path as in the proof of Lemma 1 works in time linear in the number of vertices.

Furthermore, one can propose a $(2,p,3)$-generating set for $\mathrm{PSL}(2,p)$ considered in [GY]. The authors prove that the corresponding Cayley graph contains a Hamiltonian cycle. A recent conjecture by Lubotzky [Lu2] (see also [Lu1]) claims that every bounded size generating set of $\mathrm{PSL}(2,p)$ is an expander, with a universal

$\varepsilon > 0$ independent of p and the generating set. Would this imply that these Cayley graphs are 3-regular Hamiltonian expanders? Well, we don't know. Proving expansion (theoretically, or in practice) is not easier than Hamiltonicity, and for this particular set of generators the expansion is unknown.

Let us comment also that in fact the expander graphs studied in [LPS] are Schrier graphs and easily contain a Hamiltonian path.

7) One wonders whether Theorem 2 can be proved by using Lemma 1 or Lemma 2. Indeed, Lemma 2 suffices, but gives a somewhat weaker constant: for simple groups it requires 3 generators instead of 2 (note that the degrees of the Cayley graphs are 4 in both cases). The situation with Lemma 1 is more interesting, and may also seem promising in light of a well known result [MSW] that, with one exception, all finite simple groups are generated by three involutions.

By now all finite simple groups generated by three involutions, two of which commute, have been classified. In papers [N1-N4], Nuzhin completed classification of all but sporadic simple groups which are generated by three involutions, two of which commute (he refers to such groups as $(2, 2 \times 2)$-generated.) In particular, he showed that all groups of Lie type of rank ≥ 4 have such generators (few series of groups of small rank do not). A recent investigation of sporadic groups by means of explicit computation and character analysis showed that all sporadic simple groups except for M_{11}, M_{22}, M_{33} and M^cL are $(2, 2 \times 2)$-generated [N5,Ti,Ma].

As there seem to be a confusion over the history of $(2, 2 \times 2)$-generated groups, let us add few more references for a complete picture. The problem was proposed by Mazurov in 1980 (see [MK]). The case of alternating groups A_n, for n large enough, was solved in a much greater generality in [Co]. He showed that $A_n = \langle x, y, t\rangle$, such that $x^2 = y^3 = t^2 = (xt)^2 = (yt)^2 = 1$, with (x, y, t) satisfying few other relations. Taking $\alpha = t$, $\beta = xt$, $\gamma = yt$ gives the desired three involutions with $\alpha\beta = \beta\alpha$. In [N2], and, later, in [SC], the authors independently completed classification, unaware of the previous work. Also, paper [TZ], independetly of [N3,N4] proves that groups of Lie type of large enough rank are $(2, 2 \times 2)$-generated.

8) One can ask whether Hamiltonian 3-regular expanders can be obtained as Schreier graphs of an infinite group with Kazhdan's property (T), an approach pioneered by Margulis [M1] (see also [Lu1]). In fact, one can indeed generate $\mathrm{SL}(k, \mathbb{Z})$, $k \geq 3$, by two elements, one of which is an involution, and then proceed using Lemma 2 or 3. Since the resulting graphs are 4-regular, this result is a bit weaker than that of Theorem 3. Since for every fixed $k \geq 3$, these groups have (T), the corresponding finite Schreier graphs are expanders.

Similarly, one can ask whether $\mathrm{SL}(k, \mathbb{Z})$ are $(2, 2 \times 2)$-generated for $k \geq 3$, so that one can use Lemma 1 in this setting. It turns out that the group $\mathrm{SL}(3, \mathbb{Z})$ is not $(2, 2 \times 2)$-generated, as the following simple argument by Humphries [Hu2] shows (see also [Hu1]): If $\mathrm{SL}(3, \mathbb{Z}) = \langle \alpha, \beta, \gamma\rangle$, then the involutions α, β, γ have 2-dimensional (-1)–eigenspaces V_α, V_β, V_γ. If $\alpha\beta = \beta\alpha$, then $V_\alpha = V_\beta$. Therefore, $\dim(W) \geq 1$, where $W = V_\alpha \cap V_\beta \cap V_\gamma$. Since all three involutions fix W, this implies that they cannot generate $\mathrm{SL}(3, \mathbb{Z})$.

On the other hand, it is was shown recently in [TZ] that the groups $\mathrm{SL}(k, \mathbb{Z})$ are $(2, 2 \times 2)$-generated when $k \geq 14$. The authors present an explicit triple of involutions to prove the result. Taking appropriate quotients, this produces Hamiltonian 3-regular expanders in $\mathrm{SL}(k, q)$ for every fixed $k \geq 14$, and all but finitely many primes q. Similar results also hold for other types (see [TZ]). We leave the details to the reader.

9) Here is a straightforward way to obtain weaker versions of the theorems. Recall a celebrated Fleischner Theorem in Graph Theory that the square of every connected graph is Hamiltonian [F] (see also [Di], §10.3). Now take a Cayley graph of a finite group G with $k = d(G)$ generators and square it. The result is also a Cayley graph of G with at most $2k^2 + k$ generators (we need to include all pairwise products of generators and their inverses, as well as the original generators). This immediately implies the existence of $O(\log |G|)$ Hamiltonian generating set in every finite group G. A similar construction implies existence of Hamiltonian expanders that are also Cayley graphs of $\mathrm{PSL}(2, p)$. We omit the details.

10) Researching the literature we discovered references [RS] and [SC], the latter of which seemed to contain Lemma 1. We found the proof very sketchy, as it uses a rather unclear topological argument. In fact, another version of this argument already appears in [RS], stated in a different (and somewhat archaic) language. A posteriori, one can view our proof of Lemma 1 as a rigorous Combinatorial version of the very same argument. Similarly, Lemma 3 and its proof are essentially the same as in [Ra] (see Theorem 3.1). For the sake of consistency and completeness, we decided not to alter the exposition.

11) Before we conclude, let us quote Babai [B] once again: "*Even the following, less ambitious problem is open: does every finite group have a minimum Cayley graph with a Hamilton cycle?*" In fact, our Theorem 2 is a step in this direction; it is sharp for simple groups, but off for other classes of finite groups.

Denote by $\zeta(G)$ the smallest size of a generating set, such that the corresponding Cayley graph contains a Hamiltonian path. Determining $\zeta(G)$ for various finite groups G is a problem implicit in [RS]. Now Babai's question can be interpreted as to whether $\zeta(G) = d(G)$, the size of the smallest generating set. Lemma 4 is equivalent to the inequality $\zeta(G) \le \zeta(H) + \zeta(G/H)$. Now Theorem 2 implies that $\zeta(G) \le r(G) + 2m(G)$. In particular, for finite simple nonabelian groups G, we have $\zeta(G) = d(G) = 2$. Similarly, it implies that $\zeta(\mathbb{Z}_2^r) = d(\mathbb{Z}_2^r) = r$, another sharp result.

Little is known for general classes of groups. We suggest general nilpotent groups as the first interesting case. Let G be a finite nilpotent group, and let $G = G_0 \supset G_1 \supset \ldots \supset G_\ell = 1$ be the lower central series $G_i = [G, G_{i-1}]$, and let $H_i = G_i/G_{i-1}$. It is easy to see that $d(G) = d(G/[G,G]) = d(H_1)$, while our bounds give only $\zeta(G) \le \sum_i \zeta(H_i) = \sum_i d(H_i)$. In a different direction, let H_p be Sylow p-subgroups of G. From the theorem of Witte [Wi], we have $\zeta(G) \le \sum_p \zeta(H_p) = \sum_p d(H_p)$, while $d(G) = \max_p d(H_p)$. We believe one should be able to close this gap.

To conclude, consider the case in which our bound $\zeta(G)$ is quite far from $d(G)$. Indeed, consider $G_n = (A_n)^{n!/8}$. When n is large enough, these groups are 2-generated, i.e. have $d(G_n) = 2$ [KaL] (see also [BP]). Theorem 2 gives a bound $\zeta(G_n) \le n!/4$, and this is the best bound we can prove. Improving this bound is an ultimate challenge for the reader. Similarly, Philip Hall's group $G = A_5^{19}$ [Ha], with $d(G) = 2$, is a beautiful (but computationally unapproachable) potential counterexample to Lovász conjecture.

Finally, we should mention here that the authors inquired about a potential counterexample: Cayley graph of A_5^2 generated by two elements one of which is an involution. Both Bill Cook and Frank Ruskey independently reported that this graph is Hamiltonian. Oh, well...

Acknowledgements

We are grateful to Noga Alon, Brian Alspach, Marston Conder, William J. Cook, Mark Cooke, Alan Frieze, Steve Humphries, Bill Kantor, Don Knuth, Laci Lovász, Alex Lubotzky, Yakov Nuzhin, Frank Ruskey, Jan Saxl, Dan Spielman, Benny Sudakov, Alexei V. Timofeenko, and Nick Wormald for interesting comments, remarks and/or help with the references. The first named author was partially supported by the NSA and NSF.

References

[AKS] M. Ajtai, J. Komlos, E. Szemeredi, *Sorting in $c \log n$ parallel steps*, Combinatorica **3** (1983), 1–19.

[AR] N. Alon, Y. Roichman, *Random Cayley graphs and expanders*, Random Structures and Algorithms **5** (1994), 271–284.

[B] L. Babai, *Automorphism groups, isomorphism, reconstruction*, in Handbook of Combinatorics (R. L. Graham, M. Groetschel, and L. Lovasz, eds.), Elsevier, 1996.

[BP] L. Babai, I. Pak, *Strong bias of group generators: an obstacle to the "product replacement algorithm"*, J. Algorithms **50** (2004), 215–231.

[CDG] F. Chung, P. Diaconis, R. Graham, *Universal cycles for combinatorial structures*, Discrete Math. **110** (1992), 43–59.

[Ch] V. Chvátal, *Tough graphs and Hamiltonian circuits*, Discrete Math. **5** (1973), 215–228.

[CW] R. C. Compton, S. G. Williamson, *Doubly adjacent Gray codes for the symmetric group*, Linear and Multilinear Algebra **35** (1993), 237–293.

[Co] M. D. E. Conder, *More on generators for alternating and symmetric groups*, Quart. J. Math. Oxford Ser. (2) **32** (1981), 137–163.

[CG] S. J. Curran, J. A. Gallian, *Hamiltonian cycles and paths in Cayley graphs and digraphs—a survey*, Discrete Math. **156** (1996), 1–18.

[D] P. Diaconis, *Group representations in probability and statistics*, Institute of Mathematical Statistics, Hayward, CA, 1988.

[Di] R. Diestel, *Graph theory,* Graduate Texts in Mathematics, Vol. 173, Springer, New York, NY, 1997.

[F] H. Fleischner, *The square of every two-connected graph is Hamiltonian*, J. Combin. Theory Ser. B **16** (1974), 29–34.

[Ga] T. Gallai, *On directed paths and circuits,* in "Theory of Graphs" (Proc. Colloq., Tihany, 1966) 115–118 Academic Press, New York, 1968.

[GJ] M. R. Garey, D. S. Johnson, *Computers and intractability. A guide to the theory of* NP*-completeness*, Freeman, SF, 1979.

[GY] H. H. Glover, T. Y. Yang, *A Hamilton cycle in the Cayley graph of the $\langle 2, p, 3\rangle$ presentation of* $\mathrm{PSL}(2, p)$, Discrete Math. **160** (1996), 149–163.

[G+] O. Goldreich, R. Impagliazzo, L. A. Levin, R. Venkatesan, D. Zuckerman, *Security Preserving Amplification of Hardness*, Proc. 31st IEEE FOCS, 1990, 318–326.

[Go] D. Gorenstein, *Finite simple groups. An introduction to their classification*, Plenum, New York, 1982.

[Ha] P. Hall, *The Eulerian functions of a group*, Quart. J. Math. **7** (1936), 134–151.

[Hu1] S. P. Humphries, *Some subgroups of* $\mathrm{SL}(3, \mathbb{Z})$ *generated by involutions*, Glasgow Math. J. **32** (1990), 127–136.

[Hu2] S. P. Humphries, personal communication, 2002.

[JLR] S. Janson, T. Łuczak, A. Rucinski, *Random graphs*, Wiley, New York, 2000.

[KaL] W. M. Kantor, A. Lubotzky, *The probability of generating a finite classical group*, Geom. Dedicata **36** (1990), 67–87.

[Kn] D. E. Knuth, *The Art of Computer Programming,* Vol. 4, draft of sections 7.2.1.1, 7.2.1.2, 2002 (available from http://www-cs-faculty.stanford.edu/ knuth/taocp.html).

[KoL] V. L. Kompel'maher, V. A. Liskovec, *Successive generation of permutations by means of a transposition basis* (in Russian), Kibernetika (1975), 17–21.

[KS] M. Krivelevich, B. Sudakov, *Sparse pseudo-random graphs are Hamiltonian*, J. Graph Theory, **42** (2003), 17–33.

[Lo1] L. Lovász, *Problem 11,* in "Combinatorial structures and their applications." University of Calgary, Calgary, Alberta, Canada (1970), Gordon and Breach, New York.

[Lo2] L. Lovász, *Combinatorial problems and exercises*, North-Holland, Amsterdam, 1979.

[Lo3] L. Lovász, personal communication, 2001.

[Lu1] A. Lubotzky, *Discrete Groups, Expanding Graphs and Invariant Measures*, Birkhauser, Boston, 1994.

[Lu2] A. Lubotzky, *Invited talk at Durham Symposium,* Durham, 2001.

[LP] A. Lubotzky, I. Pak, *The product replacement algorithm and Kazhdan's property (T)*, Journal of AMS **52** (2000), 5525–5561.

[LPS] A. Lubotzky, R. Phillips, P. Sarnak, *Ramanujan graphs.*, Combinatorica **8** (1988), 261–277.

[MSW] G. Malle, J. Saxl, T. Weigel, *Generation of classical groups*, Geom. Dedicata **49** (1994), 85–116.

[M1] G. A. Margulis, *Explicit constructions of expanders*, Problems of Information Transmission **9** (1973), 325–332.

[M2] G. A. Margulis, *Explicit group theoretic constructions of combinatorial schemes, and their applications for construction of expanders and concentrators*, Problems of Information Transmission **24** (1988), 39–46.

[Ma] V. D. Mazurov, *On the generation of sporadic simple groups by three involutions, two of which commute*, Siberian Math. J. **44** (2003), 160–164.

[MK] V. D. Mazurov, E. I. Khukhro, Eds., *Unsolved problems in group theory. The Kourovka notebook.* (Thirteenth augmented ed.), Institute of Mathematics, Novosibirsk, 1995.

[MH] J. Meng, Q. Huang, *Almost all Cayley graphs are Hamiltonian*, Acta Math. Sinica (N.S.) **12** (1996), 151–155.

[N1] Ya. N. Nuzhin, *Generating triples of involutions of Chevalley groups over a finite field of characteristic* 2 (in Russian), Algebra i Logika **29** (1990), 192–206, 261.

[N2] Ya. N. Nuzhin, *Generating triples of involutions of alternating groups* (in Russian), Mat. Zametki **51** (1992), 91–95, 142.

[N3] Ya. N. Nuzhin, *Generating triples of involutions of Lie-type groups over a finite field of odd characteristic, I* (in Russian), Algebra i Logika **36** (1997), 77–96, 118.

[N4] Ya. N. Nuzhin, *Generating triples of involutions of Lie-type groups over a finite field of odd characteristic, II* (in Russian), Algebra i Logika **36** (1997), 422–440, 479.

[N5] Ya. N. Nuzhin, personal communication, 2002.

[Pa] I. Pak, *Mixing time and long paths in graphs*, in Proc. 13th ACM-SIAM SODA, 2000.

[Pó] L. Pósa, *Hamiltonian circuits in random graphs*, Discrete Math. **14** (1976), 359–364.

[Ra] R. A. Rankin, *A campanological problem in group theory II*, Proc. Camb. Phil. Soc. **62** (1966), 11–18.

[RS] E. Rapaport-Strasser, *Cayley color groups and Hamilton lines*, Scripta Math. **24** (1959), 51–58.

[RVW] O. Reingold, S. Vadhan, A. Wigderson, *Entropy Waves, The Zig-Zag Graph Product, and New Constant-Degree Expanders and Extractors*, Proc. 41st IEEE FOCS, 2000.

[RW] R. W. Robinson, N. C. Wormald, *Almost all regular graphs are Hamiltonian*, Random Structures and Algorithms **5** (1994), 363–374.

[Sc] P. E. Schupp, *On the structure of Hamiltonian cycles in Cayley graphs of finite quotients of the modular group*, Theoret. Comput. Sci. **204** (1998), 233–248.

[SS] M. Sipser, D. A. Spielman, *Expander Codes*, IEEE Transactions on Information Theory **42(6)** (1996), 1710–1722.

[SC] D. Sjerve, M. Cherkassoff, *On groups generated by three involutions, two of which commute,* in The Hilton Symposium 1993 (Montreal, PQ), 169–185, CRM Proc. Lecture Notes, 6, Amer. Math. Soc., Providence, RI, 1994.

[TZ] M. C. Tamburini, P. Zucca, *Generation of certain matrix groups by three involutions, two of which commute*, J. Algebra **195** (1997), 650–661.

[Ti] A. V. Timofeenko, *On generating triples of involutions of large sporadic groups.*, Discrete Math. Appl. **13** (2003), 291–300, available at `http://icm.krasn.ru/refextra.php?id=2869`.

[V] L. Valiant, *Graph theoretic properties in computational complexity*, J. Comp. Sys. Sci. **13** (1976), 278–285.

[Wa] H. Walther, *Über die Nichtexistenz eines Knotenpunktes, durch den alle längsten Wege eines Graphen gehen* (in German), J. Combin. Theory **6** (1969), 1–6.

[WZ] A. Wigderson, D. Zuckerman, *Expanders that Beat the Eigenvalue Bound, Explicit Construction and Applications*, Proc. of the 25th STOC, 1993, 245–251.

[Wi] D. Witte, *Cayley digraphs of prime-power order are Hamiltonian*, J. Combin. Theory Ser. B **40** (1986), 107–112.

[WG] D. Witte, J. Gallian, *A survey: Hamiltonian cycles in Cayley graphs*, Discrete Math. **51** (1984), 293–304.