Cayley digraphs of given degree and their diameter

Manuel Lladser
Applied Mathematics
University of Colorado

in collaboration with
P. Potočnik J. Šiagiová
J. Širáň & M. C. Wilson

Notation.

G is a finite group of order n.

$G^* := G \setminus \{1\}$.

$S \subset G^*$ has cardinality k.

Cayley digraph associated with S.

$Cay(G, S)$ denotes the directed graph with vertex set G and edges $(g, g \cdot s)$, with $g \in G$ and $s \in S$.

Diameter.

The diameter of the Cayley digraph associated with S is:

$$\mathrm{Diam}(S) \stackrel{def}{=} \max_{g_1 \neq g_2} d_S(g_1, g_2) = \max_{g \in G^*} d_S(1, g),$$

where $d_S(g_1, g_2)$ is the length of the shortest path in $Cay(G, S)$ that starts at g_1 and ends at g_2.

Problem motivation.

Known facts.

- Almost all graphs and digraphs have diameter 2. [BOLLOBÁS'79]

If the events $[g \in S]$, with $g \in G$, are independent and each occurs with probability $1/2$ then:

- Almost all Cayley graphs have diameter 2. [MENG & LIU'97]
- Almost all Cayley digraphs have diameter 2. [MENG & HUANG'98]

Problem.

For which $k = k(n)$ is $\mathrm{Diam}(S)$, with $S \sim \mathit{Uniform}\binom{G^*}{k}$, almost surely equal to 2 as n tends to infinity.

Bounds on probability of [Diam > 2].

Recall:

$$\text{Diam}(S) = \max_{g \in G^*} d_S(1, g).$$

Note:

$$d_S(1, g) \leq 2 \quad \Leftrightarrow \quad g \in S \text{ or } (\exists s \in S) : \{s, s^{-1}g\} \subset S.$$

Bounds on probability of [Diam > 2].

Recall:

$$\text{Diam}(S) = \max_{g \in G^*} d_S(1, g).$$

Note:

$$d_S(1, g) \leq 2 \quad \Leftrightarrow \quad g \in S \text{ or } X(g).$$

Bounds on probability of [Diam > 2].

Recall:

$$\text{Diam}(S) = \max_{g \in G^*} d_S(1, g).$$

Note:

$$d_S(1, g) \leq 2 \quad \Leftrightarrow \quad g \in S \text{ or } X(g).$$

Lower-bound.

$$\mathbb{P}(\text{Diam} \leq 2) \leq \min_{g \in G^*} \mathbb{P}(g \in S \text{ or } X(g))$$

$$\begin{aligned} \Longrightarrow \quad \mathbb{P}(\text{Diam} > 2) &\geq \max_{g \in G^*} \mathbb{P}(g \notin S \text{ and } \overline{X(g)}) \\ &= \max_{g \in G^*} \mathbb{P}(\overline{X(g)} \mid g \notin S) \cdot \mathbb{P}(g \notin S) \\ &= \left(1 - \tfrac{k}{n-1}\right) \cdot \max_{g \in G^*} \mathbb{P}(\overline{X(g)} \mid g \notin S) \end{aligned}$$

Bounds on probability of [Diam > 2].

Recall:

$$\text{Diam}(S) = \max_{g \in G^*} d_S(1, g).$$

Note:

$$d_S(1, g) \leq 2 \quad \Leftrightarrow \quad g \in S \text{ or } X(g).$$

Upper-bound.

$$\begin{aligned}
\Longrightarrow \quad \mathbb{P}(\text{Diam} > 2) &\leq \sum_{g \in G^*} \mathbb{P}(g \notin S \text{ and } \overline{X(g)}) \\
&= \sum_{g \in G^*} \mathbb{P}(\overline{X(g)} \mid g \notin S) \cdot \mathbb{P}(g \notin S) \\
&\leq (n - 1 - k) \cdot \max_{g \in G^*} \mathbb{P}(\overline{X(g)} \mid g \notin S)
\end{aligned}$$

Summary.

Theorem. [LL-POTOČNIK-ŠIAGIOVÁ-ŠIRÁŇ-WILSON]

If $S \sim Uniform\binom{G^*}{k}$ then

$$\left(1 - \frac{k}{n-1}\right) \cdot M \leq \mathbb{P}(\text{Diam} > 2) \leq (n-1-k) \cdot M,$$

where

$$M \stackrel{def}{=} \max_{g \in G^*} \mathbb{P}(\overline{X(g)} \mid g \notin S).$$

THE ABELIAN CASE

Abelian case.

Theorem. [LL-POTOČNIK-ŠIAGIOVÁ-ŠIRÁŇ-WILSON]

If G is Abelian then

$$M = \max_{g \in G^*} \mathbb{P}(\overline{X(g)} \mid g \notin S) = 2^k \cdot \binom{n-2}{k}^{-1} \cdot \begin{cases} \binom{(n-3)/2}{k} & \text{, for } n \text{ odd;} \\ \binom{(n-2)/2}{k} & \text{, for } n \text{ even.} \end{cases}$$

Abelian case.

Proof. Since

$$\mathbb{P}(\overline{X(g)} \mid g \notin S) = \frac{\#\left\{ S \subset \binom{G^* \setminus \{g\}}{k} \text{ s.t. } (\forall x \in G^* \setminus \{g\}) : \{x, x^{-1}g\} \not\subseteq S \right\}}{\binom{n-2}{k}},$$

to compute M need to maximaze the numerator among all $g \in G^*$.

Fix g and define $T_x = \{x, x^{-1}g\}$.

Note:

$$\begin{aligned} T_x \cap T_y \neq \emptyset \quad &\text{iff} \quad x = y \text{ or } x^{-1}g = y \text{ or } y^{-1}g = x \text{ or } x^{-1}g = y^{-1}g \\ &\text{iff} \quad x = y \text{ or } g = xy \qquad \text{(Abelian!)} \\ &\text{iff} \quad T_x = T_y = \{x, y\} \end{aligned}$$

$\Longrightarrow$ the sets T_x, with $x \in G^* \setminus \{g\}$, partition $G^* \setminus \{g\}$.

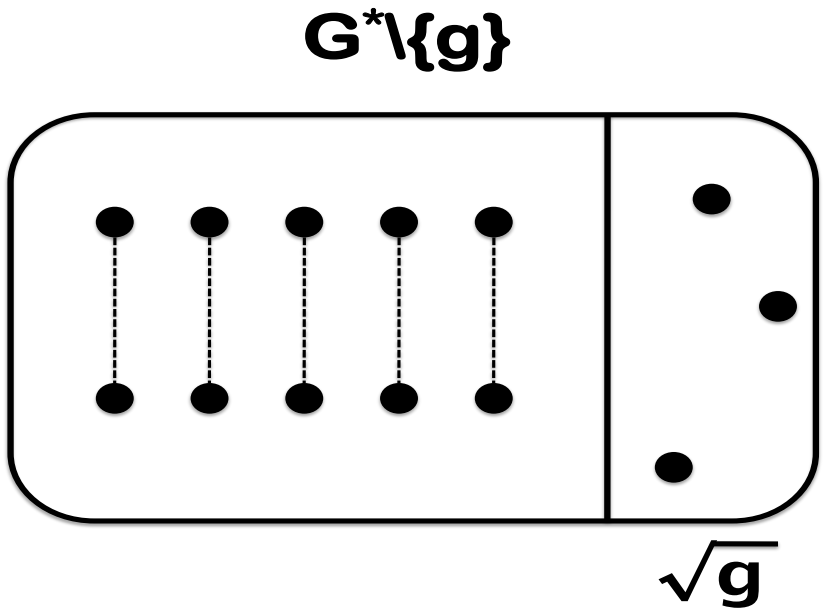
Abelian case.

Proof. Since

$$\mathbb{P}(\overline{X(g)} \mid g \notin S) = \frac{\#\left\{S \subset \binom{G^* \setminus \{g\}}{k} \text{ s.t. } (\forall x \in G^* \setminus \{g\}) : \{x, x^{-1}g\} \not\subseteq S\right\}}{\binom{n-2}{k}},$$

to compute M need to maximaze the numerator among all $g \in G^*$.

Fix g and define $T_x = \{x, x^{-1}g\}$.



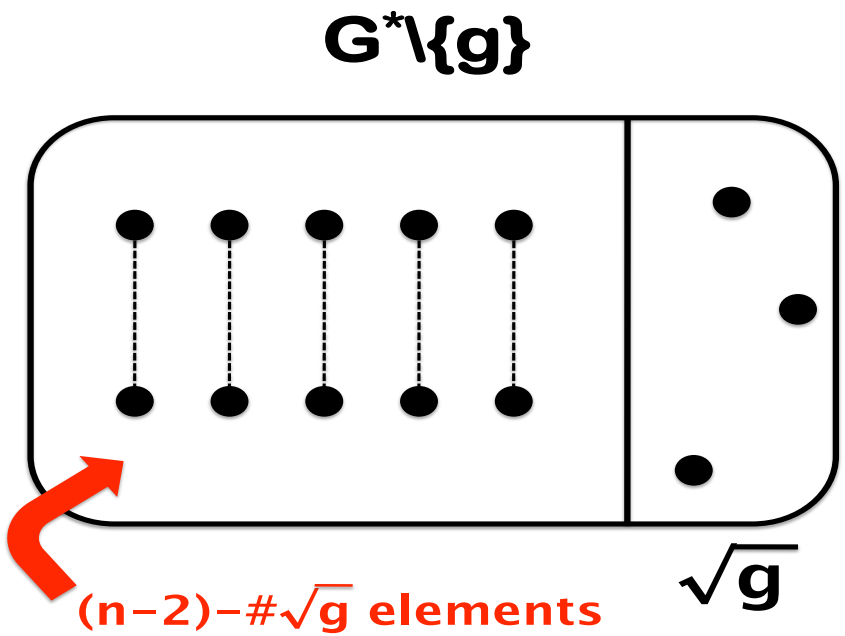
Abelian case.

Proof. Since

$$\mathbb{P}(\overline{X(g)} \mid g \notin S) = \frac{\#\left\{ S \subset \binom{G^* \setminus \{g\}}{k} \text{ s.t. } (\forall x \in G^* \setminus \{g\}) : \{x, x^{-1}g\} \not\subseteq S \right\}}{\binom{n-2}{k}},$$

to compute M need to maximaze the numerator among all $g \in G^*$.

Fix g and define $T_x = \{x, x^{-1}g\}$.



Abelian case.

Proof. Since

$$\mathbb{P}(\overline{X(g)} \mid g \notin S) = \frac{\#\left\{ S \subset \binom{G^* \setminus \{g\}}{k} \text{ s.t. } (\forall x \in G^* \setminus \{g\}) : \{x, x^{-1}g\} \not\subseteq S \right\}}{\binom{n-2}{k}},$$

to compute M need to maximaze the numerator among all $g \in G^*$.

Fix g and define $T_x = \{x, x^{-1}g\}$.

$$\Longrightarrow \mathbb{P}(\overline{X(g)} \mid g \notin S) = \frac{\binom{(n-2-\#\sqrt{g})/2}{k} \cdot 2^k}{\binom{n-2}{k}}$$

Abelian case.

Proof. Since

$$\mathbb{P}(\overline{X(g)} \mid g \notin S) = \frac{\#\left\{ S \subset \binom{G^* \setminus \{g\}}{k} \text{ s.t. } (\forall x \in G^* \setminus \{g\}) : \{x, x^{-1}g\} \not\subseteq S \right\}}{\binom{n-2}{k}},$$

to compute M need to maximaze the numerator among all $g \in G^*$.

Fix g and define $T_x = \{x, x^{-1}g\}$.

$$\implies \quad \mathbb{P}(\overline{X(g)} \mid g \notin S) = \frac{\binom{(n-2-\#\sqrt{g})/2}{k} \cdot 2^k}{\binom{n-2}{k}}$$

Lemma. [LL-POTOČNIK-ŠIAGIOVÁ-ŠIRÁŇ-WILSON]

- If n is odd then $\#\sqrt{g} = 1$ for all g.
- If n is even the $\#\sqrt{g} = 0$ for at least one g.

Abelian case.

Proof. Since

$$\mathbb{P}(\overline{X(g)} \mid g \notin S) = \frac{\#\left\{ S \subset \binom{G^* \setminus \{g\}}{k} \text{ s.t. } (\forall x \in G^* \setminus \{g\}) : \{x, x^{-1}g\} \not\subseteq S \right\}}{\binom{n-2}{k}},$$

to compute M need to maximaze the numerator among all $g \in G^*$.

Fix g and define $T_x = \{x, x^{-1}g\}$.

$$\implies \quad \mathbb{P}(\overline{X(g)} \mid g \notin S) = \frac{\binom{(n-2-\#\sqrt{g})/2}{k} \cdot 2^k}{\binom{n-2}{k}}$$

$$\implies \quad M = 2^k \cdot \binom{n-2}{k}^{-1} \cdot \begin{cases} \binom{(n-3)/2}{k} & , \text{ for } n \text{ odd} \\ \binom{(n-2)/2}{k} & , \text{ for } n \text{ even} \end{cases}$$

Q.E.D.

Abelian case.

Corollary. [LL-POTOČNIK-ŠIAGIOVÁ-ŠIRÁŇ-WILSON]

For each $c \in (0, 1/2)$, the probability of a random Cayley digraph of degree $k = \lfloor cn \rfloor$ on an Abelian group of order n having diameter 2 is at least $1 - O(exp(-c^2 n/2))$.

Corollary. [LL-POTOČNIK-ŠIAGIOVÁ-ŠIRÁŇ-WILSON]

For each $\delta \in (1/2, 1)$, the probability of a random Cayley digraph of degree $k = \lfloor n^\delta \rfloor$ on an Abelian group of order n having diameter 2 is at least $1 - O(exp(-n^{2\delta-1}/2))$.

Remark. Do to Moore's bound, no Cayley digraph of degree $k < \sqrt{n}$ on a any group has diameter 2.

THE GENERAL CASE

General case.

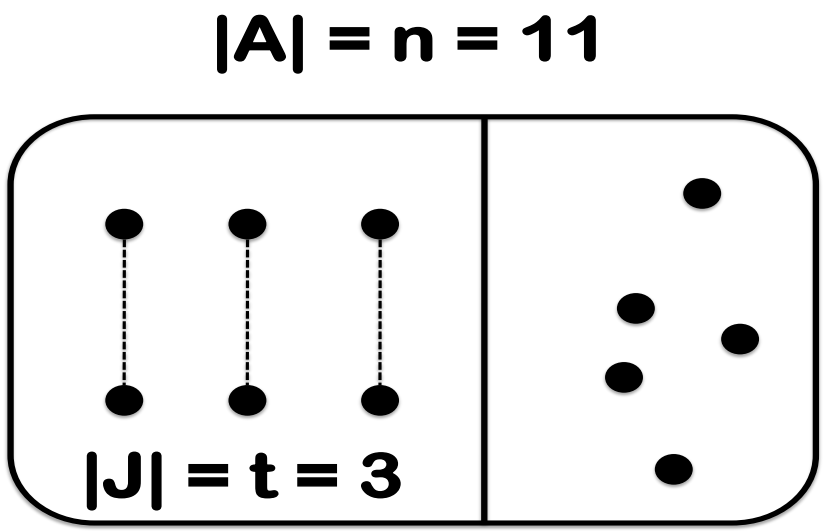
Definition.

Let A be a set of cardinality n and J a set of t pairwise disjoint unordered pairs. $a(n, k, t)$ denotes the number of k-subsets of a A that contain—as a subset—none of the pairs from J.

General case.

Definition.

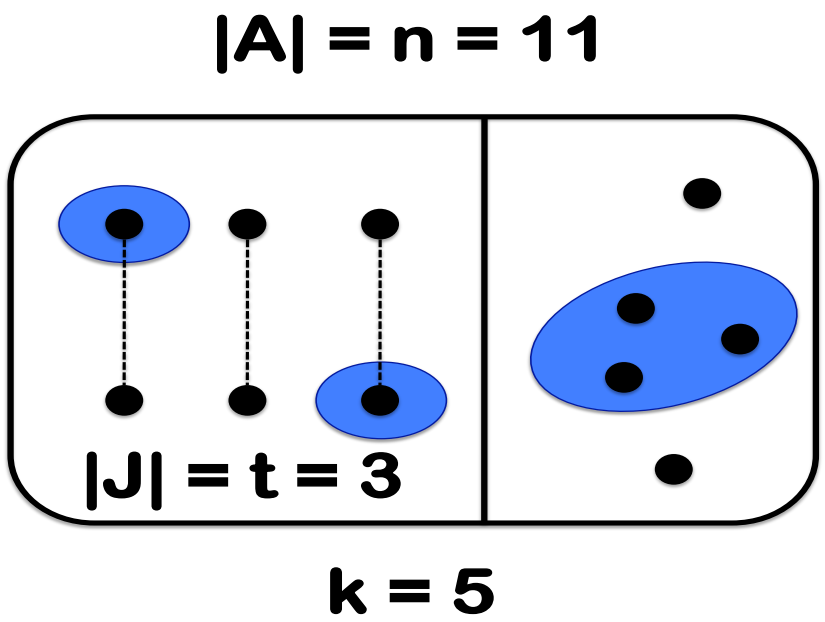
Let A be a set of cardinality n and J a set of t pairwise disjoint unordered pairs. $a(n, k, t)$ denotes the number of k-subsets of a A that contain—as a subset—none of the pairs from J.



General case.

Definition.

Let A be a set of cardinality n and J a set of t pairwise disjoint unordered pairs. $a(n, k, t)$ denotes the number of k-subsets of a A that contain—as a subset—none of the pairs from J.



General case.

Definition.

Let A be a set of cardinality n and J a set of t pairwise disjoint unordered pairs. $a(n,k,t)$ denotes the number of k-subsets of A that contain—as a subset—none of the pairs from J.

Theorem. [LL-POTOČNIK-ŠIAGIOVÁ-ŠIRÁŇ-WILSON]

For a general group G:

$$M \leq \binom{n-2}{k}^{-1} \cdot a(3t+1,k,t), \text{ with } t = \begin{cases} \lfloor (n-2)/3 \rfloor & \text{, for } n \text{ odd} \\ \lfloor (n-1)/3 \rfloor & \text{, for } n \text{ even} \end{cases}$$

Remark. An anonymous referee just showed to us that $M \leq \binom{n-2}{k}^{-1} \cdot a(2t,k,t)$, with $t = \lfloor (n-2)/2 \rfloor$.

General case.

Definition.

Let A be a set of cardinality n and J a set of t pairwise disjoint unordered pairs. $a(n,k,t)$ denotes the number of k-subsets of A that contain—as a subset—none of the pairs from J.

Lemma. [LL-POTOČNIK-ŠIAGIOVÁ-ŠIRÁŇ-WILSON]

If $n \geq (k+t)$ and $n \geq 2t$ then

$$a(n,k,t) = \sum_{\ell=0}^{k} \binom{n-2t}{\ell} \cdot \binom{t}{k-\ell} \cdot 2^{k-\ell} = [x^k]\,(1+x)^{n-2t}(1+2x)^t.$$

General case.

Lemma. [LL-POTOČNIK-ŠIAGIOVÁ-ŠIRÁŇ-WILSON]

Define $d_1 = (n-2t)/n$, $d_2 = t/n$, $d_3 = k/n$, and

$$r = \frac{2d_3}{(1-3d_3) + \sqrt{(1-3d_3)^2 + 8d_3(d_1+d_2-d_3)}}.$$

The following applies:

- If $r \to +\infty$ then $a(n,k,t) = O(2^t)$.
- If r stays in a compact subset of $(0,+\infty)$ then

  $$a(n,k,t) = \Theta\left(n^{-1/2} \cdot \exp\left\{n(d_1 \ln(1+r) + d_2 \ln(1+2r) - d_3 \ln r)\right\}\right).$$
- If $r \to 0^+$ then

  $$a(n,k,t) = \Theta\left(k^{-1/2} \exp\left\{n(d_1 \ln(1+r) + d_2 \ln(1+2r) - d_3 \ln r)\right\}\right).$$

Proof. Saddle-point Method in the lines of [GARDY'95; BANDERIER, FLAJOLET, SCHAEFFER & SORIA'00; PEMANTLE & WILSON'04; LL'06].

Abelian case.

Corollary. [LL-POTOČNIK-ŠIAGIOVÁ-ŠIRÁŇ-WILSON]

If $C \subset (0, 1/2]$ is a compact set then there exists $\gamma > 0$ such that the probability of a random Cayley digraph of order n and degree k having diameter 2 is at least $1 - O(\sqrt{n} \cdot \exp\{-n \cdot \gamma\})$, as n tends to infinity, uniformly for all n and k such that $k/n \in C$.

Corollary. [LL-POTOČNIK-ŠIAGIOVÁ-ŠIRÁŇ-WILSON]

For each $\delta \in (1/2, 1)$, the probability of a random Cayley digraph of degree $k = \Theta(n^\delta)$ on a group of order n having diameter 2 is at least $1 - O(n^{1-\delta/2} \cdot \exp\{-n^{2\delta-1}/3))$.

To do ...

- Asymptotic order of the phase transition where $\mathbb{P}(\text{Diam} > 2)$ goes from very unlikely to extremely likely. [PEMANTLE?]

... Questions?

... Thank you for your attention!