Searching for Permutation Groups

Manhattan Algebra Day

Robert Gilman

Stevens Institute of Technology

December 7, 2018

Random elements of groups

Computational problems for finite and finitely presented groups have been studied for over a hundred years.

Random group elements are useful for debugging and testing group algorithms among other things.

The product replacement algorithm works for finite groups but not for infinite groups.

$\Sigma \to G$ is a choice of semigroup generators for the infinite group G.

$\overline{w}$ is the image of $w \in \Sigma^+$.

It seems reasonable that $\overline{w}$ is close to random if w is a random word of length $|w| \leq n$ for large n.

But then sets $X \subset \Sigma^+$ of asymptotic density 0 are virtually invisible.

$$lim_{n\to\infty} \frac{|X \cap \Sigma^{\leq n}|}{|\Sigma^{\leq n}|} = 0$$

$\overline{w}$ is never equal to 1 in G.

The disadvantage for debugging and testing algorithms is obvious.

Algorithmic search

Replace $\Sigma^{\leq n}$ by C_n, the set of all words with *descriptions* of length at most n.

Theorem 1.

If $X \subset \Sigma^+$ and X contains an infinite decidable subset, then X has positive lower asymptotic density:

$$\liminf_{n \to \infty} \frac{|X \cap C_n|}{|C_n|} > 0$$

Thus we can search more effectively for elements of X.

For large enough n the probability that $\overline{w} = 1$ in a 2-generator group seems to be at least 0.15.

There are implementation issues.

Descriptions

Definition 2.

A description of $w \in \Sigma^+$ is a program p in a fixed programming language together with an input $v \in \Sigma^+$ such that p with input v prints w and halts.

Programs are certain words over some big alphabet.

Code the letters of the big alphabet as words of a fixed length ℓ over Σ.

Reserve one word of length ℓ to mark the end of p and the beginning of v.

Thus a description pv is itself a word over Σ.

Consequently $|C_n| \leq |\Sigma|^{n+1}$

Proof of Theorem 1

Theorem 1.

If $X \subset \Sigma^+$ contains an infinite decidable subset, then

$$\liminf_{n\to\infty} \frac{|X \cap C_n|}{|C_n|} > 0$$

1. $\Sigma^n \subset C_{n+c}$.
2. There exists a computable injection $f : \Sigma^+ \to X$.
3. $f(C_{n+c}) \subset X \cap C_{n+c+c_f}$.
4. $|\Sigma|^n \leq |X \cap C_{n+c+c_f}|$.

$$\frac{|X \cap C_{n+c+c_f}|}{|C_{n+c+c_f}|} \geq \frac{|\Sigma|^n}{|\Sigma|^{n+c+c_f+1}} = \frac{1}{|\Sigma|^{c+c_f+1}}$$

More about C_n

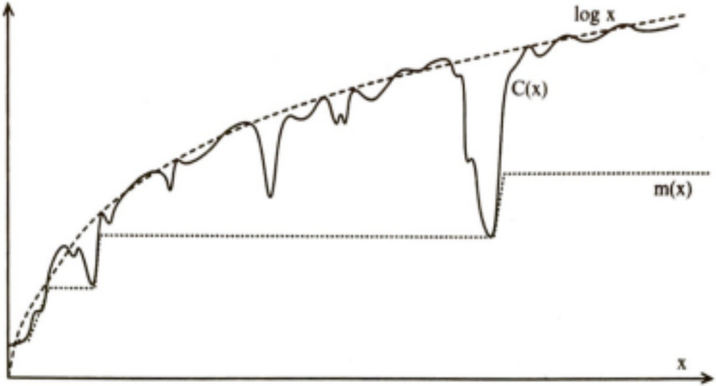
Let $\Sigma = \{0, 1\}$.

The size of the smallest description of $w \in \Sigma^+$ is $C(w)$, the Kolmogorov complexity of w.

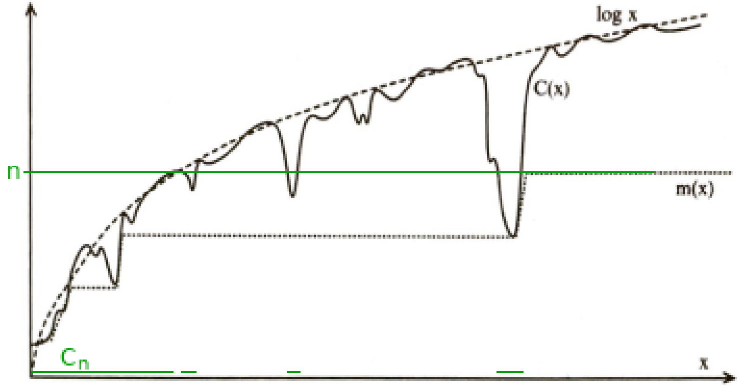
Identify Σ^+ with N via

N	1	2	3	4	5	6	7	8	$\cdots$
$\{0,1\}^+$	0	1	00	01	10	11	000	001	$\cdots$

$C(w)$ becomes a function $C : N \to N$



The function $C : N \to N$.



The function $C : N \to N$.

References

There are not many applications of Kolmogorov complexity to group theory.

1. A. Nies and K. Tent, 2017.
2. I. Kapovich and P. Schupp, 2005.
3. R. Grigorchuk, 1985.

The standard reference is Li and Vitányi.

Shen, Uspensky and Vereshchagin is also good.

Implementation

Unfortunately $C(w)$ is incomputable and known approximations are infeasible in practice.

Instead we do algorithmic searches based on heuristic approximations to the sets C_n.

In particular we allow only a very restricted set of programs.

Finitely generated groups

$X \subset \Sigma^+ \to G$, $\Sigma = \{a, A, b, B\}$

Descriptions have the form pv where

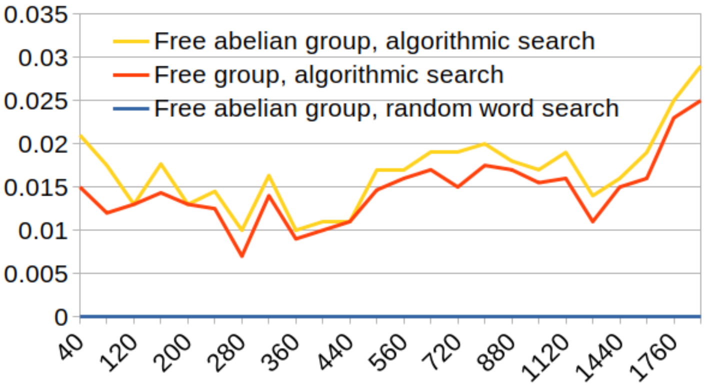
$$pv = \underbrace{ab, bB, aB, AA,}_{f} \underbrace{bb, BA, BB, AB,}_{g} abAA$$

describes

$$(f \circ g)(abAA) = aBaBaBaBbBaBaB$$

$C'_{d,c,M}$ consists of descriptions pv with $v \leq M$ and d homomorphisms specified by tuples of words of length c.

Algorithmic search is performed by choosing random descriptions from $C'_{d,c,M}$.



Observed probability of words of various lengths defining the identity in the free groups of rank 2 and the free abelian group of rank 2.

Permutation groups

Finding permutation groups with which to debug and test permutation group algorithms can be a problem.

Two random permutations in S_n generate a subgroup other than S_n or A_n with probability at most $\frac{1}{n} + \frac{8.8}{n^2}$. [Morgan, Roney-Dougal 2015]

We change the search problem slightly so that our search method applies.

S_n acts on $[1, \ldots, n]$.

S_ω is the direct limit of $S_1 \subset S_2 \subset \cdots \subset S_n \subset \cdots$.

$\{0,1\}^+ \to N \to S_\omega \times S_\omega$ is a computable enumeration.

$X \subset \{0,1\}^+$ is the inverse image of all pairs which do not generate any S_n or A_n in the direct limit above.

Algorithmic search proceeds as before.

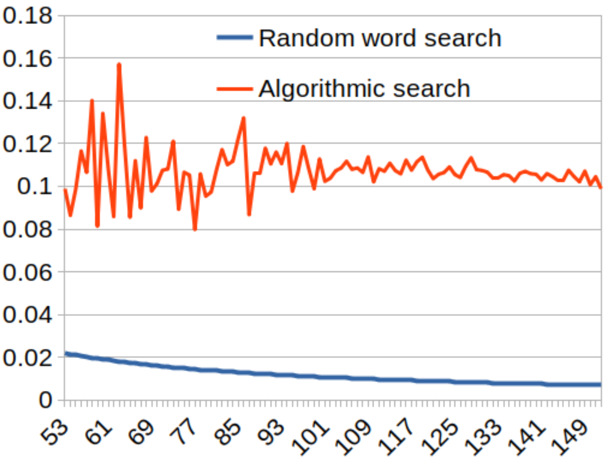
Descriptions use polynomials instead of semigroup homomorphisms.

$$\underbrace{8, 2, 3, 1}_{p};\underbrace{6, 7, 4, 2}_{q}; 15$$

describes

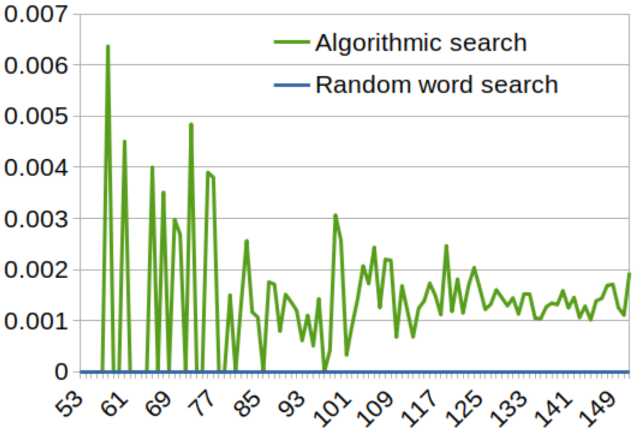
$$(8x^3 + 2x^2 + 3x + 1) \circ (6x^3 + 7x^2 + 4x + 2)(15) = 83879080636024.$$

Avoiding S_n and A_n



Observed probability of avoiding S_n and A_n for various permutation degrees. The line at the bottom is the bound $\frac{1}{n} + \frac{8.8}{n^2}$.

Finding solvable permutation groups.



Observed probability of finding a solvable permutation group for various permutation degrees.

Terminal - bob@bob-ThinkPad-T440s: ~

File Edit View Terminal Tabs Help

```
bob@bob-ThinkPad-T440s:~$ magma
Magma V2.24-2     Thu Dec  6 2018 19:54:57 on bob-ThinkPad-T440s [Seed =
796571549]

+-------------------------------------------------------------------+
|       This copy of Magma has been made available through a        |
|                   generous initiative of the                      |
|                                                                   |
|                         Simons Foundation                         |
|                                                                   |
| covering U.S. Colleges, Universities, Nonprofit Research entities,|
|               and their students, faculty, and staff              |
+-------------------------------------------------------------------+

Type ? for help.  Type <Ctrl>-D to quit.
>
```