MATHEMATICS OF COMPUTATION
VOLUME 64, NUMBER 209
JANUARY 1995, PAGES 407–410

THE LARGEST PRIME DIVIDING THE MAXIMAL ORDER OF AN ELEMENT OF S_n

JON GRANTHAM

ABSTRACT. We define $g(n)$ to be the maximal order of an element of the symmetric group on n elements. Results about the prime factorization of $g(n)$ allow a reduction of the upper bound on the largest prime divisor of $g(n)$ to $1.328\sqrt{n \log n}$.

Let S_n be the symmetric group on n letters.

Definition. $g(n) = \max\{\operatorname{ord}(\sigma) \mid \sigma \in S_n\}$.

The first work on $g(n)$ was done by Landau [1] in 1903. He showed that $\log g(n) \sim \sqrt{n \log n}$ as $n \to \infty$. In 1984, Massias [2] showed an upper bound for $\frac{\log g(n)}{\sqrt{n \log n}}$,

$$\log g(n) \leq a\sqrt{n \log n} \qquad a = 1.05313\ldots, \qquad n \geq 1,$$

with a attained for $n = 1, 319, 166$.

Let $P(g(n))$ be the largest prime divisor of $g(n)$. In 1968, Nicolas [4] proved that $P(g(n)) \sim \sqrt{n \log n}$ as $n \to \infty$. In 1989, Massias, Nicolas, and Robin [3] showed that $P(g(n)) \leq 2.86\sqrt{n \log n}$, $n \geq 2$. They conjectured that $\frac{P(g(n))}{\sqrt{n \log n}}$ achieves a maximum ($1.265\ldots$) for $n \geq 5$ at $n = 215$, with $P(g(215)) = 43$. They note that improving this bound using the techniques of their proof would require "very extensive computation," and even then would not reduce the constant in the bound below 2.

Using different techniques, however, we can improve this result to the following

Theorem. *For each integer $n \geq 5$, we have*

$$P(g(n)) \leq 1.328\sqrt{n \log n}.$$

Our proof begins with the simple observation that

$$g(n) = \max\{\operatorname{ord}(\sigma) \mid \sigma \in S'_n\},$$

where S'_n is the subset of S_n consisting of elements that are the product of disjoint cycles of prime power length.

Received by the editor January 7, 1992 and, in revised form, March 17, 1994.
1991 *Mathematics Subject Classification.* Primary 20B40.
A portion of this research, including the computations, was done at the Supercomputing Research Center. The author would also like to thank the referee for helpful suggestions.

0025-5718/95 \$1.00 + \$.25 per page

To see this, recall the fact that we can write any $\sigma \in S_n$ as the product of disjoint cycles. Then $\mathrm{ord}(\sigma)$ is the least common multiple of the cycle lengths. Consider a cycle of length ab with $(a, b) = 1$, $a, b > 1$. The product of a cycle of length a with one of length b also has order ab and is a permutation on fewer elements. Thus, given any element of S_n, we may find another that has the same order and is a product of disjoint cycles of prime power length.

Definition. For each natural number M, let $l(M) = \sum_{p^\alpha \| M} p^\alpha$.

We observe that $l(M)$ is the shortest length of a permutation of order M. Thus, we can characterize $g(n)$ in terms of l as follows:

$$g(n) = \max\{M \mid l(M) \le n\}.$$

In particular, $l(g(n)) \le n$.

Nicolas [6] describes an algorithm for computing $g(n)$. Employing a variation of this algorithm, I computed exact values of $g(n)$ for $n \le 500,000$ on a Sun 4/390. The accuracy of the computation was checked by calculating values of $g(n)$ using the set G described in [3] and verifying that they matched those in the computations. Analysis of the computations confirmed that for $5 \le n \le 500,000$, $\frac{P(g(n))}{\sqrt{n \log n}}$ attains a maximum at $n = 215$.

Lemma 1 (Nicolas [5]). *Let p, p', and q be distinct primes, with $q \ge p + p'$. If q divides $g(n)$, then at least one of p and p' divides $g(n)$.*

Proof. Suppose p and p' are primes not dividing $g(n)$. Assume there is a prime $q \ge p + p'$ with $q \mid g(n)$. Without loss of generality, $p < p'$. Choose k such that

$$p^k + p' \le q \le p^{k+1} + p' - 1.$$

Let $M = \frac{p^k p' g(n)}{q}$. Since $q \mid g(n)$, M is an integer. Then

$$l(M) \le l(g(n)) + (p^k + p' - q) \le l(g(n)) \le n.$$

Thus, an element of order M can be written as a permutation on n letters. Also,

$$\begin{aligned} p^k p' - q &\ge p^k p' - p^{k+1} - p' + 1 = p^k(p' - p) - p' + 1 \\ &\ge p(p' - p) - p' + 1 = (p-1)(p' - p - 1) \ge 0. \end{aligned}$$

Therefore, $p^k p' > q$, so $M > g(n)$. But $g(n)$ is the maximal order of a permutation on n letters. Thus, we have a contradiction, and the lemma is proven. □

Write $q = P(g(n))$. We immediately get the following

Corollary. *At most one prime less than $\frac{q}{2}$ fails to divide $g(n)$.*

Lemma 2. *Suppose $0 < \alpha < \beta < 1$. If at least one prime in the interval $(\alpha q, \beta q)$ divides $g(n)$, then at most one prime in the interval $(\sqrt{\beta} q, \frac{(1+\alpha)q}{2})$ fails to divide $g(n)$.*

Proof. If two primes in the interval $(\sqrt{\beta} q, \frac{(1+\alpha)q}{2})$ fail to divide $g(n)$, call them p and p'. Let q' be a prime in the interval $(\alpha q, \beta q)$ dividing $g(n)$. Let $M = \frac{pp'}{qq'} g(n)$. Then

$$l(M) \le p + p' - q - q' + l(g(n)) \le (1+\alpha)q - q - \alpha q + l(g(n)) = l(g(n)).$$

But $pp' - qq' > (\sqrt{\beta}q)^2 - q(\beta q) = 0$, so $M > g(n)$, giving a contradiction. $\square$

Proof of Theorem. By the computations, we may take $n > 500{,}000$. We may also assume $q \geq 1.3\sqrt{500000 \log 500000} > 3329$. Using the results of Schoenfeld [8] for large q, and computations for small $q > 3329$, we see that there are always at least two primes in the intervals $(\alpha_i q, \beta_i q)$, with $\alpha_1 = .2426$, $\beta_1 = .25$, $\alpha_2 = .3746$, $\beta_2 = .386$, $\alpha_3 = .4632$, $\beta_3 = .4723$, $\alpha_4 = .5248$, $\beta_4 = .5352$, $\alpha_5 = .57$, $\beta_5 = .5812$, $\alpha_6 = .6044$, $\beta_6 = .6162$, $\alpha_7 = .6312$, $\beta_7 = .6435$, $\alpha_8 = .6534$, $\beta_8 = .6652$, and $\alpha_9 = .6714$, $\beta_9 = .6834$. By Lemma 1, at most one of the two or more primes in any of the first three intervals fails to divide $g(n)$. Applying Lemma 2, we get that at most one prime in each interval $(\sqrt{\beta_i}q, \frac{(1+\alpha_i)q}{2})$ fails to divide $g(n)$, for $i \leq 3$. This fact in turn implies that at most one prime in each interval $(\alpha_i q, \beta_i q)$ fails to divide $g(n)$ for $4 \leq i \leq 9$. Applying Lemma 2 again, we see that at most one prime in each interval $(\sqrt{\beta_i}q, \frac{(1+\alpha_i)q}{2})$ fails to divide $g(n)$ for $1 \leq i \leq 9$.

We note that these intervals cover $(.5q, .8357q)$. So at most ten primes less than $.8357q$ fail to divide $g(n)$, and they can be at most $\frac{q}{2}$, $\frac{(1+\alpha_1)q}{2}$, ..., and $\frac{(1+\alpha_9)q}{2}$.

Therefore,

$$g(n) \geq \frac{q \prod_{p \leq .8357q} p}{\frac{q}{2} \prod \frac{1+\alpha_i}{2} q}.$$

Taking logarithms, we get

$$\log g(n) \geq \theta(.8357q) - \log\frac{1}{2} - \sum \log\left(\frac{1+\alpha_i}{2}q\right),$$

where θ is the Chebyshev function, $\theta(x) = \sum_{p \leq x} \log p$.

For $q > 3329$ the sum of the last two terms on the right is less than $.01338q$, so

$$\log g(n) \geq \theta(.8357q) - .01338q.$$

Using the estimates for $\theta(x)$ in [7], we get

$$\log g(n) \geq .79307q.$$

From [3], $1.05314\sqrt{n \log n} \geq \log g(n)$, so

$$1.328\sqrt{n \log n} \geq \frac{1.05314}{.79307}\sqrt{n \log n} \geq q.$$

It is likely that further computation would be able to show that $\frac{P(g(n))}{\sqrt{n \log n}}$ attains a maximum at $n = 215$ for **all** $n \geq 5$.

Bibliography

1. E. Landau, *Über die Maximalordnung der Permutationen gegebenen Grades*, Archiv der Math. und Phys. (1903), 92–103.

2. J.-P. Massias, *Majoration explicite de l'ordre maximum d'un élément du groupe symétrique*, Ann. Fac. Sci. Toulouse Math. **6** (1984), 269–280.

3. J.-P. Massias, J.-L. Nicolas, and G. Robin, *Effective bounds for the maximal order of an element in the symmetric group*, Math. Comp. **53** (1989), 665–678.

4. J.-L. Nicolas, *Sur l'ordre maximum d'un élément dans le groupe S_n des permutations*, Acta Arith. **14** (1968), 315–332.
5. ——, *Ordre maximal d'un élément du groupe des permutations et "highly composite numbers"*, Bull. Soc. Math. France **97** (1969), 129–191.
6. ——, *Calcul de l'ordre maximum d'un élément du groupe symétrique S_n*, RAIRO Ser. Rouge **3** (1969), 43–50.
7. J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.
8. L. Schoenfeld, *Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II*, Math. Comp. **30** (1976), 337–360.

Department of Mathematics, University of Georgia, Athens, Georgia 30602
E-mail address: `grantham@math.uga.edu`