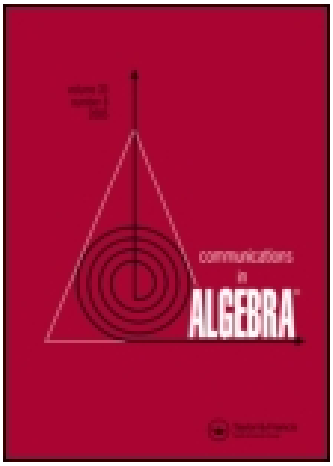

Communications in Algebra
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/lagb20

On the length of subgroup chains in the symmetric group

László Babai [a] [b]
[a] Department of Algebra , Eotvos University , Budapest, H-1088, Hungary
[b] Department of Computer Science , University of Chicago , Chicago, IL, 60637
Published online: 27 Jun 2007.

COMMUNICATIONS IN ALGEBRA, 14(9), 1729-1736 (1986)

On the length of subgroup chains in the symmetric group

László Babai

Department of Algebra
Eötvös University
Budapest, Hungary H-1088

and

Department of Computer Science
University of Chicago
Chicago, IL 60637

Abstract

We prove that for $n \geq 2$, the length of every subgroup chain in S_n is at most $2n-3$. The proof rests on an upper bound for the order of primitive permutation groups, due to Praeger and Saxl. The result has applications to worst case complexity estimates for permutation group algorithms.

1. Introduction

By a *subgroup chain of length m* in a finite group G we mean a strictly descending chain

$$G = G_0 > G_1 > \cdots > G_m = 1 \tag{1}$$

starting with G and ending with the identity. S_n and A_n denote the symmetric and alternating groups of degree n, resp.

In this note, we prove the following.

Theorem. *For $n \geq 2$, the length of every subgroup chain in S_n is at most $2n-3$.*

On the other hand we shall see (Corollaries 3 and 4) that S_n has a subgroup chain of length $(3n/2)-2$ for infinitely many values of n and a chain of length at least $(3n/2)-\log_2 n-1$ for every $n \geq 2$.

0092-7872/86/1409-1729$3.50/0

Conjecture. *For $n \geq 2$ the length of every subgroup chain in S_n is at most* $(3n/2)-2$.

Let $h(G)$ denote the length of the longest chain of subgroups of the finite group G (the *height* of G). Let $h(n)=h(S_n)$. Here is a table of the first values of $h(n)$. The values for $8 \leq n \leq 11$ were kindly provided by Greg Butler [4]; the proofs rest on results from [5],[7],[17] and on ad hoc arguments.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$h(n)$	0	1	2	4	5	6	7	10	11	12	13	≥ 15	≥ 16	≥ 17	≥ 18	≥ 22

The Theorem asserts that $h(n) \leq 2n-3$ for every n. We actually have an explicit formula for a function that may always be equal to $h(n)$.

Let $k(n)$ denote the number of 1's in the binary expansion of n. Let $f(n)=\lceil 3n/2\rceil-k(n)-1$ where $\lceil x\rceil$ denotes the smallest integer $\geq x$.

Problem. Is $h(n)=f(n)$ for every n ?

The table above shows that equality does indeed hold for $1 \leq n \leq 11$. By Corollary 4, $h(n) \geq f(n)$ for every n.

We note that the trivial estimate $h(G) \leq \log_2|G|$ yields $h(n) < n\log_2 n - cn$ for a positive constant c. This was improved by Knuth [13] to $h(n)=O(n\log\log n)$. Part of the motivation for the problem comes from computational complexity theory. The analysis of the worst-case running time of *algorithms on permutation groups* often depends on an estimate for $h(n)$. In particular, our result *improves Knuth's worst case bound* for the running time of Sims' [17] permutation group representation algorithm (construction of strong generators from an arbitrary list of generators).

Corollary. *Knuth's version of Sims' algorithm finds strong generators (and thereby tests membership and computes order) for a permutation group given by a list of generators in time $O(N^5)$, where N is the length of the input.*

We note that the $O(N^5)$ worst case bound was achieved by M. Jerrum [9] using a more sophisticated version of Sims' algorithm.

One observes that $O(N^5)$ is just a marginal improvement over Knuth's $O(N^5\log\log N)$ and the $O(N^5)$ bound seems very much an overestimate of the actual running time. Similar marginal improvements follow for other permutation group algorithms [10], [11], [12], [15] (cf. [3]). With all this said, the main motivation for our Theorem remains purely aesthetic.

Acknowledgments. The author is grateful to E. M. Luks for valuable discussions on the subject and to Greg Butler [4] for providing the values of $h(n)$ for $8 \leq n \leq 11$, thus motivating the Problem stated above, as well as for pointing out references [5] and [7].

2. Preliminaries

First we prove that the function $h(G)$ is additive in the following sense.

Lemma 1. *If N is a normal subgroup of G then*

$$h(G)=h(N)+h(G/N). \tag{2}$$

Proof. Clearly, the left hand side is not less than the right hand side. We shall see that it is not greater either.

Consider the following equalities for subgroups $L<K\leq G$.

$$|K|=|K\cap N||KN/N|. \tag{3}$$

$$|L|=|L\cap N||LN/N|. \tag{4}$$

These equalities imply that at least one of the inclusions

$$K\cap N\geq L\cap N \quad \text{and} \quad KN/N\geq LN/N$$

is proper. Now the Lemma follows. ∎

Corollary 2. *For $n\geq 2$, we have $h(2n)\geq 2h(n)+2$.*

Proof. Consider the following chain.

$$S_{2n}>S_n wr S_2>S_n\times S_n \tag{5}$$

(Here *wr* stands for wreath product.) An application of Lemma 1 to the right end proves our inequality. ∎

Corollary 3. *If n is a power of 2 and $n\geq 2$ then $h(n)\geq(3n/2)-2$.*

Proof. By induction, using Corollary 2. ∎

Corollary 4. *For $n\geq 2$, we have $h(n)\geq(3n/2)-k(n)-1$, where $k(n)$ is the number of 1's in the binary expansion of n. In particular, $h(n)\geq(3n/2)-\log_2(n+1)-1$.*

Proof. If n is a power of 2 then $k(n)=1$ and Corollary 3 coincides with our claim. If $k(n)>1$, let $n=2^s+m$ where $m<n/2$. By induction,

$$h(n)\geq 1+h(S_{2^s}\times S_m)=1+h(2^s)+h(m)$$

$$\geq 1+(3.2^{s-1})-2+(3m/2)-k(m)-1=(3n/2)-k(n)-1. \quad ∎$$

3. Primitive groups.

First we have to give a stronger bound for primitive permutation groups, not containing the alternating group. Let $q(n)$ denote the maximum of $h(G)$ over all primitive permutation groups G of degree n other than S_n and A_n. If no such group exists, we set $q(n)=-\infty$.

Lemma 5. *For $n\geq 1$ we have $q(n)\leq 2n-5$.*

The proof requires the following result, obtained by Cheryl Praeger and Jan Saxl [16] by extending results and techniques of H. Wielandt [20].

Theorem 6 (Praeger and Saxl). *If G is a primitive permutation group of degree n then $|G|<4^n$.*

The proof of Lemma 5 will critically depend on the fact that this result holds for *every n*. We remark that asymptotically substantially better bounds can be proved: for large n, $|G|<n^{\sqrt{n}}$ [6] using the classification of finite simple groups and $|G|<n^{4\sqrt{n}\log n}$ by elementary combinatorial arguments [1], [2]. These results imply the asymptotic bound $h(n)=O(n)$ but do not yield an effective constant. Praeger and Saxl claim [16] that their bound holds for *every n*. The proof given in [16] works for $n>12000$. It is stated in [16] that refined estimates and, for $n<3000$, elementary but somewhat tedious computations prove the bound for every n.

Proof of Lemma 5. Let G be a primitive permutation group of degree n, not containing A_n. Suppose $h(G)=q(n)$. Let

$$|G|=2^r\prod_{i=1}^{t}p_i^{s_i} < 4^n \tag{6}$$

where the p_i are different odd primes.

As G is a subgroup of S_n, the term 2^r divides $n!$ and therefore

$$r\leq n-1. \tag{7}$$

Obviously,

$$q(n)=h(G)\leq r+\sum_{i=1}^{t}s_i. \tag{8}$$

Assume, by way of contradiction, that

$$r+\sum_{i=1}^{t} s_i \geq 2n-4. \tag{9}$$

On the other hand, taking the logarithm of both sides of (6) we obtain

$$r+\sum_{i=1}^{t} s_i \log_2 p_i < 2n. \tag{10}$$

Subtracting (9) from (10) we find

$$\sum_{i=1}^{t} s_i(\log_2 p_i-1) < 4. \tag{11}$$

Consequently

$$\sum_{i=1}^{t} s_i < 4/(\log_2 3-1) < 7, \tag{12}$$

and therefore

$$\sum_{i=1}^{t} s_i \leq 6. \tag{13}$$

This, combined with (7) and (8), yields

$$q(n) \leq r+6 \leq n+5. \tag{14}$$

This completes the proof of the Lemma for $n \geq 10$.

Let $u(n)$ denote the total number of prime divisors of n. (Thus $u(2^r)=r$, for example.)

Clearly, $q(n)<u(n!)$. It is easy to check that for $5 \leq n \leq 15$, the inequality $u(n!) \leq 2n-5$ holds. This is more than enough to prove the Lemma for $5 \leq n \leq 9$. Finally, the Lemma holds vacuously for $n \leq 4$ ($q(n)=-\infty$). ∎

4. Proof of the Theorem.

Let $a(n)=h(A_n)$. By Lemma 1, $a(n)=h(n)-1$ for $n \geq 2$.

Let $m=a(n)$ and let

$$A_n = G_0 > G_1 > \cdots > G_m = 1 \tag{15}$$

be a subgroup chain of maximum length.

If G_1 is *intransitive*, let Δ be one of its orbits. Let $|\Delta| = k$. By restriction to Δ we obtain a homomorphism $G_1 \to S_k$; let H denote the preimage of A_k under this homomorphism. Clearly, $[G_1:H] \leq 2$. Therefore

$$a(n)-1 = m-1 = h(G_1) \leq 1 + h(H) \leq 1 + a(k) + a(n-k). \tag{16}$$

Consequently in this case

$$h(n) \leq 1 + h(k) + h(n-k). \tag{17}$$

The above argument proves (17) for $2 \leq k \leq n-2$ only (because $a(1) \neq h(1)-1$). But (17) will trivially hold for $k=1$ and $k=n-1$ as well because $h(1)=0$ and in these cases we have $G_1 = A_{n-1}$ and therefore $a(n) = 1 + a(n-1)$.

If G_1 is transitive but *imprimitive*, let k be the number of blocks in a system of nontrivial blocks $(2 \leq k \leq n/2)$. The action on the blocks defines a homomorphism $G_1 \to S_k$; let N be the kernel of this homomorphism. The factor group $H = G_1/N$ is a subgroup of S_k and N itself is a *proper* subgroup of $S_{n/k} \times \cdots \times S_{n/k}$ (because $N \leq A_n$). By Lemma 1 we obtain

$$a(n)-1 = m-1 = h(H) + h(N) \leq h(k) + kh(n/k) - 1. \tag{18}$$

Consequently,

$$h(n) \leq 1 + h(k) + kh(n/k) \tag{19}$$

in this case.

Finally, if G_1 is *primitive*, then $a(n)-1 \leq q(n)$ and therefore, by Lemma 5,

$$h(n) \leq q(n) + 2 \leq 2n-3. \tag{20}$$

Using (17), (19) and (20), the inequality $h(n) \leq 2n-3$ $(n \geq 2)$ can now be proved by an easy induction. ∎

References

[1] L. Babai, On the order of uniprimitive permutation groups, Annals of Math. 113 (1981), 553-568

[2] L. Babai, On the order of doubly transitive permutation groups, Invent. Math. 65 (1982), 473-484

[3] L. Babai, W. M. Kantor and E. M. Luks, Computational complexity and the classification of finite simple groups, in: Proc. 24th IEEE Symp. Found. Computer Science, Tucson AZ 1983, 162-171

[4] G. Butler, private communication

[5] G. Butler and J. McKay, The transitive groups of degree up to eleven, Comm. in Algebra 11 (1983), 863-911

[6] P. J. Cameron, Finite permutation groups and finite simple groups, Bull. London Math. Soc. 13 (1981), 1-22

[7] J. Fischer and J. McKay, The nonabelian simple groups G, $|G|<10^6$ - maximal subgroups, Math. Comp. 32 (1978), 1293-1302

[8] M. L. Furst, J. Hopcroft and E.M.Luks, Polynomial time algorithms for permutation groups, 21st IEEE Symp. Found. Comp. Sci.(1980), 36-41

[9] M. Jerrum, A compact representation for permutation groups, in: Proc. 23rd IEEE Symp. on Foundations of Comp. Sci., Chicago 1982, 126-133; final version: Journal of Algorithms 7 (1986)

[10] W. M. Kantor, Polynomial time algorithms for finding elements of prime order and Sylow subgroups, Journal of Algorithms 6 (1985)

[11] W. M. Kantor, Sylow's theorem in polynomial time, J.Computer and Systems Sci. 30 (1985) 359-394

[12] W. M. Kantor and D. E. Taylor, Polynomial time versions of Sylow's theorem, Journal of Algorithms 7 (1986)

[13] D. E. Knuth, Notes on efficient representation of perm groups, unpublished notes, 1980

[14] E. M. Luks, Isomorphism of graphs of bounded valence can be tested in polynomial time, J. Computer and Systems Sci. 25 (1982), 42-65

[15] E. M. Luks, Testing simplicity of permutation groups, in preparation

[16] C. E. Praeger and Jan Saxl, On the order of primitive permutation groups, Bull. London Math. Soc. 12 (1980), 303-307

[17] C. C. Sims, Computational methods in the study of permutation groups, in: Computational problems in abstract algebra, J. Leech ed., Pergamon Press, 1970

[18] C. C. Sims, Some group-theoretic algorithms, Springer Lect. Notes in Math. 697 (1978), 108-124

[19] H. Wielandt, Finite permutation groups, Acad. Press 1964

[20] H. Wielandt, Permutation groups through invariant relations, Lecture Notes, Ohio State University, 1969

Received: June 1985