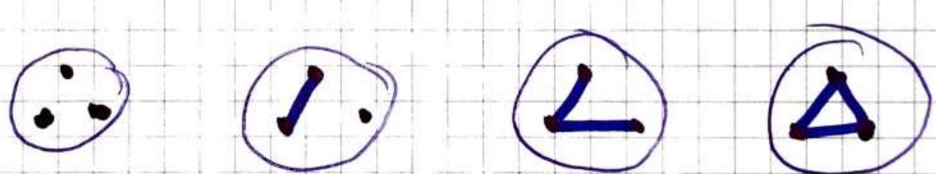
L6 (4/10/2020) Igor Pak

I. Rough Asymptotic Counting

① $\{a_n\}$, $a_n = \#$ graphs on n unlabeled vertices

OEIS A000088: 1, 2, 4, 11, 34, 156, 1044, ...

Ex $a_3 = 4$



Th (Erdös-Renyi, 1963)

$$a_n \sim \frac{1}{n!}\, 2^{\binom{n}{2}}$$

Exc Prove E-R thm.

ML: w.h.p. # edges to be changed to have symmetries is $\geq \frac{n}{2}(1-o(1))$

Cor 1 $a_n = 2^{\frac{n^2}{2}(1+o(1))}$

▷ trivially $\frac{1}{n!}\, 2^{\binom{n}{2}} \le a_n \le 2^{\binom{n}{2}}$ $\blacksquare$

---

② $\{b_n\}$, $b_n = \#$ matroids on n elts

Th [Bansal-Pendavich-van der Pol, 2014]

$$\log \log b_n = n - \frac{3}{2} \log n + \frac{1}{2} \log \frac{2}{\pi} + o(1)$$

Cor 2 $b_n = 2^{2^n n^{\Theta(1)}}$ // $b_n = 2^{(2^n / n^{3/2}) \cdot \Theta(1)}$ //

OEIS A055545 2, 4, 8, 17, 38, 98, 306, 1724, →
→ 383.172

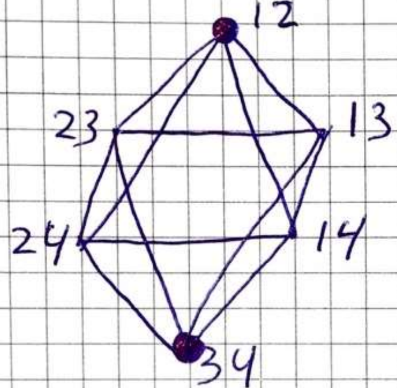
▷ / hard to compute /

Def **Johnson graph** $J(n,k)$

vertices: $\binom{[n]}{k} = \{k\text{-subsets of } [n] = \{1 \ldots n\}\}$

edges: $(A,B) \in \binom{[n]}{k}$ s.t. $|A \cap B| = k-1$.

Ex $J(4,2)$



$\mathrm{ind}\, J(4,2) = 2$

Th [Piff-Welsh, 1970]

\# matroids on n elts of rank k $\overset{①}{\geq} \frac{1}{2}\, \mathrm{ind}\, J(n,k)$

$\overset{②}{\geq} 2^{2^n n^{-5/2} \log n}$

Note $\Rightarrow$ **Cor 2**

Key exc: Read def of a matroid.

Prove ① of P-W Thm.

Proof of ② by Knuth (1974), Graham-Sloane (1980)

L/Idea: $\exists$ indep set of size $\geq \frac{1}{n}\binom{n}{k}$

$\triangleright$ $A \in \binom{[n]}{k} \longrightarrow$ 0-1 vectors in $\mathbb{R}^n$ w/ exactly k 1's

$\varphi : \{0,1\}^n \to \mathbb{Z}_n$

$\varphi(x_1 \ldots x_n) := \sum_{i=1}^{n} i\, x_i \mod n$

Observe $(A,B) \in J(n,k) \Rightarrow \varphi(A) \neq \varphi(B)$ $\blacksquare$

$\Rightarrow \operatorname{ind} J(n,k) \geq \frac{1}{n}\binom{n}{k}$

Let $k = n/2 \Rightarrow b_n \underset{PW}{\geq} 2^{\frac{1}{n}\binom{n}{n/2}} \underset{KGS}{=} 2^{2^n/n^{3/2}\,\Theta(1)}$ $\blacksquare$

③ $\{c_n\}$, $c_n = \#$ groups of order n

OEIS: A000001 $\quad 1, 1, 1, 2, 1, 2, 1, 5, 2, 2, 1, \dots$

Ex $c_4 = 2$: $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4$ | $c_p = 1$, p-prime

$c_6 = 2$: $\mathbb{Z}_6$, S_3

$c_{128} = 2328$, $c_{256} = 56092$,

$c_{512} = 10.494.213$, $c_{1024} = 49.487.365.422$

$c_{2048} = ??$ [Besche-Eick-O'Brien, 2002]

Conj $c_{2^k} / (c_1 + c_2 + \dots + c_{2^k}) \to 1$ as $k \to \infty$

"almost all groups are 2-groups"

k=10 $c_{2^{10}} / c_1 + \dots + c_{2^{10}} > 0.99$

Th [Pyber, 1993]

$$c_1 + \dots + c_n = n^{\frac{2}{27}(1+o(1))(\log n)^2}$$

/ log(# groups of order $\leq n$) $\sim \frac{2}{27}(\log n)^3$ /

≈ **Cor** $\quad c_{2^k} \geqslant 2^{\Omega(k^3)}$

[Higman, 1960]

Proof of Cor (#2-groups)

$$G_k := \langle x_1 \dots x_k \rangle / \langle x_i^2 = [x_i\, x_j]^2 = [x_i, [x_j\, x_r]] = 1 \rangle$$

$$g \in G_k \Rightarrow g = x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k} [x_1, x_2]^{\alpha_{12}} [x_1, x_3]^{\alpha_{13}} \cdots$$

where $\varepsilon_i, \alpha_{ij} \in \{0, 1\}$

<u>Let</u> $W \subseteq F_2^{\binom{k}{2}} = \langle \alpha_{ij} \rangle \leftarrow$ m-dim subspace of $\mathbb{F}_2^{\binom{k}{2}}$

$H_W := G_k / W$

$$\#\{H_W / \text{isom}\} \geq \frac{\#\, m\text{-subspaces of } \mathbb{F}_2^{\binom{k}{2}}}{\# GL(k, \mathbb{F}_2)}$$

$$\geq \binom{\binom{k}{2}}{m}_2 \; 2^{-k^2}$$

$$\geq 2^{m\left(\binom{k}{2} - m\right) - k^2}$$

$m := k(k-1)/2 - k$

$$\geq 2^{k\left(\frac{k(k-1)}{2} - k\right) - k^2}$$

$$\geq 2^{\Theta(k^3)}$$ groups of order 2^{2k} ∎

Back to commutivity testing

Def Black Box group $G = \langle s_1 \dots s_k \rangle$

1. can $x, y \to xy$ in time μ
2. can $x \to x^{-1}$ —— " ——
3. can answer $x \stackrel{?}{=} 1$ in time ν

From CS pov: this is an oracle model

Th [P, 2011]

Testing $G \stackrel{?}{=}$ abelian for black box group G requires $\Omega(k^2 \mu) + \binom{k}{2} \nu$

Proof (via adversory)

$A_0 = \mathbb{Z}_2^k$ $\qquad$ $B_0 = G_k = \langle x_1 \dots x_k \rangle / (x_i^2 = [x_i, x_j]^2 = \dots)$

Q1 $\text{word}_1 \overset{?}{=} 1$

$A_1 := A_0$, $\qquad B_1 = B_0$ if yes in B_0

$\qquad\qquad\qquad B_1 = B_0 / \text{word}_1$ if NO in B_0

Q2 $\text{word}_2 \overset{?}{=} 1$

$A_2 := A_0$, $\qquad B_2 = B_1$ is yes in B_1

$\qquad\qquad\qquad B_2 = B_1 / \text{word}_2$ if NO in B_1

$\vdots$

Need $\geq \binom{k}{2}$ Q's to distinguish

A vs B $\blacksquare$