

Conference on Combinatorial and Computational Group Theory –
on the occasion of Edmund F. Robertson’s 60th Birthday

Gareth Evans

2 June, 2003

Contents

1	Introduction	2
2	Friday, 30 May 2003	3
2.1	D. L. Johnson (Nottingham): A Prehistory of the Nottingham group	3
2.2	T. C. Hurley (Galway): Free and Basic Commutators	3
2.3	G. Pfeiffer (Galway): Monoids Braids Groups	4
2.4	A. J. Duncan (Newcastle): Quantum Algorithms and Group Theory	6
2.5	W. Nickel (Darmstadt): Schur Covers of Finite Soluble Groups	8
2.6	J. Howie (Heriot-Watt, Edinburgh): One-Relator Products of Cyclic Groups	9
3	Saturday, 31 May 2003	11
3.1	P. M. Neumann (Oxford): On Three-Star Permutation Groups	11
3.2	R. Morse (Evansville): On Computing the Nonabelian Tensor Square of the Free 2-Engel Groups	11
3.3	D. F. Holt (Warwick): The Dehn Function of Nilpotent Groups	11
3.4	R. M. Thomas (Leicester): Unsolved Problems in Automatic Semigroups	12

1 Introduction

This is a collection of notes I took whilst attending the Conference on Combinatorial and Computational Group Theory on the occasion of Edmund F. Robertson's 60th Birthday in St. Andrews between the 30th and the 31st of May, 2003.

2 Friday, 30 May 2003

2.1 D. L. Johnson (Nottingham): A Prehistory of the Nottingham group

Let s_n denote the number of up-down permutations of $1, \dots, n$. *Question:* which elementary function corresponds to the expression

$$\sum_{n \geq 0} \frac{s_n}{n!} t^n?$$

Answer: $\sec(t) + \tan(t)$.

2.2 T. C. Hurley (Galway): Free and Basic Commutators

Let G be a group and consider the lower central series of G . Let $\gamma_1 G = G$ and let $\gamma_{n+1} G = [\gamma_n G, G]$, where $[A, B]$ is the subgroup generated by the commutators $[a, b] = a^{-1}b^{-1}ab$, $a \in A$, $b \in B$. The n -th lower central factor of G is given by $\frac{\gamma_n G}{\gamma_{n+1} G}$. Suppose that G is presented as $G \cong F/R$, where F is free and R is a normal subgroup of F . *Result:*

$$\frac{\gamma_n G}{\gamma_{n+1} G} \cong \frac{\frac{\gamma_n F}{\gamma_{n+1} F}}{\frac{R \cap \gamma_n F}{R \cap \gamma_{n+1} F}}.$$

Proof: by the standard isomorphism theorem. *Note:*

$$\frac{R \cap \gamma_n F}{R \cap \gamma_{n+1} F} \cong \frac{(R \cap \gamma_n F) \gamma_{n+1} F}{\gamma_{n+1} F}.$$

Thus the structure of the lower central factors of G is known once the structure of $\frac{R \cap \gamma_n F}{R \cap \gamma_{n+1} F}$ is known. These factors are considered as the relation parts of the lower central factors of G and are an important consideration.

Now let $\mathbb{Z}[x]$ be the free associative ring on X , let $\mathbb{Z}[[x]]$ be the formal power series on X , and let A_n be the monomials of degree n in $\mathbb{Z}[x]$. The structure of the lower central factors of G is known once the structure of $\frac{R \cap \gamma_n F}{R \cap \gamma_{n+1} F}$ is known.

Theorem 2.1 $\{[x_{i_1}^{\epsilon_{i_1}}, x_{i_2}^{\epsilon_{i_2}}, \dots, x_{i_m}^{\epsilon_{i_m}}]\}$ is equivalent to $\{[x_{i_1}, x_{i_2}, x_{i_3}^{\epsilon_{i_3}}, \dots, x_{i_m}^{\epsilon_{i_m}}]\}$ with plus signs on the first two entries.

Theorem 2.2 There exists a basis $A \cup B$ for $R \cap \gamma_n F$ such that $B * U$ is a free basis for $R \cap \gamma_{n+1} F$ so that $R \cap \gamma_n F := A * B$ and $R \cap \gamma_{n+1} F := B * [\frac{B^+}{A}, A, \dots, A]$.

Suppose that X and Y are subgroups of a free group with $Y \triangleleft X$ such that X/Y is free abelian. Then we have the following theorems:

Theorem 2.3 There exists a basis $A \cup B$ for X such that $B * U$ is a free basis for Y so that $X := A * B$ and $Y := B * [\frac{B^+}{A}, A, A, \dots, A]$.

Theorem 2.4 Every element $w \in R$ can be written uniquely in the form

$$w \equiv r_1^{\alpha_1} r_2^{\alpha_2} \dots r_\ell^{\alpha_\ell} \pmod{R \wedge \gamma_{n+1}F},$$

where the r_i are the R -basic commutators of weight $\leq r$.

2.3 G. Pfeiffer (Galway): Monoids Braids Groups

An action is a monoid concept. Another ‘monoid’ idea: the orbit algorithm (given a monoid $M = \langle A \rangle$ acting on a set X , find the orbit zM of a point $z \in X$).

Given a finite group G , consider the monoid $M = (2^G, \cup)$.

- M is generated by $A = \{a\} : a \in G$.
- M acts on $\mathcal{J}(G) = \{H \in 2^G : H \leq G\}$ via $H.Y = \langle H \cup Y \rangle$ for $H \leq G, Y \leq G$.
- $\mathcal{J}(G) = \{1\}M$ is an orbit.

A Coxeter group U is a group with a presentation given by a graph like

$$s_1 - s_2 - s_3 - \dots - s_{n-1}.$$

For the symmetric group of degree n , we have $s_i = (i, i+1)$ with $s_i^2 = 1$ for all generators s_i ; and for the dihedral group of order $2m$ we have $s_1 \overset{m}{-} s_2$. In general, $s \overset{mst}{-} t$ stands for a relation ($s \neq t$), and we have mst factors on each side of the equation $sts\dots = tst\dots$. Finite Coxeter Groups are direct products of diagrams of this type.

Why are these groups ‘monoids’? Consider the length function (for $w \in W$) $\ell(w) = \min\{k : w = s_1 s_2 \dots s_k, s_i \in S\}$. $s_1 s_2 \dots s_k$ is a reduced word if $\ell(s_1 s_2 \dots s_k) = k$. Prefixes: $u \in W$ is a prefix of $w \in W$: $u \leq w$ if $w = uv$ for some $v \in W$ such that $\ell(w) = \ell(u) + \ell(v)$.

Theorem 2.5 (W, \leq) is a lattice.

Theorem 2.6 (Matsumoto’s Theorem): Given a monoid M and a map $f : S \rightarrow M$ such that $f(s)f(t)\dots = f(t)f(s)\dots$ (mst factors each side), there is a unique map $F : W \rightarrow M$ such that $F(s_1 s_2 \dots s_k) = f(s_1)f(s_2)\dots f(s_k)$ whenever $s_1 s_2 \dots s_k$ is a reduced word.

Example 2.7 If $M = (2^S, \cup)$ and $f(s) = \{s\}$, then $F(w) =$ the set of generators that occur in w does not depend on the choice of the reduced word for w .

The universal monoid satisfying the ‘braid relations’ of (W, S) is the monoid with presentation $B^+(W, S) = \langle S \mid s \dots \overset{(mst)}{\dots} t \rangle$. There exists a map $\tau : W \rightarrow B^+(W, S)$ such that $\tau(uv) = \tau(u) + \tau(v)$ if $u, v \in W$ with $\ell(uv) = \ell(u) + \ell(v)$.

A monoid M is a Garside monoid if

- M has a length function $\ell : M \rightarrow \mathbb{N}_0$, with $\ell(ab) = \ell(a) + \ell(b)$ for all $a, b \in M$;
- M has left and right cancellation: $ab = ac \Rightarrow b = c$; $ba = ca \Rightarrow \dots$;
- (M, \leq) is a lattice;
- There exists a fundamental element $\Delta \in M$ such that $P := \{m \in M : m \leq \Delta\}$ is finite and generates M .

Properties: A Garside monoid M

- Satisfies Ore's condition (left and right cancellation and any $a, b \in M$ have an lcm) and thus embeds into its group of fractions;
- Has a presentation of the form $M = \langle S \mid xf(y, x) = yf(x, y), x, y \in S \rangle$ for a suitable map $f : S \times S \rightarrow S$;
- Is biautomatic.

Reflections:

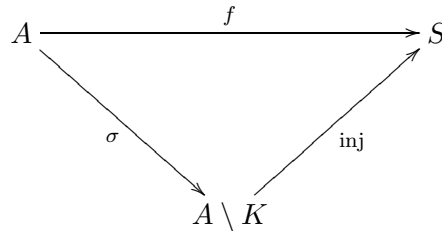
- $T = \{s^w : s \in S, w \in W\}$ is the set of reflections of W .
- Clearly $W = \langle T \rangle$.
- Reflection length $\ell_T(w)$: $\ell_T(w) = n - \dim \ker(\varphi(w) - \text{id})$, with $u \leq_T w \Leftrightarrow \ker(\varphi(u) - \text{id}) \supseteq \ker(\varphi(w) - \text{id})$.
- A Coxeter element of W is a product c of all $s \in S$ with $\ell_T(c) = n$.

Duality:

	$B^+(W, S)$	$B^+(W, T)$
Atoms	S	T
# Atoms	n	N
$\ell(\Delta)$	N	n
Δ	w_0	c
π Atoms	c	w_0
...		

2.4 A. J. Duncan (Newcastle): Quantum Algorithms and Group Theory

Our objective is to find the hidden subgroup $A \setminus K$ in the following diagram, where A is a group and S is a set:



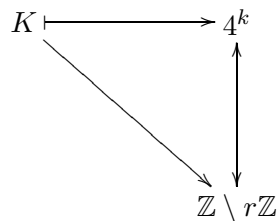
Further, given A , S and f such that some K exists, our next objective is to find K quickly, i.e. in polynomial time. Why? — this process is useful in factoring integers and in the graph isomorphism problem.

Quantum Computer:

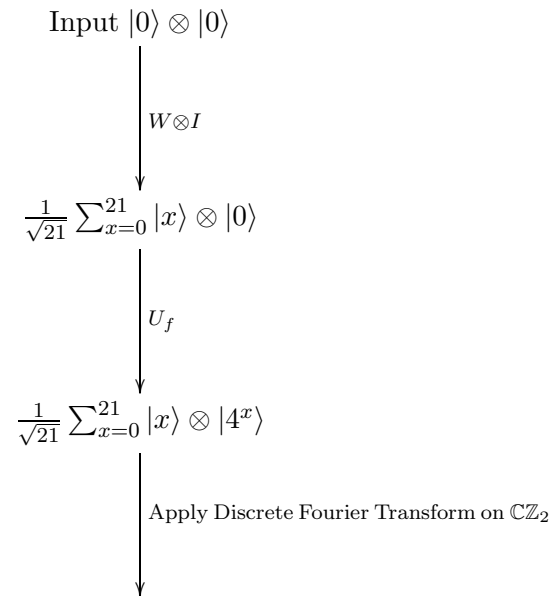
- (1) System: A complex vector space with an n -dimensional orthonormal basis denoted $|0\rangle, \dots, |n-1\rangle$.
- (2) State: A vector $|v\rangle = \sum_{i=0}^{n-1} d_i |i\rangle$ with $\sum |\alpha_i|^2 = 1$.
- (3) Evolution: Unitary transformations U , where $|v\rangle \mapsto U|v\rangle$ is one operation.
- (4) Measurement: Projection onto a basis $|v\rangle \xrightarrow{M} |j\rangle$ with probability $|\alpha_j|^2$.
- (5) Composition: V and W are m and n dimensional systems imply that $V \otimes W$ is an mn -dimensional system (we can measure one or the other or both).

Quantum hunt the subgroup: given $A \xrightarrow{f} S$, does there exist a hidden K ? We have $V_A = \sum_{a \in A} \mathbb{C}|a\rangle$, $V_S = \sum_{s \in S} \mathbb{C}|s\rangle$, $V_A \otimes V_S$, and an unitary U_f such that $V_A \otimes V_S \xrightarrow{U_f} V_A \otimes V_S$, $|a\rangle \otimes |s_0\rangle \mapsto |a\rangle \otimes |f(a)\rangle$, where $s_0 = f(0)$ (the other basis elements are mapped appropriately). The idea is to construct a sequence of unitary transformations that (for some input) will uncover K .

Example 2.8 Let us now go on the subgroup hunt $\mathbb{Z} \rightarrow \mathbb{Z}_{21}$ summarised by the following diagram (constant on $r\mathbb{Z}$, $r = |4| \in \mathbb{Z}_{21}^*$):



Using \mathbb{Z}_{21} on the LHS instead of \mathbb{Z} , we proceed as follows:

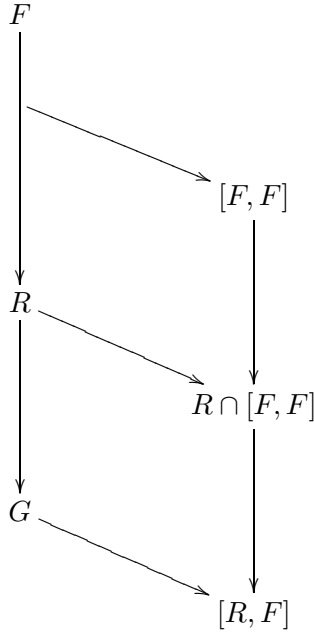


Results:

	A	S	K	
Simon	\mathbb{Z}_2^n	Finite	$\{0, S\}$	1994
Shor	\mathbb{Z}	\mathbb{Z}_n	$r\mathbb{Z}$	1994
Kitaev	Abelian	Finite acted on by A	$\text{stab}(X)$	1995
Röttger, Beth	$\mathbb{Z}_2^n \wr \mathbb{Z}_2$	Finite	Order 2	1998
Friedl et. al.	\mathbb{Z}_2	Finite	(re/lectin)	2000

2.5 W. Nickel (Darmstadt): Schur Covers of Finite Soluble Groups

Let $G = F/R$ and consider the following diagram:



Let $M(G) = \text{Tor}(R/[R, F])$, and let C be the complement to $M(G)$ in $R/[R, F]$: F/C is then a Schur cover. Result: $\text{rank } M(G) \leq \text{def}(G)$. Computing $M(G)$: in general, $M(G) = 1$ is undecidable and we need further properties.

Consider the presentation \mathbb{P} of G given by $G = \langle a_1, \dots, a_n \mid r_1 = s_1, \dots, r_m = s_m \rangle$. It follows that $F/[R, F] = \langle a_1, \dots, a_m, b_1, \dots, b_m \mid r_1 = s_1 b_1, \dots, r_m = s_m b_m, [a_i, b_j] = 1 \rangle$. If G is polycyclic then \mathbb{P}^* is polycyclic — (consistency test) \rightarrow set of relations on $b_1, \dots, b_m \rightarrow$ Presentation for $R/[R, F]$ as an Abelian group — (Smith Normal Form, $|G| < \infty$) $\rightarrow M(G)$. A GAP4 package does this.

Now let G be finite and soluble, let \mathcal{C} be the set of complements of $M(G)$ in $R/[R, F]$, let $D := \cap_{C \in \mathcal{C}} : R/D$ finite, and let $\alpha \in \text{Aut}(G)$ (α lifts to α^* of F/D ; assume that $Z(F/[R, F]) \cap R/[R, F] = R$).

Theorem 2.9 *If A is the set of all liftings of automorphisms of G to F/D , then A acts on \mathcal{C} and $F/C_1 \cong F/C_2 \Leftrightarrow C_1 \sim_H C_2$.*

Sufficient: $\text{Aut}(G) = \langle \alpha_1, \dots, \alpha_k \rangle$, one lifting for α_i , all liftings for id_G . Easy: lift α_i to an endomorphism of F/D . Questions: (1) Lift to an automorphism? (2) Describe all liftings of id_G ? (3) Does α lift to $F/[R, F]$?

2.6 J. Howie (Heriot-Watt, Edinburgh): One-Relator Products of Cyclic Groups

A one-relator product of groups A_1, \dots, A_n is a group $G = (A_1 * \dots * A_n)/N(w)$, where $N(w)$ is the normal closure of a single word $w \in A_1 * \dots * A_n$ (assumed cyclically reduced of length > 1). In particular, if A_i is free then G is a one-relator group.

Classical Results.

Theorem 2.10 *Let $G = (A_1 * \dots * A_n)/N(w)$, with A_i free for all i . Then*

- $A_i \rightarrow G$ is injective for all i (Magnus);
- The word problem is solvable (Magnus);
- The cohomology is easy to compute (Lyndon);
- We have a 2-dimensional FG (Dyer & Vasquez);
- There is no non-obvious torsion (Corollary);
- The centre is usually trivial (Neumann, Murasugi, Pietrowski);
- Subwords of w are non-trivial (Weinbaurn);
- G is locally indicable (for all finitely generated $1 \neq H < G$, H goes onto \mathbb{Z}) if it is torsion-free (Brodskii);
- We have a nice group ring if G is torsion-free (Lewin & Lewin);
- etc.!

To what extent does the theory generalise to one-relator products? Answer: very well, if (a) the A_i are locally indicable (Brodskii, Howie, Short, ...), (b) $w = v^n$ for $n \geq 4$ (Howie), or (c) $w = v^3$ not contained in involution (Duncan, Howie) — but badly in general.

Applications. Equations over groups. If $A \rightarrow G = (A * \langle t \rangle)/N(w)$ is injective, then the equation $w(t) = 1$ over A is soluble in the over-group G of A . Adjunction Problem: Given $w \in A * \langle t \rangle$, can we find a $G \supset A$ and a solution to $w(t) = 1$ in G ? Answer: Yes, if (1) A is locally indicable, and (2) $w = v^m$ for $m \geq 4$, or (3) $w = v^3$ not contained in involution, or (4) A is torsion-free and $\exp_w(t) = \pm 1$, or (5) $\ell_t(w) \leq 4$ and $\exp_w(t) \neq 0$, or (6) etc. — but not always.

Example 2.11 Let $A = \langle x \mid x^2 = 1 \rangle$ and $w = x[x^t, x^{t^2}]$: in $\langle x, t \mid x^2 = x[x^t, x^{t^2}] = 1 \rangle$, we have $xx^t = x^{t^2}x^tx^{t^2} \sim t$ so that $1 = (xx^t)^2 = [x, x^t]$, $1 = [x^t, x^{t^2}] = x$.

One-relator products of cyclics. A_i -cyclic $\Rightarrow G$ has presentation $\langle x_1, \dots, x_n \mid x_1^{p(1)} = \dots = x_n^{p(n)} = 1 \rangle$. What can we say about G ? Example: Let $G = \langle x, y \mid x^{37} = y^{37} = \dots = 1 \rangle$: what is $|G|$? Observation: If $w(x, y)$ is primitive and if p and q are distinct primes, $0 < \exp_w(x) < p$, $0 < \exp_w(y) < q$, then $\langle x, y \mid x^p = y^q = w(x, y) = 1 \rangle$ is trivial.

Proper Power Relations: $\langle x_1, \dots, x_n \mid x_i^{p(i)} = V(x_1, \dots, x_n)^m = 1 \rangle$ ($m > 1$) is well-behaved, e.g. (1) factor groups $\langle x_i \mid x_i^{p(i)} \rangle$ embed; (2) it is infinite when $\chi := 1 - n + \frac{1}{m} + \sum \frac{1}{p(i)} \leq 0$; (3) it is large (i.e. $\supset F_2$) when $\chi < 0$. In particular, we have generalised triangle groups: $G = \langle x, y \mid x^p = y^q = w(x, y)^r = 1 \rangle$ is well-behaved. Further, there exist nice (essential) representations to $PSL(2, \mathbb{C})$ and indeed to $SO(3)$. The finite generalised triangle groups are classified.

Non-Proper Power Relations. There exist presentations $\langle x, y \mid x^p = y^q = w(x, y) = 1 \rangle$ of the trivial group with $p, q, \ell(w)$ arbitrarily high. What if we have > 2 generators? Question: If p, q and r are distinct primes (e.g. 2, 3, 5), can the group $G_w = \langle x, y, z \mid x^p = y^q = z^r = w(x, y, z) = 1 \rangle$ be trivial for any w ? Answer: No (Howie, 2002). Question: Can an n -relator product of $2n + 1$ (cyclic) groups be trivial? Answer: Unknown.

3 Saturday, 31 May 2003

3.1 P. M. Neumann (Oxford): On Three-Star Permutation Groups

Let Ω be a set, let $\Omega^{\{k\}}$ be the set of k -subsets of Ω , let G be a subgroup of $\text{Sym}(\Omega)$, and let $G^r := G_{\{r\}}$ (for $r \subseteq \Omega$). G is said to be a 3-star group if $G^\Theta \neq 1$ for all $\Theta \in \Omega^{\{3\}}$.

Some examples (we focus on primitive groups G): (1) G almost generously 2-transitive $\Rightarrow G$ is a three-star group (hence ‘most’ finite 2-transitive groups); (2) $\text{AGL}(d, 5)$, $\text{AGO}(d, 3)$ and $\text{AO}(d, 2)$ (for d even); (3) H wr S_2 on Γ^2 when H is generously 2-transitive on Γ ; (4) Sym on $\Gamma^{\{2\}}$.

A little suborbit theory: Assume that G is transitive on Ω . Let $G_\alpha :=$ stabiliser of α (for $\alpha \in \Omega$), let suborbit $:= G_\alpha$ -orbit in Ω , and let orbital $:= G$ -orbit in $\Omega \times \Omega$. Fact: there is a natural one-to-one correspondence between suborbits and orbitals. Let $\text{rank}(G) :=$ number of suborbits (or orbitals). Fact: Orbitals come in ‘pairs’. Fact: G is generously 1-transitive $\Leftrightarrow \Gamma = \Gamma^*$ for all suborbits ($\Gamma^* := \{(w_1, w_2) \in \Omega^2 \mid (w_2, w_1) \in \Gamma\}$).

Theorems: (1) If $|\Omega| > 3$ then a positive 3²-group is generously transitive; (2) If G is a finite primitive 3-star group then $\text{rank}(G) \leq 3$; (3) There exist infinite primitive 3-star groups of arbitrarily large rank.

3.2 R. Morse (Evansville): On Computing the Nonabelian Tensor Square of the Free 2-Engel Groups

Given a group G , we define the nonabelian tensor square $G \otimes G$ as the group generated by the symbols $g \otimes g'$ for all $g, g' \in G$ subject to $gg' \otimes h = ({}^g g' \otimes {}^g h)(g \otimes h)$ and $g \otimes hh' = (g \otimes h)({}^h g \otimes {}^h h')$ for all $g, g', h, h' \in G$ when ${}^g h = ghg^{-1}$. The original idea came from a paper by Ronald Brown, David Johnson and Edmund Robertson in 1987. Algorithms were implemented in Cayley, Magma and GAP, and the current work looks to computerise the infinite case.

3.3 D. F. Holt (Warwick): The Dehn Function of Nilpotent Groups

Let G be a group presented by a finite set of generators X and a finite set of relators R . $W = \{w \in (X \cup X^{-1})^* \mid w =_G 1\}$ is the word problem. Let us assume that W is solvable or decidable. The following table shows the time or space needed to decide whether $w \in W$ for $|w| \leq n$:

	Time	Space
Basic	$T_G(n) \geq$	$S_G(n)$
Constructive	$D_G(n) >$	$FL_G(n)$

For Coxeter Groups, we have $T_G(n) = O(n^{1+\epsilon})$, $\epsilon > 0$.

Given $w \in W$, we have a reduction sequence for w : $R(w) = w = w_0 \rightarrow w_1 \rightarrow w_2 \rightarrow \dots \rightarrow w_a = \epsilon$ (the empty word), where $w_i \rightarrow w_{i+1}$ is a single application of a defining relation and free reduction. Now let $a = a(R(w))$ and let $h(R(w)) = \max\{|w_i| \mid 1 \leq i \leq a\}$. More definitions: $a(w) = \min\{a(R(w)) \mid R(w) \text{ is a reduction sequence of } w\}$; $h(w) = \min\{h(R(w)) \mid R(w) \text{ is a reduction sequence of } w\}$; $D_G(n) = \max\{a(w) \mid |w| \leq n\}$; and $FL_G(n) = \max\{h(w) \mid |w| \leq n\}$. Result: $D_G(n) = O(n) \Leftrightarrow G$ is word hyperbolic.

If G is cyclic free abelian then $D_G(n) = \Theta(n^2)$ and $T_G(n) = S_G(n) = FL_G(n) = O(n)$ ($S_G(n) = O(n)$ means that W is context sensitive). Question: Does $S_G(n) = O(n)$ imply that $FL_G(n) = O(n)$? This is true for automatic groups and $S_G(n) = O(\log n)$ if G is linear.

If G is nilpotent of class c , then $G = \gamma_1(G) > \gamma_2(G) > \dots > \gamma_{c+1}(G) = 1$, $S_G(n) = O(n)$ and $T_G(n) = O(n)$. Gromov's Conjecture (1990): $D_G(n) = \Theta(n^{1+c})$. Hidber: $D_G(n) = O(n^{2^c})$, $FL_G(n) = O(n^c)$ (note that $FL =$ 'filling length').

Theorem 3.1 (*S. Gerster, D. Holt, T. Riley*): $D_G(n) = O(n^{c+1})$, $FL_G(n) = O(n)$.

3.4 R. M. Thomas (Leicester): Unsolved Problems in Automatic Semigroups

Let A be a set of symbols so that A^* consists of all finite words. The word problem can be stated as the question $\alpha =_G \beta$? Let L be a regular language accepted by a finite state automata so that $L\varphi = G$. An automatic structure (A, L) is said to be prefix-closed if L is prefix-closed, and every automatic group has a prefix closed automatic structure.

Question: Does every automatic semigroup have a prefix-closed automatic structure?

Every finitely generated abelian group is automatic, but this does not generalise to commutative semigroups.

Definition 3.2 A semigroup S generated by a finite set A is said to have bounded indegree if there exists a k such that for all $s \in S$ we have

$$|\{t \in S : s = ta \text{ for some } a \in A\}| \leq k.$$

Question: If every finitely generated commutative semigroup with bounded indegree automatic?

Relations R and L are defined on S by aRb (respectively aLb) if $aS' = bS'$ (respectively $S'a = S'b$); H is the intersection of L and R .

Question: Is every finitely generated commutative semigroup finitely many H -classes automatic?

Question: Is there a 'nice' geometric characterisation of automatic semigroups (or classes of automatic semigroups)? — compare with the fellow-traveller property.

If G is the group $\langle a, b : ab^m = b^na \rangle$ and if S is a semigroup embedded in G , then S is automatic but G is not automatic.

Question: If φ is a semigroup presentation, if S and G are the subgroup and group defined by φ , if S embeds in G and if G is automatic, does it follow that S is automatic?