J. Teräväinen (2022) "Almost All Alternating Groups are Invariably Generated by Two Elements of Prime Order," International Mathematics Research Notices, Vol. 00, No. 00, pp. 1–16
https://doi.org/10.1093/imrn/rnac354

Almost All Alternating Groups are Invariably Generated by Two Elements of Prime Order

Joni Teräväinen*

Department of Mathematics and Statistics, University of Turku, 20014 Turku, Finland

**Correspondence to be sent to: e-mail: joni.p.teravainen@gmail.com*

We show that for all $n \leq X$ apart from $O(X\exp(-c(\log X)^{1/2}(\log\log X)^{1/2}))$ exceptions, the alternating group A_n is invariably generated by two elements of prime order. This answers (in a quantitative form) a question of Guralnick, Shareshian, and Woodroofe.

1 Introduction

We say that a finite group G is *invariably generated* by elements $g_1,\dots,g_k$ if for any $g_1',\dots,g_k' \in G$ with g_i' belonging to the conjugacy class of g_i, we have $\langle g_1',\dots,g_k'\rangle = G$. In other words, the subset $\{g_1,\dots,g_k\}$ generates the group even if we replace each element by any of its conjugates.

Invariable generation of finite simple groups has received considerable attention. It is known that every finite simple group is invariably generated by two elements of unspecified order [1,2]. Invariable generation by a few random elements has been studied, among others, in [3–7]. The expected number of random elements required for invariable generation has been studied, for instance, in [2,8]. Dolfi *et al.* [9] asked the question: which finite simple groups are invariably generated by two elements of prime (or prime power) order?

We shall focus on invariable generation of the alternating groups A_n. For the alternating groups, Shareshian and Woodroofe [10] showed that for $n \geq 8$, a power of two, the group A_n fails to be invariably generated by two elements of prime order.

Received March 23, 2022; Revised November 18, 2022; Accepted December 4, 2022

Nevertheless, it is possible that A_n is always generated by an element of prime order together with an element of prime power order; in fact, Guralnick *et al.* [11, Section 5] recently asked this question in the following form (see also [10, Questions 1.2–1.4] and [9, Section 6]).

Question 1.1. For every $n \geq 5$, is the alternating group A_n invariably generated by an element whose order is a prime power divisor p^a of n, together with an element of prime order $r > \sqrt{n}$?

Guralnick *et al.* [11] proved that all $5 \leq n \leq 10^{15}$ have this property, which provides considerable numerical evidence for Question 1.1. Shareshian and Woodroofe [10] proved that the asymptotic lower density of such n is at least $1 - 10^{-28}$ (with $a = 1$ above).

In this paper, we prove the following almost-all result on invariable generation of the alternating groups A_n.

Theorem 1.2 (Almost all alternating groups are invariably generated by two prime order elements). There exists a constant $c > 0$ such that, for all $n \leq X$ apart from $\ll X\exp(-c(\log X)^{1/2}(\log\log X)^{1/2})$ exceptions, the alternating group A_n is invariably generated by an element of order p together with an element of order r for some primes p, r. Moreover, we may require that $p \mid n$ and $r > n/\exp(2(\log n)^{1/2}(\log\log n)^{1/2})$.

Here, and in the rest of the paper, c stands for a (very small) positive constant that is the same on every occurrence.

It was proved in [10] that under the Riemann hypothesis almost all n satisfy Question 1.1 (with $a = 1$). Guralnick *et al.* [11] state: "It would already be somewhat interesting to give a proof that does not rely on the Riemann Hypothesis that the set of counterexamples to Question 1.1 has asymptotic density 0." Theorem 1.3 achieves this, with a quantitative "quasi-polynomial" saving on the size of the exceptional set.

Theorem 1.2 will be deduced as a consequence of some group-theoretic considerations combined with the following result on products of exactly two primes in short intervals proved in Section 5.

Theorem 1.3 (Power-saving exceptional set for products of two primes in short intervals). Let $(\log X)^C \leq h \leq X^{1/10}$ for large enough $C \geq 1$. Then, for all integers $1 \leq x \leq X$ apart from $\ll Xh^{-c}$ exceptions, there exist $\geq ch/(\log X)$ products of two primes $p_1p_2 \in [x, x+h]$ with $h^{1-2c} \leq p_1 \leq h^{1-c}$.

Remark 1.4. The key aspect of Theorem 1.3 is the size of the exceptional set. By [12, Theorem 1.1] (improving on [13]), for $h = (\log X)^{2.1}$ the interval $[x, x+h]$ almost always contains products of two primes, and in fact, the exceptional set in that result is power-saving in h in the regime $(\log X)^{2.1} \leq h \leq (\log X)^C$ (i.e., one has an exceptional set of the size $\ll X/h^{c_0}$ for some constant $c_0 > 0$). However, in the complementary range $h \geq (\log X)^{\psi(X)}$ with $\psi(X)$ tending to infinity relatively rapidly, the method there does not give such a good exceptional set.

It turns out that we will need Theorem 1.3 only for $h = \exp((\log X)^{1/2}(\log\log X)^{1/2})$, but we give a proof in the larger range $(\log X)^C \leq h \leq X^{1/10}$ as it may be of independent interest.

We also remark that even under the Riemann hypothesis, we are not aware of a proof that there are $\ll Xh^{-1/2-\varepsilon}$ exceptional intervals $[x, x+h]$ with $x \leq X$ not containing a product of two primes, with $\varepsilon > 0$ fixed.

By [10, eq. (1.1)], our main theorem has the following implication for common prime divisors of binomial coefficients.

Corollary 1.5. There exists a constant $c > 0$ such that, for all $n \leq X$ apart from $\ll X\exp(-c(\log X)^{1/2}(\log\log X)^{1/2})$ exceptions, there exist two primes p_1, p_2 (depending on n) such that for each $1 \leq i \leq n-1$ at least one of p_1, p_2 divides $\binom{n}{i}$.

This improves on [10, Theorem 1.5], where it was shown that the set of exceptional $n \leq X$ has size $\leq (10^{-28} + o(1))X$. One would expect that there are no exceptional n. Let us also mention that assuming very strong information on primes in short intervals, namely Cramér's conjecture, one can show that there are $O(X^{1/2+o(1)})$ exceptional $n \leq X$ both for Corollary 1.5 and Theorem 1.2 (see [11, Subsection 4.3]).

2 Notation

The symbols p, p_i, r always stand for prime numbers.

We denote by (a, b) the greatest common divisor of two natural numbers a, b. As usual, Λ denotes the von Mangoldt function.

We use the Vinogradov asymptotic notation $A \ll B$ to denote that there exists a constant C such that $|A| \leq CB$.

In the course of the proof, we shall need maximal subgroups of A_n. The maximal subgroups H of A_n are classified into three types.

- We say that H is *intransitive* if there exist $i, j \in [n]$ such that under the natural action of H on $[n]$, we have $i \cdot h \neq j$ for all $h \in H$. Otherwise, we say that H is transitive. If H is an intransitive maximal subgroup, then H fixes some set $X \subset [n]$ with $1 \leq |X| < n$ under the action of H on $[n]$.
- We say that H is *imprimitive* if it is transitive and there is a proper partition π of $[n]$ into parts of size ≥ 2 such that the action of H on $[n]$ permutes these parts. By the maximality of H, we may assume that the parts in π all have the same size.
- We say that H is *primitive* if it is transitive but not imprimitive.

It is clear that each maximal subgroup must be of one of these three types.

3 Group-Theoretic Lemmas

The group theory part of our argument can be abstracted into similar ingredients as the arguments in [11].

Proposition 3.1. Let $n \geq 25$ be an integer. Suppose that the following hold for some primes $r > \sqrt{2n}$ and $p \mid n$ and for $t = \lfloor n/r \rfloor$.

(i) n is not a prime power.
(ii) n is not of the form $(q^d - 1)/(q - 1)$ for any integers $q \geq 2$ and $d \geq 3$.
(iii) $n - tr \geq 3$.
(iv) $(t, n) = 1$.
(v) $p \nmid ar+b$ for any integers a, b with $0 \leq a \leq t$, $0 \leq b \leq n-tr$, and $0 < ar+b < n$.

Then A_n is invariably generated by an element of order p together with an element of order r.

Proof. We may assume that $p \geq 3$, since if $p = 2$ condition (v) cannot hold. Denote $u = n - tr \in [3, r)$. Let $g_1 \in A_n$ be a product of n/p disjoint cycles of length p, and let $g_2 \in A_n$ be a product of t disjoint cycles of length r and u fixed points. Since disjoint cycles commute, g_1 has order p and g_2 has order r. Since conjugation preserves cycle structure, any conjugates of g_1, g_2 are still of the same form. Hence, it suffices to show that $\langle g_1, g_2 \rangle = A_n$.

Suppose that $\langle g_1, g_2 \rangle \neq A_n$. Let $H \neq A_n$ be the maximal subgroup of A_n that contains $\langle g_1, g_2 \rangle$. By the classification of maximal subgroups of A_n (Subsection 2), H must be either primitive, imprimitive, or intransitive.

Case 1. Suppose H is primitive. Recall that H contains g_2, which is a product of t r-cycles and u fixed points. By [11, Theorem 2.4 and Remark 2.5], this implies that one of the following holds:

- $n = \frac{q^d-1}{q-1}$ for some integers $q \geq 2$ and $d \geq 3$;
- $u \leq 2$;
- n is a prime power.

However, these are all impossible by our assumptions (i), (ii), (iii).

Case 2. Suppose H is imprimitive. Then H preserves some partition π of $[n]$ into d parts of size n/d for some $d \mid n$, $1 < d < n$. Note that the base r representation of n is $n = tr + u$. Hence, g_2 is a *base r-element*. (We say that an element $g \in A_n$ is a *base-p element* if, given the base p representation $n = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots$, the element g has α_0 fixed points and α_i cycles of length p^i for all i.) By [11, Lemma 3.6], the base r-element g_2 fixing π implies that $d \mid (t, u)$ or $n/d \mid (t, u)$. In either case, $(t, u) > 1$, so that also $(t, n) = (t, tr + u) > 1$, which contradicts our assumption (iv).

Case 3. Lastly, suppose H is intransitive. Then there is a subset $X \subset [n]$ of some size $1 < k < n$ such that H is the stabilizer of X. Now, g_1 fixing X implies that $k = pm$ for some integer m, while g_2 fixing X implies that $k = ar + b$ for some $0 \leq a \leq t$, $0 \leq b \leq u$, with $0 < ar + b < n$. But, by assumption (v), both of these cannot happen. ■

Note that Proposition 3.1 does not handle the case of prime (or prime power) n; for these, we need the following complementary lemma.

Lemma 3.2. Let $n \geq 2$. Let p, r be primes with $p \mid n$ and $r < n - 2 < n \leq r + p$. Then A_n is invariably generated by an element of order r together with an element of order p.

Proof. This follows from [11, Lemma 3.3] with $a = 1$ by taking the permutation x, there to be a product of n/p disjoint cycles of length p. ■

4 Proof of Theorem 1.2 Assuming Theorem 1.3

In this section, we prove Theorem 1.2 assuming Theorem 1.3 (which in turn is proved in Section 5). Throughout this section, let

$$h := \exp((\log X)^{1/2}(\log\log X)^{1/2}).$$

By Theorem 1.3, for all $n \leq X$ outside an admissible exceptional set, there exist $\gg h/(\log X)$ products of two primes

$$p_1 p_2 \in [n-h, n-3] \text{ with } h^{1-2c}/2 \leq p_1 \leq h^{1-c}.$$

By Proposition 3.1 (with $r = p_2$, $t = p_1$) and the union bound, it suffices to show that each of the assumptions (i)–(v) of Proposition 3.1 fails for $\ll X \exp(-c(\log X)^{1/2}(\log\log X)^{1/2})$ integers $n \leq X$. Assumption (iii) is automatically satisfied with our choices. If (i) fails, then $n = p^a$ is a prime power, and if $a = 1$, then Lemma 3.2 tells us that A_n is generated by an element of order r together with an element of order p. There are $\ll X^{1/2}$ integers $n \leq X$ of the form p^a with p prime and $a \geq 2$, so this is also an acceptable exceptional set. We are left with showing that the properties (ii), (iv), (v) are true for all but the stated number of exceptional n. The smallness of exceptions to assumptions (ii), (iv), (v) will follow from the following five lemmas.

Lemma 4.1 (Dealing with very large prime factors). Suppose that n is large enough and that $p \mid n$ for some prime $p \geq n^{0.9}$. Then, A_n is invariably generated by an element of order p together with an element of prime order $r > n/2$.

Proof. By the prime number theorem in short intervals (one could replace the exponent 0.9 here by 0.525 by [14], but the above suffices for our purposes), there is a prime $r \in (n - n^{0.9}, n-3] \subset (n-p, n-3]$ for all $n \geq N_0$. Hence, the claim follows from Lemma 3.2. ■

Lemma 4.2 (Exceptions to assumption (ii)). The number of $n \leq X$ that are of the form $(q^d - 1)/(q-1)$ with $q \geq 2$ and $d \geq 3$ is $\ll \sqrt{X}$.

Proof. The number of $n \leq X$ of the form $(q^3-1)/(q-1) = 1 + q + q^2$ is trivially $\ll \sqrt{X}$. Similarly, for any $d \geq 4$, the number of n of the form $(q^d-1)/(q-1)$ is $\ll X^{1/(d-1)} \ll X^{1/3}$. Since necessarily $d \leq (\log X)/(\log 2)$, the claim follows. ■

Lemma 4.3 (Exceptions to assumption (iv)). Let $n \in [X^{1/2}, X]$. The number of products of two primes $p_1 p_2 \in [n-h, n]$ with $h^{1-2c}/2 \leq p_1 \leq h^{1-c}$ and $p_1 \mid n$ is $o(h/(\log X))$.

Proof. We can very crudely bound

$$\sum_{\substack{h^{1-2c}/2\le p_1\le h^{1-c}\\ p_1\mid n}}\ \sum_{(n-h)/p_1\le p_2\le n/p_1} 1 \ll \sum_{\substack{p_1\ge h^{1-2c}/2\\ p_1\mid n}} \frac{h}{p_1} \ll \frac{h(\log X)}{h^{1-2c}} = o\left(\frac{h}{\log X}\right).$$

■

Lemma 4.4 (Exceptions to assumption (v) with large prime divisor). For all but $\ll X/h^{1/2}$ integers $n \le X$, the following holds.

The number of products of two primes $p_1p_2 \in [n-h, n]$ with $h^{1-2c}/2 \le p_1 \le h^{1-c}$ that satisfy $p \mid ap_2+b$ for some prime $p \mid n$, $h^3 \le p \le X^{0.9}$ and some $0 \le a \le p_1$, $0 \le b \le h$ with $0 < ap_2 + b < n$ is $o(h/(\log X))$.

Proof. Suppose $p \mid ap_2 + b$ with $0 \le a \le p_1$ and $0 \le b \le h$. If $a = p_1$, then $p \mid n$, $p \mid ap_2 + b$ implies $p \mid n - p_1p_2 - b \in (0, h]$. But as $p > h$, this is not possible. Similarly, if $a = 0$, then $p \mid b \in [1, h]$, which contradicts $p > h$. Now, denoting

$$\mathcal{S}_p := \{j \in \mathbb{Z} :\ aj + b \equiv 0 \pmod p \text{ for some } 1 \le a < p_1, 0 \le b \le h\},$$

we can write the condition $p \mid ap_2 + b$ with a, b as above in the form $p_2 \in \mathcal{S}_p$. It then suffices to show, for every $h^3 \le p \le X^{0.9}$, that

$$\sum_{\substack{n-h\le p_1p_2\le n\\ p_2\in\mathcal{S}_p}} 1 \le \frac{h}{(\log X)^2}$$

holds for all but $\ll X/(h^{0.9}p)$ integers $n \le X$, $n \equiv 0 \pmod p$. Indeed, once we have this, the claim follows from the union bound and the fact that any $n \le X$ has $\ll (\log X)/(\log h)$ prime factors $p > h^3$.

Using the inequality $|\{n \le X : b_n \ge \lambda\}| \le \lambda^{-1}\sum_{n\le X} b_n$ with $b_n \ge 0$, we can estimate

$$\left|\left\{n \le X :\ p \mid n \text{ and } \sum_{\substack{n-h\le p_1p_2\le n\\ h^{1-2c}/2\le p_1\le h^{1-c}\\ p_2\in\mathcal{S}_p}} 1 \ge \frac{h}{(\log X)^2}\right\}\right|$$

$$\le \frac{(\log X)^2}{h} \sum_{m\le X/p}\ \sum_{h^{1-2c}/2\le p_1\le h^{1-c}}\ \sum_{\substack{(pm-h)/p_1\le \ell\le pm/p_1\\ \ell\in\mathcal{S}_p}} 1. \tag{4.1}$$

Note then that $\ell \in \mathcal{S}_p$ for some $\ell \in [(pm-h)/p_1, pm/p_1]$ implies that for some $1 \le a < p_1$, we have

$$\frac{apm}{p_1} \in [-2h, 2h] \pmod p.$$

Therefore, we have

$$\frac{am}{p_1} \in \left[-\frac{2h}{p}, \frac{2h}{p}\right] \pmod 1.$$

But if $p_1 \nmid am$, then by denoting by $\|\cdot\|$, the distance to the nearest integer, we have

$$\left\|\frac{am}{p_1}\right\| \ge \frac{1}{p_1} > \frac{2h}{p},$$

since $p \ge h^3$ and $p_1 \le h^{1-c}$. We must therefore have $p_1 \mid am$, so $p_1 \mid m$. Hence, (4.1) is bounded by

$$\begin{aligned}
&\ll \frac{(\log X)^2}{h} \sum_{m \le X/p} \sum_{h^{1-2c}/2 \le p_1 \le h^{1-c}} \frac{h}{p_1} 1_{p_1 \mid m} \\
&\ll (\log X)^2 \sum_{h^{1-2c}/2 \le p_1 \le h^{1-c}} \frac{X}{pp_1^2} \\
&\ll \frac{X}{ph^{0.9}},
\end{aligned}$$

recalling that $p_1 p \ll X^{0.9+o(1)}$ and $p_1 \ge h^{1-2c} \ge h^{0.9}(\log X)^2$ if we take $c < 1/25$. As noted before, this was enough to conclude the proof. ■

Lemma 4.5 (Bounding the number of smooth numbers). The number of $n \le X$ that have no prime factors larger than h^3 is $\ll X \exp(-c(\log X)^{1/2}(\log\log X))$.

Proof. Let $s = (\log X)/(\log h^3) = (\log X)^{1/2}/(3(\log\log X)^{1/2})$. Then, by a standard smooth number estimate (see, e.g., [15, Corollary 1.3]), the number of h^3-smooth integers up to X is

$$\ll Xs^{-(1+o(1))s} \ll X \exp(-c(\log X)^{1/2}(\log\log X)^{1/2}),$$

provided we take $c < 1/6$. ■

Combining Lemmas 4.1– 4.5, Theorem 1.2 follows (assuming still Theorem 1.3).

Remark 4.6. Note that the size of our exceptional set arose essentially from solving the equation $h^{-c} = s^{-s}$ with $s = (\log X)/(\log h)$ and $c \asymp 1$. Since it does not seem easy to obtain a saving larger than $h^{-O(1)}$ for the size of the exceptional set in Theorem 1.3 even under the Riemann hypothesis, it seems that a new idea would be required to improve on the size of our exceptional set in Theorem 1.2.

5 Proof of Theorem 1.3

Throughout this section, let $\varepsilon > 0$ be a small enough absolute constant. We can restate Theorem 1.3 in the following quantitative form.

Theorem 5.1. Let $(\log x)^C \le h \le X^{1/10}$ for large enough $C \ge 1$. Then, for all integers $1 \le x \le X$ apart from $\ll Xh^{-\varepsilon}$ exceptions, we have

$$\sum_{\substack{x \le n_1 n_2 \le x+h \\ h^{1-2\varepsilon} \le n_1 \le h^{1-\varepsilon}}} \Lambda(n_1)\Lambda(n_2) = h \sum_{h^{1-2\varepsilon} \le n_1 \le h^{1-\varepsilon}} \frac{\Lambda(n_1)}{n_1} + O(h(\log X)^{-100}). \tag{5.1}$$

By Mertens's theorem, we have

$$\sum_{h^{1-2\varepsilon} \le n_1 \le h^{1-\varepsilon}} \frac{\Lambda(n_1)}{n_1} = \left(\log \frac{1-\varepsilon}{1-2\varepsilon} + o(1)\right) \log h$$

and $\log((1-\varepsilon)/(1-2\varepsilon)) > \varepsilon$ for $\varepsilon \in (0, 1/2)$. Hence, noting that $\Lambda(n_1) \le \log h, \Lambda(n_2) \le \log X + 1$ and trivially bounding the contribution of the higher prime powers to Λ, we see that Theorem 5.1 directly implies Theorem 1.3 with $c = \varepsilon$.

We will prove Theorem 5.1 via the method of Dirichlet polynomials. The main hurdle in the proof is that we do not know a zero-free strip of constant width for the Riemann zeta function. Given our current knowledge on the zero-free region of the Riemann zeta function (i.e., the Vinogradov–Korobov zero-free region), we cannot hope to have an error term better than $h \exp(-(\log X)^{1/3+o(1)})$ on the right of (5.1). Hence, (5.1) cannot be directly converted into a variance estimate that we could hope to

unconditionally prove. This issue is amended by defining a *model function* $\widetilde{\Lambda}$ for the von Mangoldt function such that $\widetilde{\Lambda}$ "resonates" with the zeros of the Riemann zeta function of large real part in exactly the same way as the von Mangoldt function itself, and therefore the Dirichlet polynomial of $\Lambda - \widetilde{\Lambda}$ satisfies power-saving Dirichlet polynomial bounds. More precisely, we define $\widetilde{\Lambda}$ as follows.

Definition 5.2 (A model for the von Mangoldt function). For a given $X \geq 2$, define

$$\widetilde{\Lambda}(n) := 1 - \sum_{\substack{\rho=\beta+i\gamma \\ \beta \geq 1-10\varepsilon \\ |\gamma| \leq X^{1.1}}} n^{\rho-1},$$

where the sum is over the nontrivial zeros ρ of the Riemann zeta function.

We have the following lemma on the size of the model function $\widetilde{\Lambda}(n)$.

Lemma 5.3. For $n \in [X^{0.1}, 2X]$, we have $|\widetilde{\Lambda}(n) - 1| \ll \exp(-(\log X)^{0.33})$.

Proof. We have

$$\begin{aligned}\widetilde{\Lambda}(n) - 1 &= - \sum_{\substack{\rho=\beta+i\gamma \\ \beta \geq 1-10\varepsilon \\ |\gamma| \leq X^{1.1}}} n^{\rho-1} \\ &\ll \sum_{\substack{\rho=\beta+i\gamma \\ \beta \geq 1-10\varepsilon \\ |\gamma| \leq X^{1.1}}} X^{0.1(\beta-1)}.\end{aligned}$$

By the Vinogradov–Korobov zero-free region, we necessarily have $\beta \leq \beta_0 := 1 - (\log X)^{-0.667}$ for $X \geq X_0$. Hence, by splitting the values of β into intervals of length $\leq 1/(\log X)$, we have

$$\sum_{\substack{\rho=\beta+i\gamma \\ \beta \geq 1-10\varepsilon \\ |\gamma| \leq X^{1.1}}} X^{0.1(\beta-1)} \ll (\log X) \max_{1-10\varepsilon \leq \beta \leq \beta_0} X^{0.1(\beta-1)} N(\beta, X^{1.1}),$$

where $N(\beta, T)$ denotes the number of zeros ρ of the Riemann zeta function with $\mathrm{Re}(\rho) \geq \beta$, $|\mathrm{Im}(\rho)| \leq X$. We may assume that $\varepsilon \leq 10^{-8}$, say. By a zero density estimate for the

Riemann zeta function near the 1-line [16], for $\beta \geq 1 - 2 \cdot 10^{-7}$ (say), we have

$$N(\beta, X^{1.1}) \ll (X^{1.1})^{100(1-\beta)^{3/2}} \ll X^{0.1(1-\beta)/2}. \tag{5.2}$$

Hence, we have

$$\max_{1-10\varepsilon \leq \beta \leq \beta_0} (\log X) X^{0.1(\beta-1)} N(\beta, X^{1.1}) \ll X^{0.04(\beta_0-1)} \ll \exp(-(\log X)^{0.33}),$$

giving the claim. ■

With the help of our model function, we can state a variance estimate that will turn out to imply Theorem 5.1.

Proposition 5.4 (A variance estimate). Let $(\log X)^C \leq h \leq X^{1/9}$ for large enough $C \geq 1$. Also, let $H = X^{1-10\varepsilon}$. Then we have

$$\int_{X/2}^{X} \left| \sum_{\substack{x \leq n_1 n_2 \leq x+h \\ h^{1-2\varepsilon} \leq n_1 \leq h^{1-\varepsilon}}} \Lambda(n_1)(\Lambda - \widetilde{\Lambda})(n_2) - \frac{h}{H} \sum_{\substack{x \leq n_1 n_2 \leq x+H \\ h^{1-2\varepsilon} \leq n_1 \leq h^{1-\varepsilon}}} \Lambda(n_1)(\Lambda - \widetilde{\Lambda})(n_2) \right|^2 \mathrm{d}x \ll h^{2-4\varepsilon} X.$$

Proof of Theorem 5.1 assuming Proposition 5.4. By Lemma 5.3 and Chebyshev's inequality, it suffices to show for all $x \in [X/2, X]$ that

$$\sum_{\substack{x \leq n_1 n_2 \leq x+H \\ h^{1-2\varepsilon} \leq n_1 \leq h^{1-\varepsilon}}} \Lambda(n_1)(\Lambda(n_2) - 1) \ll_A H(\log X)^{-A} \tag{5.3}$$

and

$$\sum_{\substack{x \leq n_1 n_2 \leq x+h' \\ h^{1-2\varepsilon} \leq n_1 \leq h^{1-\varepsilon}}} \Lambda(n_1)(\widetilde{\Lambda}(n_2) - 1) \ll_A h'(\log X)^{-A} \tag{5.4}$$

for $h' \in \{h, H\}$.

The first claim (5.3) follows directly by writing

$$\sum_{\substack{x\le n_1n_2\le x+H\\ h^{1-2\varepsilon}\le n_1\le h^{1-\varepsilon}}}\Lambda(n_1)(\Lambda(n_2)-1)=\sum_{h^{1-2\varepsilon}\le n_1\le h^{1-\varepsilon}}\Lambda(n_1)\sum_{x/n_1\le n_2\le (x+H)/n_1}(\Lambda(n_2)-1)$$

and applying the prime number theorem in short intervals to the n_2 sum.

For the proof of (5.4), note simply that by Lemma 5.3 for $x\in[X/2,X]$, we have

$$\sum_{\substack{x\le n_1n_2\le x+h'\\ h^{1-2\varepsilon}\le n_1\le h^{1-\varepsilon}}}\Lambda(n_1)|\widetilde{\Lambda}(n_2)-1|\ll\sum_{h^{1-2\varepsilon}\le n_1\le h^{1-\varepsilon}}\frac{(\log h)h'}{n_1}\exp(-(\log X)^{0.33})\ll_A\frac{h'}{(\log X)^A}.$$

■

Before proving Proposition 5.4, we shall reduce it to mean squares of Dirichlet polynomials.

Proposition 5.5 (Mean square bound for a product of two prime Dirichlet polynomials). Let

$$P_1(s):=\sum_{h^{1-2\varepsilon}\le n\le h^{1-\varepsilon}}\Lambda(n)n^{-s},\quad \widetilde{P}(s)=\sum_{X/(2h^{1-\varepsilon})\le n\le X/h^{1-2\varepsilon}}(\Lambda-\widetilde{\Lambda})(n)n^{-s}.$$

Also, let $(\log X)^C\le h\le X^{1/9}$ with $C\ge 1$ large enough. Then we have

$$\int_{h^{10\varepsilon}}^{X/h^{1-4\varepsilon}}|P_1(1+it)|^2|\widetilde{P}(1+it)|^2\,\mathrm{d}t\ll h^{-4\varepsilon}.$$

Proof of Proposition 5.4 assuming Proposition 5.5. This is a standard Perron formula argument. Let

$$a_n=\sum_{\substack{n=n_1n_2\\ h^{1-2\varepsilon}\le n_1\le h^{1-\varepsilon}\\ X/(2h^{1-\varepsilon})\le n_2\le X/h^{1-2\varepsilon}}}\Lambda(n_1)\Lambda(n_2),\quad S_y(x)=\frac{1}{y}\sum_{x\le n\le x+y}a_n,\quad F(s)=\sum_n a_nn^{-s}.$$

Also, let $H = X^{1-10\varepsilon}$. By [13, Lemma 1], we have (in [13, Lemma 1], a_n is assumed to be supported in $[X, 2X]$, but this is actually not used in the proof)

$$\int_{X/2}^{X} \left| \frac{1}{h} S_h(x) - \frac{1}{H} S_H(x) \right|^2 \mathrm{d}x \ll h^{-10\varepsilon} + \int_{h^{10\varepsilon}}^{X/h} |F(1+it)|^2 \,\mathrm{d}t + \max_{T \geq X/h} \frac{X}{Th} \int_{T}^{2T} |F(1+it)|^2 \,\mathrm{d}t.$$

Now the claim follows by applying the mean value theorem for Dirichlet polynomials in the range $T \geq X/h^{1-4\varepsilon}$. ■

Before proving Proposition 5.5, we need one more lemma.

Lemma 5.6. For $2 \leq |t| \leq X$, we have

$$|\widetilde{P}(1+it)| \ll 1/|t| + X^{-8\varepsilon}.$$

Proof. Let $Q_1 = X/(2h^{1-\varepsilon})$, $Q_2 = X/h^{1-2\varepsilon}$. By a slight variant of the explicit formula (which is proved in the same way; cf. arguments in [17, Section 5]), for $2 \leq |t| \leq X$, we have

$$\sum_{Q_1 \leq n \leq Q_2} \Lambda(n) n^{-1-it} = -\frac{Q_2^{it} - Q_1^{it}}{it} - \sum_{\substack{\rho = \beta + i\gamma \\ |\gamma| \leq X^{1.1}}} \frac{Q_2^{\rho-1-it} - Q_1^{\rho-1-it}}{\rho - it} + O\left(\frac{Q_2 (\log Q_2)^3}{X^{1.1}} \right).$$

Here, the error term is $\ll X^{-10\varepsilon}$ (if $\varepsilon \leq 1/110$) and the first term is $\ll |t|^{-1}$. Note that the contribution of $\beta < 1 - 10\varepsilon$ above is $\ll X^{-8\varepsilon}$, using $\sum_{\rho : |\mathrm{Im}(\rho)| \leq X^{1.1}} 1/|\rho - it| \ll (\log X)^2$ and $Q_1 \gg X/h \gg X^{8/9}$.

On the other hand, we have

$$\sum_{Q_1 \leq n \leq Q_2} \widetilde{\Lambda}(n) n^{-1-it} = \sum_{Q_1 \leq n \leq Q_2} n^{-1-it} - \sum_{\substack{\rho = \beta + i\gamma \\ \beta \geq 1 - 10\varepsilon \\ |\gamma| \leq X^{1.1}}} \sum_{Q_1 \leq n \leq Q_2} n^{\rho - 2 - it}.$$

By Perron's formula, for any ξ with $\mathrm{Re}(\xi) \leq 1$, we have

$$\sum_{Q_1 \leq n \leq Q_2} n^{\xi - 2 - it} = \frac{1}{2\pi i} \int_{1 - X^{10\varepsilon} i}^{1 + X^{10\varepsilon} i} \zeta(s + 2 - \xi + it) \frac{Q_2^s - Q_1^s}{s} \,\mathrm{d}s + O(X^{-9\varepsilon}).$$

Shifting the line of integration to $\mathrm{Re}(s) = \mathrm{Re}(\xi) - 2$ and applying the residue theorem and the estimate $|\zeta(iu)| \ll (1+|u|)^{1/2}$, this is

$$\frac{Q_2^{\xi-1-it} - Q_1^{\xi-1-it}}{\xi - 1 - it} + O(X^{-9\varepsilon}),$$

since either the simple pole at $s = \xi - 1 - it$ is captured by the integral unless $|\mathrm{Im}(\xi) - t| \geq X^{10\varepsilon}$. Applying the above with $\xi = 1$ and $\xi = \rho$, and recalling (5.2), the claim follows. ■

Proof of Proposition 5.5. We apply the Matomäki–Radziwiłł [18] method. We split the integration domain into two sets

$$\mathcal{T}_1 = \{h^{10\varepsilon} \leq t \leq X/h^{1-4\varepsilon} : \ |P_1(1+it)| \geq h^{-5\varepsilon}\}, \quad \mathcal{T}_2 = [h^{10\varepsilon}, X/h^{1-4\varepsilon}] \setminus \mathcal{T}_1.$$

By the mean value theorem for Dirichlet polynomials, we trivially have

$$\int_{\mathcal{T}_1} |P_1(1+it)|^2 |\widetilde{P}(1+it)|^2 \, \mathrm{d}t \ll h^{-10\varepsilon} \left(\frac{X/h^{1-4\varepsilon} + X/h^{1-\varepsilon}}{X/h^{1-\varepsilon}} \right) \ll h^{-4\varepsilon}.$$

Consider then the integral over $\mathcal{T}_2$. By a large values estimate ([13, Lemma 6], which is proved by raising P_1 to a large power and applying the mean value theorem), if $\mathcal{U} \subset \mathcal{T}_2$ is any well-spaced subset (i.e., any two of its elements are separated by ≥ 1), then (taking C large in terms of ε), we have

$$|\mathcal{U}| \ll X^{11\varepsilon}.$$

On the other hand, for some well-spaced $\mathcal{U} \subset \mathcal{T}_2$, we have

$$\int_{\mathcal{T}_2} |P_1(1+it)|^2 |\widetilde{P}(1+it)|^2 \, \mathrm{d}t \ll \sum_{t \in \mathcal{U}} |P_1(1+it)|^2 |\widetilde{P}(1+it)|^2,$$

and crudely bounding $|P_1(1+it)| \ll 1$ and using Lemma 5.6, we can bound this by

$$\ll h^{-10\varepsilon} + |\mathcal{U}| X^{-16\varepsilon} \ll h^{-10\varepsilon} + X^{-5\varepsilon} \ll h^{-4\varepsilon}.$$

This proves the claim. ■

Funding

This work was supported by Academy of Finland grant no. [340098].

Acknowledgments

The author thanks Ben Green for bringing the topic of invariable generation to his attention.The author also thanks the referees for helpful comments.

References

[1] Guralnick, R. and G. Malle. "Simple groups admit Beauville structures." *J. Lond. Math. Soc. (2)* 85, no. 3 (2012): 694–721.

[2] Kantor, W. M., A. Lubotzky, and A. Shalev. "Invariable generation and the Chebotarev invariant of a finite group." *J. Algebra.* 348 (2011): 302–14. http://10.1016/j.jalgebra.2011.09.022.

[3] Dixon, J. D. "The probability of generating the symmetric group." *Math. Z.* 110 (1969): 199–205. 10.1007/BF01110210.

[4] Eberhard, S., K. Ford, and B. Green. "Invariable generation of the symmetric group." *Duke Math. J.* 166, no. 8 (2017): 1573–90. http://10.1215/00127094-0000007X.

[5] Garzoni, D. and E. McKemmie. "On the probability of generating invariably a finite simple group." (2020): preprint arXiv:2008.03812.

[6] McKemmie, E. "Invariable generation of finite classical groups." *J. Algebra* 585 (2021): 592–615. http://10.1016/j.jalgebra.2021.06.020.

[7] Pemantle, R., Y. Peres, and I. Rivin. "Four random permutations conjugated by an adversary generate $\mathcal{S}_n$ with high probability." *Random Structures Algorithms* 49, no. 3 (2016): 409–28.

[8] Lucchini, A. "The Chebotarev invariant of a finite group: a conjecture of Kowalski and Zywina." *Proc. Amer. Math. Soc.*146, no. 11 (2018): 4549–62. http://10.1090/proc/13805.

[9] Dolfi, S., R. M. Guralnick, M. Herzog, and C. E. Praeger. "A new solvability criterion for finite groups." *J. Lond. Math. Soc. (2)*85, no. 2 (2012): 269–81.

[10] Shareshian, J. and R. Woodroofe. "Divisibility of binomial coefficients and generation of alternating groups." *Pacific J. Math.* 292, no. 1 (2018): 223–38. http://10.2140/pjm.2018.292.223.

[11] Guralnick, R. M., J. Shareshian, and R. Woodroofe. "On invariable generation of alternating groups by elements of prime and prime power order." (2022): preprint arXiv:2201.12371.

[12] Matomäki, K. and J. Teräväinen. "Almost primes in almost all short intervals II." *Transactions of the American Mathematical Society* (forthcoming).

[13] Teräväinen, J. "Almost primes in almost all short intervals." *Math. Proc. Cambridge Philos. Soc.* 161, no. 2 (2016): 247–81. http://10.1017/S0305004116000232.

[14] Baker, R. C., G. Harman, and J. Pintz. "The difference between consecutive primes. II." *Proc. London Math. Soc. (3)* 83, no. 3 (2001): 532–62.

[15] Hildebrand, A. and G. Tenenbaum. "Integers without large prime factors." *J. Théor. Nombres Bordeaux*. 5, no. 2 (1993): 411–84. http://10.5802/jtnb.101.

[16] Ford, K. “Vinogradov’s integral and bounds for the Riemann zeta function.” *Proc. London Math. Soc. (3)* 85, no. 3 (2002): 565–633.

[17] Iwaniec, H. and E. Kowalski. *Analytic Number Theory*, vol. 53. American Mathematical Society Colloquium Publications. Providence, RI: American Mathematical Society, 2004.

[18] Matomäki, K. and M. Radziwiłł. “Multiplicative functions in short intervals.” *Ann. of Math. (2)* 183, no. 3 (2016): 1015–56.