The length and depth of a group

Tim Burness

Interactions between group theory, number theory, combinatorics and geometry

Isaac Newton Institute, Cambridge
March 17th 2020

University of BRISTOL

Length

Let G be a finite group. An **unrefinable chain** is a sequence of subgroups

$$G = G_0 > G_1 > \cdots > G_{t-1} > G_t = 1$$

such that each G_i is maximal in G_{i-1}.

The **length** $\ell(G)$ is the **maximal** length of an unrefinable chain.

Let $\Omega(n)$ be the number of prime divisors of $n \in \mathbb{N}$ (incl. multiplicities).

- $\ell(G) \leqslant \Omega(|G|) \leqslant \log_2 |G|$
- G soluble $\implies \ell(G) = \Omega(|G|)$: a composition series is unrefinable
- Length is **monotonic** and **additive**: if $H \leqslant G$ and $N \trianglelefteq G$, then

$$\ell(H) \leqslant \ell(G) \quad \text{and} \quad \ell(G) = \ell(N) + \ell(G/N)$$

Connections

Minimal generation (Babai, 1980s).

Let $G \leqslant S_n$ be a permutation group and let $\{x_1, \ldots, x_d\}$ be a generating set for G of minimal size. Then

$$G = \langle x_1, \ldots, x_d \rangle > \langle x_1, \ldots, x_{d-1} \rangle > \cdots > \langle x_1 \rangle > 1$$

is strictly descending, so $d \leqslant \ell(G) \leqslant \ell(S_n)$.

Automorphisms of soluble groups (Solomon & Turull, 1980s).

Suppose $H = G{:}A$ with $|G|, |A|$ coprime and $C_G(A) = 1$.

- **Thompson, 1959.** If A has prime order, then G is nilpotent.
- CFSG $\implies$ G is soluble, so let $h(G)$ be the Fitting height of G.
- **Conjecture.** $h(G) \leqslant \ell(A)$

Depth

The **length** $\ell(G)$ is the **maximal** length of an unrefinable chain.

The **depth** $\lambda(G)$ is the **minimal** length of an unrefinable chain.

- $\lambda(G) \leqslant \ell(G)$
- **Iwasawa, 1941:** $\ell(G) = \lambda(G) \iff G$ is supersoluble
- Depth is **not** monotonic **nor** additive: if $N \trianglelefteqslant G$, then

$$\lambda(G/N) \leqslant \lambda(G) \leqslant \lambda(N) + \lambda(G/N)$$

Example. Suppose $G = \mathrm{AGL}_1(8) = (C_2)^3{:}C_7$ and $N = (C_2)^3$.

Then $\lambda(G) = 2$, $\lambda(N) = 3$ and $\lambda(G/N) = 1$.

The length of S_n

Theorem (Cameron, Solomon & Turull, 1989).

$$\ell(S_n) = \lfloor (3n-1)/2 \rfloor - b(n)$$

where $b(n)$ is the number of 1s in the base 2 expansion of n.

Example. $\ell(S_6) = \lfloor 17/2 \rfloor - 2 = 6$

$$S_6 > S_4 \times S_2 > (S_2 \wr S_2) \times S_2 > (S_2)^3 > (S_2)^2 > S_2 > 1$$

Need to show: $G < S_n$ maximal $\implies \ell(G) \leqslant \lfloor (3n-1)/2 \rfloor - b(n) - 1$

- By induction on n, we may assume G acts primitively on $\{1, \ldots, n\}$
- Recall that $\ell(G) \leqslant \log_2 |G|$
- O'Nan-Scott Theorem $\rightsquigarrow$ G is almost simple. Now apply CFSG...

The depth of S_n

Theorem (B, Liebeck & Shalev, 2018). $\lambda(S_n) \leqslant 24$ for all n.

Sketch. Suppose $G = S_n$ and $n \geqslant 12$ is even. There are primes p, q, r s.t.

$$n = p + q + r + 3$$

by [Helfgott, 2013]. Set $H = S_{p+1} \times S_{q+1} \times S_{r+1} < G$.

If $t \geqslant 5$ is a prime and $t \notin \{7, 11, 23\}$ then there is an unrefinable chain

$$S_{t+1} > A_{t+1} > \mathrm{L}_2(t) > K$$

with $K \in \{A_4, S_4, A_5\}$. Here $\lambda(K) \leqslant 3$, so $\lambda(S_{t+1}) \leqslant 6$ and $\lambda(H) \leqslant 18$.

Typically, $G > S_{p+q+2} \times S_{r+1} > H$ is unrefinable, so $\lambda(G) \leqslant 20$.

Length for groups of Lie type

Theorem (Solomon & Turull, 1991).

Let G be a simple group of Lie type over $\mathbb{F}_q$ with twisted Lie rank r (e.g. $G = \mathrm{L}_{r+1}(q)$ or $\mathrm{U}_{2r+1}(q)$).

- If q is even (and $G \neq \mathrm{U}_{2r+1}(2)$), then

$$\ell(G) = \ell(B) + r = \Omega(|B|) + r$$

  where B is a Borel subgroup of G.

- Same conclusion holds if $q = p^k$ is odd and $k = k(p) \gg 0$.

Example. If $G = \mathrm{L}_2(7)$ then $B = C_7{:}C_3$ and $\ell(B) + r = 3$, but

$$G > S_4 > S_2 \wr S_2 > S_2 \times S_2 > S_2 > 1$$

and thus $\ell(G) = \Omega(|G|) = \Omega(168) = 5$.

Depth for groups of Lie type

Lemma. Let $G = \mathrm{L}_2(p^k)$, with p an odd prime and k odd. Then

$$\lambda(G) = \Omega(k) + \lambda(\mathrm{L}_2(p)) = \Omega(k) + c \;\text{ with } c \in \{2, 3, 4\}$$

Corollary. Given $n \in \mathbb{N}$, there is a simple group G with $\lambda(G) > n$.

Theorem (BLS, 2018). If G is a simple group of Lie type over $\mathbb{F}_{p^k}$ with p odd, then

$$\lambda(G) \leqslant 3\Omega(k) + 36$$

The same bound holds for $p = 2$ if we exclude the groups

$$\mathrm{L}_2(2^k),\ {}^2B_2(2^k) \text{ and } \mathrm{U}_{2r+1}(2^k)$$

Example. Let $G = \mathrm{Sp}_{2r}(2^k)$, where $r \geqslant 4$ is even and $k \geqslant 1$. Then

$$\lambda(G) \leqslant \Omega(k) + 25.$$

- Suppose $k > 1$ and write $k = k_1 \cdots k_t$ as a product of primes. Then

$$G > \mathrm{Sp}_{2r}(2^{k/k_1}) > \mathrm{Sp}_{2r}(2^{k/k_1 k_2}) > \cdots > \mathrm{Sp}_{2r}(2)$$

  is unrefinable, so $\lambda(G) \leqslant \Omega(k) + \lambda(\mathrm{Sp}_{2r}(2))$ for all k.

- Finally, we observe that $S_{2r+2} < \mathrm{Sp}_{2r}(2)$ is maximal (embedded via the fully deleted permutation module over $\mathbb{F}_2$), so

$$\lambda(G) \leqslant \Omega(k) + 1 + \lambda(S_{2r+2}) \leqslant \Omega(k) + 25.$$

A very similar argument gives $\lambda(G) \leqslant \Omega(k) + 28$ if $r \geqslant 5$ is odd.

Example. Let $G = \mathrm{L}_2(2^k)$ with $k \geqslant 3$ prime. Then

$$\lambda(G) = 2 + \min\{\Omega(2^k - 1), \Omega(2^k + 1)\}$$

Let H be a maximal subgroup of G. Then either

- $H = (C_2)^k{:}C_{2^k-1}$ and $\lambda(H) = 1 + \Omega(2^k - 1)$, or
- $H = D_{2(2^k \pm 1)}$ and $\lambda(H) = 1 + \Omega(2^k \pm 1)$.

Therefore

$$\begin{aligned} \lambda(G) &= 1 + \min\{\lambda(H) : H < G \text{ maximal}\} \\ &= 2 + \min\{\Omega(2^k - 1), \Omega(2^k + 1)\} \end{aligned}$$

whereas $3\Omega(k) + 36 = 39$.

Length and depth for sporadic simple groups

G	$\ell(G)$	$\lambda(G)$						
M_{11}	7	4	HS	12	5	Co_3	14	4
M_{12}	8	4	Suz	17	4	Fi_{22}	21	5
M_{22}	10	4	McL	12	5	Fi_{23}	25	4
M_{23}	11	3	Ru	17	5	Fi_{24}'	28	4
M_{24}	14	4	He	13	6	HN	19	5
J_1	6	4	Ly	15	4	Th	20	4
J_2	10	4	O′N	13	5	$\mathbb{B}$	46	3
J_3	10	5	Co_1	26	5	$\mathbb{M}$	52	4
J_4	26	4	Co_2	22	4			

Example. $\mathbb{B} > C_{47}{:}C_{23} > C_{47} > 1$ is an unrefinable chain of length 3

Small length

Lemma. If G is (non-abelian) simple, then $\lambda(G) \geqslant 3$ and $\ell(G) \geqslant 4$.

Proof. Suppose $G > H > 1$ is unrefinable.

Then $H = C_p$ for a prime p and $N_G(H) = G$ or H, so either

- H is normal, or
- $H \cap H^g = 1$ for all $g \in G \setminus H$ and G is a Frobenius group on G/H.

In both cases, G has a proper nontrivial normal subgroup.

Question. Are there any simple groups G with $\ell(G) = 4$?

A theorem of Heath-Brown

Question. Are there any simple groups G with $\ell(G) = 4$?

Theorem (Janko, 1963). For G simple, $\ell(G) = 4$ iff $G = A_5$, or $G = \mathrm{L}_2(p)$, p prime, $\Omega(p \pm 1) \leqslant 3$ and $p \equiv \pm 3, \pm 13 \pmod{40}$:

$$p \in \{13, 43, 67, 173, 283, 317, 653, 787, 907, 1867, \dots\}$$

Question. Are there infinitely many?

Theorem (Heath-Brown, 2019)

There are infinitely many prime numbers p with $\Omega(p \pm 1) \leqslant 8$.

Corollary. There are infinitely many simple groups G with $\ell(G) \leqslant 9$

Small depth

Theorem (BLS, 2018). The simple G with $\lambda(G) = 3$ are known.

Examples.

- A_{2p+1}, where p is a Sophie Germain prime, $p \neq 3, 5, 11$
- ${}^2B_2(2^k)$, where $2^k - 1$ is a Mersenne prime
- $\mathrm{L}_2(3^k)$ with $k \geqslant 3$ prime: $\mathrm{L}_2(3^k) > A_4 > C_3 > 1$ is unrefinable

Corollary. There are infinitely many simple G with $\lambda(G) = 3$.

To determine the simple groups G with $\lambda(G) = 4$, we need to know the simple groups with a simple maximal subgroup of depth 3...

Length vs depth

Chain difference and ratio: $\mathrm{cd}(G) = \ell(G) - \lambda(G)$, $\mathrm{cr}(G) = \ell(G)/\lambda(G)$

- **Iwasawa, 1941.** $\mathrm{cd}(G) = 0 \iff \mathrm{cr}(G) = 1 \iff G$ supersoluble
- **Brewster, Ward & Zimmermann, 1993.** The simple G with $\mathrm{cd}(G) = 1$ are known (A_6 and $\mathrm{L}_2(p)$ for certain primes p)
- **BLS, 2019.** For G simple, $\mathrm{cr}(G) \geqslant 5/4$ is best possible

Question. Do we have $\lambda(G) = O(\log_2 \ell(G))$ for all simple G?

Example. $G = \mathrm{L}_2(2^k)$, $k \geqslant 3$ prime

$$\ell(G) = 1 + \ell(B) = k + 1 + \Omega(2^k - 1)$$
$$\lambda(G) = 2 + \min\{\Omega(2^k \pm 1)\}$$

Very hard question. Do we have $\Omega(2^k - 1) \leqslant \log_2 k$ for primes $k \gg 0$?

Infinite groups

Let G be a connected algebraic group over an algebraically closed field K of characteristic $p \geqslant 0$. Here an **unrefinable chain** is a sequence

$$G = G_0 > G_1 > \cdots > G_{t-1} > G_t = 1$$

where each G_i is a **maximal closed connected** subgroup of G_{i-1}.

Length $\ell(G)$: **maximal** length of an unrefinable chain.

Depth $\lambda(G)$: **minimal** length of an unrefinable chain.

Let N be a closed connected normal subgroup of G.

- $\lambda(G) \leqslant \ell(G) \leqslant \dim G$
- $\ell(G) = \ell(N) + \ell(G/N)$
- $\lambda(G/N) \leqslant \lambda(G) \leqslant \lambda(N) + \lambda(G/N)$

Example. Let $G = \mathrm{SL}_2(K)$, $B = \{\begin{pmatrix} * & * \\ & * \end{pmatrix}\}$ and $T = \{\begin{pmatrix} * & \\ & * \end{pmatrix}\}$. Then

$$G > B > T > 1$$

is unrefinable and $\lambda(G) = \ell(G) = \dim G = 3$.

Theorem (BLS, 2019). Let G be connected, with radical $R(G)$ and unipotent radical $R_u(G)$. Let B be a Borel subgroup of $G/R_u(G)$.

- G soluble $\implies \ell(G) = \lambda(G) = \dim G$
- $\ell(G) = \lambda(G) \implies G$ soluble or $G/R(G) = A_1$
- $\ell(G) = \dim R_u(G) + \dim B + \mathrm{rank}\,(G/R_u(G))'$
- G simple $\implies \ell(G) = \dim B + \mathrm{rank}\, G$

$$\ell(G) = \dim R_u(G) + \dim B + r, \text{ where } r = \operatorname{rank}(G/R_u(G))'$$

Sketch. Induction on $\dim G$.

- $\dim G = 1$: $G = U_1$ or T_1 ✓
- Easy reduction to G simple.
- Let M be a maximal connected subgroup of G.

  By [Borel-Tits, 1971], M is either parabolic or reductive.
- If $M = QL$ is parabolic, then by additivity and induction

$$\ell(M) = \dim Q + \dim B_L + \operatorname{rank} L' = \dim B + r - 1$$

- Similarly, if M is reductive, then induction gives

$$\ell(M) = \dim B_M + \operatorname{rank} M' < \dim B - 1 + \operatorname{rank} M' \leqslant \dim B + r - 1$$

In contrast, $\lambda(G)$ depends on the characteristic $p \geqslant 0$ of the field K.

Example. If $G = E_8$ then

$$\lambda(G) = \begin{cases} 4 & \text{if } p = 0 \text{ or } p \geqslant 23 \\ 5 & \text{if } 5 \leqslant p \leqslant 19 \\ 7 & \text{if } p = 3 \\ 9 & \text{if } p = 2 \end{cases}$$

For instance, if $p = 0$ or $p \geqslant 23$, then G has a maximal A_1 subgroup, so

$$G > A_1 > U_1T_1 > T_1 > 1$$

is unrefinable. On the other hand, if $p = 2$ then

$$G > D_8 > B_4 > B_2B_2 > B_2 > A_1A_1 > A_1 > U_1T_1 > T_1 > 1$$

turns out to be an unrefinable chain of minimal length.

Theorem (BLS, 2019). Let G be a simple algebraic group.

- If $p = 0$, then $\lambda(G) \leqslant 6$, with equality if and only if $G = A_6$.
- If $p > 0$ and G is exceptional, then $\lambda(G) \leqslant 9$, with equality if and only if $G = E_8$ and $p = 2$.
- If $p > 0$ and G is classical of rank r, then

$$\lambda(G) \leqslant 2(\log_2 r)^2 + 12$$

and $\lambda(G) \to \infty$ as $r \to \infty$.

The proofs rely heavily on work of **Dynkin**, **Liebeck**, **Seitz**, **Testerman** and others on the subgroup structure of simple algebraic groups.

Further directions: Lie groups

Let G be a **compact connected** Lie group and define $\ell(G)$ and $\lambda(G)$ as for algebraic groups.

Theorem (BLS, 2020). If G is simple, then

G	SU_n	Sp_n	SO_n	G_2	F_4	E_6	E_7	E_8
$\ell(G)$	$2n-2$	$\frac{3}{2}n-1$	$n+\lfloor\frac{n}{4}\rfloor-1$	5	11	13	15	20

$$\lambda(G) = \begin{cases} 2 & G = SU_2 \\ 4 & G = SU_n\,(n \geqslant 4,\ n \neq 7),\ SO_7,\ SO_{2r}\,(r \geqslant 4),\ E_6 \\ 5 & G = SU_7 \\ 3 & \text{otherwise} \end{cases}$$

In general, $\ell(G) = \lambda(G) \iff G$ is a torus or $G' = SU_2$

Further directions: Algebras

Let A be a finite dimensional associative algebra over a field k. Define $\ell(A)$ and $\lambda(A)$ with respect to chains

$$A = A_0 > A_1 > \cdots > A_{t-1} > A_t = 0$$

where each A_i is a **maximal** k**-subalgebra** of A_{i-1}.

Some results. (Sercombe & Shalev, 2020)

- Length is additive with respect to ideals
- $\ell(\mathrm{M}_n(k)) = n - 1 + \ell(\mathrm{D}_n(k)) + \ell(\mathrm{U}_n(k)) = 2n - 1 + \frac{1}{2}n(n-1)$
- If D is a division algebra over k, then

$$\ell(\mathrm{M}_n(D)) = n - 1 + n \cdot \ell(D) + \frac{1}{2}n(n-1) \cdot |D : k|$$

- If A is nilpotent, then $\ell(A) = \lambda(A) = \dim A$

Algebras

Theorem (Sercombe & Shalev, 2020).

- If $J(A)$ is the Jacobson radical and $A/J(A) = \prod_i \mathrm{M}_{n_i}(D_i)$, then

$$\ell(A) = \dim J(A) + \sum_i \left(n_i - 1 + n_i \ell(D_i) + \frac{1}{2} n_i (n_i - 1) |D_i : k| \right)$$

- For a division algebra D over k: $\lambda(\mathrm{M}_n(D)) \leqslant 6 \log_2 n + \lambda(D)$

- For $k = \bar{k}$: $3 \log_2 n + 1 \leqslant \lambda(\mathrm{M}_n(k)) \leqslant 6 \log_2 n + 1$

- For $k = \bar{k}$: $\ell(A) = \lambda(A) \iff A/J(A) = \prod_i \mathrm{M}_{n_i}(k),\ n_i \leqslant 2$