Diameters of Cayley graphs of soluble groups

John Wilson, Oxford

(wilsonjs@maths.ox.ac.uk)

Ischia, April 2010

$G = \langle S \rangle$ a group of order $\leqslant N$, p prime.

How hard is it to decide whether $p \mid |G|$ and, if so, to find some $g \in G$ of order divisible by p?

More precisely, consider products

$$g = s_1^{\pm 1} s_2^{\pm 1} \dots s_d^{\pm 1} \quad (s_i \in S).$$

What is the smallest d for which some such g has order divisible by p (if p does divide $|G|$)?

Example. $G = \mathsf{SL}_n(2)$,

$$S = \{1 + e_{12}, 1 + e_{23}, \dots, 1 + e_{n-1,n}, 1 + e_{n1}\}.$$

Any $n-1$ elements of S lie in a Sylow 2-subgroup, so need g of length $d \geqslant n$ to 'find' elements of odd order.

$|\mathsf{SL}_n(2)| \sim 2^{n^2}$, so $d \sim (\log_2 |G|)^{1/2}$.

A hard problem, so restrict to soluble groups.

Corollary 1. $\exists\ \kappa$ with the following property.

If $G = \langle S \rangle$ is soluble, $|G| \leqslant N$ and $p \mid |G|$ then some $g = s_1^{\pm 1} s_2^{\pm 1} \ldots s_d^{\pm 1}$ (with $s_i \in S$) has order divisible by p, where

$d \leqslant \min\{\kappa \lfloor \log_p N \rfloor, 200(\lfloor \log_p N \rfloor)^2\}$.

More precisely, if n is the smallest rank of a p-chief factor of G, then $d \leqslant \min\{\kappa n, 200 n^2\}$.

(This bound—for soluble groups—may be asymptotically too big.)

Let G be finitely generated, generating set S.

The Cayley graph of G w.r.t. S has

- vertex set G, and

- an edge connecting g_1, g_2 if $g_2 = g_1 s^{\pm 1}$ for some $s \in S$.

The ball $B_S(n)$ of radius n (with centre 1) is

$\{t_1 t_2 \dots t_n \mid t_i \in S \cup S^{-1} \cup \{1\}\}$.

G finite: the diameter $D_S(G)$ is the smallest d with $B_S(d) = G$.

Diameters for different gen. sets can differ.

Write $D(G) = \max\{D_S(G) \mid S \text{ a gen. set}\}$.

Examples. (1) $G = \langle s \rangle$ cyclic of order m: then $G = \{1, s^{\pm 1}, s^{\pm 2}, \ldots, s^{\pm \lfloor m/2 \rfloor}\}$, and

$D_S(G) = D(G) = \lfloor m/2 \rfloor$.

(2) (JSW, 2003). Suppose G abelian, write G as direct product of cyclic groups of orders $s_1, s_2 \ldots, s_r$ with $s_i \mid s_{i-1}$ for $i > 1$. Then $D(G) = \sum \lfloor s_i/2 \rfloor$.

(3) $G = \langle a, t \mid a^{26} = t^3 = 1,\, a^t = a^3 \rangle = H \rtimes \langle t \rangle$.

Then $D(H) = 13$, $D(G) \leqslant 7$.

D isn't monotonic.

Theorem 1. Let $G \leqslant \mathrm{GL}_n(p)$, G soluble, completely reducible, V the natural module. Then

(1) $D(G) \leqslant \kappa|V|$ where $\kappa \approx 50$.

(2) If also $G \leqslant \mathrm{Sp}_n(p)$ then $D(G) \leqslant \kappa'|V|^{1/2}$ where κ' is a constant.

Notes. (1) The bounds are asymptotically right: $\mathrm{GL}_n(p)$, $\mathrm{Sp}_n(p)$ have cyclic (irreducible, Singer) subgroups of order $p^n - 1$, $p^{n/2} + 1$ respectively.

(2) Restriction to CR subgroups?

Difficulty: failure of D to be monotonic.

Remedy: introduce bigger functions $E(G)$, $w(G)$ with good inheritance properties.

$E(G) = \max\{1 + 2D(H) \mid H \leqslant G\}$

E is monotonic, and $E(G) \leqslant E(K)E(G/K)$.

If $K \leqslant G = \langle S \rangle$ and T a transversal with $1 \in T$ then

$K = \langle \{t_1^{-1} s t_2 \mid s \in S,\, t_i \in T\} \cap K \rangle$;

so if $K \triangleleft G$ then K has generating set of elements of $B_S(d)$ where $d = 1 + 2D(G/K)$.

For G soluble, let $\mathcal{C}$ be a chain

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_r = G$$

with each G_i/G_{i-1} abelian. Define

$$w_{\mathcal{C}}(G) = \prod_i (1+2D(G_i/G_{i-1})) = \prod_i E(G_i/G_{i-1}),$$

Define $w(G) = \min\{w_{\mathcal{C}}(G)\}$.

- if $H \leqslant G$ then $w(H) \leqslant w(G)$
- if $K \lhd G$ then $w(G) \leqslant w(K)w(G/K)$
- $E(G) \leqslant w(G)$
- if derived length $\mathrm{dl}(G) = l$ then $w(G^{(r)}) \leqslant r^l w(G)$ for all r.

($G^{(r)}$ = dir. product of r copies of G.)

Example. (1) $G = \mathrm{GL}_3(2)$.

(a) $\exists\, K \triangleleft G$ with $K \cong Q_8$, $G/K \cong S_3$.

Easy to check that $D(Q_8) = 2$, $D(S_3) = 3$, and D monotonic on subgroups of Q_8, S_3.

So $E(Q_8) = 5$, $E(S_3) = 7$. Hence $E(G) \leqslant 35$.

(b) G has a unique shortest series with abelian factors; factors C_2, $C_2 \times C_2$, C_3, C_2.

$D(C_2) = D(C_3) = 1$, $D(C_2 \times C_2) = 2$, so $w(C_2) = w(C_3) = 3$, $w(C_2 \times C_2) = 5$.

Hence $w(G) = 3^3 \cdot 5 = 135$.

(c) The natural module has order 9, less than the above estimates for $D(G)$.

(2) However if $p \geqslant 17$ and G is a soluble subgroup of $\mathrm{GL}_n(p)$ then $w(G) \leqslant p^n$.

- if $\mathrm{dl}(G) = l$ then $w(G^{(r)}) \leqslant r^l w(G)$.

This is very effective in cutting down possibilities needing examination.

E.g. G irred. soluble, $G \leqslant \mathrm{GL}_n(p)$. If G imprimitive, then $G \leqslant H \,\mathrm{wr}\, T$ with H soluble, $H \leqslant \mathrm{GL}_m(p)$, T a transitive subgroup of S_r, where $mr = n$, so

$w(G) \leqslant r^l w(H) w(T)$ where $l = \mathrm{dl}(H)$.

(Newman, 1972): bounds for $\mathrm{dl}(H)$ for H soluble, $H \leqslant \mathrm{GL}_m(F)$.

Now try to use induction on n.

Lemma. If T transitive soluble in S_n then $w(T) \leqslant n^{(5/2)\log_9 9n}$.

Suprunenko's Theorem. Let G be maximal primitive soluble subgroup of $\mathsf{GL}_n(p)$. Then G has a unique maximal abelian normal subgroup A; it is cyclic of order $p^l - 1$ where $l \mid n$, its centralizer C embeds in $\mathsf{GL}_r(p^l)$ where $r = n/l$, and G/C is cyclic of order l_1 where $l_1 \mid l$. If $A = C$ then $l_1 = l$.

Assume that $A \neq C$. Then $\exists\ u > 1$ with $u \mid r$ such that

(i) C/A has a unique maximal abelian normal subgroup B/A; it has elementary abelian Sylow subgroups and order u^2;

(ii) $C/B \leqslant \prod_{i=1}^{s} \mathsf{Sp}_{2k_i}(q_i)$, where $u = \prod_{i=1}^{s} q_i^{k_i}$ is the prime factorization of u. The image of C in each $\mathsf{Sp}_{2k_i}(q_i)$ is completely reducible.

Need to prove something more general than Theorem 1 (b).

Definition. A finite $\mathbb{Z}G$-module is a symplectic G-module if it has a non-singular skew-symmetric form preserved by G.

Theorem 2 (b). There is a bound on all $E(G/C_G(M))/|M|^{1/2}$ with G soluble and M a completely reducible symplectic G-module.

Major step: bound orders of M for such pairs (M, G) having no symplectic submodules N with larger $E(G/C_G(N))/|N|^{1/2}$.

Let $G = \langle S \rangle$, with S finite.

$B_S(n) = \{t_1 t_2 \ldots t_n \mid t_i \in S \cup S^{-1} \cup \{1\}\}$.

$l_S(g) = \min\{n \mid g \in B_S(n)\}$.

$\beta_S(n) = |B_S(n)| = |\{g \mid l_S(g) \leqslant n\}|$.

If $G = \langle S_1 \rangle = \langle S_2 \rangle$ let $\mu = \max\{l_{S_1}(t) \mid t \in S_2\}$

Then $l_{S_1}(g) \leqslant \mu\, l_{S_2}(g)$, so $\beta_{S_2}(n) \leqslant \beta_{S_1}(\mu n)$

G has polynomial growth (PG) if

$\exists\ a, b > 0$ with $\beta_S(n) \leqslant a n^b$ for all n.

(M Gromov, 1982): The groups of PG are just the virtually nilpotent (vN) groups.

Problem. Fix a, b. Prove that there are only finitely many finite simple groups G with gen. sets S such that $\beta_S(n) \leqslant an^b$ for all n.

Doesn't seem to follow easily from CFSG.

But it is an immediate corollary of Gromov's theorem!

(M Gromov, 1982): The groups of PG are just the virtually nilpotent (vN) groups.

(Grigorchuk, 1989): If $G = \langle S \rangle$ is residually nilpotent and $\beta_S(n)/e^{n^{1/2}} \to 0$ as $n \to \infty$ then G is vN.

(JSW, 2003): Let $\alpha : \mathbb{N} \to \mathbb{R}$ satisfy

$$\alpha(n)/e^{(1/2)(\log n)^{1/2}} \to 0 \quad \text{as } n \to \infty,$$

and let $G = \langle S \rangle$ be residually soluble and satisfy $\beta_S(n) \leqslant e^{\alpha(n)}$ for all n. Then G is vN.

Corollary 2 (April 2, 2010): If $G = \langle S \rangle$ is residually soluble and $\beta_S(n)/e^{(n^{1/7})/10} \to 0$ as $n \to \infty$ then G is vN.

So if $\beta_S(n)/e^{(n^{1/7})/10} \to 0$ then β_S is bounded by a polynomial.