Fractal Groups

Monday, October 4, 2021 5:12 PM

the Burnside Problem

Let G be a group such that every element of G has finite order. is G finite?

pause for suggestions......

$\mathbb{Q}/\mathbb{Z}$ ✓

$G = \bigoplus_{n \in \mathbb{N}} C_p$ is an easy counterexample

What if G is finitely generated?

Ways of building torsion groups:

ugly
- Combinatorial group theory
  - Golod-Shafarevich groups 1964
  - free burnside groups 1968 - present
  - Tarski monsters 1980

pretty
- Fractal Groups
  - Grigorchuck group 1980
  - Gupta-Sidki group 1983
  - Generalizations .....

$\langle x, y \mid \cdots \rangle$

$\langle x_1, \dots x_d \mid r_1, \dots r_r \rangle$ if finite, $r \geq \frac{d^2}{4}$

group theory advice: people with G last names and S last names make good co-authors.

a, $b = (a, a^{-1}, 1, 1, \dots, b)$

Fractal Groups:

Intuition: a group is fractal if G "looks like" $G \times G$ (or G^n)

What do groups look like? - Geometric Group Theory

G "looks like" it's cayley graph

Cayley graphs for $\mathbb{Z}$

$\mathbb{Z} = \langle 1 \rangle$

$\mathbb{Z} = \langle 2, 3 \rangle$

these better look the same ...

$D_\infty = \langle x, y \mid yxy = x^{-1} \rangle = \mathbb{Z} \rtimes C_2$

we should have D_∞ "looks like" $\mathbb{Z}$

def: we say G and H are commensurable (look the same)
if there are subgroups $K \le G$, $K' \le H$ so:

- $K \cong K'$
- $[G:K]$ is finite
- $[H:K']$ is finite

Examples:

- $\mathbb{Z}$ and D_∞ are commensurable

  $\mathbb{Z} \cong \langle x \rangle \le D_\infty$, and $[D_\infty : \langle x \rangle] = 2$

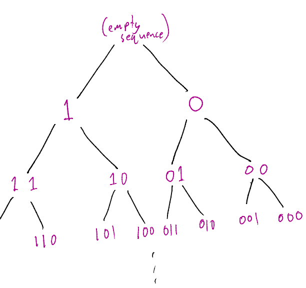
- all finite groups are commensurable

- (non-trivial) $SL_2(\mathbb{Z})$ and the free group $\langle a, b \rangle$ are commensurable

Key example!

let G be the automorphism group of a complete binary tree:

T:



$T = 2^{<\omega}$ is the set of finite sequences of 0's and 1's

for $r, s \in T$, we say $r \prec s$ if r is an initial segment of s
(so $10 \prec 1001$)

G is the set of $\prec$-preserving functions from T to T

thm: G and $G \times G$ are commensurable

notation: for $v \in T$, let $T_v = \{x \in T \mid v \prec x\}$, the set of vertices below T

for $n \in \mathbb{N}$, let $T_n = \{v \in T \mid |v| = n\}$, the n^{th} level of T

pf: let $H = St(T_1)$ be the pointwise stabilizer

$[G:H] < \infty$

why?

index is 2 since acts on T_1

$H \cong G \times G$

why?

picture ✓

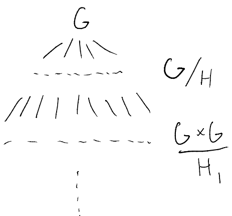
So G and $G \times G$ are commensurable $\square$

the remainder of this talk will only examine automorphisms of trees.

here's why you should be okay with that:

Very sketchy lemma: every fractal group is a subgroup of $Aut(T)$ for a tree T

very sketchy proof: Suppose G and $G \times G$ are commensurable (G^n works similarly)



let $H_0 \leq G$, $G \times G$ with finite index in each

$H_1 = H_0 \cap (H_0 \times H_0)$ has finite index in $G \times G$

$H_2 = H_1 \cap (H_1 \times H_1)$ has finite index in G^4

build a tree where $T_n = G^{2^n} / H_n$

G acts on this tree

$\square$ ← good enough

remark: if $G < Aut(T)$ and $v \in T$, then $St_G(v) \curvearrowright T_v$

if T is a regular tree, $T_v \cong T$, so we have a map $\varphi_v : St_G(v) \to Aut(T)$

def: $G \leq Aut(T)$ is (weakly) self-replicating if, for every vertex v, $im(\varphi_v) \leq G$.

if G is self-replicating and $T = 2^{<\omega}$, for $x \in St_G(T_1)$, we will write

$x = (y, z)$ or $x = \overset{\wedge}{y\ \ z}$

where $y = \varphi_1(x)$ and $z = \varphi_0(x)$

The Grigorchuck Group

this is the first interesting example of a fractal group

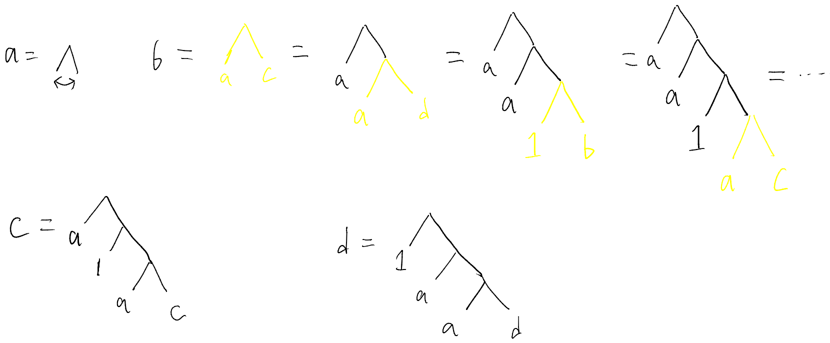
$G \leq Aut(2^{<\omega})$, and is generated by the following 4 elements

a swaps the first level and moves nothing else

b, c, d stabilize the first level, and are defined inductively by:

$b = (a, c)$ $\quad$ $c = (a, d)$ $\quad$ $d = (1, b)$

in pictures:

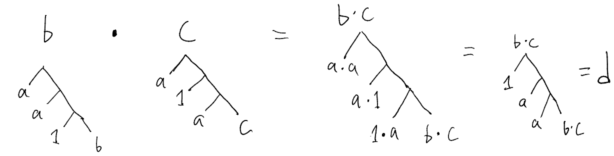


Some relations:

$a^2 = 1$

$b^2 = c^2 = d^2 = 1$

$bc = d$ $\longrightarrow$



Cor: G is a quotient of $\langle a\rangle * \langle b,c,d\rangle = C_2 * (C_2 \times C_2)$

def: a word in G is <u>reduced</u> if it is reduced as an element of $C_2 * (C_2 \times C_2)$

i.e. it has the form

$$(a) \bullet a \bullet a \bullet a \bullet \cdots\cdots \bullet (a)$$

where each $\bullet$ is either b, c, or d

Thm: G is infinite

pf: let $H = St_G(T_1)$. $\longrightarrow \langle b, c, d, b^a, c^a, d^a \rangle$

Clearly $[G:H] = 2$.

also, $H \leq G \times G$ as G is self-replicating — It is true, but not yet clear, it has finite index

let $\pi_1 : H \to G$ be the projection onto the first component

lemma: π_1 is surjective

pf: let w be a word in G, ex: $w = abac$

rewrite each letter as follows

$a \to b$

$b \to ada$

$c \to aba$

$d \to aca$

w becomes

$b(ada)b(aba)$

$= (a,b)(b,1)(a,b)(c,a)$

$= (\underbrace{abac}_{w}, b1ba)$

this always has even # of a's, so it's in H and the first component will be w $\square$

So, if $|G| < \infty$, we'd have $|G| < |H|$ since $H \twoheadrightarrow G$

but $[G;H] = 2$, so $|H| < |G|$ $\Rightarrow\Leftarrow$

So G is infinite $\square$

Thm: Every element of G has finite order (moreover, G is a 2-group)

pf: we will show by induction on n that every reduced word w of length n has order some power of 2.

base cases:

$n=1$: $w = a, b, c,$ or d ✓

$n=2$:

- $a \cdot d$ has order 4

$$(ad)^2 = (ada)d = (b \quad 1) \cdot (1 \quad b)$$

$$= (b, b) \leftarrow \text{Clearly has order } 2$$

$da = a(ad)a^{-1}$, so it also has order 4

- $a \cdot c$ has order 8

$$(ac)^2 = (aca)c = (d, a)(a, d) = (da, ad)$$

$\nwarrow$ order 4

So does ca.

- $(ab)^2 = (aba)b = (ca, ac)$

So ab and ba have order 16

$n=3$: a reduced word of length 3 is like one of the following:

$aba \leftarrow$ conjugate to b

$bab \leftarrow$ conjugate to a

$bad \leftarrow$ conjugate to ac

$$b(bad)b = (bb)a(db) = ac$$

general case:

- if n is odd, ≥ 3

w is conjugate to a word of length $n-1$ or $n-2$

- $w = a \begin{smallmatrix} b \\ c \\ d \end{smallmatrix} \cdots \begin{smallmatrix} b \\ c \\ d \end{smallmatrix} a$ — conjugate by a
- $w = ba \cdots ab$
- $w = ba \cdots ad$

conjugate by b

• $w = b\,a \cdots a\,b$

• $w = b\,a \cdots a\,d$

conjugate by b

induction ✓

• if n is even:

$w = a \substack{b\\c\\d}\, a \substack{b\\c\\d} \cdots a \substack{b\\c\\d}$ or $\cancel{w = \substack{b\\c\\d}\, a \substack{b\\c\\d}\, a \cdots \substack{b\\c\\d}\, a}$

conjugate by a

now we have 2 cases:

$\frac{n}{2}$ is even:

$$w = a \substack{b\\c\\d}\, a \substack{b\\c\\d}\, a \substack{b\\c\\d}\, a \substack{b\\c\\d} \cdots a \substack{b\\c\\d}\, a \substack{b\\c\\d}$$

$$\left(a \substack{b\\c\\d}\, a\right) \substack{b\\c\\d} \left(a \substack{b\\c\\d}\, a\right) \substack{b\\c\\d} \cdots \left(a \substack{b\\c\\d}\, a\right) \substack{b\\c\\d}$$

each of these stabilizes level 1, so we rewrite them

$$\underbrace{\left(\substack{b\\c\\d}, \substack{a\\1}\right) \cdot \left(\substack{a\\1}, \substack{b\\c\\d}\right) \cdot \left(\substack{b\\c\\d}, \substack{a\\1}\right) \cdots \left(\substack{a\\1}, \substack{b\\c\\d}\right)}_{\frac{n}{2} \text{ terms}}$$

$$= \Big(\underbrace{\substack{b\\c\\d} \cdot \substack{a\\1} \cdot \substack{b\\c\\d} \cdots \substack{a\\1}}_{\text{length } \frac{n}{2}} ,\ \underbrace{\substack{a\\1} \cdot \substack{b\\c\\d} \cdot \substack{a\\1} \cdots \substack{b\\c\\d}}_{\text{length } \frac{n}{2}} \Big)$$

after reductions, these both correspond to words of length $\leq \frac{n}{2}$

by induction, both parts have finite order, hence so does w

$\frac{n}{2}$ is odd:

let $k = \frac{n}{2}$

$w = a\,u_1\,a\,u_2 \cdots a\,u_k$

$w^2 = a\,u_1\,a\,u_2 \cdots a\,u_k\,a\,u_1\,a\,u_2\,a \cdots u_k$

$(a\,u_1\,a)\,u_2 \cdots (a\,u_k\,a)\,u_1\,(a\,u_2\,a) \cdots u_k$

....same argument as above....

$= (w_1, w_0)$ both length $\leq n$

● suppose some $u_m = d$

$w^2 = a\,u_1\,a\,u_2\,a \cdots a\,u_m\,a \cdots a\,u_k\,a\,u_1\,a \cdots a\,u_m\,a \cdots a\,u_k$

$$= (a\,u_1\,a)\,u_2\,(a \cdots a)\,\underset{(1,\,b)}{\underset{\parallel}{u_m}}\,(a \cdots)(a\,u_k\,a)\,u_1\,(a \cdots)\underset{(b,\,1)}{\underset{\parallel}{(a\,u_m\,a)}}(\cdots a)\,u_k$$

because of this 1, length$(w_1) \leq n-2$ after reducing

because of this 1, length$(w_0) \leq n-2$ after reducing

this !, length $(w_1) \leq n-2$ after reducing

because of this !, length $(w_0) \leq n-2$ after reducing

So, w_1 and w_0 have finite order by induction, so w^2 must also (and therefore w)

- Suppose no u_m is d, but some u_m is c:

$$w^2 = (a\, u_1\, a) u_2 (a \cdots a) \underset{(a,\, d)}{\underset{\parallel}{u_m}} (a \cdots)(a\, u_k\, a) u_1 (a \cdots)(a\, \underset{(d,\, a)}{\underset{\parallel}{u_m}}\, a)(\cdots a) u_k$$

both w_1 and w_0 are already reduced words with length n

however, these two d's ensure both w_1 and w_0 have a d in them

So, by the green case, w_1 and w_0 have finite order, so w^2 does too

- Suppose no u_m is d or c:

$w = a\, b\, a\, b \cdots a\, b$

so $w \in \langle a, b \rangle$, which is a finite group (D_8 or D_{16} depending on convention)

hence w has finite order

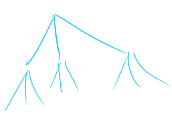
$\square$

Thm: G is a fractal group, commensurable with $G \times G$

proof omitted for time constraints

Generalizations

Can we build an infinite 3 group like this?



pause for ideas!!!

here's one:

$G < \mathrm{Aut}(3^{<\omega})$ is generated by:

- a, a^2 cyclically permute the first level $a =$  $a^2 =$ 

  a-type generators

- b, c, d, e, f, g, h, i stabilize the first level and are defined recursively by

  b-type generators

  $b = (1, a, c)$
  $c = (1, a^2, d)$
  $d = (1, a^2, e)$
  $e = (1, 1, f)$

$b = (1, a, c)$
$c = (1, a^2, d)$
$d = (1, a^2, e)$
$e = (1, 1, f)$
$f = (1, a^2, g)$
$g = (1, a, h)$
$h = (1, a, i)$
$i = (1, 1, b)$

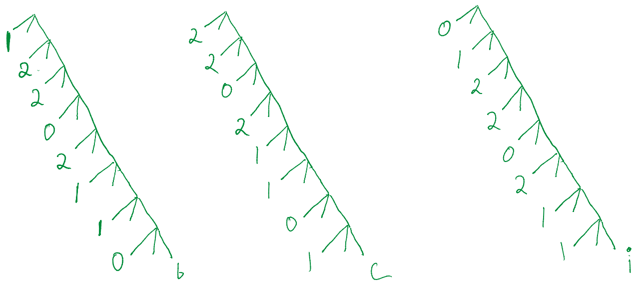
b-type generators

properties of this group:

- a-type generators form a finite subgroup A
- b-type generators form a finite subgroup $\mathcal{B}$

  this isn't obvious at all, but I'll show one example

$$b \cdot c = i$$



- G is self-replicating (and fractal)
- G is infinite for the same reason as above
- If you rewrite a letter, it takes at most 4 times to get a 0.

so we can recreate the proofs above to show G is a 3-group

caviats: when $a^{-1} \neq a$, rewriting looks a bit different:

$$\begin{aligned}
& a\,b\,a\,e\,a^2\,h\,a^2\,b \\
= \; & a\,b\,a^{-1}a\,a\,e\,a^2\,h\,a^2\,b \\
= \; & (a\,b\,a^{-1})\,a^2\,e\,a^2\,h\,a^2\,b \\
= \; & (a\,b\,a^{-1})(a^2\,e\,a^{-2})\,a^2 a^2\,h\,a^2\,b \\
\cdots = \; & (a\,b\,a^{-1})(a^2\,e\,a^{-2})(a\,h\,a^{-1})(b)
\end{aligned}$$

general observations:

① A seems to be the additive group of a finite field $\mathbb{F}$

② B seems to be a subspace of the vector space $\mathbb{F}^n$

③ if $(a_1, a_2, \ldots a_n) \in B$, so is $(a_2, \ldots a_n, a_1)$

④ every element of B has a 0 in it somewhere

Coding Theory:

def: A $[n, k]$ linear code over a finite field $\mathbb{F}$ is a k dimensional subspace of $\mathbb{F}^n$

example: $\{000, 110, \ldots\}$ is a $[3, 2]$ code over $\mathbb{F}_2$

example: $\left\{\begin{matrix} 0\,0\,0, \\ 1\,1\,0, \\ 1\,0\,1, \\ 0\,1\,1, \end{matrix}\right\}$ is a $[3,2]$ code over $\mathbb{F}_2$

Why is this called a code?

WARNING: the following example has useful applications

Suppose Alice wants to send Bob a message

the message is 4 bits long, but Alice can send 7 bits.

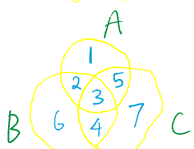
Eve can chose to flip 1 bit before Bob gets the message

Can Alice ensure Bob gets the right message?

stage direction:

Change to new page for this

Why is this a linear code?



Valid codewords satisfy:

A: $1+2+3++5 = 0$

B: $2+3+4++6 = 0$

C: $3+4+5++7 = 0$

$$\text{codewords} = \ker\left(\begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}\right)$$

why does it correct errors?

every non-0 codeword has at least 3 1's in it

thus, any 2 messages differ in at least 3 positions

so, if only 1 bit is flipped, the closest codeword will be right

What about condition 3 we wanted?

def: a Cyclic code is a linear code such that

if $\overline{a} = (a_1, a_2, a_3, \dots, a_n)$ is a codeword, so is

$\overline{a}^{\circlearrowleft} = (a_2, a_3, \dots, , {}_n, {}_1)$

Convention: we identify a codeword $\overline{a}$

with the polynomial $a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_n x^0$

$$\overline{a}^{\circlearrowleft} = a_2 x^{n-1} + \dots + a_n x^1 + a_1$$

$x \cdot \bar{a} = a_1 x^n + a_2 x^{n-1} + \cdots + a_n x^1$

$x\bar{a} - \bar{a} = a_1 (x^n - 1) \equiv 0 \mod x^n - 1$

def 2: a length n cyclic code over $\mathbb{F}$ is an ideal in $\mathbb{F}[x]/(x^n-1)$

ideal = closed under $\underbrace{\text{addition, multiplication by } \mathbb{F},}_{\text{linear subspace}}$ and $\underbrace{\text{multiplication by } x}_{\text{cyclic shifts}}$

how do I find cyclic codes?

Ideals in $\mathbb{F}[x]/(x^n-1)$ $\longleftrightarrow$ Ideals in $\mathbb{F}[x]$ containing (x^n-1)

$\longleftrightarrow$ $\underbrace{\text{Polynomials in } \mathbb{F}[x] \text{ dividing } x^n - 1}$

Tell computer "factor x^n-1 mod p"

Computer gives answers

example: find all length 3 cyclic codes over $\mathbb{F}_2$

x^3+1 factors as $(x+1)(x^2+x+1)$

Codes:

called "generator polynomial"

1 – everything is a codeword

$(x+1)$ – codewords are: $\{0 \quad x+1 \quad x^2+x \quad x^3+x^2 = x^2+1\}$

$\{000, 011, 110, 101\}$

(x^2+x+1) – codewords are: $\{0, \quad x^2+x+1\}$

$\{000, \quad 111\}$

(x^3+1) – only 0 is a codeword

more examples:

- the useful example has generator polynomial x^3+x^2+1 which divides x^7-1 over $\mathbb{F}_2$
- the code for the 3-group I conjured out of nowhere corresponds to $x^6+2x^5+2x^4+0x^3+2x^2+1x+1$ which divides x^8-1 over $\mathbb{F}_3$

What about condition 4 (every element has a 0)?

for the good field $\mathbb{F}_2$:

the only codeword without 0 is $111\cdots1$

so, we need generator polynomials $g(x)$ such that:

$g(x) \mid x^n - 1$

$g(x) \nmid x^{n-1} + x^{n-2} + \cdots + x^0 = \frac{x^n-1}{x-1}$

any combination of factors of x^n-1 including $x-1$ generates an suitable code, which we can make into a torsion group

for bad fields with more than 2 elements:

this condition is hard to check

fortunately, there are always examples

Thm: Cyclic hamming codes always exist over $\mathbb{F}_q$

pf: take a primative element of $\mathbb{F}_{q^m}$, β.

define $C = \{ p \in \mathbb{F}_q[x] \mid f(\beta) = 0 \}$

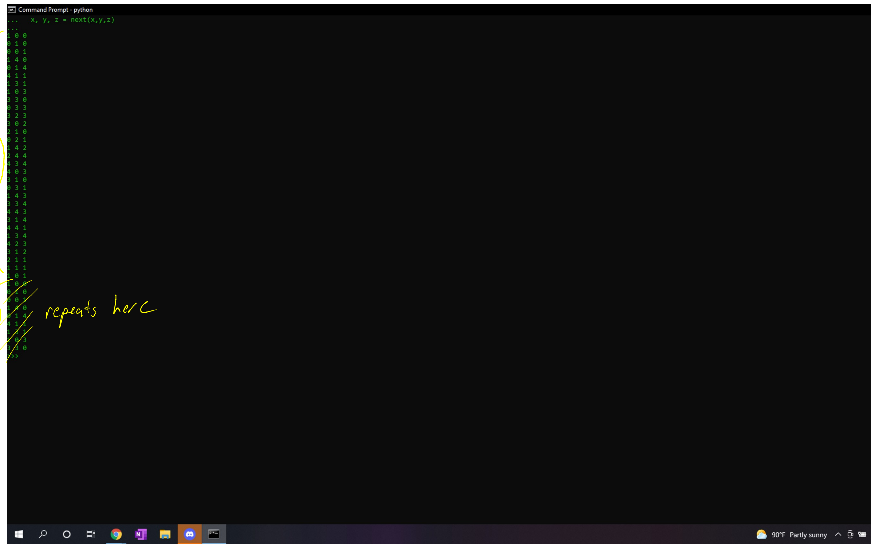
C will be a hamming code. ← as I haven't defined these, this is vacuously true. $\square$

Thm: The dual of any cyclic hamming code satisfies (4)

pf: by intimidation, this is true $\square$

Example: Here is a minimal cyclic code over $\mathbb{F}_5$ satisfying (4).

It is a $[31, 3]$ code with these collumns as generators

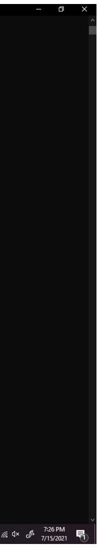


repeats here

there are also examples that do not arise this way,

the smallest is a $[7, 3]$-code over $\mathbb{F}_4$ w/ generator

0 0 1 1 1 0 1


7:26 PM
7/15/2021