① Lecture 4 Burnside's problem

I A The General Burnside problem states as follows:

Pb1 Let G be a group generated by finitely many elements such that ~~the~~ each $x \in G$ has finite order i.e. $\exists$ some n (depending) on x s.t. $x^n = 1$. Is then G a finite group?

Such groups are called periodic or torsion groups. The orders $n(x)$ of elements $x \in G$ are not assumed to be bounded here. A particular case is of interest, namely when all order n are of the form p^k for some prime p (groups are then called (periodic) p-groups). The original problem of Burnside was the case when all orders are bounded i.e.

Pb2 Is the group $\underbrace{\text{generated}}_{B(m,n)}$ by m generators $a_1, \dots a_m$ and relations

$$x^n = 1 \quad , \text{for } \underline{\text{all}} \text{ words } x \text{ in } a_1, \dots a_m$$

finite and if yes what is its order?

The groups $B(m,n)$ are free Burnside group of ~~order~~ exponent n.

I B Elementary results

Proposition 1: $B(m,2)$ is finite.

Proof The group is commutative since $x^2 = 1 \Rightarrow x = x^{-1}$ and so

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

Thus $B(m,2)$ has 2^m elements. $\square$

Theorem (Burnside 1902) $B(m,3)$ is finite.

Proof Induction on m. If $m=1$ then $B(1,3) = \mathbb{Z}/3\mathbb{Z}$.

Suppose $B(m,3)$ finite of order N. We obtain $B(m+1,3)$ by adding one more generator g and relations $x^3 = 1$ involving g.

Thus any $x \in B(m+1,3)$ can be expressed as

$$(*) \qquad x = u_1 g^{\pm 1} u_2 g^{\pm 1} \dots u_{k-1} g^{\pm 1} u_k \quad , \quad u_i \in B(m,3).$$

Lemma We can find an expression of form $(*)$ for x with $k \leq 3$.

Proof of lemma: We have the relations

$$g u_i g = u_i^{-1} g^{-1} u_i^{-1} \qquad g^{-1} u_i g^{-1} = u_i^{-1} g u_i^{-1}$$

and thus we can modify (*) so that the exponents of g alternate. Further assume that we have a word with 3 appearance of g in alternate form

$$u_1 g u_2 g^{-1} u_3 g = u_1 g u_2 g^2 u_3 g = u_1 (g u_2 g)(g u_3 g) =$$
$$= u_1 (u_2^{-1} g^{-1} u_2^{-1})(u_3^{-1} g^{-1} u_3^{-1}) = u_1 u_2^{-1} g^{-1} u_2^{-1} u_3^{-1} g^{-1} u_3^{-1}$$

Thus any such words reduces to a word with only two g's. By induction on h we can reduce (*) to a word with $k \leq 3$ $\square$

Thus the number of elements of $B(n+1, 3)$ is at most

$$N + 2N^2 + 2N^3 < \infty \quad \square$$

Rk: Levi, van der Waerden ont trouvé $|B(m,3)| = 3^{m + \binom{m}{2} + \binom{m}{3}}$.

I C Exponent 4.

Theorem (Sanov) $B(m,4)$ is finite.

Proof Start with the following lemma

Lemma: Let H, G be periodic groups satisfying $x^4 = 1$ $\forall x$. Suppose

$$G = \langle H, d; \text{ such that } d^2 \in H \rangle$$

If H is finite then G is finite.

Pf of lemma: Every element x of G has the form

(*) $\quad x = h_1 d h_2 d \ldots h_{k-1} d h_k$

Since $(dh)^4 = 1$ we get

(**) $\quad dhd = h^{-1} d^{-1} h^{-1} d^{-1} h^{-1} = h^{-1} d (d^2 h^{-1} d^2) d h^{-1} = h^{-1} d h' d h^{-1}$ where

$$h' = d^2 h^{-1} d^2 \in H$$

Using (**) we

$$h_1 d h_2 \underline{d h_3 d} = h_1 d (h_2 h_3^{-1}) d h_3' d h_3^{-1}$$

so that the first term between d's, namely h_2 was replaced by $h_2 h_3^{-1}$. But we could also replace first h_3 by $h_3 h_4^{-1}$ and further h_2 by $h_2 h_4 h_3^{-1}$. By induction we can replace in (*) h_2 by any of the following

$$\mathcal{S} = \{ h_2 h_3^{-1}, \; h_2 h_4 h_3^{-1}, \; h_2 h_4 h_5^{-1} h_3^{-1}, \ldots$$
$$h_2 h_4 \ldots h_{2s} h_{2s+1}^{-1} h_{2s-1}^{-1} \ldots h_3^{-1}, \ldots \}$$

If the group H is finite, then for s large enough the

(3) elements of $\mathcal{S}$ cannot be distinct so that $\exists\, s, r$ for which

$$h_2 h_4 \cdots h_{2r} h_{2r+1}^{-1} \cdots h_3^{-1} = h_2 h_4 \cdots h_{2s} h_{2s+1}^{-1} \cdots h_3^{-1}$$

If say $r<s$ this implies that

$$(***) \quad h_{2r+2} \cdots h_{2s} h_{2s+1}^{-1} \cdots h_{2r+3}^{-1} = 1 \quad \text{holds in } H.$$

Further using again $(**)$ we can replace the occurrence of h_{2r} in $(*)$ by

$$h_{2r+2} \cdots h_{2s} h_{2s+1}^{-1} \cdots h_{2r+3}^{-1}$$

Thus we have

$$(****)\ x = h_1 d h_2 d \cdots d h_{2r+1} d\, h_{2r+2}\, d h_{2r+3} d \cdots d h_k =$$

$$= h_1 d h_2 d \cdots d \left(h_{2r+2} h_{2r+4} \cdots h_{2s} h_{2s+1}^{-1} \cdots h_{2r+3}^{-1} \right) d\, h'_{2r+3} d \cdots d h_k =$$

$$= h_1 d h_2 d \cdots d \quad h_{2r+1} \, d^2 h'_{2r+3} \, d\, h'_{2r+4} d \cdots d h_k$$

by $(***)$

However $h_{2r+1} d^2 h'_{2r+3} \in H$ and thus relation $(****)$ shows that we can reduce the number of occurences of d to finitely many $\square$

Now we proceed by induction on m. $B(1,4) = \mathbb{Z}/4\mathbb{Z}$ is finite. Next $B(m,4)$ supposed finite then $B(m+1,4)$ is obtained by adjoining generator b with $b^4 = 1$. Let $G < B(m+1,4)$ be the subgroup generated by $B(m,4)$ and $d = b^2$.

Then $d^2 = b^4 = 1$ hence $d^2 \in B(m,4)$ and lemma implies G finite. Further $B(m+1,4)$ is obtained from G by adjoining b with $b^2 = d \in G$; again lemma shows $B(m+1,4)$ is finite. $\square$

Remark 1) M. Hall proved that $B(m,6)$ is finite too.

2) Still unknown whether $B(2,5)$ is finite...

I) Adyan-Novikov result

Theorem (Adyan-Novikov 1968) The group $B(m,n)$ is infinite for $m > 1$ and odd $n \geq 665$. Their abelian subgroups are finite (Tarski monster). Ivanov-Lysenok improved for all even $n > 2^{13}$.

II Construction of p-groups

Theorem (Golod-Shafarevich 1965) For each prime $p \geq 2$ there is a finitely generated p-group which is infinite.

Further examples by Aliochin, Suschanski, Grigorchuk, Gupta-Sidki etc.

By a theorem of Kaloujnine any finitely generated residually finite p-group can be embedded in the automorphism group of a regular tree.

II A Grigorchuk construction

Let $\mathbb{D} \subset (0,1)$ denote the set of dyadic numbers i.e. $\{ \frac{p}{2^q},\ p, q \in \mathbb{Z}_+ \} \cap (0,1)$.

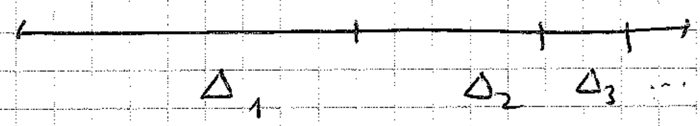
We consider transformations of $E = (0,1) - D$ in itself.

Set $\Pi(x) : E \to E$ the map piecewise linear permuting the two halves of $(0,1)$

$$\Pi(x) = \begin{cases} x + 1/2, & 0 < x < 1/2 \\ x - 1/2, & 1/2 < x < 1 \end{cases}$$

Let also T denote the identity map $T : E \to E$.

Divide $(0,1)$ into two equal parts, the left part denoted Δ_1; divide the right halve into two parts, the left half of which is denoted Δ_2 and so on.



Thus E is partitioned in $\coprod \Delta_i$, where the length of $\Delta_i = \frac{1}{2^i}$.

Each infinite sequence $Z_1 Z_2 \ldots Z_p \ldots$, $Z_i \in \{\Pi, T\}$ defines a map $E \to E$ that acts on the interval Δ_j like the element $Z_j \in \{\Pi, T\}$ i.e.

$$\begin{cases} \text{- if } Z_j = \Pi \text{ then it exchanges the two halves of } \Delta_j \\ \text{- if } Z_j = T \text{ then it is identity on } \Delta_j. \end{cases}$$

Consider next the group G be the group of transformations $E \to E$ generated by

(5) a = interchange of the two halves of $(0,1)$

b = $\Pi\Pi T\ \Pi\Pi T\ \Pi\Pi T$ ... periodic sequence

c = $\Pi T \Pi\ \Pi T \Pi\ \Pi T \Pi$ periodic sequence.

Theorem (Grigorchuk 1980) The group G (Grigorchuk group) is an infinite 2-group with 3 generators.

Proof. We show first that G is infinite. Consider $d = bc$.

~~Proposition~~ Then d = $T\Pi\Pi\ T\Pi\Pi\ T\Pi\Pi$ ... (periodic sequence).

We verify immediately that

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

$$bc = cb = d \quad , \quad cd = dc = b$$

$$bd = db = c$$

Therefore any element of G can be written as

(1) $\quad w = h_0 a h_1 \cancel{a} h_2 \dots h_{k-1} a h_k$

(where h_0, h_k might be 1) and $h_i \in \{b, c, d\}$.

Define $H \subset G$ be the subgroup of those elements $w \in G$ which admit an expression (1) with an even occurences of a.

Lemma $H \triangleleft G$ is a normal subgroup of G and H is generated by

$$b, c, d, \ aba, \ aca, \ ada$$

Pf of lemma: Clear. $\square$

Each element of H acts on E and preserves the partition of $(0,1)$ into two ~~E~~ intervals Δ_1 and $(0,1) - \Delta_1$.

Let then $\varphi_1(x)$ be the restriction of $x|_{\Delta_1}$ and

$\varphi_2(x)$ the restriction of $x|_{(0,1) - \Delta_1}$.

Denote also by a_1, b_1, c_1, d_1 the analogues of a, b, c, d for the interval $(0, \frac{1}{2})$ and a_2, b_2, c_2, d_2 the analogues for the other falbe $(\frac{1}{2}, 1)$.

By direct inspection we find $\varphi_1(x), \varphi_2(x)$ as follows:

$$(2)\begin{cases} x & b & c & d & aba & aca & ada \\ \varphi_1(x) & a_1 & a_1 & 1 & c_1 & d_1 & b_1 \\ \varphi_2(x) & c_2 & d_2 & b_2 & a_2 & a_2 & 1 \end{cases}$$

Furthermore the map $\varphi: H \longrightarrow G_1 \times G_2$, $\varphi(x) = (\varphi_1(x), \varphi_2(x))$ is a group homomorphism, where G_1, G_2 are copies of G acting on $[0,1/2)$ and $(1/2, 1)$ respectively. Remark that φ is injective.

Lemma G is infinite.

Proof: $\varphi(H) \subset G_1 \times G_2$ and the projection $p_1(\varphi(H))$ of $\varphi(H)$ onto the first factor is surjective because all generators a_1, b_1, c_1, d_1 belong.

Thus $\operatorname{card}(H) \geq \operatorname{card} \varphi(H) \geq \operatorname{card}(p_1\varphi(H)) \geq \operatorname{card}(G)$.

But H is a proper subgroup of G ($a \notin H$) and thus $\operatorname{card}(H) = \operatorname{card} G = \infty$ $\square$

The next step is to prove that every element $w \in G$ is of order 2^m for some m, by induction on the length $|w|$ of w, in the expression (1). This is clear if $w \in \{a, b, c, d\}$.

Let now $|w| = r$ and suppose that for each word y with $|y| < r$ ~~and~~ we have $y^{2^{m(y)}} = 1$. Possibly replacing w by a conjugate we can assume that $w = a h_1 a h_2 \dots a h_k$, $|w| = 2k = r$.

Case (i) k is even. Then $w \in H$. It is clear from (2) that.

$$|\varphi_1(a h_1 a h_2)| \leq 2 \quad , \quad |\varphi_2(a h_1 a h_2)| \leq 2$$

Therefore $|\varphi_j(w)| \leq k < r$, $j = 1,2$. By the induction hypothesis $\varphi_j(w)$ are of order $2^{m_j(w)} \Rightarrow (\varphi_1(w), \varphi_2(w)) \in G \times G$ is of order 2^m ~~and~~ $\Rightarrow \varphi$ injective $\Rightarrow$ w is of order 2^m.

Case (ii) k is odd. Let then consider

$$w^2 = a h_1 a h_2 \dots a h_k a h_1 \dots a h_k$$

and then $w^2 \in H$. We have $|w|^2 = 2r$ and using (2) we have $|\varphi_i(w^2)| \leq 2k = r$, $i = 1,2$.

(A) if the letter $d \in \{h_1, \dots, h_k\}$. By passing to a conjugate of x we can assume that $h_1 = d$. From (2) we find that

(7)

$\varphi_2(adah_2) \in \{c_2, d_2, b_2\}$

$\varphi_1(ah_k ad) \in \{c_1, d_1, b_1\}$.

$\Rightarrow$ $|\varphi_j(w^2)| < r$ and we can apply induction hypothesis and (case i)

$\Rightarrow$ w^2 order $2^m \Rightarrow w$ order 2^{m+1}.

(B) $c \in \{h_1, \dots, h_k\}$, and assume $h_1 = c$. Then

$d_1 \in \varphi_1(acah_2)$

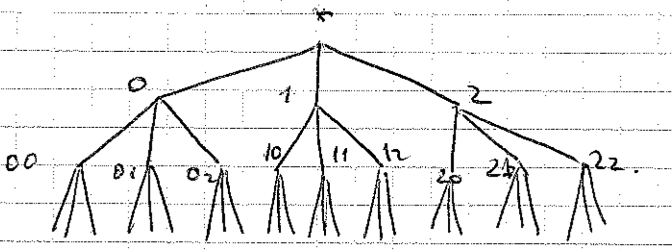
$d_2 \in \varphi_2(ah_k ac)$

$\Rightarrow$ the letter d_i appears in the word $\varphi_i(w^2)$.

Since $|\varphi_i(w^2)| \leq r$ we can use case (ii)(A) to show that $\varphi_i(w^2)$ are of order $2^{m_i} \Rightarrow w^2$ is of order $2^m \Rightarrow w$ is of order 2^{m+1}. $\square$.

II B The Gupta-Sidki construction.

Let T be the infinite ternary tree with a root $*$ with vertices labelled using the triadic expansion; if u is a vertex of T let T_u denote the subtree of T with root u, which is isomorphic to T. If G acts on T let G_u be a copy of G acting on the subtree T_u, and for each $g \in G$ let $g_u \in G_u$ be the corresponding element.



T

Consider the following automorphisms t and a of T

- t cyclically permute the branches 0, 1 and 2, i.e. in terms of labels

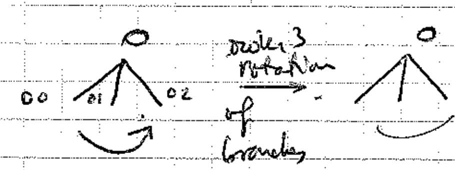
(1) $t(a_1, a_2, a_3, \dots, a_n) = (a_1 + 1 \pmod 3, a_2, a_3, \dots, a_n)$

where $(a_1, a_2, \dots, a_n)$ is the label of the vertex $v \in T$.

- a is defined by the inductive procedure below:

(i) a fixes the vertices 0, 1, 2.

(ii)
- a acts on T_0 as t_0
- a acts on T_1 as t_1^2



- a acts on T_2 as above (a acts on T) namely it fixes 20, 21, 22 and
  - a acts on T_{20} as t_{20}
  - a acts on T_{21} as t_{21}^2
  - a acts on T_{22} following the pattern above i.e. fixes 220, 221, 222 and etc.

There is a closed formula for a; let $(i_1,\dots,i_k)\in T$, $i_1=\dots=i_{u-1}=2$, $i_u\neq 2$; Then

(2) $$a(i_1,\dots,i_k) = (i_1,\dots,i_u,\overline{i_{u+1}},i_{u+2},\dots,i_k)$$

where $$\overline{i_{u+1}} = \begin{cases} i_{u+1}+1 \mod 3 & \text{if } i_u=0\\ i_{u+1}+2 \mod 3 & \text{if } i_u=1\end{cases}$$

It is clear that $t^3=a^3=1$.

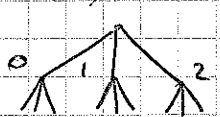
Definition The Gupta-Sidki group $G=G(3)$ is the group of automorphisms of the tree T generated by a and t.

Theorem (Gupta-Sidki) The group $G(3)$ is an infinite 3-group.

Proof Let $\varphi: G(3)\to \mathbb{Z}/3$ be the morphism sending $u\in G_3$ to the cyclic permutation $(0,1,2)\to(u(0),u(1),u(2))$. Consider $H=\ker\varphi$ which is an index 3 subgroup of G.

Lemma H is generated by a, $b=tat^{-1}$ and $c=t^2at^{-2}$.

Pf. of lemma: Observe that the action of a, b, c is as follows:



on (T_0, T_1, T_2)

$$a = (t_0,\ t_1^2,\ a_2)$$
$$b = (a_0,\ t_1,\ t_2^2)$$
$$c = (t_0^2,\ a_1,\ t_2).$$

If $g = a^{i_1}t^{j_1}a^{i_2}t^{j_2}\cdots a^{i_n}t^{j_n}$ then we can rewrite it as:

$$(a^{i_1})(t^{j_1}a^{i_2}t^{-j_1})(t^{j_1+j_2}a^{i_3}t^{-j_1-j_2})(t^{j_1+j_2+j_3}a^{i_4}t^{-j_1-j_2-j_3})\cdots a^{i_n}t^{-j_1-\dots-j_n})t^{\sum j_i} =$$
$$= z\, t^{j_1+\dots+j_n}$$ where $z\in H$ and the claim follows □.

Lemma G_3 is infinite.

Pf. lemma: Let $\varphi_0: H\to G_0$ (= the group G acting on T_0) be $\varphi_0(h)=h|_{T_0}$. We have $\varphi_0(a)=t_0$, $\varphi_0(b)=a_0$, $\varphi_0(c)=t_0^2$ and $G_0\simeq G$ and so φ_0 is surjective. Since $H\triangleleft G$ is of index 3 and surjects onto G $\Rightarrow$ H, G are infinite. □

(9) <u>Remark:</u> Once we choosed t as the simplest automorphism of order 3 the definition of a is natural in order to get a map ψ <u>surjective</u>.

For an element $h \in H$ let $\|h\|$ be the length w.r.t. $\{a, b, c, a^{-1}, b^{-1}, c^{-1}\}$

As $a^2 = a^{-1}$, $b^2 = b^{-1}$, $c^2 = c^{-1}$ this is the same as the syllable length of h.

For $g \in G$ we write $g = h t^{\varepsilon}$ and set $(\varepsilon \in \{0,1,2\})$

$$|g| = \begin{cases} \|h\| & , \text{if } \varepsilon = 0 \\ \|h\|+1 & \text{if } \varepsilon \neq 0 \end{cases}$$

Proposition G is a 3-group.

Proof of proposition: Use induction on the length. If $|g| = 1$ then $g \in \{a^{\varepsilon}, b^{\varepsilon}, c^{\varepsilon}, \varepsilon \in \{\pm 1\}\}$ or $g = t^{\varepsilon}$. We have $g^3 = 1$.

Assume that if $|g| \leq n$ then $g^{3^n} = 1$ and let $g \in G$ with $|g| = n+1 \geq 2$.

(Case 1) $g \in H$. We analyse $\Psi : H \to G \times G \times G$, $\Psi(h) = (h|_{T_0}, h|_{T_1}, h|_{T_2})$

$\Psi = (\psi_0(h), \psi_1(h), \psi_2(h))$. We claim that

$\psi_j(h)$ have order 3^{m+1}, and as Ψ is (obviously) injective

$\Rightarrow$ g is of order 3^{m+1}. Consider ψ_0.

Write $g = w(a,b,c) = a^{i_1} b^{j_1} c^{k_1} a^{i_2} b^{j_2} c^{k_2} \ldots$

and then

$$\psi_0(g) = w(\psi_0(a), \psi_0(b), \psi_0(c)) = w(t_0, a_0, t_0^2) =$$

$$= t_0^{i_1} a_0^{j_1} t_0^{2k_1} t_0^{i_2} a_0^{j_2} t_0^{2k_2} \ldots = z(a_0, b_0, c_0) \text{ where}$$

$b_0 = t_0 a_0 t_0^2$, $c_0 = t_0^2 a_0 t_0$. We can explicitly find a word z as above by writing $w(t_0, a_0, t_0^2)$ as

$$(t_0^{i_1} a_0^{j_1} t_0^{-i_1})(t_0^{i_2+2k_1+i_1} a_0^{j_2} t_0^{-(i_2+2k_1+i_1)}) \ldots \; t_0^{\varepsilon}$$

Each term in parantheses is either $a_0^{j_1}$ or $b_0^{j_1}$ or $c_0^{j_1}$ and thus there are as many syllables in a_0, b_0, c_0 as syllables in b in w. But $w(a,b,c)$ has also syllables in a or c (since $\|w\| \geq 2$) so that, if $\psi_0(g) \in H$ then

$$\|\psi_0(g)\| < \|g\| = n+1$$

and by recurrence hypothesis $\psi_0(g)$ is of order 3^n

Now, if $\psi_0(g) \notin H$ then we will follow case (ii).
(ex. $g = ab$, $\psi_0(g) = t_0 a_0 = b_0 t_0$, $|\psi_0(g)| = 2 = \|g\|$)

(case ii)

Write now $g = h t^{\varepsilon}$, $h = w(a,b,c) \in H$, $\varepsilon \neq 0$.

Consider then $g^3 = h t^{\varepsilon} h t^{-\varepsilon} t^{2\varepsilon} h t^{-2\varepsilon} t^{3\varepsilon} = h(t^{\varepsilon} h t^{-\varepsilon})(t^{2\varepsilon} h t^{-2\varepsilon})$

$$= \begin{cases} w(a,b,c)\, w(b,c,a)\, w(c,a,b) & \text{if } \varepsilon = 1 \\ w(a,b,c)\, w(c,a,b)\, w(b,c,a) & \text{if } \varepsilon = -1 \end{cases}$$

Let us analyze then $\Psi(g^3) = (\psi_0(g^3), \psi_1(g^3), \psi_2(g^3))$

We have then (assume $\varepsilon = 1$ for simplicity)

$$\psi_0(g^3) = w(t_0, a_0, t_0^2)\, w(a_0, t_0^2, t_0)\, w(t_0^2, t_0, a_0) =$$
$$= Z(a_0, b_0, c_0)\, Z(b_0, c_0, a_0)\, Z(c_0, a_0, b_0)$$

since the factors in t cancel at the end. Here Z is the word associated to w by the procedure of case (i). Moreover

$$\|Z(a_0, b_0, c_0)\| \leq \#\text{ syllables in } b \text{ in } W(a,b,c) \Rightarrow$$
$$\|Z(a_0, b_0, c_0)\, Z(b_0, c_0, a_0)\, Z(c_0, a_0, b_0)\| \leq \text{number of syllables in } W(a,b,c)$$
$$= \|W(a,b,c)\| = |g| - 1 = n$$

By the recurrence hypothesis $\psi_0(g^3)$ is of order 3^n (as $\psi_1(g), \psi_2(g)$) and thus g^3 is of order 3^n $\Rightarrow$ g is of order 3^{n+1}. $\square$