TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Pages 000–000
S 0002-9947(XX)0000-0

SHORT PRESENTATIONS FOR ALTERNATING AND SYMMETRIC GROUPS

J.N. BRAY, M.D.E. CONDER, C.R. LEEDHAM-GREEN, AND E.A. O'BRIEN

ABSTRACT. We construct two kinds of presentations for the alternating and symmetric groups of degree n: the first are on two generators in which the number of relations is $O(\log n)$ and the presentation length is $O(\log^2 n)$; the second have a bounded number of generators and relations and length $O(\log n)$.

1. INTRODUCTION

A long-standing question is the existence of 'simple' presentations for the alternating and symmetric groups of degree n. Many such presentations were recorded by Coxeter and Moser in their seminal monograph [8, §§6.2-6.3], and while the term 'simple' was not well defined, the number of generators and relators certainly influenced their selections.

A question of more recent interest, motivated in part by algorithmic group theory, is the existence of 'short' presentations. In a 1984 paper, Babai and Szemerédi [3] defined the *length* of a presentation to be the number of symbols required to write down the presentation. Each generator is a single symbol, and a relator is a string of symbols, where exponents are written in binary. The length of a presentation is the number of generators plus the sum of the lengths of the relators. This definition accords well with the requirement of polynomial-time analysis of computational complexity.

In [3], Babai and Szemerédi formulated the *Short Presentation Conjecture*: there exists a constant c such that every finite simple group G has a presentation of length $O(\log^c |G|)$. One motivation for this conjecture is its application to deciding in polynomial time certain key properties of finite matrix groups, such as order and membership. We refer the reader to the survey by Babai [4] for a discussion on these and related matters. The results of Babai *et al.* [1], Hulpke & Seress [12], and Suzuki [20] establish this conjecture with $c = 2$ for all finite simple groups, with the possible exception of the Ree groups ${}^2G_2(q)$.

Perhaps the best known family of presentations for the finite symmetric groups are the presentations of Moore [14]; see also [8, 6.22]. In these, the symmetric group S_n of degree n is presented in terms of the transpositions $t_k = (k, k+1)$ for $1 \leqslant k < n$, which generate S_n and satisfy the defining relations $t_k^2 = 1$ for $1 \leqslant k < n$,

2000 *Mathematics Subject Classification.* Primary 20F05, 20B30.

This work was supported in part by the Marsden Fund of New Zealand via grant UOA 0412. We thank Bob Guralnick and Bill Kantor for discussions on this topic in 2005. We thank the referee for detailed commentary, and George Havas and Igor Pak for their feedback. We are particularly grateful to Bill Kantor for his extensive and most helpful suggestions on drafts of this paper.

and $(t_{k-1}t_k)^3 = 1$ for $1 < k < n$, and $(t_jt_k)^2 = 1$ for $1 \leqslant j < k-1 < n-1$. These are now commonly known as *Coxeter relations* for S_n, because of their analogues in other contexts. For $n > 1$ the number of these relations is $n(n-1)/2$, and since each relator has bounded length, the presentation length is $O(n^2)$. By using a single transposition and an n-cycle as generators, Moore derived a shorter presentation of length $O(n \log n)$. By introducing powers of the n-cycle as (redundant) additional generators, one can readily obtain a presentation for S_n with $\lfloor n/2 \rfloor + 1$ generators, $2\lfloor n/2 \rfloor + 2$ relations, and length $O(n)$.

We now describe the main results of this paper. In Section 2 we introduce methods of 'gluing' together presentations for S_m and S_n to produce presentations for S_{m+n-1} and S_{m+n}, which are then used to prove the the following.

Theorem 1.1. *For every integer $n > 1$, the symmetric group S_n has a presentation on the generators $(1, 2)$ and $(1, 2, \ldots, n)$ in which the number of relations is $O(\log n)$ and the presentation length is $O(\log^2 n)$.*

In Section 3 we adapt these methods to construct presentations for S_n with a uniformly bounded number of generators and relations and length $O(\log n)$. Note that $O(\log n)$ is the best possible, since merely specifying the integer n needs $\Omega(\log n)$ bits. We use presentations for 2-dimensional projective linear groups to produce presentations for S_{p+q+2} for odd primes p and q, and then apply (proven) variants of the Goldbach conjecture.

Before proceeding, we define some notation in order to ease exposition. If $P = \{X \mid \mathcal{R}\}$ is a presentation, then $d(P)$ and $r(P)$ denote the cardinalities of X and $\mathcal{R}$ respectively, and $\ell(P)$ is the length of P. The *standard generators* for S_n are the transposition $(1, 2)$ and the n-cycle $(1, 2, \ldots, n)$. Note that $(1, 2)$ can be replaced by any transposition $(k, k+1)$ for $1 \leqslant k < n$, and that the choice of k is irrelevant, since conjugation by $(1, 2, \ldots, n)$ is equivalent to the obvious cyclic relabelling of the points. A presentation for S_n whose generating set contains the standard generators is called *special*. Special presentations can be particularly helpful in the constructive recognition of linear groups.

Our main theorem in Section 3 is the following.

Theorem 1.2. *For every integer $n > 1$, the symmetric group S_n has a special presentation P of length $O(\log n)$ with a uniformly bounded number of generators and relations. In particular, if n is even and $n-2$ is the sum of two odd primes, then $d(P) \leqslant 6$ and $r(P) \leqslant 24$, while if n is odd and $n-3$ is the sum of two odd primes, then $d(P) \leqslant 7$ and $r(P) \leqslant 28$; for all other values of n, $d(P) \leqslant 15$ and $r(P) \leqslant 82$.*

Note that $O(\log n)$ is the best possible presentation length, since merely specifying the integer n needs $\Omega(\log n)$ bits.

We are left with one outstanding question: Does S_n have a bounded presentation of length $O(\log n)$ on its standard generators?

By a theorem of Babai, Kantor and Lubotzky [2], the diameter of the Cayley graph for S_n on the standard generators is $\Theta(n^2)$. Hence if each non-standard generator in a special presentation is replaced by a word in the standard generators, then the length of every relator is multiplied by at most n^2. Theorem 1.2 now implies that S_n has a bounded presentation of length $O(n^2 \log n)$ on its standard generators. By exploiting the ideas used in the proof of Theorem 1.2 and a short presentation for $\mathrm{PGL}(2,p)$ given in [8, §7.5], we can reduce the length to $O(n^2)$. Whether or not there is a shorter one is an open question.

Our presentations for S_n give rise to presentations for the alternating group A_n with similar characteristics, as we explain in Section 4. In particular, we have the following consequence of Theorems 1.1 and 1.2.

Theorem 1.3. *For every integer $n > 2$, the alternating group A_n has:*

(a) *a 2-generator presentation with $O(\log n)$ relations and length $O(\log^2 n)$;*
(b) *a presentation of length $O(\log n)$ with a uniformly bounded number of generators and relations;*
(c) *a 2-generator presentation with a uniformly bounded number of relations.*

Theorem 1.3(c) provides a positive answer to a question of Campbell *et al.* [7] about the existence of a 2-generator presentation for A_n with a bounded number of relators.

A weaker version of some of these results was announced in 2004; see [15], where our original motivation is also described — namely the challenge of finding short presentations for groups of Lie type on specific generating sets. In particular, our presentations for A_n and S_n can be used in conjunction with the algorithms of Beals *et al.* [5] to verify constructive recognition of black-box representations of these groups.

Simultaneously, and independent of our work, Guralnick, Kantor, Kassabov and Lubotzky obtained similar but stronger results about short presentations of A_n and S_n with a bounded number of generators and relations.

In [10] they use a more refined definition of presentation length, namely the number of generators plus the sum of the lengths of the relators as words in the corresponding free group (see [18, pp. 190–191]), and obtain a result which is optimal for that metric. They also exploit properties of $\mathrm{PSL}(2,p)$, but in other respects their approach is substantially simpler; for example, instead of the Goldbach conjecture, they use Bertrand's Postulate (proved by Chebyshev in 1850).

In a major extension, they use their presentations for A_n and S_n to prove that every nonabelian finite simple group of rank r over $\mathrm{GF}(q)$, with the possible exception of the Ree groups ${}^2G_2(q)$, has a presentation with a bounded number of generators and relations and total length $O(\log r + \log q)$; again this result is optimal. In a more recent paper [11], they show that both A_n and S_n have presentations with 3 generators, 7 relators, and length $O(\log n)$.

After we completed this work we learned from Bill Kantor about a 1972 construction by Sass [17] of a short presentation for A_{p+2} for prime p. This could be used to obtain similar results.

2. Building presentations for S_{m+n} from S_m and S_n

We first introduce simple constructions to build special presentations for S_{m+n-1} and S_{m+n} from special presentations for S_m and S_n. The key idea is to 'glue' the presentations together using a single transposition.

Lemma 2.1. *Given special presentations P_m and P_n for the symmetric groups S_m and S_n of degrees $m, n \geqslant 3$, there exist special presentations P_{m+n-1} and P_{m+n} for*

S_{m+n-1} and S_{m+n}, respectively, such that:

$$\begin{array}{rclrcl} d(P_{m+n-1}) & \leqslant & d(P_m)+d(P_n)+1, & d(P_{m+n}) & \leqslant & d(P_m)+d(P_n)+2, \\ r(P_{m+n-1}) & \leqslant & r(P_m)+r(P_n)+8, & r(P_{m+n}) & \leqslant & r(P_m)+r(P_n)+12, \\ \ell(P_{m+n-1}) & \leqslant & \ell(P_m)+\ell(P_n)+O(1), & \ell(P_{m+n}) & \leqslant & \ell(P_m)+\ell(P_n)+O(1). \end{array}$$

Moreover, if $d(P_m) = d(P_n) = 2$ then in each case the resulting presentation can be simplified to one on the two standard generators, with at most $r(P_m) + r(P_n) + 12$ relations, and length $\ell(P_m) + \ell(P_n) + O(\log m + \log n)$.

Proof. Let $P_m = \{A \,|\, \mathcal{R}\}$ and $P_n = \{B \,|\, \mathcal{S}\}$, with (a, v) and (b, w) standing for the standard generators of S_m and S_n. We first show that

$$\begin{aligned} P_{m+n} = \{\, A, B, t, y \,|\, & \mathcal{R}, \mathcal{S}, t^2, (at)^3, (tb)^3, [a, b], [a, w], [v, b], [v, w], \\ & [av, t], [vav^{-1}, t], [t, wb], [t, w^{-1}bw], y^{-1}wtv \,\} \end{aligned}$$

is a special presentation for S_{m+n}.

Let G be the group defined by this presentation, and observe that there exists an epimorphism $\theta\colon G \to S_{m+n}$ under which

$$\begin{array}{rclrcl} a & \mapsto & (m{-}1, m), & v & \mapsto & (1, 2, \dots, m), \\ b & \mapsto & (m{+}1, m{+}2), & w & \mapsto & (m{+}1, m{+}2, \dots, m{+}n), \\ t & \mapsto & (m, m{+}1), & y & \mapsto & (1, 2, \dots, m, m{+}1, m{+}2, \dots, m{+}n). \end{array}$$

Now in G, define $t_{m-1} = a$ and $t_{m-i-1} = v^i a v^{-i}$ for $1 \leqslant i \leqslant m-2$, and also $t_m = t$, and $t_{m+1} = b$ and $t_{m+i+1} = w^{-i} b w^i$ for $1 \leqslant i \leqslant n-2$.

By the choice of a and v, the elements t_i for $1 \leqslant i < m$ generate a subgroup isomorphic to S_m and hence satisfy the Coxeter relations for S_m, and similarly, the elements t_{m+i} for $1 \leqslant i < n$ satisfy the Coxeter relations for S_n. Also the relations $(at)^3 = (tb)^3 = 1$ imply that $(t_i t_{i+1})^3 = 1$ for $1 \leqslant i \leqslant m+n-2$.

Next, we show that $[t_j, t_k] = (t_j t_k)^2 = 1$ whenever $1 \leqslant j < k-1 < m+n-1$. If $j < k < m$ or $m < j < k$, then this follows from the presentation P_m or P_n, respectively; if $j < m < k$, then it follows from the four relations $[a, b] = [a, w] = [v, b] = [v, w] = 1$, as these imply that $\langle a, v\rangle$ commutes with $\langle b, w\rangle$. The elements av and vav^{-1} generate a subgroup of index m in $\langle a, v\rangle \cong S_m$ containing the involutions $t_1, t_2, \dots, t_{m-2}$, and wb and $w^{-1}bw$ generate a subgroup of index n in $\langle b, w\rangle \cong S_n$ containing $t_{m+2}, t_{m+3}, \dots, t_{m+n-1}$. Accordingly, the four relations $[av, t] = [vav^{-1}, t] = [t, wb] = [t, w^{-1}bw] = 1$ imply that t centralises $\langle t_1, t_2, \dots, t_{m-2}\rangle$ and $\langle t_{m+2}, t_{m+3}, \dots, t_{m+n-1}\rangle$, and so we obtain also $[t_j, t_m] = 1$ for $1 \leqslant j \leqslant m-2$ and $[t_m, t_k] = 1$ for $m+2 \leqslant k \leqslant m+n-1$.

Hence the $m+n-1$ involutions t_i generate a subgroup satisfying the Coxeter relations for S_{m+n}. The relations in P_m and P_n imply that each of the elements of A or B is expressible as a word in these t_i, and the relation $y^{-1}wtv = 1$ then implies the same for y, and therefore the involutions t_i generate G. Thus G is isomorphic to S_{m+n}, and the rest follows easily, by observing that $a = yty^{-1}$, $v = (yt)^{m-1}y^{-(m-1)}$, $b = y^{-1}ty$ and $w = y^{-(n-1)}(ty)^{n-1}$.

A similar construction without the gluing transposition gives the following special presentation for S_{m+n-1} with the required properties:

$$\begin{aligned} P_{m+n-1} = \{\, A, B, y \,|\, & \mathcal{R}, \mathcal{S}, (ab)^3, [a, wb], [a, w^{-1}bw], [v, wb], [v, w^{-1}bw], \\ & [av, b], [vav^{-1}, b], y^{-1}wv \,\}. \end{aligned}$$

□

As a basis for induction, the constructions used in Lemma 2.1 are not the best possible, since doubling the degree roughly doubles both the number of relations and the presentation length. Taking $m = n$, however, we can express one copy of S_n as a conjugate of another and obtain the following.

Lemma 2.2. *Given a special presentation P_n for S_n where $n \geqslant 3$, there exists a special presentation Q_{2n} for S_{2n} with $d(Q_{2n}) \leqslant d(P_n) + 1$, $r(Q_{2n}) \leqslant r(P_n) + 6$, and $\ell(Q_{2n}) \leqslant \ell(P_n) + O(1)$. Moreover, if $d(P_n) = 2$ then Q_{2n} can be simplified to one on the two standard generators, with at most $r(P_n) + 6$ relations, and length $\ell(P_n) + O(\log n)$.*

Proof. As in the proof of Lemma 2.1, one can show that if x, w stand for the standard generators of S_n in P_n, then

$$\{\, A, y \mid \mathcal{R}, y^{2n}, (xy)^{2n-1}, [x, wy^{-1}], [w^2xw^{-1}, wy^{-1}], [x, y^n]^2, [x, y^{n-1}]^2 \,\}$$

is a special presentation for S_{2n}, with y standing for the $2n$-cycle $(1, 2, \ldots, 2n)$. In particular, $w = y^{-(n-1)}(yx)^{n-1}$ (since this relation is satisfied by the corresponding elements in S_{2n}), and the final assertion follows. □

Theorem 1.1 now follows from Lemma 2.2 and its obvious analogue for S_{2n-1}.

3. Short presentations for S_n with a bounded number of relations

As a first step in this section, we give a variant of our ‘gluing’ constructions.

Lemma 3.1. *Let $P = \{A, t \mid \mathcal{R}\}$ and $Q = \{B, t \mid \mathcal{S}\}$ be presentations for S_{m+1} and S_{n+1}, with $m, n \geqslant 1$, such that the generator t stands for a transposition in both cases. Let M and N be sets of words on the sets $A \cup \{t\}$ and $B \cup \{t\}$ standing for generators of the natural subgroups S_m and S_n fixing a point moved by t, respectively, and let $[M, N]$ denote the set of all commutators $[u, v]$ with $u \in M$ and $v \in N$. Then $\{\, A, B, t \mid \mathcal{R}, \mathcal{S}, [M, N] \,\}$ is a presentation for S_{m+n}, again with the generator t standing for a transposition. If y and z stand for an $(m{+}1)$-cycle in S_{m+1} and an $(n{+}1)$-cycle in S_{n+1}, respectively, then zyt stands for an $(m{+}n)$-cycle in S_{m+n}.*

Proof. Observe that there is a natural homomorphism from the group G with the given presentation onto S_{m+n} under which the subgroups generated by M and N map to $\mathrm{Sym}(\{1, \ldots, m\})$ and $\mathrm{Sym}(\{m{+}1, \ldots, m{+}n\})$, respectively, and t maps to the transposition $(m, m{+}1)$.

Choose m generators $a_1, a_2, \ldots, a_m$ for $\langle M, t\rangle = \langle A, t\rangle \cong S_{m+1}$ that satisfy the Moore presentation for S_{m+1}, with $\langle a_1, \ldots, a_{m-1}\rangle = \langle M\rangle$ and $a_m = t$; similarly, choose n generators $b_1, b_2, \ldots, b_n$ for $\langle N, t\rangle = \langle B, t\rangle \cong S_{n+1}$ that satisfy the Moore presentation for S_{n+1}, with $b_1 = t$ and $\langle b_2, \ldots, b_n\rangle = \langle N\rangle$. Also define $a_{m+j-1} = b_j$ for $1 < j \leqslant n$, and let $S = \{a_1, \ldots, a_{m+n-1}\}$, a set of involutory generators for $\langle M, t, N\rangle = \langle A, t, B\rangle = G$.

Now consider a Coxeter relation $(a_ia_j)^{m_{ij}} = 1$. If $1 \leqslant i \leqslant j \leqslant m$ then this holds in $\langle M, t\rangle$, or if $m \leqslant i \leqslant j \leqslant m{+}n{-}1$ then it holds in $\langle N, t\rangle$, and otherwise, if $1 \leqslant i < m < j$ then it holds since $a_i \in M$ commutes with $a_j \in N$. Thus $G = \langle S\rangle \cong S_{m+n}$. Finally, if y and z are elements of G standing for the $(m{+}1)$-cycle $(1, 2, \ldots, m{+}1)$ and the $(n{+}1)$-cycle $(m, m{+}1, \ldots, m{+}n)$, respectively, then zty stands for the $(m{+}n)$-cycle $(1, 2, \ldots, m{+}n)$. □

Corollary 3.2. Let $P = \{A, t \mid \mathcal{R}\}$ be a presentation for S_{m+1}, such that the generator t stands for a transposition, and let a and c be words on the set $A \cup \{t\}$ standing for generators of the natural subgroup S_m fixing a point moved by t. Then $\{\, A, b, t \mid \mathcal{R}, b^2, (bt)^3, [a, b], [c, b] \,\}$ is a presentation for S_{m+2}, with the generators b and t standing for transpositions. This presentation has $|A| + 2$ generators, $|\mathcal{R}| + 4$ relations, and length $\ell(P) + O(1)$. An element standing for an $(m{+}2)$-cycle in S_{m+2} can be expressed in the form yb, where y stands for an $(m{+}1)$-cycle in S_{m+1}.

Proof. Take $n = 2$, $B = N = \{b\}$ and $M = \{a, c\}$ in Lemma 3.1. □

We next recall two facts which we will use to construct a special presentation of length $O(\log p)$ for S_{p+2}, when p is an odd prime.

Proposition 3.3 (Sunday [19]). Let p be an odd prime. Then $\mathrm{PSL}(2, p)$ has presentation $\{\, a, c \mid a^p, acacac^{-1}, (a^{(p+1)/2}ca^4c)^2 \,\}$, of length $O(\log p)$, where the generators a and c may be taken as standing respectively for the linear fractional transformations $z \mapsto z{+}1$ and $z \mapsto -1/z$.

Proposition 3.4 (Burnside [6] and Miller [13]). If $n \geqslant 3$ then S_{n+1} has presentation $\{\, a_1, a_2, \ldots, a_n \mid a_i^2, (a_ia_j)^3, (a_ia_ja_ia_k)^2$ *for all distinct* $i, j, k \,\}$, with generator a_i standing for the transposition $(i, n + 1)$ for $1 \leqslant i \leqslant n$.

In the latter, it suffices to use for each unordered triple $\{i, j, k\}$ just one relation of the form $(a_ia_ja_ia_k)^2$, because the relator $(a_ia_ja_ia_k)^2$ is conjugate to $(a_ia_ka_ia_j)^2$, and equivalent to $(a_ja_ia_ja_k)^2$ since $(a_ia_j)^3 = 1$.

Theorem 3.5. *Let p be an odd prime, and let λ be a primitive element of* $\mathrm{GF}(p)$, *with inverse μ. Then*

$$\begin{aligned}\{\, a, c, t \;\mid\; & a^p,\ acacac^{-1},\ (a^{(p+1)/2}ca^4c)^2,\\ & t^2,\ [t, a],\ [t, ca^\lambda ca^\mu c],\ [t, c]^3,\ (tt^ctt^{ca})^2,\ (tt^ctt^{ca^\lambda})^2,\ (at^c)^{p+1} \,\}\end{aligned}$$

is a 3*-generator* 10*-relator presentation of length $O(\log p)$ for S_{p+2}, in which att^c stands for a $(p{+}2)$-cycle and t stands for a transposition. If $p \equiv 3 \bmod 4$, then the relator $(tt^ctt^{ca^\lambda})^2$ is redundant and just* 9 *relators are needed.*

Proof. Let G be the group with the given presentation. Then there is an epimorphism $\theta : G \to S_{p+2}$, where S_{p+2} acts on $\{\star, \infty\} \cup \mathrm{GF}(p)$, such that θ maps t to the transposition $(\star, \infty)$, and maps a and c to elements that fix $\star$ and act on the projective line $\{\infty\} \cup \mathrm{GF}(p)$ in the same way as the two transformations given in Proposition 3.3. In particular, a and c generate a subgroup H isomorphic to $\mathrm{PSL}(2, p)$, and the images of a and $ca^\lambda ca^\mu c$ generate the stabiliser in H of the points $\star$ and ∞ (and centralise t). Hence t has exactly $p{+}1$ conjugates under the action of H, say u_i for $i \in \{\infty\} \cup \mathrm{GF}(p)$, where $t = u_\infty$, and θ takes u_i to the transposition $(\star, i)$ for each i.

Now the relations $t^2 = [t, c]^3 = (tt^ctt^{ca})^2 = (tt^ctt^{ca^\lambda})^2 = 1$ give $u_\infty^2 = (u_\infty u_0)^3 = (u_\infty u_0 u_\infty u_1)^2 = (u_\infty u_0 u_\infty u_\lambda)^2 = 1$. Next, we use the facts that $\mathrm{PSL}(2, p)$ is doubly-transitive on the projective line $L = \{\infty\} \cup \mathrm{GF}(p)$, and has just two orbits on ordered triples of distinct points of L, namely the orbits of $(\infty, 0, 1)$ and $(\infty, 0, \lambda)$. These give all that is required to invoke Proposition 3.4, and so the subgroup K generated by these $p{+}1$ conjugates of t is isomorphic to S_{p+2}. Moreover, if $p \equiv 3$ mod 4, then the relator $(tt^ctt^{ca^\lambda})^2$ can be dropped because in that case $\mathrm{PSL}(2, p)$

has a single orbit on unordered triples of points of L — see the observation after Proposition 3.4.

On the other hand, the relator $(at^c)^{p+1}$ may be written as a^{p+1} times a product of conjugates of t^c, and as $a^p = 1$ it follows that a^{-1} is expressible as a product of conjugates of t^c (and hence of t). In particular, a lies in K, so all conjugates of a lie in K, and as these conjugates generate $H \cong \mathrm{PSL}(2,p)$, it follows that K contains $\langle a \rangle^H = H$, and thus $G = HK = K \cong S_{p+2}$. □

We remark that, analogously, a 3-generator 6-relator presentation of length $O(\log p)$ due to Todd [21] for $\mathrm{PGL}(2,p)$ can be used to obtain a 4-generator 12-relator presentation of length $O(\log p)$ for S_{p+2}.

Sass [17] used a presentation of Frasch [9] for $\mathrm{PSL}(2,p)$ to construct a presentation for A_{p+2} with 3 generators, at most 9 relations, and length $O(\log p)$.

Ideally, we would like to convert one of our bounded short presentations for S_{p+2} to one on its standard generators. Taking these to be $x = (\star, \infty)$ and $y = (\star, \infty, 0, 1, \ldots, p-1)$, and a, c and t as in Theorem 3.5, we have $x = t$ and $y = att^c$, and conversely $a = yxy^{-1}xy$. We cannot, however, express c as a short word in x and y, and suspect that this cannot be done.

Instead we apply Lemma 3.1 to Theorem 3.5 and obtain the following:

Theorem 3.6. *Let p and q be odd primes, and let λ and μ be primitive elements of $\mathrm{GF}(p)$ and $\mathrm{GF}(q)$, with inverses ρ and σ respectively. Then*

$$\begin{aligned} \{\, a, c, d, f, t \quad | \quad & a^p, acacac^{-1}, (a^{(p+1)/2}ca^4c)^2, d^q, dfdfdf^{-1}, (d^{(q+1)/2}fd^4f)^2, \\ & t^2, [t,a], [t, ca^\lambda ca^\rho c], [t,d], [t, fd^\mu fd^\sigma f], [t,c]^3, [t,f]^3, \\ & (tt^ctt^{ca})^2, (tt^ftt^{fd})^2, (tt^ctt^{ca^\lambda})^2, (tt^ftt^{fd^\mu})^2, (at^c)^{p+1}, (dt^f)^{q+1}, \\ & [a,d], [a,f], [c,d], [cf,t]^2 \,\} \end{aligned}$$

is a 5-generator 23-relator presentation of length $O(\log p + \log q)$ for S_{p+q+2}, in which at^ftt^cd stands for a $(p+q+2)$-cycle and t stands for a transposition. If $p \equiv 3$ mod 4 then the relator $(tt^ctt^{ca^\lambda})^2$ is redundant, and if $q \equiv 3$ mod 4 then the relator $(tt^ftt^{fd^\mu})^2$ is redundant.

Proof. Take $m = p+1$ and $n = q+1$, and $A = \{a, c\}$ and $B = \{d, f\}$, with $M = \{a, t^{ct}\}$ and $N = \{d, t^{ft}\}$. Then using Lemma 3.1, we obtain the desired presentation for S_{p+q+2}, but with the relators $[a, t^{ft}]$, $[d, t^{ct}]$ and $[t^{ct}, t^{ft}]$ in place of $[a,f]$, $[c,d]$ and $[cf,t]^2$. Since t commutes with both a and d in this group, the relations $[a,f] = 1$ and $[c,d] = 1$ imply that $[a, t^{ft}] = 1$ and $[d, t^{ct}] = 1$; further the relation $[t^{ct}, t^{ft}] = 1$ is equivalent to $1 = [t^c, t^f] = (ctcftf)^2$ and hence to $[cf,t]^2 = (fctcft)^2 = 1$. □

Proof of Theorem 1.2. Suppose n is even. If $n-2$ is the sum of two odd primes (as implied by the Goldbach conjecture), then Theorem 3.6 gives a bounded presentation of length $O(\log n)$ for S_n, in which the n-cycle $(1, 2, \ldots, n)$ can be expressed as a word of length 9 in the generators. Adding an additional generator to represent this n-cycle then gives a special presentation with the required properties. Similarly, if n is odd and $n-3$ is the sum of two odd primes, then the above argument gives a suitable presentation for S_{n-1}, to which Corollary 3.2 may be applied.

Even if the Goldbach conjecture is false, for sufficiently large n a theorem of Vinogradov [22] implies that $n-2$ or $n-3$ is expressible as a sum of three odd primes p, q, r. Theorem 3.6 then gives a 5-generator 23-relator presentation for S_{q+r+2}, which can be used with Theorem 3.5 and Lemma 3.1 to produce a presentation for $S_{p+q+r+2} = S_n$ or S_{n-1}, with $5+3-1 = 7$ generators and at most $23{+}10{+}2\times 2 = 37$ relations, and length $O(\log n)$. The appropriate long cycle is expressible as a word of length $9+1+5 = 15$ in the generators, and the rest follows easily.

Alternatively, we can resort to a theorem of Ramaré [16] which states that every even positive integer is a sum of at most six primes. We partition the primes into three pairs, use Theorem 3.5 or Theorem 3.6 as appropriate for each pair, and then apply Lemma 3.1 twice to glue the three presentations together. For even n, this gives a presentation for S_n on at most 13 generators with at most $(23{+}23{+}4){+}23{+}\,4 = 77$ relations, with the n-cycle $(1, 2, \ldots, n)$ expressible as a word of length at most $(9+1+9)+1+9 = 29$ in the generators. For odd n, again we can construct a suitable presentation for S_{n-1}, and then apply Corollary 3.2. □

4. Alternating groups

Presentations for the alternating groups A_n are obtainable easily from those for S_n, using the Reidemeister-Schreier process (as described in [18, Chapter 6]).

If P is any presentation for S_n, let E and O be the subsets of generators in P that stand for even and odd permutations in S_n, respectively. For a Schreier transversal for A_n in S_n, we may take $\{1, t\}$ where t is any one of the generators in O (such as one standing for a single transposition). The Schreier generators for A_n then consist of all elements of the form u and tut^{-1} where $v \in E$, together with all elements of the form $tv^{\pm 1}$ where $v \in O$, and the Reidemeister-Schreier relators are just those in the presentation for S_n, rewritten in terms of these Schreier generators, plus conjugates of these by the element t^{-1}.

Hence if Q is the resulting presentation for A_n, then $d(Q) \leqslant 2d(P) - 2$, $r(Q) \leqslant 2r(P)$ and $\ell(Q) \leqslant 2\ell(P)$.

If P is defined on the standard generators $x = (1, 2)$ and $y = (1, 2, \ldots, n)$, then the presentation Q for A_n is on the two n-cycles y and xyx when n is odd, or the two $(n-1)$-cycles xy and xy^{-1} when n is even. Note also that if P is a special presentation with a bounded number of generators and relations, then any non-standard generator can be eliminated by the addition of one further relation, and so P gives rise to a presentation for S_n on the standard generators, and hence to a 2-generator presentation for A_n, with a bounded number of relations.

Thus we obtain Theorem 1.3 as a consequence of Theorems 1.1 and 1.2.

References

1. L. Babai, A.J. Goodman, W.M. Kantor, E.M. Luks, and P.P. Pálfy, Short presentations for finite groups. *J. Algebra* **194** (1997), 79–112.
2. L. Babai, W.M. Kantor and A. Lubotzky, Small-diameter Cayley graphs for finite simple groups. *European J. Combin.* **10** (1989), no. 6, 507–522.
3. László Babai and Endre Szemerédi, On the complexity of matrix group problems, I. In *Proc. 25th IEEE Sympos. Foundations Comp. Sci.*, pages 229–240, 1984.
4. László Babai, Randomization in group algorithms: conceptual questions. Groups and Computation, II (New Brunswick, NJ, 1995), 1–17, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., 28, Amer. Math. Soc., Providence, RI, 1997.
5. Robert Beals, Charles R. Leedham-Green, Alice C. Niemeyer, Cheryl E. Praeger, and Ákos Seress, A black-box group algorithm for recognizing finite symmetric and alternating groups. I. *Trans. Amer. Math. Soc.* **355** (2003), 2097–2113.
6. W. Burnside, *Theory of Groups of Finite Order*, 2nd ed. Dover Publications, Inc., New York, 1955, xxiv+512 pp.

7. C.M. Campbell, G. Havas, C. Ramsay, and E.F. Robertson, Nice efficient presentations for all small simple groups and their covers. *LMS J. Comput. Math.* **7** (2004), 266–283.
8. H.S.M. Coxeter and W.O.J. Moser, *Generators and Relations for Discrete Groups*, 4th ed. Springer-Verlag (Berlin), 1980, ix+169 pp.
9. H. Frasch, Die Erzeugenden der Hauptkongruenzgruppen für Primzahlstufen. *Math. Ann.* **108**, 229–252.
10. R.M. Guralnick, W.M. Kantor, M. Kassabov and A. Lubotzky, Presentations of finite simple groups: a quantitative approach. *J. Amer. Math. Soc.* **21**, 711–774, 2008.
11. R.M. Guralnick, W.M. Kantor, M. Kassabov and A. Lubotzky, Presentations of finite simple groups: a computational approach. To appear *J. European Math. Soc.*
12. Alexander Hulpke and Ákos Seress, Short presentations for three-dimensional unitary groups. *J. Algebra*, 245:719–729, 2001.
13. G. A. Miller, Abstract definitions of all the substitution groups whose degrees do not exceed seven, *Amer. J. Math.* **33** (1911), 363–372.
14. E.H. Moore, Concerning the abstract groups of order $k!$ and $\frac{1}{2}\,k!$, *Proc. London Math. Soc.* **28** (1897), 357–366.
15. E.A. O'Brien, Towards effective algorithms for linear groups. *Finite Geometries, Groups and Computation*, (Colorado), September 2004. De Gruyter, Berlin, 163–190, 2006.
16. O. Ramaré, On Šnirelman's constant. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **22** (1995), 645–706.
17. Hartmut Sass, Eine abstrakte Definition gewisser alternierender Gruppen. *Math. Z.* **128** (1972), 109–113.
18. Charles C. Sims, *Computation with finitely presented groups.* Cambridge University Press, 1994, xiii+604 pp.
19. J.G. Sunday, Presentations of the groups $\mathrm{SL}(2,m)$ and $\mathrm{PSL}(2,m)$. *Canad. J. Math.* **24** (1972), 1129–1131.
20. Michio Suzuki, On a class of doubly transitive groups. *Ann. of Math. 2*, 75:105–145, 1962.
21. J.A. Todd, A note on the linear fractional group. *J. London Math. Soc.* **7** (1932), 195–200.
22. I.M. Vinogradov, *The method of trigonometrical sums in the theory of numbers* (Russian). *Trav. Inst. Math. Stekloff* **23** (1947). 109 pp.

School of Mathematical Sciences, Queen Mary, University of London, London E1 4NS, United Kingdom

Department of Mathematics, University of Auckland, Auckland, New Zealand

School of Mathematical Sciences, Queen Mary, University of London, London E1 4NS, United Kingdom

Department of Mathematics, University of Auckland, Auckland, New Zealand