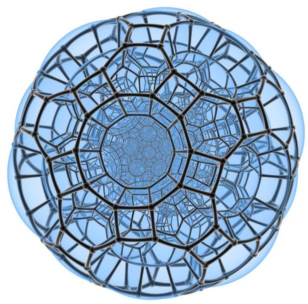
Problems: New, Old and Unusual

Igor Pak, UCLA

National University of Ireland

Galway, Ireland, December 1, 2009



Generating random group elements problem:

★ Given a finite *black box* $G = \langle g_1, \ldots, g_k \rangle$,
generate *random* (nearly uniform) group elements.

Can: algorithm with $\mathrm{Poly}(\log |G|, k)$ time.

Want: algorithm with $O(k \log |G|)$ time.

We can: always assume $k = O(\log |G|)$.

We want: have $k = O(1)$.

Three algorithms:

1. Babai algorithm (1991)

time: $O(\log^5 |G|)$ [Babai], $O(\log^4 |G|)$ [Pak'00]
space: $\ell = O(\log |G|)$ (in both cases)

Idea: Take $\ell = O(\log |G|)$ repeated r.w. on G of length L.
Keep adding endpoints of r.w.'s to your generating set.
The last r.w. gives random group elements.

Better bounds?

For a *lazy r.w.* on Γ =Cayley(G, S), with $\langle S \rangle = G$, $|S| = k$

Known bounds:

1) mixing time $= O(\Delta^2 k \log |G|)$, where $\Delta = \mathrm{diam}(\Gamma)$.
[Alon, Babai, Chung, Jerrum-Sinclair, Diaconis-Strook]

2) mixing time $= O(\Delta N k \log |G|)$, where $N = N(\Gamma)$ is a maximal multiplicity of an element in shortest paths [Diaconis & Saloff-Coste]

Conjecture [Diaconis, Peres] mixing time $= O(\Delta^2 k)$.

Conjecture [Pak] mixing time $= O(\Delta N k \log \log |G|)$.

This would give $O^*(\log^3 |G|)$ bound for the Babai Algorithm

2. Product replacement algorithm (1995, 2002)

(Leedham-Green & Soicher, [CLMNO], Leedham-Green & Murray)

space: $\Omega(k + \log\log|G|)$ [Pak, Lubotzky, Detomi-Lucchini-Morini]
(that's what it takes to avoid the bias discovered in [Babai-Pak])

time: $O^*(\log^9|G|)$ [Pak'00], $O^*(\log^5|G|)$ [Pak, unpublished]
space: $O^*(\log|G|)$ (in both cases)

time: $O(k\log|G|)$, space: $O(k)$ [Lubotzky-Pak, + more]
(very special cases, or very special assumptions)

Idea: take a r.w. on generating ℓ-tuples $(g_1, \ldots, g_\ell)$:
Repeatedly use random substitutes $g_i \leftarrow g_i g_j^{\pm 1}$ or $g_i \leftarrow g_j^{\pm 1} g_i$
Output random components of the ℓ-tuple

3. Random subproducts algorithm [Cooperman'02]

time: $O(\log^2 |G|)$ [Dixon'08]
space: $O(\log |G|)$

Idea: Take repeated *random subproducts*

$$g = g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k}, \quad \varepsilon_i \in \{0, 1\}$$

Add new subproducts to your generating set;
Repeat this $O(\log |G|)$ times.

Making k smaller

Problem: Does there exist a $\mathrm{Poly}(\log|G|)$ time algorithm with space $\ell = O(k)$?

Conjecture 1. Yes, if G is simple, $k = O(1)$.

In fact, PRA will probably work for simple groups of Lie type. Moreover, even Babai Algorithm will probably work in this case.

Conjecture 2. No, for general finite G and k.

If I had to guess, take $G = (A_n)^{n!/8}$, where $n \to \infty$, and $k = 2$.

Complexity theory: even the case $\ell = (\log|G|)^\alpha$ with $\alpha < 1$, does not follow from known results.

What is known:

Conjecture [Babai]: The diameter of *every* Cayley graph of a simple group is $O(\log^c |G|)$.

Now known for $\mathrm{SL}(n, q)$, [Dinai, 2006], [Helfgott, 2008]

This implies that a single round of of length $L = O(\log^c |G|)$ in the Babai Algorithm will suffice for Conjecture 1.

Prediction: Eventually (in the next 10 years) Babai conjecture will be established for all simple groups of Lie type.

For A_n there is much less hope, despite recent polynomiality results of [Babai-Beals-Seress], [Babai-Heyes].

Conjecture* [Lubotzky]: The *every* Cayley graph of a simple group of Lie type with bounded rank, is an *expander*.

In particular, the diameter of Cayley graphs is $O(\log |G|)$ then.
Also implies that PRA works in *linear time* [Gamburd-Pak]

Has been established in [Brouillard-Gamburd'09+] for $\mathrm{SL}(2, p)$, some p.
(based on [Gamburd-Shahshahani], [Bourgain-Gamburd], [Helfgott])

Theorem [Brouillard-Gamburd + Gamburd-Pak]
For infinitely many primes p, the PRA on $\mathrm{SL}(2, p)$ with $\ell \geq 8$ takes linear time $O(\log p)$.

Sum / products ideas

Conjecture [Erdős-Szemerédi] *For every finite* $A \subset \mathbb{N}$ (*also* $\mathbb{F}_q$, $\mathbb{C}$) *either* $|A + A| = O(|A|)$, *or* $|A \cdot A| = O(|A|)$.

Open, but $|A+A| \cdot |A \cdot A| = O(|A|^3)$ is known, as well as many versions over the finite field [Bourgain-Katz-Tao, Konyagin, Tao, Solymozi, etc.]

Lemma [Helfgott]
For $A \subset \mathrm{SL}(2,p)$, $|A| < p^{3-\delta}$, we have

$$|A \cdot A \cdot A| > |A|^{1+\varepsilon}$$

for some $\varepsilon = \varepsilon(\delta) > 0$.

Other groups?

Open Problem: Variation for S_n ???

Theorem [Freiman]

For every finite group G with the generating set S, and $A \subset G$, either $|A \cdot A| > \frac{4}{3}|A|$, or $|S \cdot A \cdot A| > 2|A|$.

This result lies in the heart of Dixon's analysis of the random subproduct algorithm.

Lemma [Freiman] *Suppose that G is a group and that $B \subseteq G$ is a set with $|B \cdot B^{-1}| < \frac{4}{3}|B|$. Then $B \cdot B^{-1}$ is a subgroup of G.*

Proof: For every $b_1, b_2 \in B$ we have $|Bb_1^{-1} \cap Bb_2^{-1}| > \frac{2}{3}|B|$. Thus, there are more than $\frac{2}{3}|B|$ pairs $(x_1, x_2) \in B^2$ with $x_1^{-1}x_2 = b_1^{-1}b_2$. In particular, we have $|B^{-1} \cdot B| < \frac{3}{2}|B|$. From here, for every fixed $b_1, b_2 \in B$ we have $|b_1^{-1}B \cap b_2^{-1}B| > \frac{1}{2}|B|$. Thus, there are more than $\frac{1}{2}|B|$ pairs $(x_1, x_2) \in B^2$ with $x_1x_2^{-1} = b_1b_2^{-1}$.

Similarly for any fixed b_3, b_4^{-1} there are more than $\frac{1}{2}|B|$ pairs $(x_3, x_4) \in B^2$ with $x_3x_4^{-1} = b_3b_4^{-1}$. By the pigeonhole principle we may choose (x_1, x_2) and (x_3, x_4) so that $x_2 = x_3$, which means that $(b_1b_2^{-1})(b_3b_4^{-1}) = x_1x_4^{-1} \in B \cdot B^{-1}$. $\square$

Thank you!