The Smoothed Pólya–Vinogradov Inequality

Enrique Treviño

Swarthmore College

Integers Conference
October 28, 2011

Pólya–Vinogradov

Let χ be a Dirichlet character to the modulus $q > 1$. Let

$$S(\chi) = \max_{M,N} \left| \sum_{n=M+1}^{M+N} \chi(n) \right|$$

The Pólya–Vinogradov inequality (1918) states that there exists an absolute universal constant c such that for any Dirichlet character $S(\chi) \leq c\sqrt{q}\log q$.

Under GRH, Montgomery and Vaughan showed that $S(\chi) \ll \sqrt{q}\log\log q$.

Paley showed in 1932 that there are infinitely many quadratic characters such that $S(\chi) \gg \sqrt{q}\log\log q$.

Further results regarding Pólya–Vinogradov

Granville and Soundararajan showed that one can save a small power of $\log q$ in the Pólya–Vinogradov inequality. Goldmakher improved it to

Theorem (Goldmakher, 2007)

For each fixed odd number $g > 1$, for $\chi \pmod q$ of order g,

$$S(\chi) \ll_g \sqrt{q}(\log q)^{\Delta_g + o(1)}, \quad \Delta_g = \frac{g}{\pi} \sin \frac{\pi}{g}, \quad q \to \infty.$$

Moreover, under GRH

$$S(\chi) \ll_g \sqrt{q}(\log \log q)^{\Delta_g + o(1)}.$$

Furthermore, there exists an infinite family of characters $\chi \pmod q$ of order g satisfying

$$S(\chi) \gg_{\epsilon, g} \sqrt{q}(\log \log q)^{\Delta_g - \epsilon}.$$

Explicit Pólya–Vinogradov

Theorem (Hildebrand, 1988)

For χ a primitive character to the modulus $q > 1$, we have

$$|S(\chi)| \leq \begin{cases} \left(\frac{2}{3\pi^2} + o(1)\right)\sqrt{q}\log q \quad , & \chi \text{ even}, \\ \left(\frac{1}{3\pi} + o(1)\right)\sqrt{q}\log q \quad , & \chi \text{ odd}. \end{cases}$$

Theorem (Pomerance, 2009)

For χ a primitive character to the modulus $q > 1$, we have

$$|S(\chi)| \leq \begin{cases} \frac{2}{\pi^2}\sqrt{q}\log q + \frac{4}{\pi^2}\sqrt{q}\log\log q + \frac{3}{2}\sqrt{q} \quad , & \chi \text{ even}, \\ \frac{1}{2\pi}\sqrt{q}\log q + \frac{1}{\pi}\sqrt{q}\log\log q + \sqrt{q} \quad , & \chi \text{ odd}. \end{cases}$$

Smoothed Pólya–Vinogradov

Let M, N be real numbers with $0 < N \leq q$, then define $S^*(\chi)$ as follows:

$$S^*(\chi) = \max_{M,N} \left| \sum_{M \leq n \leq M+2N} \chi(n) \left(1 - \left| \frac{n-M}{N} - 1 \right| \right) \right| .$$

Theorem (Levin, Pomerance, Soundararajan, 2009)

Let χ be a primitive character to the modulus $q > 1$, and let M, N be real numbers with $0 < N \leq q$, then

$$S^*(\chi) \leq \sqrt{q} - \frac{N}{\sqrt{q}}.$$

Some Applications of the Smoothed Pólya–Vinogradov

- To prove a conjecture of Brizolis (Levin, Pomerance, Soundararajan) that for every prime $p > 3$ there is a primitive root g and an integer $x \in [1, p-1]$ with $\log_g x = x$, that is, $g^x \equiv x \pmod{p}$.
- Pólya–Vinogradov was used to prove a conjecture of Mollin (Granville, Mollin and Williams) that the least inert prime p in a real quadratic field of discriminant D is $\leq \sqrt{D}/2$. We used the Smoothed Pólya–Vinogradov to improve this to $p \leq D^{0.45}$.

Proof of the Smoothed PV

- Let $H(t) = \max\{0, 1 - |t|\}$.
- $S^*(\chi) = \frac{1}{\tau(\bar{\chi})} \sum_{j=1}^{q} \bar{\chi}(j) \sum_{n \in \mathbb{Z}} e(nj/q) H\left(\frac{n-M}{N} - 1\right)$.
- The Fourier transform of H, $\widehat{H}$, is nonnegative and $\widehat{H}(0) = 1$.
- Using Poisson summation, the fact that $\chi(n)$ and $e(n)$ have absolute value 1 and that $|\tau(\bar{\chi})| = \sqrt{q}$ for primitive characters χ yields

$$|S^*(\chi)| \leq \frac{N}{\sqrt{q}} \sum_{\substack{k \in \mathbb{Z} \\ (k,q)=1}} \widehat{H}\left(\frac{kN}{q}\right).$$

Proof of the Smoothed PV

- Let $H(t) = \max\{0, 1 - |t|\}$.
- $S^*(\chi) = \frac{1}{\tau(\bar{\chi})} \sum_{j=1}^{q} \bar{\chi}(j) \sum_{n \in \mathbb{Z}} e(nj/q) H\left(\frac{n-M}{N} - 1\right)$.
- The Fourier transform of H, $\widehat{H}$, is nonnegative and $\widehat{H}(0) = 1$.
- Using Poisson summation, the fact that $\chi(n)$ and $e(n)$ have absolute value 1 and that $|\tau(\bar{\chi})| = \sqrt{q}$ for primitive characters χ yields

$$|S^*(\chi)| \leq \frac{N}{\sqrt{q}} \sum_{\substack{k \in \mathbb{Z} \\ (k,q)=1}} \widehat{H}\left(\frac{kN}{q}\right).$$

Proof of the Smoothed PV

- Let $H(t) = \max\{0, 1 - |t|\}$.
- $S^*(\chi) = \frac{1}{\tau(\bar{\chi})} \sum_{j=1}^{q} \bar{\chi}(j) \sum_{n \in \mathbb{Z}} e(nj/q) H\left(\frac{n-M}{N} - 1\right).$
- The Fourier transform of H, $\widehat{H}$, is nonnegative and $\widehat{H}(0) = 1$.
- Using Poisson summation, the fact that $\chi(n)$ and $e(n)$ have absolute value 1 and that $|\tau(\bar{\chi})| = \sqrt{q}$ for primitive characters χ yields

$$|S^*(\chi)| \leq \frac{N}{\sqrt{q}} \sum_{\substack{k \in \mathbb{Z} \\ (k,q)=1}} \widehat{H}\left(\frac{kN}{q}\right).$$

Proof of the Smoothed PV

- Let $H(t) = \max\{0, 1 - |t|\}$.
- $$S^*(\chi) = \frac{1}{\tau(\bar{\chi})} \sum_{j=1}^{q} \bar{\chi}(j) \sum_{n \in \mathbb{Z}} e(nj/q) H\left(\frac{n-M}{N} - 1\right).$$
- The Fourier transform of H, $\widehat{H}$, is nonnegative and $\widehat{H}(0) = 1$.
- Using Poisson summation, the fact that $\chi(n)$ and $e(n)$ have absolute value 1 and that $|\tau(\bar{\chi})| = \sqrt{q}$ for primitive characters χ yields

$$|S^*(\chi)| \leq \frac{N}{\sqrt{q}} \sum_{\substack{k \in \mathbb{Z} \\ (k,q)=1}} \widehat{H}\left(\frac{kN}{q}\right).$$

Proof

$$
\begin{aligned}
|S^*(\chi)| &\leq \frac{N}{\sqrt{q}} \sum_{\substack{k \in \mathbb{Z} \\ (k,q)=1}} \widehat{H}\left(\frac{kN}{q}\right) \\
&\leq \sqrt{q}\left(\sum_{k \in \mathbb{Z}} \frac{N}{q} \widehat{H}\left(\frac{kN}{q}\right) - \frac{N}{q} \sum_{k \in \mathbb{Z}} \widehat{H}(kN)\right) \\
&= \sqrt{q}\left(\sum_{t \in \mathbb{Z}} H\left(\frac{qt}{N}\right) - \frac{N}{q} \widehat{H}(0)\right) \\
&= \sqrt{q} - \frac{N}{\sqrt{q}}.
\end{aligned}
$$

Corollaries

Corollary

Let χ be a primitive character to the modulus $q > 1$, let M, N be real numbers with $0 < N \leq q$ and let m be a divisor of q such that $1 \leq m \leq \frac{q}{N}$. Then

$$|S^*(\chi)| \leq \frac{\phi(m)}{m}\sqrt{q}.$$

Corollary

Let χ be a primitive character to the modulus $q > 1$, , then

$$|S^*(\chi)| \leq \frac{\phi(q)}{q}\sqrt{q} + 2^{\omega(q)-1}\frac{N}{\sqrt{q}}.$$

Quick Application

- Let D be a fundamental discriminant. Consider $\chi(n) = \left(\frac{D}{n}\right)$, where $\left(\frac{D}{\cdot}\right)$ is the Kronecker symbol. Then χ is a primitive Dirichlet character.
- Assume the least prime p such that $\chi(p) = -1$ is greater than y for some y. Then

$$S_\chi(N) = \sum_{n \le 2N} \chi(n) \left(1 - \left|\frac{n}{N} - 1\right|\right)$$
$$\ge \sum_{\substack{n \le 2N \\ (n,D)=1}} \left(1 - \left|\frac{n}{N} - 1\right|\right) - 2 \sum_{\substack{y < p \le 2N \\ \chi(p)=-1}} \sum_{\substack{n \le \frac{2N}{p} \\ (n,D)=1}} \left(1 - \left|\frac{np}{N} - 1\right|\right).$$

Quick Application

- Let D be a fundamental discriminant. Consider $\chi(n) = \left(\frac{D}{n}\right)$, where $\left(\frac{D}{\cdot}\right)$ is the Kronecker symbol. Then χ is a primitive Dirichlet character.
- Assume the least prime p such that $\chi(p) = -1$ is greater than y for some y. Then

$$S_\chi(N) = \sum_{n \leq 2N} \chi(n) \left(1 - \left|\frac{n}{N} - 1\right|\right)$$

$$\geq \sum_{\substack{n \leq 2N \\ (n,D)=1}} \left(1 - \left|\frac{n}{N} - 1\right|\right) - 2 \sum_{\substack{y < p \leq 2N \\ \chi(p)=-1}} \sum_{\substack{n \leq \frac{2N}{p} \\ (n,D)=1}} \left(1 - \left|\frac{np}{N} - 1\right|\right).$$

Imprimitive Case

Corollary (Levin, Pomerance, Soundararajan)

Let χ be a primitive character to the modulus $q > 1$, then

$$|S^*(\chi)| \leq \frac{q^{3/2}}{N} \left\{\frac{N}{q}\right\} \left(1 - \left\{\frac{N}{q}\right\}\right). \quad (1)$$

In particular, $|S^*(\chi)| < \sqrt{q}$.

Theorem

Let χ be a non-principal Dirichlet character to the modulus $q > 1$, then

$$|S^*(\chi)| < \frac{4}{\sqrt{6}}\sqrt{q}.$$

Lowerbound for the smoothed Pólya–Vinogradov

Theorem (ET)

Let χ be a primitive character to the modulus $q > 1$, then

$$S^*(\chi) \geq \frac{2}{\pi^2}\sqrt{q}.$$

Therefore, the order of magnitude of $S^*(\chi)$ is $\sqrt{q}$.

More Work

Let $q > 1$ be an integer and let χ be a primitive Dirichlet character mod q. Let

$$S_\chi(M,N) = \sum_{M \le n \le 2N} \chi(n) \left(1 - \left|\frac{n-M}{N} - 1\right|\right).$$

We're interested in

$$A(q) = \min_{\chi} \max_{M,N} \left|S_\chi(M,N)\right|,$$

and

$$B(q) = \max_{\chi} \max_{M,N} \left|S_\chi(M,N)\right|.$$

- From earlier theorems we know

$$A(q) > \frac{2}{\pi^2},$$

and

$$B(q) < 1.$$

- Kamil Adamczewski wrote code to find $A(q)$ and $B(q)$ for small q ($q \leq 200$).
- $A(q)$ is around 0.45 in all modulus that have been computed. In those examples, $B(q)$ is between 0.7 and 0.8.

- From earlier theorems we know

$$A(q) > \frac{2}{\pi^2},$$

and

$$B(q) < 1.$$

- Kamil Adamczewski wrote code to find $A(q)$ and $B(q)$ for small q ($q \leq 200$).
- $A(q)$ is around 0.45 in all modulus that have been computed. In those examples, $B(q)$ is between 0.7 and 0.8.

- From earlier theorems we know

$$A(q) > \frac{2}{\pi^2},$$

and

$$B(q) < 1.$$

- Kamil Adamczewski wrote code to find $A(q)$ and $B(q)$ for small q ($q \leq 200$).
- $A(q)$ is around 0.45 in all modulus that have been computed. In those examples, $B(q)$ is between 0.7 and 0.8.

Thank you!