18.317 Combinatorics, Probability, and Computations on Groups	10 September 2001
Lecture 2	
Lecturer: Igor Pak	*Scribe: Jason Burns*

The probability of generating a group, part 2

Some notation from last time:

Let G be a group. We will write $\varphi_k(G)$ for the probability that k random elements of G generate the entire group. (We assume that all the elements are chosen independently, and each group element is equally likely.) For example, $\varphi_1(G) \neq 0$ if and only if G is cyclic.

We also define $\ell(G)$ as the length of the longest subgroup chain in G; that is, $\ell(G)$ is the largest ℓ such that

$$1 = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_\ell = G.$$

Yesterday[1] we proved that, if $|G| \leq 2r$ (or even if we only have $\ell(G) \leq r$), then $\varphi_k(G) \geq \varphi_k(\mathbb{Z}_2^r)$.

Today, we'll estimate $\varphi_k(\mathbb{Z}_2^r)$. We argued last time that this was the worst possible case (that is, $\varphi_k(G) \geq \varphi_k(\mathbb{Z}_2^r)$ whenever $|G| \leq 2^r$), so this immediately leads to a lower bound for $\varphi_k(G)$ ...

Theorem 1 *Let $G = \mathbb{Z}_2^r$. Then $\varphi_r(G) > \frac{1}{4}$, $\varphi_{r+1}(G) > \frac{1}{2}$, and in general $\varphi_{r+j}(G) > 1 - \frac{c}{2^j}$ for some constant c.*

To make our estimate, we'll use two famous identities of Euler (1748):

$$\prod_{j=1}^{\infty}(1 - z^j) = 1 + \sum_{m=1}^{\infty}(-1)^m\left(z^{\frac{m(3m-1)}{2}} + z^{\frac{m(3m+1)}{2}}\right)$$

and

$$\prod_{j=0}^{\infty}\frac{1}{1 - tz^j} = 1 + \sum_{m=1}^{\infty}\frac{t^m}{(1-z)(1-z^2)\cdots(1-z^m)}.$$

Proof of Theorem 1

One way of visualizing $\varphi_k(\mathbb{Z}_2^r)$ is as follows. Consider $\mathbb{Z}_2^r$ as an r-dimensional vector space over the two-element field $\mathbb{Z}_2$. Then we're asking for the probability that a given set of k vectors span the whole space of r dimensions. Or, put in another way,

$$k\left\{\underbrace{\begin{bmatrix} a_1, & a_2, & \cdots, & a_r \\ b_1, & b_2, & \cdots, & b_r \\ & \cdots & & \\ z_1, & z_2, & \cdots, & z_r \end{bmatrix}}_{r}\right.$$

[1] Last Friday, actually, but it *feels* like only yesterday.

if we make a matrix out of our k vectors, what is the probability that matrix has rank r? — Just when all r of the columns are independent, of course.

$$k\left\{\underbrace{\begin{bmatrix} a_1 & a_2 & & a_r \\ b_1 & b_2 & & b_r \\ \vdots & \vdots & \vdots & \vdots \\ z_1 & z_2 & & z_r \end{bmatrix}}_{r}\right.$$

The probability that the first column is nonzero is $(1-\frac{1}{2^k})$. The probability that the second column is linearly independent of the first row is $(1-\frac{1}{2^{k-1}})$. In general, the probability that the j-th column is linearly independent of the previous $j-1$ columns is $(1-\frac{2^{j-1}}{2^k})$, and hence the probability that all the columns are linearly independent is $\varphi_k(\mathbb{Z}_2^r) = \prod_{j=1}^r (1-\frac{2^{j-1}}{2^k})$.

Now, we already know that $\mathbb{Z}_2^r$ cannot be generated by fewer than r elements, and indeed $\varphi_k(\mathbb{Z}_2^r) = 0$ for $k < r$, according to the formula we've just derived. How about for $k = r$? Then we have the estimate

$$\begin{aligned}
\varphi_r(\mathbb{Z}_2^r) &= (1-\frac{1}{2^r})(1-\frac{1}{2^{r-1}})\cdots(1-\frac{1}{2}) \\
&> \prod_{j=1}^{\infty}(1-\frac{1}{2^j}) \\
&= \underbrace{1-\frac{1}{2^1}-\frac{1}{2^2}}_{=\frac{1}{4}}+\underbrace{\frac{1}{2^5}+\frac{1}{2^7}-\frac{1}{2^{12}}-\frac{1}{2^{15}}+\cdots}_{>0} \\
&> \frac{1}{4}.
\end{aligned}$$

Did you notice how we used one of Euler's famous identities in the third line?

One down, two to go. For $\varphi_{r+1}(\mathbb{Z}_2^r)$, we just mimic the previous argument.

$$\begin{aligned}
\varphi_{r+1}(\mathbb{Z}_2^r) &= (1-\frac{1}{2^{r+1}})(1-\frac{1}{2^r})\cdots(1-\frac{1}{2^2}) \\
&> \prod_{j=2}^{\infty}(1-\frac{1}{2^j}) \\
&= (1-\frac{1}{2})^{-1}\prod_{j=1}^{\infty}(1-\frac{1}{2^j}) \\
&= 2\prod_{j=1}^{\infty}(1-\frac{1}{2^j}) \\
&> 2\cdot\frac{1}{4} \\
&= \frac{1}{2}.
\end{aligned}$$

We'll use a different estimate for the general case.

$$
\begin{aligned}
\varphi_{r+k}(\mathbb{Z}_2^r) &= (1-\frac{1}{2^{r+k}})(1-\frac{1}{2^{r+k-1}})\cdots(1-\frac{1}{2^{k+1}}) \\
&> \prod_{j=1}^{\infty}(1-tz^j) \qquad (\text{let } t=\frac{1}{2^k} \text{ and } z=\frac{1}{2}) \\
&= (1+\sum_{m=1}^{\infty}\frac{t^m}{(1-z)(1-z^2)\cdots(1-z^m)})^{-1}
\end{aligned}
$$

Now, to get a lower bound on this, we need an upper bound on the quantity in parentheses. The denominator of the sum might look familiar — it's just $\varphi_m(\mathbb{Z}_2^m) = (1-z)(1-z^2)\cdots(1-z^m)$, which we already determined was at least $\frac{1}{4}$.

$$
\begin{aligned}
1+\sum_{m=1}^{\infty}\frac{t^m}{\varphi_m(\mathbb{Z}_2^m)} &< 1+4\sum_{m=1}^{\infty}t^m \\
&< 1+4\frac{t}{1-t} \\
&= 1+4\frac{\frac{1}{2^k}}{1-\frac{1}{2^k}} \\
&< 1+4\frac{\frac{1}{2^k}}{\frac{1}{2}} \\
&= 1+\frac{8}{2^k}
\end{aligned}
$$

Hence

$$
\varphi_{r+k}(\mathbb{Z}_2^r) > \frac{1}{1+\frac{8}{2^k}} > 1-\frac{8}{2^k}.
$$

You can, of course, make a better estimate.

Random Group Processes: Loose Ends

We can turn this around, and ask what the probability is that the elements we pick *don't* generate a group. Let $\delta(t) = 1-\varphi_t(G)$, where G is (as usual) a finite group. Obviously $\delta(t+1) \le \delta(t)$, and in general $\delta(t+s) \le \delta(t)\delta(s)$ since we're picking each element independently. So δ is submultiplicative, it decays exponentially[2], and if you've been paying attention you should be able to estimate when δ first drops below $\frac{1}{2}$.

Yet another way of posing this question, as you may recall from last lecture, is to ask how many elements we have to pick to generate G. Recall that we defined the *stopping time* τ to be the number of elements we have to pick, one at a time, to generate G. Of course, it depends on which elements we pick, but we can estimate it.

Proposition 2 $E(\tau) = \sum_{\tau=0}^{\infty}\delta(\tau)$.

[2]The exponent turns out to be the smallest index of a proper subgroup of G.

Proof: $\sum_{t=0}^{\infty} \delta(t) = \sum_{t=0}^{\infty} \Pr(\tau > t) = \sum_{t=0}^{\infty} t \cdot \Pr(\tau = t) = E(t)$. ■

We know $E(\tau)$ in terms of δ, and we know δ in terms of $\varphi_k(G)$, and we have the estimate $\varphi_{k+r}(G) > 1 - \frac{8}{2^k}$ from above. So we can estimate $E(\tau)$:

Corollary 3 *For any group G, $E(\tau) \leq \ell(G) + C$, where C is a constant.*

Proof: The worst possible case for a given $r = \ell(G)$ is $\mathbb{Z}_2^r$, and in that case, $\varphi_{k+r}(H) > 1 - \frac{8}{2^k}$, as we proved earlier today. So $\delta_{m+k}(G)$ is less than $\frac{8}{2^k}$, and $E(\tau) < r + \sum_{k+1}^{\infty} \frac{8}{2^k} = r + 8$. ■

Next time ...

Babai proved that two random elements of S_n generate either A_n or S_n, with probability $1 - \frac{1}{n} + O(\frac{1}{n^2})$[3].

Tomorrow we'll prove that, using classification of the finite simple groups.

(Where does the $\frac{1}{n}$ come from?, you may ask. Well, let's suppose that the two permutations never mix some of the n elements — that they permute k elements, and the other $n-k$ separately. Specifically, if they both fix a point, that gives rise to our $\frac{1}{n}$ term. (Only one pair in n^2 fixes a given point under both permutations — but there are n points to choose from. Hence $\frac{1}{n}$.))

[3]Dixon proved the weaker result $1 - O(\frac{1}{(\log \log n)^2})$.