Discrete Mathematics and Theoretical Computer Science DMTCS vol. **14:2**, 2012, 83–90

Random Cayley digraphs of diameter 2 *and given degree*

Manuel E. Lladser[1†] Primož Potočnik[2‡] Jozef Širáň[3,4§] Mark C. Wilson[5¶]

[1] *Department of Applied Mathematics, University of Colorado, Boulder, CO 80309-0526, USA*
[2] *Faculty of Mathematics and Physics, University of Ljubljana, Ljubljana, Slovenia*
[3] *Department of Mathematics, Open University, U.K.*
[4] *Department of Mathematics, SvF, Slovak University of Technology, Bratislava, Slovakia*
[5] *Department of Computer Science, University of Auckland, Private Bag 92019 Auckland, New Zealand*

received 25th August 2011, revised 24th August 2012, accepted 10th September 2012.

We consider random Cayley digraphs of order n with uniformly distributed generating sets of size k. Specifically, we are interested in the asymptotics of the probability that such a Cayley digraph has diameter two as $n \to \infty$ and $k = f(n)$, focusing on the functions $f(n) = \lfloor n^\delta \rfloor$ and $f(n) = \lfloor cn \rfloor$. In both instances we show that this probability converges to 1 as $n \to \infty$ for arbitrary fixed $\delta \in (\frac{1}{2}, 1)$ and $c \in (0, \frac{1}{2})$, respectively, with a much larger convergence rate in the second case and with sharper results for Abelian groups.

Keywords: Random digraph, Cayley digraph, degree, diameter.

1 Introduction

It is well known that almost all graphs and digraphs have diameter two [Bol79]. This result has been generalized and strengthened in various directions, of which we shall be interested in restrictions to Cayley graphs and digraphs.

In [ML97] it was proved that almost all Cayley digraphs have diameter two, and in [MH98] this was extended to Cayley graphs. The random model used in [ML97, MH98] is the most straightforward one: in terms of Cayley digraphs for a given group G of order n, one chooses a random generating set by choosing its elements among the non-identity elements of G independently and uniformly, each with probability $1/2$. Observe that such generating sets have size at least $n/2$ with probability at least $1/2$, in which case a simple counting argument shows that the corresponding Cayley digraphs have diameter at most two. The less trivial part of [ML97] therefore concerns random Cayley digraphs in which the number of generators is at most half of the order of the group.

†Email: manuel.lladser@colorado.edu
‡Email: primoz.potocnik@fmf.uni-lj.si
§Email: j.siran@open.ac.uk
¶Email: mcw@cs.auckland.ac.nz

1365–8050 © 2012 Discrete Mathematics and Theoretical Computer Science (DMTCS), Nancy, France

This motivates a study of random Cayley digraphs in which the number of generators is restricted. In this case one cannot use the model of [ML97]. Instead, we let every generating set of the Cayley digraph of a fixed degree appear with equal probability. The fundamental question here is: For which functions f is it true that the diameter of a random Cayley digraph of an arbitrary group of order n and of degree $f(n)$ is asymptotically almost surely equal to 2 as n tends to infinity? By the well-known Moore bound for graphs or digraphs of diameter two we know that f has to increase at least as fast as $\sqrt{n}$. A study of the behaviour of the problem for functions of the form $f(n) = \lfloor n^\delta \rfloor$ for the powers δ satisfying $1/2 \leq \delta < 1$ is therefore natural in this context. However, even the case when $f(n) = \lfloor cn \rfloor$ for a constant c seems not to have been investigated before and, as we shall see, leads to an interesting asymptotic analysis.

The probability that a random Cayley digraph of (in- and out-) degree k on a group of order n has diameter 2 will be estimated in Section 3 in terms of a certain combinatorial function the asymptotic analysis of which yields the following main results, proved in Section 4:

- For every c such that $0 < c < 1/2$, the probability of a random Cayley digraph of degree $\lfloor cn \rfloor$ on a given group of order n having diameter 2 is at least $1 - O(\exp(-c^2 n/2))$.
- For every δ such that $1/2 < \delta < 1$, the probability of a random Cayley digraph of degree $\lfloor n^\delta \rfloor$ on a given group of order n having diameter 2 is at least $1 - O(\exp(-n^{2\delta-1}/2))$.
- There is a constant c_1 such that for every function μ defined on positive integers, with $\mu(n) \to \infty$ as $n \to \infty$, the probability of a random Cayley digraph of degree $\lfloor \sqrt{2n \ln(c_1 n \mu(n))} \rfloor$ on a group of order n having diameter 2 tends to 1 as $n \to \infty$.
- There is a positive constant $c_2 < 1$ such that for every ε with $0 < \varepsilon < c_2$ the probability of a random Cayley digraph of degree $\lfloor \sqrt{2n \ln(c_2/\varepsilon)} \rfloor$ on an Abelian group of order n having diameter 2 has limes superior not exceeding $1 - \varepsilon$.

2 The model

Throughout, let G be a finite group of order n and let k be a positive integer not exceeding $n - 2$. The set of non-trivial elements of G will be denoted by G^*. For a set A and an integer r, the symbol $\binom{A}{r}$ stands for the set of all subsets of A of size r.

For $S \in \binom{G^*}{k}$, the *Cayley digraph on G relative to S*, denoted by $\mathrm{Cay}(G, S)$, is the k-valent digraph with vertex set G and arc set $\{(g, gs) : g \in G, s \in S\}$. The *distance* $\partial_S(g, h)$ from the vertex g to the vertex h in $\mathrm{Cay}(G, S)$ is the length of the shortest directed path from g to h in $\mathrm{Cay}(G, S)$. The *diameter* $\mathrm{diam}(\mathrm{Cay}(G, S))$ is the smallest integer d such that for every ordered pair (g, h) the distance from g to h is at most d.

We are now ready to introduce our model for random Cayley digraphs of a given valence. Let $\mathcal{P}(G, k)$ be the probability space $(\mathcal{B}, 2^{\mathcal{B}}, \Pr)$ where $\mathcal{B} = \binom{G^*}{k}$, $2^{\mathcal{B}}$ is the power set of $\mathcal{B}$, and $\Pr$ is the uniformly distributed probability measure on $\mathcal{B}$. Since $|\mathcal{B}| = \binom{n-1}{k}$, $\Pr(\{S\}) = \binom{n-1}{k}^{-1}$ for all $S \in \mathcal{B}$. More generally, for every subset $L \subseteq G^*$ of size ℓ, the probability that a random set $S \in \mathcal{B}$ contains L as a subset is given by

$$\Pr(S \supseteq L) = \Pr\left(\left\{S \in \binom{G^*}{k} : L \subseteq S\right\}\right) = \binom{n-1-\ell}{k-\ell}\binom{n-1}{k}^{-1}. \tag{1}$$

Before proceeding, note that one could think of a seemingly easier model, where each element of G^* is chosen to be a member of S independently and with probability $k/(n-1)$. This model may well be equivalent to our model and it may well be possible to prove their equivalence in a way similar to arguments about the equivalence of the two standard models of random graphs (cf. Chapter 2 of [Bol79]). In view of the length of the arguments of Chapter 2 of [Bol79], however, research into a possible equivalence of the two models should be the object of a separate article, which is the reason why we chose not to pursue this direction.

Let $\mathrm{Diam}\colon \mathcal{B} \to \mathbb{R}$ be the random variable on the space $\mathcal{P}(G,k)$ defined by letting, for every $S \in \binom{G^*}{k}$,

$$\mathrm{Diam}(S) = \mathrm{diam}(\mathrm{Cay}(G,S)). \tag{2}$$

The main goal of this article is to derive bounds on the probability of the event $\mathrm{Diam}(S) > 2$ and study the asymptotic behavior of the bounds.

Since Cayley digraphs are vertex-transitive, the diameter of $\mathrm{Cay}(G,S)$ coincides with the maximum value of $\partial_S(1,y)$ over all $y \in G^*$. Clearly, $\partial_S(1,y) \le 2$ if and only if $y \in S$, or there exists $x \in S$ such that $(1,x,y)$ is a directed path from 1 to y of length 2. The latter is equivalent to requiring that $\{x, x^{-1}y\} \subseteq S$; in particular, the events in the following definition play an important role in the analysis.

Definition 2.1 *For $x, y \in G^*$, let*

$$T(x,y) = \left\{ S : S \in \binom{G^*}{k},\ \{x, x^{-1}y\} \subseteq S \right\} \quad \textit{and} \quad X(y) = \bigcup_{x \in G^* \setminus \{y\}} T(x,y).$$

If S is an arbitrary element of $\binom{G^*}{k}$ and $\mathrm{Diam}(S) \le 2$ then, for each $y \in G^*$, $y \in S$ or $S \in X(y)$. Hence $\Pr(\mathrm{Diam} \le 2) \le \min_{y \in G^*} \Pr(y \in S \text{ or } S \in X(y))$. In particular, if $\Pr(\overline{X(y)} \mid y \notin S)$ denotes the conditional probability of the complement $\overline{X(y)}$ of $X(y)$ given that $y \notin S$, we have:

$$\Pr(\mathrm{Diam} > 2) \ge \max_{y \in G^*} \Pr(y \notin S \text{ and } S \notin X(y)) = (1 - \frac{k}{n-1}) \cdot \max_{y \in G^*} \Pr(\overline{X(y)} \mid y \notin S),$$

where the last identity is a direct consequence of (1). On the other hand, if $\mathrm{Diam}(S) > 2$ then there exists $y \in G^*$ such that $y \notin S$ and $S \notin X(y)$. This results in

$$\Pr(\mathrm{Diam} > 2) \le \sum_{y \in G^*} \Pr(\overline{X(y)} \mid y \notin S) \cdot \Pr(y \notin S) \le (n-k-1) \cdot \max_{y \in G^*} \Pr(\overline{X(y)} \mid y \notin S)\ .$$

These inequalities immediately lead to the following result:

Proposition 2.2 *The random variable* Diam *satisfies*

$$(1 - \frac{k}{n-1}) \cdot M \le \Pr(\mathrm{Diam} > 2) \le (n-k-1) \cdot M\ , \tag{3}$$

where

$$M = \max_{y \in G^*} \Pr(\overline{X(y)} \mid y \notin S)\ . \tag{4}$$

Notice that the upper and lower bounds in (3) differ by a linear factor of order n. These bounds will be used in Section 4 for asymptotic estimates on the probability of the event $[\mathrm{Diam} > 2]$.

3 Probability estimates

We begin with an auxiliary result on groups that we will need later. If G is a group and $y \in G$, we say that $z \in G$ is a *square root* of y if $z^2 = y$.

Lemma 3.1 *Let G be a finite group. If the order of G is odd, then every $y \in G$ has a unique square root in G. If the order of G is even, then there exists at least one element $y \in G$ with no square root in G.*

Proof: Consider the mapping $s : G \to G$, $x \mapsto x^2$. Suppose first that $|G| = 2m + 1$ is odd; in particular, $x^{2m+1} = 1$, for all $x \in G$, due to Lagrange's theorem. Hence, for every $x, y \in G$, we see that $x^2 = y^2$ implies that $x = x^{2m+2} = y^{2m+2} = y$. So s is a bijection and therefore each $y \in G$ has a unique square root in G if the group has odd order. On the other hand, if $|G|$ is even, G has a non-trivial involution x. Since $s(x) = 1 = s(1)$, s is not a bijection. Since G is finite, it follows that s is not surjection, and so there is an element $y \in G$ with no square root in G. □

The basis for our estimates on the probability $\Pr(\text{Diam} > 2)$ is provided by a bound on M which we state and prove next.

Proposition 3.2 *For each group G of order $n \geq 3$ and every k such that $1 \leq k \leq n-2$ we have*

$$M \;\leq\; 2^k \binom{t}{k} \binom{n-2}{k}^{-1} \;\; where \;\; t = \lfloor (n-2)/2 \rfloor \,, \tag{5}$$

with equality if G is Abelian.

Proof: If $y \in G^*$, we will use the symbol G_y^* to denote the set $G^* \backslash \{y\}$. For each $y \in G^*$ let $X'(y) = \{S \in \binom{G_y^*}{k} : \{x, x^{-1}y\} \not\subset S \text{ for all } x \in G_y^*\}$. We claim that

$$M = \chi \cdot \binom{n-2}{k}^{-1} \;\; where \;\; \chi = \max_{y \in G^*} |X'(y)| \,. \tag{6}$$

Indeed, for each $y \in G^*$, the distribution of S when the condition on the event $[y \notin S]$ is uniform over the set $\binom{G_y^*}{k}$. In particular, $\Pr(\overline{X(y)} \mid y \notin S) = \binom{n-2}{k}^{-1} |X'(y)|$, and the claim now follows from the definition of M in (4).

By Lemma 3.1 we know that if G is odd, then for every $y \in G^*$ there exists a unique $x = x_y \in G$ such that $x^2 = y$. For each $y \in G^*$ we let $W_y = G_y^*$ if $|G|$ is even, and $W_y = G^* \backslash \{y, x_y\}$ if $|G|$ is odd. It can be checked that for every fixed $y \in G^*$ the mapping $x \mapsto \gamma_y(x)$ given by $\gamma_y(x) = x^{-1}y$ is a permutation of this newly introduced set W_y. Notice that the size of W_y is always even. Further, observe that for all $y \in G^*$ we have $S \in X'(y)$ if and only if $S \subset W_y$, $|S| = k$, and $S \cap \gamma_y(S) = \emptyset$. Letting $w(\gamma_y) = |\{S \subset W_y : |S| = k,\ S \cap \gamma_y(S) = \emptyset\}|$, this observation combined with (6) gives

$$\chi = \max\nolimits_{y \in G^*} w(\gamma_y) \,. \tag{7}$$

To estimate $w(\gamma_y)$ we will extend the definition of w to arbitrary permutations by letting, for an arbitrary permutation α_y of the set W_y,

$$w(\alpha_y) = |\{S \subset W_y : |S| = k,\ S \cap \alpha_y(S) = \emptyset\}| \,. \tag{8}$$

Our strategy will be to show that for every $y \in G^*$ there exists an *involution* β_y on the set W_y such that $w(\gamma_y) \leq w(\beta_y) = \binom{t}{k}2^k$.

We will construct β_y by defining it on every orbit $O \subset W_y$ of γ_y successively. Since the construction will work for all $y \in G^*$ we will suppress subscripts on permutations and let $W_y = W$, $\gamma_y = \gamma$ and $\beta_y = \beta$ in the description of the construction. Suppose first that $|O|$ is even. The restriction of γ on O is a cyclic permutation; let O^1 and O^2 be the two orbits of γ^2 on O. Define the restriction of β on O by letting $\beta(z) = \gamma(z)$ if $z \in O_1$ and $\beta(z) = \gamma^{-1}(z)$ of $z \in O_2$. It is easy to check that for each subset $T \subset O$ the condition $T \cap \gamma(T) = \emptyset$ implies that $T \cap \beta(T) = \emptyset$.

The case of orbits of odd size requires more attention. Since $|W|$ is even, γ has an even number of orbits of odd size on W. Let us partition the set of odd-sized orbits of γ into ordered pairs and let (O_1, O_2) be such a pair. Then, γ induces cyclic permutations, say, $(u_1, \ldots, u_{2r+1})$ and $(v_1, \ldots, v_{2s+1})$, of O_1 and O_2, respectively, for some $r, s \geq 0$. Define the restriction of β on $O_1 \cup O_2$ by letting $\beta = (u_{2r+1}u_{2r}) \ldots (u_3u_2)(u_1v_1)(v_2v_3) \ldots (v_{2s}v_{2s+1})$. Let T be a subset of $O_1 \cup O_2$ such that $T \cap \gamma(T) = \emptyset$. We construct a new set T^o out of T as follows. If $u_1, u_3, v_1, v_3 \in T$, we take the smallest i and j such that both u_{2i+1} and v_{2j+1} lie outside T; the condition $T \cap \gamma(T) = \emptyset$ implies that such i and j exist and $2 \leq i \leq r-1$ and $2 \leq j \leq s-1$. In this situation we let $T^o = (T \backslash \{u_1, v_1\}) \cup \{u_{2i+2}, v_{2j+2}\}$, and it is obvious that $T^o \cap \beta(T^o) = \emptyset$. If $u_1, u_3, v_1 \in T$ but $v_3 \notin T$, we let $T^o = (T \backslash \{u_1\}) \cup \{u_{2i+2}\}$, where i is defined as before. In the case when $v_1, v_3, u_1 \in T$ but $u_3 \notin T$ we proceed symmetrically, swapping u and v (with appropriate subscripts). If $u_1, v_1 \in T$ but $u_3, v_3 \notin T$, we let $T^o = (T \backslash \{u_1\}) \cup \{v_2\}$. In all these cases it is easy to check that $T^o \cap \beta(T^o) = \emptyset$. In all the remaining cases we let $T^o = T$, noticing again that $T^o \cap \beta(T^o) = \emptyset$.

Finally, let S be a subset of W such that $|S| = k$ and $S \cap \gamma(S) = \emptyset$. We define S' by letting $S' \cap O = S \cap O$ for every even-sized orbit O of γ, and $S' \cap (O_1 \cup O_2) = (S \cap (O_1 \cup O_2))^o$ for each ordered pair (O_1, O_2) of odd-sized orbits of γ from our fixed pairing of such orbits, as introduced above. The key point to observe is that the assignment $S \mapsto S'$ is injective. Moreover, the facts about the sets T and T^o listed in the previous two paragraphs imply that $S' \cap \beta(S') = \emptyset$.

The above arguments prove that $w(\gamma_y) \leq w(\beta_y)$ for all $y \in G^*$. Further, since β_y is a product of $t = \lfloor (n-2)/2 \rfloor$ cycles of length 2, the quantity $w(\beta_y)$ defined in (8) is equal to $\binom{t}{k}2^k$ since a set $S \subset W_y$ with $|S| = k$ such that $S \cap \beta_y(S) = \emptyset$ arises precisely by choosing k cycles of β_y length 2 out of t such cycles and choosing one of the two elements in each chosen 2-cycle. These facts combined with (7) and (6) imply the bound in our Proposition for general groups.

If G is Abelian, choose $y \in G^*$ arbitrarily if G has odd order, and let $y \in G^*$ be an element with no square root if the order of G is even. Then the permutation γ_y of W_y is an involution with no fixed point and hence $\beta_y = \gamma_y$ in this case, implying equality for Abelian groups. □

In combination with Proposition 2.2 this gives the following consequence.

Proposition 3.3 *Letting* $t = \lfloor (n-2)/2 \rfloor$ *and* $a(n,k) = 2^k \binom{t}{k} \binom{n-2}{k}^{-1}$, *the random variable* Diam *satisfies*

$$1 - (n-k-1)a(n,k) \leq \Pr(\text{Diam} \leq 2)$$

for general groups, and

$$1 - (n-k-1)a(n,k) \leq \Pr(\text{Diam} \leq 2) \leq 1 - (1 - \frac{k}{n-1})a(n,k)$$

for Abelian groups. □

4 Asymptotic analysis

In the context of Proposition 3.3 with $t = \lfloor (n-2)/2 \rfloor$ we write

$$a(n,k) = b(t,k)c(t,k), \tag{9}$$

where

$$b(t,k) = 2^k \binom{t}{k} \binom{2t}{k}^{-1} \text{ and } c(t,k) = 1 \text{ if } n \text{ is even, } c(t,k) = \frac{2t-k+1}{2t+1} \text{ if } n \text{ is odd.}$$

For the asymptotic analysis of the behaviour of binomial coefficients appearing in $b(t,k)$ we use Stirling's approximation. To state the result of the corresponding routine calculations in a concise form, for $0 < \lambda < 1$ let

$$\begin{aligned} R(\lambda) &= (2-\lambda)\ln(1-\lambda/2) - (1-\lambda)\ln(1-\lambda)\,, \\ P(\lambda) &= \left(\frac{2-\lambda}{2-2\lambda}\right)^{1/2}\,, \text{ and} \\ C(t,\lambda) &= 1 + O(t^{-1}) + O((t\lambda)^{-1}) + O((t(1-\lambda))^{-1}) \qquad \text{as } t \to \infty. \end{aligned}$$

Then, writing $k = \lambda t$, routine calculation with the help of Stirling's approximation yields

$$b(t,k) = \exp(tR(\lambda))\, P(\lambda)\, C(t,\lambda)\,; \tag{10}$$

the terms R, P and C represent the exponential rate, the leading coefficient, and the correction term. The exponential rate $R(\lambda)$ is easily seen to be negative for $0 < \lambda < 1$. Furthermore $C(t,\lambda)$ tends to 1 for each fixed $\lambda \in (0,1)$ as $t \to \infty$. Note also that

$$R(\lambda) = (2-\lambda)\ln(1-\lambda/2) - (1-\lambda)\ln(1-\lambda) = -\lambda^2/4 + O(\lambda^3) \text{ for } 0 < \lambda < 1. \tag{11}$$

Our first result about the behaviour of $\Pr(\text{Diam} \le 2)$ in the case of general groups deals with the situation where $k \approx cn$ for some $c < 1/2$. In our asymptotic calculations for $n \to \infty$ we may then replace $\lambda = k/t$ for $t = \lfloor (n-2)/2 \rfloor$ with the value $2c$. Combining now (9), (10) and (11). with the lower bound of Proposition 3.3 we arrive at the following result:

Theorem 4.1 *For each c such that $0 < c < 1/2$, the probability of a random Cayley digraph on a group of order n and degree $\lfloor cn \rfloor$ having diameter 2 is at least $1 - O(n \cdot \exp(-c^2 n/2))$.* □

We now turn to the case where $k \approx n^\delta$ with $1/2 < \delta < 1$. For $k = \lambda t$ with $\lambda = o(1)$ as $t \to \infty$, the approximation (11) is still valid, and we also have $C(t,\lambda) = 1 + O(\lambda)$. Thus, if k grows at least as fast as n^δ with $\delta > 1/2$, for asymptotic computation we may replace k with $2n^{\delta-1}t$ and set $\lambda = 2n^{\delta-1}$. Then, the exponent $tR(\lambda)$ in (10) may be replaced with $-n^{2\delta-1}/2$, which implies exponential decay if $\delta > 1/2$. Using the lower bound of Proposition 3.3 again, we have the following conclusion.

Theorem 4.2 *For every δ such that $1/2 < \delta < 1$, the probability of a random Cayley digraph on a group of order n and degree $\lfloor n^\delta \rfloor$ having diameter 2 is at least $1 - O(n \cdot \exp(-n^{2\delta-1}/2))$.* □

It is natural to ask what happens when $k \approx \sqrt{n}$. By the Moore bound for diameter two, the probability of a random Cayley digraph of degree k and order n (for a general group) having diameter 2 is zero if $k < \lfloor\sqrt{n}\rfloor$. It is interesting to note that if the right-hand side is increased by a factor of 2, then for an arbitrary n of the form $n = 2^{2d}$ there exists a Cayley (di)graph of order n and degree $k = 2\sqrt{n} = 2 \cdot 2^d$ on an elementary Abelian group of order n, which has diameter 2. Indeed, representing vertices of the graph as $2d$-dimensional 0–1 vectors, it is sufficient to consider a generating set of the form $S_1 \cup S_2$ where S_1 and S_2 consists of all non-zero vectors having the first d and the last d coordinates equal to zero, respectively. It follows that the probability that a random Cayley (di)graph on an elementary Abelian 2-group of order n and degree $k = 2\sqrt{n}$ has diameter 2 is positive. This, of course, does not allow to make any conclusion as to how large this probability might be.

However, our approximation above shows that if $k = \lfloor c\sqrt{n}\rfloor$, then the lower bound from Proposition 3.3 tends to negative infinity as $n \to \infty$, while the upper bound for Abelian groups converges to $1 - \exp(-c^2/2)$. In particular, this shows that, when restricted to Cayley graphs on Abelian groups of order n and valence $c\sqrt{n}$, the probability $\Pr(\text{Diam} \leq 2)$ does *not* tend to 1 as $n \to \infty$, for any value of c.

This brings us to the question in the Introduction concerning the threshold for $k = f(n)$ at which the asymptotic value of the upper bound on $\Pr(\text{Diam} \leq 2)$ undergoes a phase transition, switching abruptly from 0 to 1 as k increases. Our previous findings allow us to give a more precise information about the transition.

Theorem 4.3 *Let G be a finite group of order n and let $P(n,k)$ denote the probability that a random Cayley digraph of degree $k = \lfloor f(n)\rfloor$ on G has diameter at most* 2*.*

- *There is a constant $c_1 > 0$ such that for an arbitrary function μ defined on positive integers, with $\mu(n) \to \infty$ as $n \to \infty$, we have: if $f(n) \geq \sqrt{2n\ln(c_1 n\mu(n))}$, then $\lim_{n\to\infty} P(n,k) = 1$.*
- *In the case of Abelian groups, there is a positive constant $c_2 < 1$ such that for every ε with $0 < \varepsilon < c_2$ we have: if $f(n) \leq \sqrt{2n\ln(c_2/\varepsilon)}$, then $\limsup_{n\to\infty} P(n,k) \leq 1 - \varepsilon$.*

Proof: To simplify the asymptotic calculations we may replace t with $n/2$ and $\lambda = k/t$ with $2k/n$. Moreover, by (11), (10) and other findings accumulated at the beginning of this Section, together with the fact that the coefficient at λ^3 in the $O(\lambda^3)$ term in (11) is positive, for sufficiently large n and for $k = o(n^{2/3})$ we have an upper bound on $a(n,k)$ of the form $\exp(-k^2/(2n)) \leq a(n,k) \leq c_1 \cdot \exp(-k^2/(2n))$ for some positive constant c_1 that absorbs the multiplication effect of the term $e^{tO(\lambda^3)} = e^{O(k^3/n^2)}$ appearing in (11) and of the terms $P(\lambda)$, $C(t,\lambda)$ from (10). Combining this with Proposition 3.3 we obtain, for $k \geq \lfloor\sqrt{n}\rfloor$ and $k = o(n^{2/3})$,

$$\Pr(\text{Diam} \leq 2) \;\geq\; 1 - c_1 \cdot n \cdot \exp(-k^2/(2n)) \quad \text{for general groups, and} \tag{12}$$

$$\Pr(\text{Diam} \leq 2) \;\leq\; 1 - c_2 \cdot \exp(-k^2/(2n)) \quad \text{for Abelian groups,} \tag{13}$$

where the positive constant $c_2 < 1$ absorbs the effect of multiplication by $1 - k/(n-1)$ appearing in Proposition 3.3; note that for $k = o(n^{2/3})$ this constant can be chosen arbitrarily close to 1 for sufficiently large n.

Clearly it is sufficient to prove the statement in the case when μ has polynomial growth. Routine limit calculation using this assumption show that if $k = \lfloor\sqrt{2n\ln(c_1 n\mu(n))}\rfloor$, then $c_1 n\, \exp(-k^2/(2n)) \cdot$

$\mu(n) \to 1$ as $n \to \infty$. Thus, for every $\varepsilon > 0$ there exists an $n(\varepsilon)$ such that for all $n > n(\varepsilon)$ we have $c_1 n \exp(-k^2/(2n)) < (1+\varepsilon)/\mu(n)$. Since $\mu(n) \to \infty$ as $n \to \infty$, for the same ε we have $\mu(n) > 1 + 1/\varepsilon$ for n sufficiently large. The last two inequalities with (12) yield $P(n,k) > 1 - \varepsilon$ for all sufficiently large n (depending on ε). Consequently, for $k \geq \lfloor \sqrt{2n \ln(c_1 n \mu(n))} \rfloor$ we have $P(n,k) \to 1$ as $n \to \infty$.

In the Abelian case, for every positive $\varepsilon < c_2$ let $k = \lfloor \sqrt{2n \ln(c_2/\varepsilon)} \rfloor$. For such a function k we have $\exp(-k^2/(2n)) \to \varepsilon/c_2$ as $n \to \infty$. By (13) this means that $\limsup_{n\to\infty} P(n,k) \leq 1 - \varepsilon$ for all $k \leq \lfloor \sqrt{2n \ln(c_2/\varepsilon)} \rfloor$. □

It is possible to derive still a slightly more detailed information about $P(n,k)$ by further asymptotic analysis of the inequalities (12) and (13), but for the sake of conciseness we chose to highlight just the two items contained in Theorem 4.3. We remark, however, that substantial refinements would require improvements on the bounds of Proposition 3.3 which differ by a factor of $n - 1$.

Although our asymptotic analysis answers a number of natural questions about the probability of a random Cayley digraph of a fixed degree having diameter 2, some questions still remain. For example, the case $k \sim c\sqrt{n}$ is not settled by our analysis for general groups, nor is the exact asymptotic order of the phase transition where $\Pr(\mathrm{Diam} \leq 2)$ switches from almost impossible to almost inevitable. We know that this order is at most $\sqrt{n \ln n}$ and definitely exceeds $\sqrt{n}$, and we conjecture that for both Abelian and general groups, $\sqrt{n \ln n}$ is the correct order.

Acknowledgements

Work on this paper begun at the University of Auckland, New Zealand, when the second author was visiting the third author thanks to the support of the local Department of Mathematics and NZIMA. Their enquiries about asymptotic analysis led from Auckland to Slovenia (M. Petkovšek) to Pennsylvania (H. Wilf) and then via Robin Pemantle to the first and the fourth author, the latter being blissfully unaware in Auckland of the existence of the work going on in the same building! The authors also thank Jana Šiagová from Slovak University of Technology, Bratislava, Slovakia, who was originally involved in discussions on the topic and decided to withdraw at a later stage.

The second author was partially supported by the ARRS Grant J1-0540. Research of the third author was supported by the VEGA Research Grant 1/0781/11, APVV Research Grants 0104-07 and 0223-10, and the APVV support as part of the EUROCORES Programme EUROGIGA, project GREGAS, ESF-EC-0009-10, financed by the European Science Foundation.

References

[Bol79] B. Bollobás. *Graph Theory, An Introductory Course*. Springer, 1979.

[MH98] J. Meng and Q. Huang. Almost all Cayley graphs have diameter 2. *Discrete Math.*, 178:267–269, 1998.

[ML97] J. Meng and X. Liu. The diameters of almost all Cayley digraphs. *Acta Math. Appl. Sinica (English Ser.)*, 13:400–413, 1997.