Random Cayley graphs

Demetres Christofides

Institute of Theoretical Computer Science, Charles University in Prague
christofidesdemetres@gmail.com

In this talk we will present some open problems concerning random Cayley graphs.

1 Introduction

Recall that given a group G and a subset S of G, the Cayley graph $\Gamma = \Gamma(G;S)$ of G with respect to S has the elements of G as its vertex set and has an edge between g and h if and only if $hg^{-1} \in S$ or $gh^{-1} \in S$. We ignore any loops or multiple edges. In particular, whether $1 \in S$ or not is immaterial. Observe for example that Γ is connected if and only if the set S generates the group G. Throughout this talk, we will often refer to the set S as the generating set of the graph Γ irrespectively of whether it is a generating set for the group G or not.

The model $\mathcal{G}(G,p)$, where $p \in (0,1)$ is the probability space of all graphs $\Gamma(G;S)$ in which every element of G is assigned to the set S independently at random with probability p. The model $\mathcal{G}(G,k)$, where $k \in \{0,1,2,\ldots,n\}$ is the probability space of all graphs $\Gamma(G;S)$ in which S is picked uniformly amongst all subsets of G of size k. One would expect these models to have many similarities with the familiar models $\mathcal{G}(n,p)$ and $\mathcal{G}(n,M)$. This is indeed the case and we refer the reader to [1] for some of these similarities. There are however many differences between these models. An obvious difference is that every graph in $\mathcal{G}(G,p)$ is regular while with high probability this is not the case in the model $\mathcal{G}(n,p)$ (unless in the trivial cases in which p is either so large or so small that with high probability forces G to be complete or empty respectively). This difference also motivates the comparison of the model $\mathcal{G}(G,p)$ with the model $\mathcal{G}_{n,r}$, the probability space of all r-regular graphs on $\{1,2,\ldots,n\}$ taken with the uniform measure. These two models still have significant differences. For example, every graph $\Gamma \in \mathcal{G}(G,p)$ is not only regular, but in fact it has a high degree of symmetry. More specifically, every element g of G defines an automorphism of Γ by right multiplication and so G is a subgroup of $\mathrm{Aut}(\Gamma)$. On the other hand, it is known that for every $3 \leqslant r \leqslant n-4$, graphs in $\mathcal{G}_{n,r}$ have with high probability a trivial automorphism group [3]. Given the success of random graphs in settling many graph theory questions and the fact that random Cayley graphs have some important properties not shared by other random graph models, we see that their study is highly desirable.

2 Clique numbers

Recall that for almost every graph $\Gamma \in \mathcal{G}(n, 1/2)$ its clique number is asymptotic to $2\log_2 n$. It would be natural therefore to expect that a similar result, up to a constant factor say, holds for random Cayley graphs as well. Note that when speaking about random Cayley graphs, the group G and thus its order is fixed. So strictly speaking it does not really make sense to speak of events occurring with high probability. Instead, we have to consider a family of groups G_k for which their orders tends to infinity. When we take the family of cyclic groups, it was confirmed by Green [2] that this is indeed the case, i.e. that if $\Gamma \in \mathcal{G}(\mathbb{Z}_n, 1/2)$ then with high probability we have that $\omega(\Gamma) = \Theta(\log n)$. However rather surprisingly in the same paper it was also shown that this is not the case for all families of groups. In particular it was shown that if $\Gamma \in \mathcal{G}(\mathbb{Z}_2^m, 1/2)$, then with high probability we have that $\omega(\Gamma) = \Theta(\log n \log\log n)$, where $n = 2^m$ is the size of $\mathbb{Z}_2^m$.

The best bounds we know today for a general family of groups are the following.

Theorem 2.1 (Christofides and Markström [1]). *Let G be a group of order n and let $\Gamma \in \mathcal{G}(G, 1/2)$. Then with high probability $\frac{1}{4}\log_2 n \leqslant \omega(\Gamma) \leqslant 27(\log_2 n)^2$.*

As we have already mentioned, it does not make sense to speak about asymptotic results for a fixed group. However throughout this talk we choose to abuse notation. The above result should be interpreted as a result for families of groups instead.

The lower bound is rather satisfying when compared with the bound from random graphs but the upper bound is not. Given Green's example we cannot expect to reduce the exponent of $\log n$ down to linear but in fact we believe that it is not quadratic.

Conjecture 2.2. *There is an $\varepsilon > 0$ such that if G is a group of order n and $\Gamma \in \mathcal{G}(G, 1/2)$ then with high probability $\omega(\Gamma) \leqslant (\log_2 n)^{2-\varepsilon}$.*

In fact we believe that the right answer should be almost linear.

Conjecture 2.3. *For every $\varepsilon > 0$ if G is a group of order n and $\Gamma \in \mathcal{G}(G, 1/2)$ then with high probability $\omega(\Gamma) \leqslant (\log_2 n)^{1+\varepsilon}$.*

There are even some reasons to believe that the family $\mathbb{Z}_2^n$ has the largest clique number amongst all random Cayley graphs.

Problem 2.4. *Is it true that if G is a group of order n and $\Gamma \in \mathcal{G}(G, 1/2)$ then with high probability $\omega(\Gamma) = O(\log n \log\log n)$?*

3 Hamiltonicity

A famous conjecture of Lovász [4] says that every connected Cayley graph is Hamiltonian. (In fact the conjecture concerns vertex-transitive graphs but here we restrict attention only to Cayley graphs.) Since this is considered a very difficult conjecture one could at least try to prove it in the case of random Cayley graphs. So let us first consider when a random Cayley graph becomes connected. On the one hand, if we consider cyclic groups of prime order, the Cayley graph is connected as long as the generating set S contains at least one non-trivial element. On the other hand, if we consider the group $\mathbb{Z}_2^n$, even deterministically we need $|S| \geqslant n = \log_2 |\mathbb{Z}_2^n|$ in order for the Cayley graph to become connected. (To see this consider $\mathbb{Z}_2^n$ as a vector space of dimension n over the field of two elements.) It turns out that taking slightly more elements one can guarantee that every random Cayley graph is connected.

Theorem 3.1 (Christofides and Markström [1])**.** *Let G be a group of order n, let $\delta > 0$ and let $\Gamma \in \mathcal{G}(G, (1+\delta)\log_2 n)$. Then with high probability Γ is connected.*

For the appearance of Hamilton cycles, the best result in this direction is (essentially) the following.

Theorem 3.2 (Christofides and Markström [1])**.** *Let G be a group of order n, and let $\Gamma \in \mathcal{G}(G, (\log n)^3)$. Then with high probability Γ is Hamiltonian.*

Towards confirming the Lovász conjecture for random Cayley graphs Pak [5] suggested the following conjecture.

Conjecture 3.3. *There exists a $C > 1$ such that if G is a group of order n, and $\Gamma \in \mathcal{G}(G, C\log_2 n)$ then with high probability Γ is Hamiltonian.*

In fact, if the Lovász conjecture is true then one can take C to be essentially equal to 1.

Conjecture 3.4. *Let G be a group of order n, let $\delta > 0$ and let $\Gamma \in \mathcal{G}(G, (1+\delta)\log_2 n)$. Then with high probability Γ is connected.*

References

[1] D. Christofides and K. Markström, Random Latin square graphs, to appear in Random Structures Algorithms.

[2] B. Green, Counting sets with small sumset, and the clique number of random Cayley graphs, Combinatorica **25** (2005), 307–326.

[3] J. H. Kim, B. Sudakov and V. H. Vu, On the asymmetry of random regular graphs and random graphs, Random Structures Algorithms **21** (2002), 216–224.

[4] L. Lovász, *Problem 11* in *Combinatorial Structures and their Applications*, Gordon and Breach Science Publishers, 1970.

[5] I. Pak and R. Radoičić, Hamiltonian paths in Cayley graphs, Discrete Math. **309** (2009), 5501–5508.