On multiplicative character sums

Mei-Chu Chang

Methods from arithmetic combinatorics originating in Endre Szemeredi's work have significant applications in analytic number theory, in particular to bounding exponential sums and character sums. Two results that play a key role are Sum-product theorems and the Balog-Szemeredi-Gowers theorem.

Sum-product theorem

- Sum set

$$A + A = \{a_1 + a_2 : a_i \in A\}$$

- Product Set

$$AA = \{a_1 a_2 : a_i \in A\}$$

Sum-product theorem

- Sum set

$$A + A = \{a_1 + a_2 : a_i \in A\}$$

- Product Set

$$AA = \{a_1 a_2 : a_i \in A\}$$

- ERDÖS-SZEMERÉDI

Theorem. $A \subset \mathbf{Z}$, $|A| = N$

$$|A + A| + |AA| > N^{1+\delta}$$

for $N >> 0$ *and* $\delta =$ *abs const.*

Sum-product theorem

- Sum set

$$A + A = \{a_1 + a_2 : a_i \in A\}$$

- Product Set

$$AA = \{a_1 a_2 : a_i \in A\}$$

- ERDÖS-SZEMERÉDI

Theorem. $A \subset \mathbf{Z}$, $|A| = N$

$$|A + A| + |AA| > N^{1+\delta}$$

for $N >> 0$ *and* $\delta =$ *abs const.*

<u>Erdös-Szemerédi Conjecture</u>

$$|A + A| + |AA| > cN^{2-\epsilon}, \forall\, \epsilon > 0,$$

where $c = c(\epsilon)$.

Many people worked on this problem. The most noticeable result is the one by Elekes, using Szemeredi-Trotter theorem. The record holder is Solymosi. Many people study the problem in other algebraic structures, in particular, finite fields and integer residue rings. The theory has many applications in pseudo-randomness and exponential sums.

Balog-Szemeredi-Gowers theorem

Theorem.

- $\langle R, +\rangle =$ *group*
- $A, B \subset R$, $|A| = |B| = N$

Balog-Szemeredi-Gowers theorem

Theorem.

- $\langle R, +\rangle =$ *group*
- $A, B \subset R$, $|A| = |B| = N$

- $\mathcal{G} \subset A \times B$,

$$|\mathcal{G}| > \frac{1}{K} N^2$$

and

$$|\{x + y : (x, y) \in \mathcal{G}\}| < KN$$

Balog-Szemeredi-Gowers theorem

pplied in additive or multiplicative form.

Theorem.

- $\langle R, +\rangle =$ *group*
- $A, B \subset R$, $|A| = |B| = N$

- $\mathcal{G} \subset A \times B$,

$$|\mathcal{G}| > \frac{1}{K} N^2$$

and

$$|\{x + y : (x, y) \in \mathcal{G}\}| < KN$$

$\Longrightarrow \quad \exists A_1 \subset A, \quad B_1 \subset B \quad$ *s. t.*

$$|A_1 + B_1| < K^C N$$

$$|\mathcal{G} \cap (A_1 \times B_1)| > K^{-C} N^2$$

where $C =$ *abs const.*

- $\chi =$ Dirichlet character mod q if

  $\chi : \mathbb{Z}/q\mathbb{Z} \to \{z \in \mathbb{C} : |z| = 1\}$

  $\chi(mn) = \chi(m)\chi(n)$

  $\chi(m) = 0$ if $\gcd(m, q) \neq 1$

- $\chi =$ Dirichlet character mod q if

  $\chi : \mathbb{Z}/q\mathbb{Z} \to \{z \in \mathbb{C} : |z| = 1\}$

  $\chi(mn) = \chi(m)\chi(n)$

  $\chi(m) = 0$ if $\gcd(m, q) \neq 1$

- $$\Big|\sum_{m=a+1}^{a+b} \chi(m)\Big|$$

- $\chi =$ Dirichlet character $\bmod q$ if

  $\chi : \mathbb{Z}/q\mathbb{Z} \to \{z \in \mathbb{C} : |z| = 1\}$

  $\chi(mn) = \chi(m)\chi(n)$

  $\chi(m) = 0$ if $\gcd(m, q) \neq 1$

- $$\Big|\sum_{m=a+1}^{a+b} \chi(m)\Big|$$

- 1. $q >> 0$

  2. $\chi \neq \chi_0$

  3. Want
  $$\Big|\sum_{m=a+1}^{a+b} \chi(m)\Big| < b\, q^{-\epsilon}$$

- POLYA-VINOGRADOV (1918)

Theorem. $\chi =$ *Dirichlet character* $\bmod p$
$\chi \neq$*principal*

$$\Rightarrow \Bigg| \sum_{m=a+1}^{a+b} \chi(m) \Bigg| < C p^{\frac{1}{2}} (\log p)$$

• POLYA-VINOGRADOV (1918)

Theorem. $\chi =$ *Dirichlet character* $\bmod p$
$\chi \neq$*principal*

$$\Rightarrow \Big| \sum_{m=a+1}^{a+b} \chi(m) \Big| < C p^{\frac{1}{2}} (\log p)$$

• BURGESS improvement (1962)

Theorem. $\forall \varepsilon > 0$, $\exists \delta > 0$ *s. t. if* $b > p^{\frac{1}{4}+\varepsilon}$

$$\Rightarrow \Big| \sum_{m=a+1}^{a+b} \chi(m) \Big| \ll p^{-\delta} b$$

Corollary. *Smallest quad non-res* $\bmod p$ *is at most* $p^{\frac{1}{4\sqrt{e}}+\varepsilon}$

Extensions of Burgess Method to Finite Fields $\mathbb{F}_{p^n}$

- $\{\omega_1, \ldots, \omega_n\}$ =basis for $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$

$$x \in \mathbb{F}_{p^n}, \quad x = x_1\omega_1 + \cdots + x_n\omega_n$$

- $B = \left\{ \sum_{j=1}^{n} x_j\omega_j : x_j \in [N_j, N_j{+}H_j], \quad \forall i \right\}$

Extensions of Burgess Method to Finite Fields $\mathbb{F}_{p^n}$

- $\{\omega_1, \ldots, \omega_n\}$ =basis for $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$

$$x \in \mathbb{F}_{p^n}, \quad x = x_1\omega_1 + \cdots + x_n\omega_n$$

- $B = \left\{ \sum_{j=1}^{n} x_j\omega_j : x_j \in [N_j, N_j + H_j], \quad \forall i \right\}$

- non-trivial estimates

$$\left| \sum_{x \in B} \chi(x) \right| < |B|\, p^{-\epsilon}$$

(BURGESS, KARACUBA, DAVENPORT-LEWIS, $\cdots$)

Theorem. *(DAVENPORT-LEWIS, 1963)*

- $\{\omega_1, \ldots, \omega_n\}$ = *arbitrary basis*

- $B = \left\{ \sum_{j=1}^{n} x_j \omega_j : x_j \in [N_j, N_j + H_j], \quad \forall i \right\}$

$H_j = H$, $\forall j$

with $H > p^{\frac{n}{2(n+1)}+\varepsilon}$ *for some* $\varepsilon > 0$

Theorem. *(DAVENPORT-LEWIS, 1963)*

- $\{\omega_1, \ldots, \omega_n\}$ = *arbitrary basis*

- $B = \Big\{ \sum_{j=1}^{n} x_j \omega_j : x_j \in [N_j, N_j + H_j], \quad \forall i \Big\}$

$H_j = H$, $\forall j$

with $H > p^{\frac{n}{2(n+1)}+\varepsilon}$ *for some* $\varepsilon > 0$

$\Longrightarrow$ *for* $p > p(\varepsilon)$ $\quad \Big| \sum_{x \in B} \chi(x) \Big| < (p^{-\varepsilon_1} H)^n$

for some $\varepsilon_1 = \varepsilon_1(\varepsilon) > 0$

Theorem. *(DAVENPORT-LEWIS, 1963)*

- $\{\omega_1, \ldots, \omega_n\}$ = *arbitrary basis*

- $B = \left\{ \sum_{j=1}^{n} x_j \omega_j : x_j \in [N_j, N_j + H_j], \quad \forall i \right\}$

$H_j = H$, $\forall j$

with $H > p^{\frac{n}{2(n+1)}+\varepsilon}$ *for some* $\varepsilon > 0$

$\implies$ *for* $p > p(\varepsilon)$ $\quad \left| \sum_{x \in B} \chi(x) \right| < (p^{-\varepsilon_1} H)^n$

for some $\varepsilon_1 = \varepsilon_1(\varepsilon) > 0$

- For $n = 1$, this is Burgess' result

- $\frac{n}{2(n+1)} \to \frac{1}{2}$ for n large

Theorem. *KARACUBA '70, BURGESS '67 ($n = 2$)*

- θ=*algebraic integer*

irr$_{\mathbb{Z}}(\theta)$ *is irreducible* $(\bmod\, p)$

- $\omega_1 = 1, \omega_2 = \theta, \ldots, \omega_n = \theta^{n-1}$

$$\omega_i \omega_j = \sum_{1 \le r \le n} d_{ijr} \omega_r \qquad \textit{with } |d_{ijr}| < C$$

Theorem. *KARACUBA '70, BURGESS '67* ($n = 2$)

- θ=*algebraic integer*

irr$_{\mathbb{Z}}(\theta)$ *is irreducible* $(\bmod p)$

- $\omega_1 = 1, \omega_2 = \theta, \dots, \omega_n = \theta^{n-1}$

$$\omega_i \omega_j = \sum_{1 \le r \le n} d_{ijr} \omega_r \qquad \textit{with } |d_{ijr}| < C$$

- $B = \left\{ \sum_{j=1}^{n} x_j \omega_j : x_j \in [N_j, N_j + H_j], \quad \forall i \right\}$

$H_j > p^{\frac{1}{4}+\varepsilon}, \quad \forall j$ *for some* $\varepsilon > 0$

$$\Longrightarrow \left| \sum_{x \in B} \chi(x) \right| < p^{-\delta} |B|$$

Theorem. *(CH, 07)*

- $\{\omega_1, \ldots, \omega_n\}$ = *arbitrary basis*

- $B = \left\{ \sum_{j=1}^{n} x_j \omega_j : x_j \in [N_j, N_j + H_j], \quad \forall i \right\}$

$$\prod_{j=1}^{n} H_j > \left(p^n\right)^{\frac{2}{5}+\varepsilon}$$

for some $\varepsilon > 0$

Theorem. *(CH, 07)*

- $\{\omega_1, \ldots, \omega_n\}$ = *arbitrary basis*

- $B = \Big\{ \sum_{j=1}^{n} x_j \omega_j : x_j \in [N_j, N_j + H_j], \quad \forall i \Big\}$

$$\prod_{j=1}^{n} H_j > \left(p^n\right)^{\frac{2}{5}+\varepsilon}$$

for some $\varepsilon > 0$

$$\Longrightarrow \Big| \sum_{x \in B} \chi(x) \Big| \ll p^{-\frac{\varepsilon^2}{4}} |B|,$$

Theorem. *(CH, 07)*

- $\{\omega_1, \dots, \omega_n\}$ = *arbitrary basis*

- $B = \Big\{ \sum_{j=1}^{n} x_j \omega_j : x_j \in [N_j, N_j + H_j], \quad \forall i \Big\}$

$$\prod_{j=1}^{n} H_j > \Big(p^n\Big)^{\frac{2}{5}+\varepsilon}$$

for some $\varepsilon > 0$

$$\Longrightarrow \Big| \sum_{x \in B} \chi(x) \Big| \ll p^{-\frac{\varepsilon^2}{4}} |B|,$$

unless n =*even*

$\chi|_{F_2}$ =*principal, where* $F_2 < \mathbb{F}_{p^n}$, $|F_2| = p^{n/2}$

$$\Big| \sum_{x \in B} \chi(x) \Big| \le \max_{\xi} |B \cap \xi F_2| + O(p^{-\frac{\varepsilon^2}{4}} |B|)$$

Theorem. *(Konyagin, 09)*

- $\{\omega_1, \ldots, \omega_n\}$ = *arbitrary basis*

- $B = \left\{ \sum_{j=1}^{n} x_j \omega_j : x_j \in [N_j, N_j + H_j], \quad \forall i \right\}$

$$H_j > p^{\frac{1}{4}+\epsilon}, \ \forall j$$

$$\Longrightarrow \left| \sum_{x \in B} \chi(x) \right| \ll_n p^{-\delta} |B| e$$

where $\delta = \delta(\epsilon) > 0$.

Character Sums over Arithmetic Progressions

$\mathbb{F}_p$ only (similar results for $\mathbb{F}_{p^n}$ with worse exponent)

Theorem. *(Ch 07)*

$P =$ *proper* d*-dim gen arith progression in* $\mathbb{F}_p$

$$|P| > p^{\frac{2}{5}+\varepsilon},\ \textit{some}\ \varepsilon > 0$$

Character Sums over Arithmetic Progressions

$\mathbb{F}_p$ only (similar results for $\mathbb{F}_{p^n}$ with worse exponent)

Theorem. *(Ch 07)*

$P =$ *proper d-dim gen arith progression in* $\mathbb{F}_p$

$$|P| > p^{\frac{2}{5}+\varepsilon}, \text{ some } \varepsilon > 0$$

$\Longrightarrow$ *for* $p > p(\varepsilon, d)$,

$$\Big| \sum_{x \in P} \chi(x) \Big| < p^{-\tau} |P|$$

for some $\tau = \tau(d) > 0$

- the exponent $\frac{2}{5} < \frac{1}{2}$ does not depend on d

Corollary (CH, 07)

$A \subset \mathbb{F}_p$

(i) $|A| > p^{2/5+\varepsilon}$

(ii) $|A + A| < C_0|A|$.

Corollary (CH, 07)

$A \subset \mathbb{F}_p$

(i) $|A| > p^{2/5+\varepsilon}$

(ii) $|A + A| < C_0|A|$.

$\Longrightarrow \exists k = k(C_0, \varepsilon) \in \mathbb{Z}^+$, $\kappa = \kappa(C_0, \varepsilon)$ s.t.

$$|A^k| > \kappa p.$$

Corollary (CH, 07)

$A \subset \mathbb{F}_p$

(i) $|A| > p^{2/5+\varepsilon}$

(ii) $|A + A| < C_0|A|$.

$\Longrightarrow \exists k = k(C_0, \varepsilon) \in \mathbb{Z}^+$, $\kappa = \kappa(C_0, \varepsilon)$ s.t.

$$|A^k| > \kappa p.$$

• use Freiman's theorem, sum-product, character sums

Primitive Roots of $\mathbb{F}_{p^n}$

Corollary. $B = \{\sum \omega_j x_j ; N_j < x_j < N_j + H_j\}$

$$\prod H_j > \left(p^n\right)^{\frac{2}{5}+\varepsilon}$$

$$\implies \left|\left\{\textit{primitive roots of } \mathbb{F}_{p^n} \textit{ in } B\right\}\right|$$

$$= \frac{\varphi(p^n - 1)}{p^n - 1}|B|\Big(1 + o(p^{-\tau})\Big)$$

Primitive Roots of $\mathbb{F}_{p^n}$

Corollary. $B = \{\sum \omega_j x_j; N_j < x_j < N_j + H_j\}$

$$\prod H_j > \left(p^n\right)^{\frac{2}{5}+\varepsilon}$$

$$\Longrightarrow \quad \left|\left\{\textit{primitive roots of } \mathbb{F}_{p^n} \textit{ in } B\right\}\right|$$

$$= \frac{\varphi(p^n-1)}{p^n-1}|B|\Big(1+o(p^{-\tau})\Big)$$

combining character sums estimate with

$$\frac{\varphi(p^n-1)}{p^n-1}\left\{1+\sum_{\substack{d|p^n-1\\ d>1}} \frac{\mu(d)}{\varphi(d)} \sum_{\text{ord}(\chi)=d} \chi(x)\right\}$$

$$=\begin{cases} 1 \text{ if } x \text{ is primitive} \\ 0 \quad \text{otherwise} \end{cases}$$

Multilinear Character Sum

- $(L_i)_{1\le i\le n}$ linear forms in n variables over $\mathbb{F}_p$

$$\det(L_i)_{1\le i\le n} \neq 0$$

- $$B = \prod_{i=1}^{n} [a_i,\ a_i + H]$$

- non-trivial estimates

$$\Big|\sum_{x\in B} \chi\Big(\prod_{j=1}^{n} L_j(x)\Big)\Big| < p^{-\delta} H^n$$

Multilinear Character Sum

- $(L_i)_{1\le i\le n}$ linear forms in n variables over $\mathbb{F}_p$

$$\det(L_i)_{1\le i\le n} \neq 0$$

- $$B = \prod_{i=1}^{n} [a_i,\ a_i + H]$$

- non-trivial estimates

$$\Big| \sum_{x\in B} \chi\Big(\prod_{j=1}^{n} L_j(x) \Big) \Big| < p^{-\delta} H^n$$

Theorem. *(Burgess) Assume*

$$H > p^{\frac{1}{2} - \frac{1}{2(n+1)} + \varepsilon}.$$

$n = 1,\ H > p^{\frac{1}{4}+\varepsilon}$.
$n = 2,\ H > p^{\frac{1}{3}+\varepsilon}$.

Multilinear Character Sum

- $(L_i)_{1\le i\le n}$ linear forms in n variables over $\mathbb{F}_p$

$$\det(L_i)_{1\le i\le n} \ne 0$$

- $$B = \prod_{i=1}^{n} [a_i,\ a_i + H]$$

- non-trivial estimates

$$\Big| \sum_{x\in B} \chi\Big(\prod_{j=1}^{n} L_j(x)\Big)\Big| < p^{-\delta} H^n$$

Theorem. *(Burgess) Assume*

$$H > p^{\frac{1}{2}-\frac{1}{2(n+1)}+\varepsilon}.$$

$n = 1,\ H > p^{\frac{1}{4}+\varepsilon}.$
$n = 2,\ H > p^{\frac{1}{3}+\varepsilon}.$

Theorem. *(Bourgain-CH, 09) Assume*

$$H > p^{\frac{1}{4}+\varepsilon}, \quad \textit{for any } n.$$

Character Sums of Polynomials

- $f(x_1, \ldots, x_d)$ homog, splits over $\overline{\mathbb{F}_p}$
  $\deg(f) = d$
  $f(x_1, \ldots, x_d)$ non-reduced.

- $$B = \prod_{i=1}^{d} [a_i, a_i + H] \subset \mathbb{F}_p^d$$

Character Sums of Polynomials

- $f(x_1, \ldots, x_d)$ homog, splits over $\overline{\mathbb{F}_p}$
  $\deg(f) = d$
  $f(x_1, \ldots, x_d)$ non-reduced.
- $$B = \prod_{i=1}^{d} [a_i, a_i + H] \subset \mathbb{F}_p^d$$
- non-trivial estimates

$$\Big| \sum_{x \in B} \chi(f(x)) \Big| < p^{-\delta} H^d$$

Theorem. *(Gillett, 1973) Assume*

$$H > p^{\frac{d}{2(d+1)} + \varepsilon}.$$

Character Sums of Polynomials

- $f(x_1, \ldots, x_d)$ homog, splits over $\overline{\mathbb{F}_p}$
  $\deg(f) = d$
  $f(x_1, \ldots, x_d)$ non-reduced.
- $$B = \prod_{i=1}^{d} [a_i, a_i{+}H] \subset \mathbb{F}_p^d$$
- non-trivial estimates

$$\Big| \sum_{x \in B} \chi(f(x)) \Big| < p^{-\delta} H^d$$

Theorem. *(Gillett, 1973) Assume*

$$H > p^{\frac{d}{2(d+1)}+\varepsilon}.$$

Theorem. *(Bourgain-CH, 09) Assume*

$$H = p^{\frac{1}{4}+\varepsilon}.$$

Mixed Character Sums over $\mathbb{F}_{p^n}$

Theorem. *(CH, 09)*

- $\{\omega_1, \ldots, \omega_n\}$ = *arbitrary basis*
- $$B = \Big\{ \sum_{j=1}^{n} x_j \omega_j : x_j \in [1, H], \forall j \Big\}$$

$$H > p^{\frac{1}{4} + \kappa}$$

Mixed Character Sums over $\mathbb{F}_{p^n}$

Theorem. *(CH, 09)*

- $\{\omega_1, \ldots, \omega_n\}$ = *arbitrary basis*

- $$B = \Big\{ \sum_{j=1}^{n} x_j \omega_j : x_j \in [1, H], \forall j \Big\}$$

$$H > p^{\frac{1}{4}+\kappa}$$

- $f \in \mathbb{R}[x_1, \ldots, x_n]$ *arbitrary of degree* d

$$\Longrightarrow \Big| \sum_{x \in B} e\Big(f(x)\Big)\chi(x) \Big| < c(n,\kappa)(d+1)^2 p^{-\delta} |B|,$$

Mixed Character Sums over $\mathbb{F}_{p^n}$

Theorem. *(CH, 09)*

- $\{\omega_1, \ldots, \omega_n\} =$ *arbitrary basis*
- $$B = \Big\{ \sum_{j=1}^{n} x_j \omega_j : x_j \in [1, H], \forall j \Big\}$$

$$H > p^{\frac{1}{4}+\kappa}$$

- $f \in \mathbb{R}[x_1, \ldots, x_n]$ *arbitrary of degree* d

$$\Longrightarrow \Big| \sum_{x \in B} e\Big(f(x)\Big)\chi(x) \Big| < c(n,\kappa)(d+1)^2 p^{-\delta} |B|,$$

where $$\delta = \frac{\kappa^2 n}{4(1+2\kappa)(2n+(d+1)^2)}.$$

FRIEDLANDER-IWANIEC $\quad n = 1$, f linear

Mixed Character Sums over $\mathbb{F}_{p^n}$

Theorem. *(CH, 09)*

- $\{\omega_1, \dots, \omega_n\}$ = *arbitrary basis*

- $$B = \Big\{ \sum_{j=1}^{n} x_j \omega_j : x_j \in [1, H], \forall j \Big\}$$

$$H > p^{\frac{1}{4}+\kappa}$$

- $f \in \mathbb{R}[x_1, \dots, x_n]$ *arbitrary of degree* d

$$\Longrightarrow \Big| \sum_{x \in B} e\Big(f(x)\Big)\chi(x) \Big| < c(n,\kappa)(d+1)^2 p^{-\delta} |B|,$$

where $$\delta = \frac{\kappa^2 n}{4(1+2\kappa)(2n+(d+1)^2)}.$$

ENFLO $\sum_{x \leq \sqrt{p}} e^{2\pi i f(x)} (\frac{x}{p}) \ll p^{1/2-\epsilon}$

HEATH-BROWN

$$\sum_{N < x \leq N+H} e^{2\pi i f(x)} \chi(x) \ll H^{1-1/2^d r} p^{(r+1)/2^{d+2} r^2} + \epsilon$$

Short Character Sums with Composite Moduli

Theorem. *(CH, 10)*

- $q = q_1^m p$ *with* $(q_1, p) = 1$
- $I \subset [1, q]$ *of size* $|I| > q_1 p^{\frac{1}{4}+\kappa}$

Short Character Sums with Composite Moduli

Theorem. *(CH, 10)*

- $q = q_1^m p$ *with* $(q_1, p) = 1$
- $I \subset [1, q]$ *of size* $|I| > q_1 p^{\frac{1}{4}+\kappa}$
- $\chi =$ *mult char (mod* q*)* $\chi = \chi_1 \chi_2$

  χ_1 *(mod* q_1^m*) arbitrary*

  χ_2 *(mod* p*) non-principal*

Short Character Sums with Composite Moduli

Theorem. *(CH, 10)*

- $q = q_1^m p$ *with* $(q_1, p) = 1$
- $I \subset [1, q]$ *of size* $|I| > q_1 p^{\frac{1}{4}+\kappa}$
- $\chi =$ *mult char (mod* q*)* $\chi = \chi_1 \chi_2$

  χ_1 *(mod* q_1^m*) arbitrary*

  χ_2 *(mod* p*) non-principal*

$$\Longrightarrow \Big| \sum_{n \in I} \chi(n) \Big| < |I| \, p^{-c\kappa^2 m^{-2}}$$

Short Character Sums with Composite Moduli

Theorem. *(CH, 10)*

- $q = q_1^m p$ *with* $(q_1, p) = 1$
- $I \subset [1, q]$ *of size* $|I| > q_1 p^{\frac{1}{4}+\kappa}$
- $\chi =$ *mult char (mod* q*)* $\chi = \chi_1 \chi_2$

  χ_1 *(mod* q_1^m*) arbitrary*

  χ_2 *(mod* p*) non-principal*

$$\Longrightarrow \left| \sum_{n \in I} \chi(n) \right| < |I|\, p^{-c\kappa^2 m^{-2}}$$

Similar result:

- $q = q_1^m q_2$ with $(q_1, q_2) = 1$

  q_2 square free
- χ_2 (mod q_2) primitive

Short Character Sums with Composite Moduli

Theorem. *(CH, 10)*

- $q = q_1^m p$ *with* $(q_1, p) = 1$
- $I \subset [1, q]$ *of size* $|I| > q_1 p^{\frac{1}{4}+\kappa}$
- $\chi =$ *mult char (mod* q*)* $\chi = \chi_1 \chi_2$

  χ_1 *(mod* q_1^m*) arbitrary*

  χ_2 *(mod* p*) non-principal*

$$\Longrightarrow \Big| \sum_{n \in I} \chi(n) \Big| < |I| \, p^{-c\kappa^2 m^{-2}}$$

Similar result:

- $q = q_1^m q_2$ with $(q_1, q_2) = 1$

  q_2 square free
- χ_2 (mod q_2) primitive

$$\Longrightarrow \Big| \sum_{n \in I} \chi(n) \Big| < \left[\tau(q_2)^{c \log m} q_2^{-c\kappa^2} \right]^{\frac{1}{m^2}} |I|$$

Short Dirichlet Sums

Theorem. *(CH, 10)*

- $\chi \neq$ *principal (mod p)*
- $|t| > 1$
- $N > p^{\frac{1}{4}+\kappa}$

Short Dirichlet Sums

Theorem. *(CH, 10)*

- $\chi \neq$ *principal (mod p)*
- $|t| > 1$
- $N > p^{\frac{1}{4}+\kappa}$

$$\Rightarrow \Big| \sum_{n=1}^{N} \chi(n) n^{it} \Big| \ll N \exp\left(-c(\kappa)\frac{(\log p)^3}{(\log p|t|)^2}\right)$$

Short Dirichlet Sums

Theorem. *(CH, 10)*

- $\chi \neq$ *principal (mod p)*
- $|t| > 1$
- $N > p^{\frac{1}{4}+\kappa}$

$$\Rightarrow \Big| \sum_{n=1}^{N} \chi(n) n^{it} \Big| \ll N \exp\left(-c(\kappa) \frac{(\log p)^3}{(\log p|t|)^2} \right)$$

$\diamond$ Vinogradov's bound for $|t| > N$

$$\Big| \sum_{n=1}^{N} n^{it} \Big| \ll N \exp\left(-\, c \frac{(\log N)^3}{(\log |t|)^2} \right)$$

Short Dirichlet Sums

Theorem. *(CH, 10)*

- $\chi \neq$*principal (mod p)*
- $|t| > 1$
- $N > p^{\frac{1}{4}+\kappa}$

$$\Rightarrow \Big|\sum_{n=1}^{N} \chi(n)n^{it}\Big| \ll N \exp\left(-c(\kappa)\frac{(\log p)^3}{(\log p|t|)^2}\right)$$

$\diamond$ Vinogradov's bound for $|t| > N$

$$\Big|\sum_{n=1}^{N} n^{it}\Big| \ll N \exp\left(-c\frac{(\log N)^3}{(\log |t|)^2}\right)$$

$\diamond$ Similar results for square-free moduli

$\diamond$ Applications to zero-density estimates for $L(\sigma + it, \chi)$ with $|t|$ large and σ near 1

Around the Paley Graph Conjecture

$q =$ prime power
$q \equiv 1 \pmod 4 \Rightarrow -1$ has square root in $\mathbb{F}_q$

Around the Paley Graph Conjecture

$q =$ prime power
$q \equiv 1 \pmod 4 \Rightarrow -1$ has square root in $\mathbb{F}_q$

$$V = \mathbb{F}_q$$

$$E = \Big\{\{a, b\} \in \mathbb{F}_q \times \mathbb{F}_q : a - b \in (\mathbb{F}_q^*)^2\Big\}$$

$G = (V, E)$ is *Paley graph of order* q

Around the Paley Graph Conjecture

$q =$ prime power
$q \equiv 1 \pmod 4 \Rightarrow -1$ has square root in $\mathbb{F}_q$

$$V = \mathbb{F}_q$$

$$E = \Big\{ \{a,b\} \in \mathbb{F}_q \times \mathbb{F}_q : a - b \in (\mathbb{F}_q^*)^2 \Big\}$$

$G = (V, E)$ is *Paley graph of order* q

Problem. What is the size of the largest clique in G?

Around the Paley Graph Conjecture

$q =$ prime power
$q \equiv 1 \pmod 4 \Rightarrow -1$ has square root in $\mathbb{F}_q$

$$V = \mathbb{F}_q$$

$$E = \left\{ \{a,b\} \in \mathbb{F}_q \times \mathbb{F}_q : a - b \in (\mathbb{F}_q^*)^2 \right\}$$

$G = (V, E)$ is *Paley graph of order* q

Problem. What is the size of the largest clique in G?

• If $q = p^{2n}$, $p \neq 2$, then the clique number is p^n

A. BLOKHUIS: If $q = p^{2n}$, $p \neq 2$, then the q-cliques are lines

For q prime, it is conjectured that the clique number is $\sim \log p$

Character Sums over Sumsets

KARACUBA

Find non-trivial bound on

$$\sum_{x \in A, y \in B} \chi(x+y)$$

for $|A| \sim p^{\frac{1}{2}} \sim |B|$.

Character Sums over Sumsets

KARACUBA
Find non-trivial bound on

$$\sum_{x \in A, y \in B} \chi(x + y)$$

for $|A| \sim p^{\frac{1}{2}} \sim |B|$.

- known if $|A| > p^{\frac{1}{2}+\delta}$ and $|B| > p^{\delta}$ for some $\delta > 0$.

Theorem. *(CH, 07)*
Assume $A, B \subset \mathbb{F}_p$ *such that*

(a) $|A| > p^{\frac{4}{9}+\varepsilon}, |B| > p^{\frac{4}{9}+\varepsilon}$

(b) $|B + B| < K|B|$.

Theorem. *(CH, 07)*
Assume $A, B \subset \mathbb{F}_p$ *such that*

(a) $|A| > p^{\frac{4}{9}+\varepsilon}, |B| > p^{\frac{4}{9}+\varepsilon}$

(b) $|B+B| < K|B|$.

Then

$$\Big|\sum_{x\in A, y\in B} \chi(x+y)\Big| < p^{-\tau}|A|\,|B|,$$

where $\tau = \tau(\varepsilon, K) > 0$, $p > p(\varepsilon, K)$.

Theorem. *(CH, 07)*
Assume $A, B \subset \mathbb{F}_p$ *such that*

(a) $|A| > p^{\frac{4}{9}+\varepsilon}, |B| > p^{\frac{4}{9}+\varepsilon}$

(b) $|B + B| < K|B|$.

Then

$$\Big|\sum_{x\in A, y\in B} \chi(x+y)\Big| < p^{-\tau}|A|\,|B|,$$

where $\tau = \tau(\varepsilon, K) > 0$, $p > p(\varepsilon, K)$.

• use Freiman's theorem, sum-product estimate

Main Ingredients in Burgess' Proof

- Shifted product (Vinogradov)

- Multiplicative energy of an interval

$$E(A,B) = \left|\left\{(a_1,a_2,b_1,b_2) \in A^2 \times B^2 : a_1b_1 = a_2b_2\right\}\right|$$

Main Ingredients in Burgess' Proof

- Shifted product (Vinogradov)

- Multiplicative energy of an interval

$$E(A,B) = \left|\left\{(a_1,a_2,b_1,b_2) \in A^2 \times B^2 : a_1b_1 = a_2b_2\right\}\right|$$

Lemma. $I, J =$ *intervals with* $|I|\,|J| < p$

$$\Rightarrow E(I,J) < c \log p\, |I|\,|J|$$

(Friedlander-Iwaniec)

Main Ingredients in Burgess' Proof

- Shifted product (Vinogradov)

- Multiplicative energy of an interval

$$E(A,B) = \left|\left\{(a_1,a_2,b_1,b_2) \in A^2 \times B^2 : a_1b_1 = a_2b_2\right\}\right|$$

Lemma. $I, J =$*intervals with* $|I|\,|J| < p$

$$\Rightarrow E(I,J) < c \log p\, |I|\,|J|$$

(Friedlander-Iwaniec)

- Weil's Inequality

Theorem. $\chi =$ *mult character of* $\mathbb{F}_{p^n}$
$\chi \neq$*principal, ord*$(\chi) = d > 1$
$f \in \mathbb{F}_{p^n}[X]$ *has* m *distinct roots,* $f \neq g^d$

$$\Rightarrow \left| \sum_{x \in \mathbb{F}_{p^n}} \chi\Big(f(x)\Big) \right| \leq (m-1)p^{\frac{n}{2}}$$

Sketch of Proof

$I =$ interval, $I \subset [1, p)$, $|I| = p^{\frac{1}{4}+\varepsilon}$

$$J = [1, p^{\frac{1}{4}}], \quad T = [1, p^{\frac{\varepsilon}{2}}], \qquad y \in J, t \in T$$

Sketch of Proof

$I =$ interval, $I \subset [1, p)$, $|I| = p^{\frac{1}{4}+\varepsilon}$

$J = [1, p^{\frac{1}{4}}], \quad T = [1, p^{\frac{\varepsilon}{2}}], \qquad y \in J, t \in T$

- $\displaystyle\sum_{x \in I} \chi(x) = p^{-\frac{1}{4}-\frac{\varepsilon}{2}} \sum_{\substack{x \in I, y \in J \\ t \in T}} \chi(x + yt) + O(p^{-\frac{\varepsilon}{2}}|I|)$

Sketch of Proof

$I =$ interval, $I \subset [1, p)$, $|I| = p^{\frac{1}{4}+\varepsilon}$

$$J = [1, p^{\frac{1}{4}}], \quad T = [1, p^{\frac{\varepsilon}{2}}], \qquad y \in J, t \in T$$

- $\displaystyle\sum_{x \in I} \chi(x) = p^{-\frac{1}{4}-\frac{\varepsilon}{2}} \sum_{\substack{x \in I, y \in J \\ t \in T}} \chi(x + yt) + O(p^{-\frac{\varepsilon}{2}}|I|)$

- $\displaystyle\Big| \sum_{\substack{x \in I, y \in J \\ t \in T}} \chi(x + yt) \Big| \le \sum_{x \in I, y \in J} \Big| \sum_{t \in T} \chi(xy^{-1} + t) \Big|$

$$= \sum_{u \in \mathbb{F}_p^*} \eta(u) \Big| \sum_{t \in T} \chi(u + t) \Big|$$

$$\eta(u) = |\{x \in I, y \in J : x = uy \pmod p\}|$$

$$\bullet \left|\sum_{\substack{x\in I, y\in J\\ t\in T}} \chi(x+yt)\right| \le \sum_{x\in I, y\in J}\left|\sum_{t\in T}\chi(xy^{-1}+t)\right|$$

$$= \sum_{u\in\mathbb{F}_p^*}\eta(u)\left|\sum_{t\in T}\chi(u+t)\right|$$

$$\eta(u) = |\{x\in I, y\in J : x = uy \pmod p\}|$$

For $2r \gg 0$, Hölder's inequality gives

$$\sum_{u\in\mathbb{F}_p^*}\eta(u)\left|\sum_{t\in T}\chi(u+t)\right|$$

$$\le \underbrace{\left[\sum_u \eta(u)^{\frac{2r}{2r-1}}\right]^{1-\frac{1}{2r}}}_{(1)} \underbrace{\left[\sum_u \left|\sum_{t\in T}\chi(u+t)\right|^{2r}\right]^{\frac{1}{2r}}}_{(2)}$$

Konyagin's Argument of bounding $E(B)$

- $\{\omega_1, \dots, \omega_n\}$ = basis for F_{p^n} over F_p
  $B = B_H = \prod_{i=1}^{n} [1, H] \subset \mathbb{Z}^n$

- $$E(B) = \Big| \Big\{ (x, x', y, y') \in B^4 : \sum_i x'_i \omega_i \sum_i y_i \omega_i = \sum_i y'_i \omega_i \sum_i x_i \omega_i \Big\} \Big|$$

Konyagin's Argument of bounding $E(B)$

- $\{\omega_1, \dots, \omega_n\}$ = basis for F_{p^n} over F_p
  $B = B_H = \prod_{i=1}^n [1, H] \subset \mathbb{Z}^n$

- $E(B) = \Big| \Big\{ (x, x', y, y') \in B^4 :$

$$\sum_i x'_i \omega_i \sum_i y_i \omega_i = \sum_i y'_i \omega_i \sum_i x_i \omega_i \Big\} \Big|$$

$$\frac{y}{x} = \frac{y'}{x'} = z$$

Konyagin's Argument of bounding $E(B)$

- $\{\omega_1, \ldots, \omega_n\}$ = basis for F_{p^n} over F_p
  $B = B_H = \prod_{i=1}^n [1, H] \subset \mathbb{Z}^n$
- $E(B) = \Big| \Big\{ (x, x', y, y') \in B^4 :$

$$\sum_i x'_i \omega_i \sum_i y_i \omega_i = \sum_i y'_i \omega_i \sum_i x_i \omega_i \Big\} \Big|$$

- Fix $z \in \mathbb{F}_{p^n}$

  $\mathcal{L}_z = \Big\{ (x, y) \in \mathbb{Z}^{2n} : \sum y_i \omega_i = z \left(\sum x_i \omega_i \right) \Big\}$
- $E(B) \leq \sum_{z \in \mathbb{F}^*_{p^n}} |\mathcal{L}_z \cap B^2|^2 + O(H^{2n})$.

Konyagin's Argument of bounding $E(B)$

- $\{\omega_1, \ldots, \omega_n\}$ = basis for F_{p^n} over F_p
  $B = B_H = \prod_{i=1}^n [1, H] \subset \mathbb{Z}^n$

- $$E(B) = \left|\left\{(x, x', y, y') \in B^4 : \sum_i x'_i \omega_i \sum_i y_i \omega_i = \sum_i y'_i \omega_i \sum_i x_i \omega_i \right\}\right|$$

- Fix $z \in \mathbb{F}_{p^n}$

  $\mathcal{L}_z = \left\{(x, y) \in \mathbb{Z}^{2n} : \sum y_i \omega_i = z \left(\sum x_i \omega_i\right)\right\}$

- $E(B) \leq \sum_{z \in \mathbb{F}^*_{p^n}} |\mathcal{L}_z \cap B^2|^2 + O(H^{2n})$.

$C = [-1, 1]^{2n}$

- successive minimum $\lambda_i = \lambda_i(z) = \lambda_i(C, \mathcal{L}_z)$

$\lambda_i = \min\{\lambda > 0 : \lambda C \supset i$ indep elements of $\mathcal{L}_z\}$

- (Minkowski)

$$\frac{2^{2n}}{(2n)!}\,\frac{d(\mathcal{L}_z)}{V(C)} \leq \lambda_1 \cdots \lambda_{2n} \leq 2^{2n}\,\frac{d(\mathcal{L}_z)}{V(C)}$$

$$\lambda_1 \cdots \lambda_{2n} \sim p^n$$

- (Minkowski)

$$\frac{2^{2n}}{(2n)!}\,\frac{d(\mathcal{L}_z)}{V(C)} \le \lambda_1 \cdots \lambda_{2n} \le 2^{2n}\,\frac{d(\mathcal{L}_z)}{V(C)}$$

$$\lambda_1 \cdots \lambda_{2n} \sim p^n$$

- (Minkowski+ Mahler) $\lambda_i^* = \lambda_i(C^\circ, \mathcal{L}_z^*)$

$$\lambda_i \lambda_{2n+1-i}^* \sim 1$$

Multilinear Character Sum

- $(L_i)_{1 \le i \le n}$ linear forms in n variables over $\mathbb{F}_p$

$$\det(L_i)_{1 \le i \le n} \neq 0$$

- $$B = \prod_{i=1}^{n} [a_i,\ a_i + H]$$

- non-trivial estimates

$$\left| \sum_{x \in B} \chi\Big(\prod_{j=1}^{n} L_j(x) \Big) \right| < p^{-\delta} H^n$$

the case of multilinear character sum

- $L_i = (\ell_{i,1}, \ldots, \ell_{i,n}) \in \mathbb{Z}^n$, $\det(L_1, \ldots L_n) \neq 0$
- Estimate

$$E(B_H) = |\{(x, y, x', y') \in B_H^4 : \\ L_i x\, L_i y \equiv L_i x'\, L_i y',\ i = 1, \ldots, n\}|$$

Character Sums of Polynomials

- $f(x_1, \ldots, x_d)$ homog, splits over $\overline{\mathbb{F}_p}$
  $\deg(f) = d$
  $f(x_1, \ldots, x_d)$ non-reduced.

- $$B = \prod_{i=1}^{d} [a_i, a_i + H] \subset \mathbb{F}_p^d$$

- non-trivial estimates

$$\Big| \sum_{x \in B} \chi(f(x)) \Big| < p^{-\delta} H^d$$

the polynomial case

$$f(x+ty)$$
$$= f(x) + g_1(x,y)t + \cdots + g_{d-1}(x,y)t^{d-1} + f(y)t^d$$

- non-trivial estimate

$$\Big| \sum_{\substack{x \in B_H,\, y \in B_{H_1} \\ 0<t<p^\tau}} \chi\Big(f(x+yt)\Big) \Big|$$

where $B_{H_1} = [0, H_1)^d$, $H_1 = Hp^{-2\tau}$

the polynomial case

$$\begin{aligned} & f(x+ty) \\ = & f(x)+g_1(x,y)t+\cdots+g_{d-1}(x,y)t^{d-1}+f(y)t^d \end{aligned}$$

- non-trivial estimate

$$S = \Big| \sum_{\substack{x\in B_H,\, y\in B_{H_1} \\ 0<t<p^\tau}} \chi\Big(f(x+yt)\Big) \Big|$$

where $B_{H_1} = [0, H_1)^d$, $H_1 = Hp^{-2\tau}$

- $\displaystyle \sum_{x\in B_H,\, y\in B_{H_1}} \Big| \sum_{t<p^\tau} \chi\Big(f(x+ty)\Big) \Big|$

$$= \sum_{z_0,z_1,\ldots,z_{d-1}\in \mathbb{F}_p} \eta(z_0, z_1 \ldots, z_{d-1}) \cdot \Big| \sum_{t<p^\tau} \chi(z_0 + z_1 t + \cdots + z_{d-1}t^{d-1} + t^d) \Big|$$

$\frac{f(x)}{f(y)} = z_0, \frac{g_1(x,y)}{f(y)} = z_1, \cdots, \frac{g_{d-1}(x,y)}{f(y)} = z_{d-1}$

- $\eta(z_0, z_1, \ldots, z_{d-1})$

$$= \left| \left\{ (x, y) \in B_H \times B_H : \frac{f(x)}{f(y)} = z_0, \frac{g_1(x, y)}{f(y)} = z_1, \cdots, \frac{g_{d-1}(x, y)}{f(y)} = z_{d-1} \right\} \right|.$$

- $\eta(z_0, z_1, \ldots, z_{d-1})$

$$= \Big| \Big\{ (x,y) \in B_H \times B_H : \frac{f(x)}{f(y)} = z_0, \frac{g_1(x,y)}{f(y)} = z_1, \cdots, \frac{g_{d-1}(x,y)}{f(y)} = z_{d-1} \Big\} \Big|.$$

- $\sum \eta(z)^2$

$$= \Big| \Big\{ (x, x', y, y') \in B_H^2 \times B_{H_1}^2 : \frac{g_i(x,y)}{f(y)} = \frac{g_i(x',y')}{f(y')}, \forall i \Big\} \Big|$$

$$= \Big| \Big\{ (x, x', y, y') \in B_H^2 \times B_{H_1}^2 : f(x+ty) \text{ and } f(x'+ty'$$

have the same roots in $t \in \overline{\mathbb{F}_p} \Big\} \Big|$

- $\eta(z_0, z_1, \ldots, z_{d-1})$

$=\left|\left\{(x,y) \in B_H \times B_H :\right.\right.$
$\left.\left.\frac{f(x)}{f(y)} = z_0, \frac{g_1(x,y)}{f(y)} = z_1, \cdots, \frac{g_{d-1}(x,y)}{f(y)} = z_{d-1}\right\}\right|.$

- $\sum \eta(z)^2$

$=\left|\left\{(x,x',y,y') \in B_H^2 \times B_{H_1}^2 : \frac{g_i(x,y)}{f(y)} = \frac{g_i(x',y')}{f(y')}, \forall i\right\}\right|$

$=\left|\left\{(x,x',y,y') \in B_H^2 \times B_{H_1}^2 : f(x+ty) \text{ and } f(x'+ty'\right.\right.$
have the same roots in $\left.\left. t \in \overline{\mathbb{F}_p}\right\}\right|$

- factor

$$f(x) = \prod_{i=1}^{d} L_i(x)$$

with $L_i(x) = x_1 + \lambda_{i,2}x_2 + \cdots + \lambda_{i,d}, \lambda_{i,j} \in \overline{\mathbb{F}_p}$

- non-reduced implies

$$\det(L_i)_{1\leq i\leq d} = \begin{pmatrix} 1 & \lambda_{1,2} & \cdots & \lambda_{1,d} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ 1 & \lambda_{2,d} & \cdots & \lambda_{d,d} \end{pmatrix} \neq 0$$

- non-trivial estimate follows from multilinear case

Mixed Character Sums over $\mathbb{F}_{p^n}$

Theorem. *(CH, 09)*

- $\{\omega_1, \ldots, \omega_n\}$ = *arbitrary basis*
- $$B = \Big\{ \sum_{j=1}^{n} x_j \omega_j : x_j \in [1, H], \forall j \Big\}$$
  $$H > p^{\frac{1}{4}+\kappa}$$
- $f \in \mathbb{R}[x_1, \ldots, x_n]$ *arbitrary of degree* d

$$\Longrightarrow \Big| \sum_{x \in B} e\Big(f(x)\Big)\chi(x) \Big| < c(n,\kappa)(d+1)^2 p^{-\delta} |B|,$$

where $$\delta = \frac{\kappa^2 n}{4(1+2\kappa)(2n+(d+1)^2)}.$$

the mixed character case

- $$\Big|\sum_{x\in B_H} e\Big(f(x)\Big)\chi(x)\Big|$$
$$\le \frac{1}{p^{\varepsilon}|B_{p^{-2\varepsilon}H}|}\Big|\sum_{\substack{x\in B_H,\, y\in B_{p^{-2\varepsilon}H}\\ 0<t<p^{\varepsilon}}} e\Big(f(x+yt)\Big)\chi(x+yt)\Big|$$
$$+O(p^{-\varepsilon}H^n).$$

the mixed character case

- $$\Big|\sum_{x\in B_H} e\Big(f(x)\Big)\chi(x)\Big|$$
  $$\le \frac{1}{p^{\,\varepsilon}|B_{p^{-2\varepsilon}H}|}\Big|\sum_{\substack{x\in B_H,\ y\in B_{p^{-2\varepsilon}H}\\ 0<t<p^{\varepsilon}}} e\Big(f(x+yt)\Big)\chi(x+yt)\Big|$$
  $$+O(p^{-\varepsilon}H^n).$$
- $f(x{+}yt) = a_d(x,y)t^d{+}a_{d-1}(x,y)t^{d-1}{+}\cdots{+}a_0(x,y)$

the mixed character case

- $$\Big|\sum_{x\in B_H} e\Big(f(x)\Big)\chi(x)\Big|$$
$$\leq \frac{1}{p^{\,\varepsilon}|B_{p^{-2\varepsilon}H}|}\Big|\sum_{\substack{x\in B_H,\, y\in B_{p^{-2\varepsilon}H}\\ 0<t<p^{\varepsilon}}} e\Big(f(x+yt)\Big)\chi(x+yt)\Big|$$
$$+O(p^{-\varepsilon}H^n).$$
- $f(x+yt) = a_d(x,y)t^d + a_{d-1}(x,y)t^{d-1} + \cdots + a_0(x,y)$
- Partition $[0,1]^{d+1}$ in boxes Q_α of size $p^{-\varepsilon_1}$
- Partition $B_H \times B_{p^{-2\varepsilon}H}$ according to the boxes Q_α.

$$B_H \times B_{p^{-2\varepsilon}H} = \bigcup_\alpha \Omega_\alpha,$$

- $$\Omega_\alpha = \Big\{(x,y) \in B_H \times B_{p^{-2\varepsilon}H} : \Big(a_j(x,y)\Big)_{1\leq j\leq d+1} \in Q_\alpha \ (\text{mod } 1)\Big\}.$$

- $\theta_\alpha = (\theta_{\alpha,1}, \ldots, \theta_{\alpha,d+1}) \in Q_\alpha$, $(x,y) \in \Omega_\alpha$

$\left| e\Big(a_j(x,y)\Big) - e(\theta_{\alpha,j}) \right| < p^{-\varepsilon_1}$, for $j = 1, \ldots, d+1$

- $\theta_\alpha = (\theta_{\alpha,1}, \ldots, \theta_{\alpha,d+1}) \in Q_\alpha$, $(x, y) \in \Omega_\alpha$

$\left| e\Big(a_j(x,y)\Big) - e(\theta_{\alpha,j}) \right| < p^{-\varepsilon_1}$, for $j = 1, \ldots, d+1$

- To estimate

$$\left| \sum_{\substack{x \in B_H,\, y \in B_{p^{-2\varepsilon}H} \\ 0 < t < p^{\varepsilon}}} e\Big(f(x+yt)\Big)\chi(x+yt) \right|$$

one may replace $e\Big(f(x+yt)\Big)$ by $e\Big(\sum_{j=0}^{d} \theta_{\alpha,j}\, t^j\Big)$:
(The same θ_α for all $(x, y) \in \Omega_\alpha$)

- $\theta_\alpha = (\theta_{\alpha,1}, \dots, \theta_{\alpha,d+1}) \in Q_\alpha,\ (x,y) \in \Omega_\alpha$

$\Big| e\Big(a_j(x,y)\Big) - e(\theta_{\alpha,j}) \Big| < p^{-\varepsilon_1}$, for $j = 1, \dots, d+1$

- To estimate

$$\Big| \sum_{\substack{x \in B_H,\ y \in B_{p^{-2\varepsilon}H} \\ 0 < t < p^\varepsilon}} e\Big(f(x+yt)\Big)\chi(x+yt) \Big|$$

one may replace $e\Big(f(x+yt)$ by $e\Big(\sum_{j=0}^d \theta_{\alpha,j}\, t^j\Big)$:

- $$\Big| e\Big(f(x+yt)\Big) - e\Big(\sum_{j=0}^d \theta_{\alpha,j}\, t^j\Big) \Big|$$
$$\le 2\pi \sum_j \Big| e\Big(a_j(x,y)\Big) - e(\theta_{\alpha,j}) \Big|\, t^j$$
$$< 2\pi(d+1)p^{d\varepsilon-\varepsilon_1} \lesssim p^{-\varepsilon},\ \text{with } \varepsilon_1 = (d+1)\varepsilon$$

- $\theta_\alpha = (\theta_{\alpha,1}, \dots, \theta_{\alpha,d+1}) \in Q_\alpha, \ (x,y) \in \Omega_\alpha$

$$\left| e\Big(a_j(x,y)\Big) - e(\theta_{\alpha,j}) \right| < p^{-\varepsilon_1}, \text{ for } j = 1, \dots, d+1$$

- $$\left| e\Big(f(x+yt)\Big) - e\Big(\sum_{j=0}^{d} \theta_{\alpha,j}\, t^j \Big) \right|$$

$$\leq 2\pi \sum_j \left| e\Big(a_j(x,y)\Big) - e(\theta_{\alpha,j}) \right| t^j$$

$$< 2\pi(d+1)p^{d\varepsilon - \varepsilon_1} \lesssim p^{-\varepsilon}, \text{ with } \varepsilon_1 = (d+1)\varepsilon$$

- want to bound

$$\sum_\alpha \sum_{(x,y)\in\Omega_\alpha} \left| \sum_{t=1}^{p^{\,\varepsilon}} e\Big(\sum_{j=0}^{d} \theta_{\alpha,j}\, t^j \Big)\, \chi(x+yt) \right|$$

$$= \sum_\alpha \sum_{z\in\mathbb{F}_{p^n}} \mu_\alpha(z) \left| \sum_{t=1}^{p^{\,\varepsilon}} e\Big(\sum_{j=0}^{d} \theta_{\alpha,j}\, t^j \Big)\, \chi(z+t) \right|,$$

where $\mu_\alpha(z) = \left| \Big\{ (x,y) \in \Omega_\alpha : \frac{x}{y} = z \Big\} \right|$

Composite Moduli

- Fix $0 < a < q_1$, $(a, q_1) = 1$

Postnikov's formula

$$\begin{aligned}\chi_1(a + q_1 x) =& \chi_1(a)\chi_1(1 + q_1 \bar{a} x)\\ =& \chi_1(a) e_{q_1^m}(F(q_1 \bar{a} x)),\end{aligned}$$

where $F(x) \in \mathbb{Z}[x]$

$$F(x) = B\left(x - \frac{x^2}{2} + \cdots \pm \frac{x^{m'}}{m'}\right) \quad (m' > 2m),$$

$B \in \mathbb{Z}$ and $a\bar{a} = 1 \pmod{q_1^m}$

Composite Moduli

- Fix $0 < a < q_1$, $(a, q_1) = 1$

Postnikov's formula

$$\begin{aligned}\chi_1(a + q_1 x) =& \chi_1(a)\chi_1(1 + q_1 \bar{a} x) \\ =& \chi_1(a) e_{q_1^m}(F(q_1 \bar{a} x)),\end{aligned}$$

where $F(x) \in \mathbb{Z}[x]$

$$F(x) = B\Big(x - \frac{x^2}{2} + \cdots \pm \frac{x^{m'}}{m'}\Big) \quad (m' > 2m),$$

$B \in \mathbb{Z}$ and $a\bar{a} = 1 \pmod{q_1^m}$

- Estimate

$$\begin{aligned}&\Big|\sum_{n \in I} \chi(n)\Big| \\ &\leq \sum_{(a,q_1)=1} \Big| \sum_{a + q_1 x \in I} e_{q_1^m}(F(q_1 \bar{a} x)) \chi_2(a + q_1 x)\Big|\end{aligned}$$

and apply mixed-character bound