THE PÓLYA–VINOGRADOV INEQUALITY

SHUBHRAJIT BHATTACHARYA AND REGINALD SIMPSON

ABSTRACT. This brief paper gives an overview of the Pólya–Vinogradov inequality. The background, mathematical and historical, of the inequality is discussed. An abridged proof is provided. Some well-known consequences concerning the distribution of the values Dirichlet characters take, and the distribution of primitive roots in the multiplicative group are shown. Potential topics for contemporary research related to the inequality are explored.

1. INTRODUCTION

The Pólya–Vinogradov inequality is a significant and famous bound on incomplete sums of Dirichlet characters. There are a few different versions of it, with one very general example found in [11, Chapter 9, p. 306], which states

$$\sum_{n=M+1}^{M+N} \chi(n) \ll q^{1/2} \log q.$$

uniformly for M, N for any nonprincipal Dirichlet character $\chi(n)$ of modulus q. Several variations of this statement can be found throughout the literature, some of which impose additional restrictions on where the sum starts relative to the modulus q. For example [10] discusses partial character sums of the form $\sum_{n \leq x} \chi(n)$, and [8, Conjecture 2.6, p. 363] suggests that there are different best-possible implicit constants depending on the starting point of the sum. While the Pólya–Vinogradov bound is non-trivial for incomplete sums of Dirichlet characters, it is superseded in the trivial case when N is smaller than $q^{1/2}$, since $\left| \sum_{n=M+1}^{M+N} \chi(n) \right| \leq N$.

The mathematical background required to understand the proof of the Pólya–Vinogradov inequality arises from the study of the basic properties of Dirichlet characters and Gauss sums. While a complete explanation can be found in [11, Chapter 9], a brief overview will be given here.

In representation theory, a Dirichlet character $\chi \pmod q$ is a degree 1 representation of the group $(\mathbb{Z}/q\mathbb{Z})^\times$. Since the multiplicative group of q is abelian, every irreducible representation of the multiplicative group of q is a Dirichlet character and every representation is its own character. In analytic number theory, one treats a Dirichlet character $\chi(n)$ of modulus q as a function on the integers which is based on a representation of $(\mathbb{Z}/q\mathbb{Z})^\times$ as described above. Hence $\chi(n)$ maps n to the representation of its residue modulo q if it lies in the multiplicative group and maps n to zero otherwise. As a function of the integers, $\chi(n)$ has period q and is totally multiplicative. It inherits the orthogonality properties of the representation theory characters.

Central to the proof of the inequality is the Gauss sum $\tau(\chi)$: an inner product of the (multiplicative) Dirichlet characters modulo q and the additive characters $e(a/q) = e^{2\pi(a/q)i}$, with $\tau(\chi) = \sum_{a=1}^{q} \chi(a)e(a/q)$. From the study of Gauss sums and Dirichlet characters the relation $\chi(n) = \tau(\bar{\chi})^{-1} \sum_{a=1}^{q} \bar{\chi}(a)e(an/q)$ arises for any primitive character χ modulo q [11, Corollary 9.8, p. 288].

The inequality was proven by Pólya and Vinogradov independently of each other in 1918 [8, p.357]. Since its statement, various improvements to it have been made. Unconditionally, the implicit constant has been computed explicitly and refined [4, 9, 3].

It has also been shown [10, Theorem 2, p. 70] that under the assumption of "GRH," the Generalized Riemann Hypothesis (the condition that all non-trivial zeroes of all $L(s,\chi)$ have real part $1/2$), the bound can be improved. There have also been unconditional refinements for some characters [8, 5, 6] that satisfy certain conditions but not others.

Theorem 2 from [10] is worth examining in further detail. It states that assuming GRH, the sum $\sum_{n\leq x}\chi(n) \ll q^{1/2}\log\log q$ for any nonprincipal character χ. Montgomery and Vaughan mention that this is effectively the best possible such bound, as there is a result by Paley that shows that there are infinitely many quadratic characters where $|\sum_{n\leq x}\chi(n)| > \frac{1}{7}q^{1/2}\log\log q$. Highlighting the central importance of Gauss sums in terms of their relation to the Pólya–Vinogradov inequality is that the primary technique in [10] involves convolutions of multiplicative functions and approximations of additive characters.

In contrast, the paper [8] by Granville and Soundararajan contains several improvements in terms of both explicit constants for the inequality and special cases where better bounds are possible. This paper goes on to characterize the structure of characters whose incomplete sums are close to the expected actual upper bound found when assuming GRH is true. Using the relatively recent theory of "pretentious" characters, this paper inspired further research in this area using refinements of their techniques.

One such refinement by Goldmakher [6] gives a superior unconditional bound (Theorem 2, p. 127) for characters of odd order; the order of a character being the minimum $g \in \mathbb{N}$ such that $\chi(n)^g = 1$ or 0 for all $n \in \mathbb{Z}$. For a primitive character $\chi \pmod q$ which has odd order g, $|\sum_{n\leq x}\chi(n)| \ll_g q^{1/2}(\log q)^{1-\delta_g+o(1)}$ where $\delta_g = 1 - \frac{g}{\pi}\sin\frac{\pi}{g}$. A version with $\log\log q$ instead of $\log q$ was proven conditionally in the same Theorem, and in [7] Goldmakher and Lamzouri demonstrated the conditional estimate was unconditionally the best possible estimate: a special case of Paley's lower bound.

2. Proof of The Inequality

This section will present a proof of Pólya–Vinogradov Inequality following [11, p. 306]. The proof will use the following identity [11, Corollary 9.8, p. 288]): for a primitive Dirichlet character χ modulo q,

$$\chi(m) = \frac{1}{\tau(\overline{\chi})}\sum_{a=1}^{q}\overline{\chi}(a)e(am/q). \tag{1}$$

Theorem 2.1 (The Pólya–Vinogradov Inequality)**.** *Let χ be a nonprincipal Dirichlet character modulo q, and let M, N be any integers with $N > 0$. Then*

$$\sum_{n=M+1}^{M+N}\chi(n) \ll \sqrt{q}\log q.$$

Proof. Without loss of generality, assume $q > 1$ and assume first that χ is primitive. By (1),

$$\sum_{n=M+1}^{M+N}\chi(n) = \frac{1}{\tau(\overline{\chi})}\sum_{a=1}^{q}\overline{\chi}(a)\sum_{n=M+1}^{M+N}e(an/q). \tag{2}$$

Observe that, for $\alpha \notin \mathbb{Z}$,

$$\sum_{n=M+1}^{M+N} e(n\alpha) = \frac{e((M+N+1)\alpha) - e((M+1)\alpha)}{e(\alpha)-1} = e((2M+N+1)\alpha/2)\frac{\sin(\pi N\alpha)}{\sin(\pi\alpha)}. \quad (3)$$

When $\alpha \in \mathbb{Z}$, the inner sum in (2) is just N. But in our case, $\alpha = a/q$ is not an integer as long as $1 < a < q$. For $a = q$ the inner sum doesn't contribute since $\overline{\chi}(q) = 0$. So, combining (2) and (3) one may write:

$$\sum_{n=M+1}^{M+N} \chi(n) = \frac{1}{\tau(\overline{\chi})}\sum_{a=1}^{q} \overline{\chi}(a) e\left(\frac{a(2M+N+1)}{2q}\right)\frac{\sin(\pi aN/q)}{\sin(\pi a/q)}.$$

By Theorem 9.7 in [11, p. 287], for a primitive character modulo q, $|\tau(\overline{\chi})| = \sqrt{q}$. Therefore, by triangle inequality,

$$\left|\sum_{n=M+1}^{M+N} \chi(n)\right| < \frac{1}{\sqrt{q}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q-1} \frac{1}{\sin(\pi a/q)}. \quad (4)$$

Since $\sin(\pi a/q) = \sin(\pi - \pi a/q) = \sin(\pi(q-a)/q)$, the first half and the second half of the above sum's range are symmetric. Therefore, it suffices to compute two times the sum over the first half $1 \le a \le (q-1)/2$ when q is odd and $1 \le a \le q/2$ when q is even. Observe that when q is even then $4 \mid q$ because there are no primitive characters modulo q for $q \equiv 2 \pmod 4$. Therefore, $(q/2, q) > 1$, and hence the range of the sum will be $1 \le a \le q/2 - 1$. Both cases may be combined to write (4) as

$$\left|\sum_{n=M+1}^{M+N} \chi(n)\right| < \frac{2}{\sqrt{q}} \sum_{1\le a\le (q-1)/2} \frac{1}{\sin(\pi a/q)}. \quad (5)$$

Here the right-hand side involves the function $f(t) = \sin(\pi t)$. In the interval $[0, 1/2]$, f is concave downward and hence lies above the chord through the points $(0,0)$ and $(1/2, 1)$. Therefore, $f(t) \ge 2t$ for all $t \in [0, 1/2]$. Therefore,

$$\left|\sum_{n=M+1}^{M+N} \chi(n)\right| < \frac{2}{\sqrt{q}} \sum_{1\le a\le (q-1)/2} \frac{q}{2a} = \sqrt{q} \sum_{1\le a\le (q-1)/2} \frac{1}{a} < \sqrt{q} \sum_{1\le a\le (q-1)/2} \log\frac{1+1/2a}{1-1/2a}$$

$$= \sqrt{q} \sum_{1\le a\le (q-1)/2} \log\frac{2a+1}{2a-1} = \sqrt{q} \sum_{1\le a\le (q-1)/2} \big(\log(2a+1) - \log(2a-1)\big) \le \sqrt{q}\log q.$$

This completes the proof of the theorem for a primitive Dirichlet character. Let χ be any nonprincipal character induced by χ^* modulo d. Let r be the product of those primes dividing q but not d. Then

$$\sum_{n=M+1}^{M+N} \chi(n) = \sum_{\substack{n=M+1 \\ (n,r)=1}}^{M+N} \chi^*(n) = \sum_{n=M+1}^{M+N} \chi^*(n) \sum_{k\mid(n,r)} \mu(k)$$

$$= \sum_{k\mid r} \mu(k) \sum_{\substack{M<n\le M+N \\ k\mid n}} \chi^*(n) = \sum_{k\mid r} \mu(k)\chi^*(k) \sum_{M/k<m\le (M+N)/k} \chi^*(m),$$

where μ is the Möbius function and $\mu \star 1(n)$ is 1 when $n = 1$ and 0 otherwise. The last step makes a change of variable $n = mk$. Since χ^* is primitive and the inequality is proved for primitive characters, the inner sum is $\ll \sqrt{d} \log d$. Since $|\mu(k)\chi^*(k)| = 1$ whenever k is a product of distinct primes dividing r, by the Pólya–Vinogradov inequality for primitive characters,

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| \ll 2^{\omega(r)} \sqrt{d} \log d, \tag{6}$$

where $\omega(r)$ is the number of distinct prime factors of r. But $2^{\omega(r)} \leq \sigma(r)$, where $\sigma(r)$ denotes the number of positive divisors of r including 1 and itself. Note that there is a one–one correspondence $d \mapsto r/d$ between the first $\sigma(r)/2$ divisors of r, when ordered by theirs size, and the remaining $\sigma(r)/2$. Since $\min\{d, r/d\} \leq \sqrt{r}$, $\sigma(r)/2 \leq \sqrt{r}$. Therefore $\sigma(r) \ll \sqrt{r} \leq \sqrt{q/d}$. Also, clearly $\log d \leq \log q$. Combining this with (6),

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| \ll \sqrt{q/d}\sqrt{d} \log d \leq \sqrt{q} \log q$$

for any nonprincipal character χ modulo q. □

3. Some Applications

This section will present some applications of the Pólya–Vinogradov inequality, based on material found in [11, pp. 308–309].

Corollary 3.1. *Let χ be a nonprincipal character modulo p and n_χ be the smallest natural number n such that $\chi(n) \neq 1$. Then $n_\chi \ll_\varepsilon p^{1/(2\sqrt{e})+\varepsilon}$.*

Proof. Let $\psi(x, y)$ denote the number of integers $n \in [1, x]$ all of whose prime factors are smaller than y. Clearly, $\psi(x, y) = [x] = x + o(1)$ whenever $y \geq x$. Suppose that $\chi(n) = 1$ for all $n \leq y$. Then $\chi(n) = 1$ whenever all prime factors of n are smaller than y. Whenever $n \leq x$ has a prime factor q bigger than y, then $\chi(n) = \chi(q)\chi(n/q)$. If $y < x < y^2$, $n/q < y$ and hence $\chi(n) = \chi(q)$ for all $n \leq x < y^2$ such that $q \mid n$. Therefore,

$$\sum_{n \leq x} \chi(n) = \psi(x, y) + \sum_{y < q \leq x} \chi(q)[x/q].$$

Therefore,

$$\left| \sum_{n \leq x} \chi(n) \right| \geq \psi(x, y) - \sum_{y < q \leq x} [x/q] = [x] - 2 \sum_{y < q \leq x} [x/q] = x \left(1 - 2 \log \frac{\log x}{\log y} \right) + O\left(\frac{x}{\log x} \right).$$

If $x = \sqrt{p}(\log p)^2$, by the Pólya–Vinogradov inequality, the sum on the left-hand side is $\ll \sqrt{p} \log p$ and hence is $o(\sqrt{p}(\log p)^2) = o(x)$, while if $y > x^{1/\sqrt{e}+\varepsilon}$, then the lower bound on the right hand side is $\gg \varepsilon x$. Thus $n_\chi \ll_\varepsilon x^{1/\sqrt{e}+\varepsilon}$. □

The next corollary gives an estimate on the number of primitive roots of unity in any interval $[M + 1, M + N]$ of length $N > 0$. It is well-known that there are exactly $\varphi(p - 1)$ primitive roots modulo p in an interval of length p. If the primitive roots were uniformly distributed then the answer for an interval of length N would be $\varphi(p-1)N/p$. The Corollary below is somewhat close to this expectation:

Corollary 3.2. *The number of primitive roots modulo p in $[M+1, M+N]$ is*

$$\varphi(p-1)\frac{N}{p} + O(p^{1/2+\varepsilon}).$$

The proof is long and beyond the scope of this article. See Corollary 9.20 in [11, pp. 308–309] for further details.

4. Further Research

In this final section, topics of interest in contemporary research will be discussed. Granville and Soundararajan [8] provided several suggestions. Two conjectures in their paper are stronger than their best conditional results. A component of both conjectures is that $\left|\sum_{n\leq x}\chi(n)\right| \leq (\frac{e^\gamma}{\pi} + o(1))q^{1/2}\log\log q$ for all characters $\chi \pmod q$, effectively stating that Paley's lower bound is sharp. The second conjecture provides a set of conditions under which the upper bounds in the first conjecture become equalities. Likely, progress towards the above conjectures would be through the refinement of the explicit constants for the inequality. Such work is in progress, with [4, 9, 3] as examples of such.

Another avenue of research is finding classes of characters with even smaller upper bounds than the odd characters discussed in [8]. For example, Goldmakher [5] discusses stronger upper bounds for characters modulo friable numbers.

For incomplete sums of characters where the number of integers to be summed over is much smaller than the modulus q, there are few unconditional improvements on trivial bound given by the number of relatively prime to q integers summed, though there is some work [2] on this problem. If one assumes GRH, then $\sum_{n\leq t}\chi(n) \ll_\epsilon t^{1/2}q^\epsilon$ [1, p. 427].

On the whole, while the general shape of the Pólya–Vinogradov inequality has been relatively static over the years, research on the inequality is active and progress is steadily being made to refine it, improve it, and explore special cases where better bounds are possible.

References

[1] Jonathan W. Bober and Leo Goldmakher. The distribution of the maximum of character sums. *Mathematika*, 59(2):427–442, 2013.

[2] Matteo Bordignon. A Pólya-Vinogradov inequality for short character sums. *Canad. Math. Bull.*, 64(4):906–910, 2021.

[3] Matteo Bordignon. Partial Gaussian sums and the Pólya-Vinogradov inequality for primitive characters. *Rev. Mat. Iberoam.*, 38(4):1101–1127, 2022.

[4] D. A. Frolenkov and K. Soundararajan. A generalization of the Pólya-Vinogradov inequality. *Ramanujan J.*, 31(3):271–279, 2013.

[5] Leo Goldmakher. Character sums to smooth moduli are small. *Canad. J. Math.*, 62(5):1099–1115, 2010.

[6] Leo Goldmakher. Multiplicative mimicry and improvements to the Pólya-Vinogradov inequality. *Algebra Number Theory*, 6(1):123–163, 2012.

[7] Leo Goldmakher and Youness Lamzouri. Lower bounds on odd order character sums. *Int. Math. Res. Not. IMRN*, 2012(21):5006–5013, 2012.

[8] Andrew Granville and K. Soundararajan. Large character sums: pretentious characters and the Pólya-Vinogradov theorem. *J. Amer. Math. Soc.*, 20(2):357–384, 2007.

[9] Bryce Kerr. On the constant in the Pólya-Vinogradov inequality. *J. Number Theory*, 212:265–284, 2020.

[10] H. L. Montgomery and R. C. Vaughan. Exponential sums with multiplicative coefficients. *Invent. Math.*, 43(1):69–82, 1977.

[11] H. L. Montgomery and R. C. Vaughan. *Multiplicative Number Theory I. Classical Theory*. Cambridge University Press, 2007.