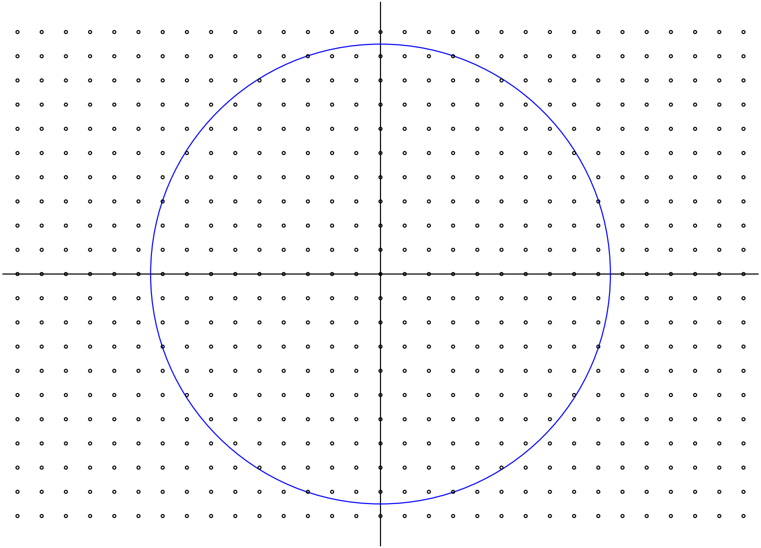
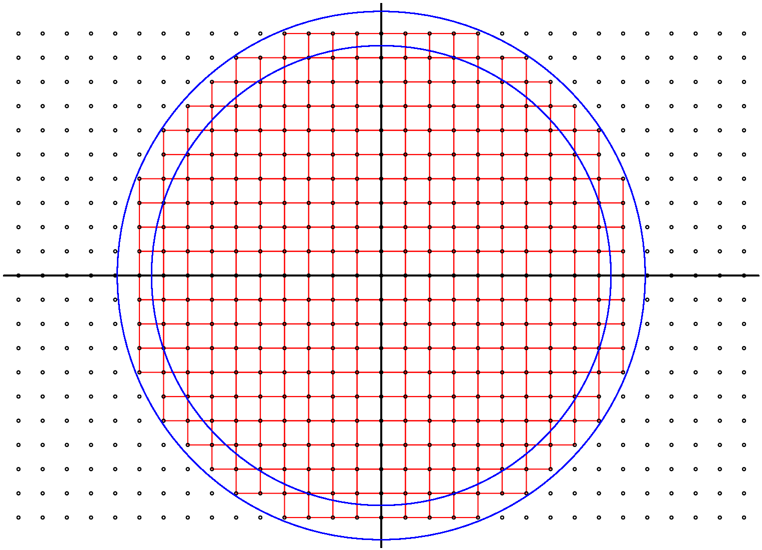
The Geometry of Equidistribution

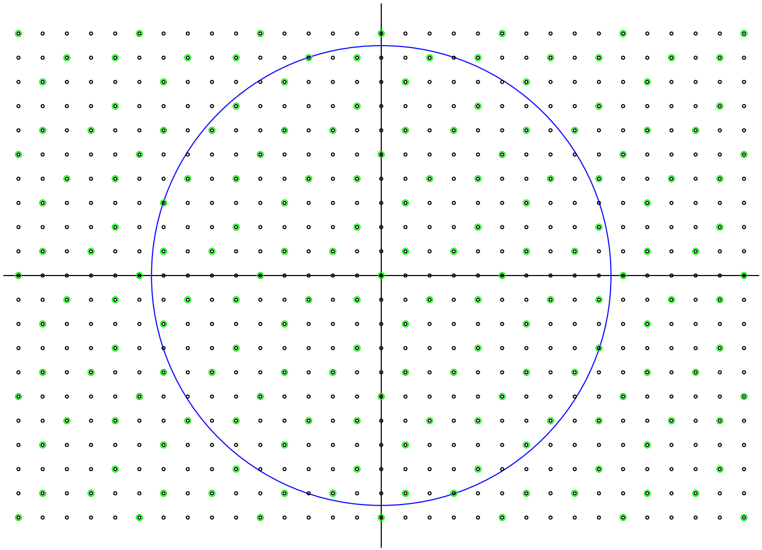
Frank Thorne

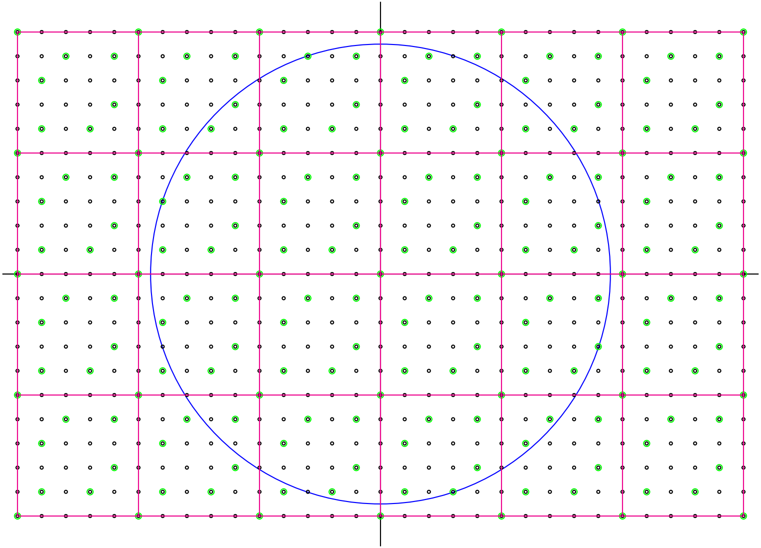
University of South Carolina

The Geometry of Arithmetic Statistics, Schloss Elmau









Example: Pólya-Vinogradov

Example: Pólya-Vinogradov

Theorem (Pólya-Vinogradov inequality, special case)

Let χ be a primitive Dirichlet character $\pmod{q}$. Then we have

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| < q^{\frac{1}{2}} \log q.$$

Example: Pólya-Vinogradov

Theorem (Pólya-Vinogradov inequality, special case)

Let χ be a primitive Dirichlet character $\pmod{q}$. Then we have

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| < q^{\frac{1}{2}} \log q.$$

Proof. By Fourier inversion, we have

$$\chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{a=1}^{q} \overline{\chi}(a) e^{2\pi i a n/q},$$

with $|\tau(\overline{\chi})| = q^{1/2}$,

Example: Pólya-Vinogradov

Theorem (Pólya-Vinogradov inequality, special case)

Let χ be a primitive Dirichlet character $\pmod{q}$. Then we have

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| < q^{\frac{1}{2}} \log q.$$

Proof. By Fourier inversion, we have

$$\chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{a=1}^{q} \overline{\chi}(a) e^{2\pi i a n/q},$$

with $|\tau(\overline{\chi})| = q^{1/2}$, so that

$$\sum_{n=M+1}^{M+N} \chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{a=1}^{q} \overline{\chi}(a) \sum_{n=M+1}^{M+N} e^{2\pi i a n/q},$$

and the innermost sum is a geometric series.

Example: Cubic fields by squarefree part

Define

$$N(Y, Z) := \{K \text{ cubic field } : |D(K)| < Y, \ F(K) < Z\}.$$

Example: Cubic fields by squarefree part

Define

$$N(Y,Z) := \left\{K \text{ cubic field } : |D(K)| < Y,\ F(K) < Z\right\}.$$

Proposition

For any positive real numbers Y and Z, we have

$$N(Y,Z) = \Big(\sum_{f<Z} C_1(f)\Big) \cdot Y + O_\epsilon(Y^{5/6}Z^{2/3} + Y^{2/3+\epsilon}Z^{4/3});$$

$$N(Y,Z) = \Big(\sum_{\substack{|d|<Y \\ \text{fund.disc}}} \mathrm{Res}_{s=1}\Phi_d(s)\Big) \cdot Z + O_\epsilon\Big(Y^{7/6}Z^{2/3+\epsilon}\Big).$$

The standard setup (Bhargava et al.)

We are given:

The standard setup (Bhargava et al.)

We are given:

- A vector space V with an integral structure (e.g. binary cubic forms);

The standard setup (Bhargava et al.)

We are given:

- A vector space V with an integral structure (e.g. binary cubic forms);
- An algebraic group G acting on V, again with an integral structure (e.g. $\mathrm{GL}(2)$);

The standard setup (Bhargava et al.)

We are given:

- A vector space V with an integral structure (e.g. binary cubic forms);
- An algebraic group G acting on V, again with an integral structure (e.g. GL(2));
- A $G(\mathbb{Z})$-invariant 'discriminant' defined on V;

The standard setup (Bhargava et al.)

We are given:

- A vector space V with an integral structure (e.g. binary cubic forms);
- An algebraic group G acting on V, again with an integral structure (e.g. GL(2));
- A $G(\mathbb{Z})$-invariant 'discriminant' defined on V;
- $N(X) :=$ number of $G(\mathbb{Z})$-orbits $v \in V(\mathbb{Z})$ with $0 < |\mathrm{Disc}(v)| < X$;

The standard setup (Bhargava et al.)

We are given:

- A vector space V with an integral structure (e.g. binary cubic forms);
- An algebraic group G acting on V, again with an integral structure (e.g. GL(2));
- A $G(\mathbb{Z})$-invariant 'discriminant' defined on V;
- $N(X) :=$ number of $G(\mathbb{Z})$-orbits $v \in V(\mathbb{Z})$ with $0 < |\mathrm{Disc}(v)| < X$;
- $N(X, q) :=$ above, with congruence conditions $\pmod{q}$.

A proof template

A three-step proof template in arithmetic statistics:

A proof template

A three-step proof template in arithmetic statistics:

3. Apply sieves, etc. to obtain arithmetic consequences.

A proof template

A three-step proof template in arithmetic statistics:

2. Prove results of the shape
$$N(X, q) = \omega(q) X^a + O(X^{\alpha} q^{\beta}),$$
where $\alpha < a$ and $\beta \in \mathbb{R}$ are as small as possible.
3. Apply sieves, etc. to obtain arithmetic consequences.

A proof template

A three-step proof template in arithmetic statistics:

1. Bound or evaluate some Fourier transforms.
2. Prove results of the shape

$$N(X, q) = \omega(q) X^a + O(X^\alpha q^\beta),$$

   where $\alpha < a$ and $\beta \in \mathbb{R}$ are as small as possible.
3. Apply sieves, etc. to obtain arithmetic consequences.

A proof template

A three-step proof template in arithmetic statistics:

1. Bound or evaluate some Fourier transforms.
2. Prove results of the shape

$$N(X, q) = \omega(q)X^a + O(X^\alpha q^\beta),$$

where $\alpha < a$ and $\beta \in \mathbb{R}$ are as small as possible.

3. Apply sieves, etc. to obtain arithmetic consequences.

Today: Investigate Step 1 further.

The Fourier Transform

Let $\Phi_p : V(\mathbb{Z}/q\mathbb{Z}) \to \mathbb{C}$ be the characteristic function of our congruence conditions,

The Fourier Transform

Let $\Phi_p : V(\mathbb{Z}/q\mathbb{Z}) \to \mathbb{C}$ be the characteristic function of our congruence conditions,

... or any other $G(\mathbb{Z}/q\mathbb{Z})$-invariant function.

The Fourier Transform

Let $\Phi_p : V(\mathbb{Z}/q\mathbb{Z}) \to \mathbb{C}$ be the characteristic function of our congruence conditions,

... or any other $G(\mathbb{Z}/q\mathbb{Z})$-invariant function.

Define
$$\widehat{\Phi_q}(y) := q^{-\dim V} \sum_{x \in V(\mathbb{Z}/q\mathbb{Z})} \Phi(x) e^{-2\pi i [x,y]/q}.$$

Theorem (Poisson summation)

For a finite dimensional lattice $V(\mathbb{Z})$, we have

$$\sum_{v \in V(\mathbb{Z})} \phi(v) = \sum_{w \in \widehat{V(\mathbb{Z})}} \widehat{\phi}(w).$$

The Million Pound Poisson Hammer

Theorem (Poisson summation)

For a finite dimensional lattice $V(\mathbb{Z})$, we have

$$\sum_{v \in V(\mathbb{Z})} \phi(v) = \sum_{w \in \widehat{V(\mathbb{Z})}} \widehat{\phi}(w).$$

(Subject to pesky convergence issues.)

The Million Pound Poisson Hammer

Theorem (Poisson summation)

For a finite dimensional lattice $V(\mathbb{Z})$, we have

$$\sum_{v \in V(\mathbb{Z})} \phi(v) = \sum_{w \in \widehat{V(\mathbb{Z})}} \widehat{\phi}(w).$$

(Subject to pesky convergence issues.)

Theorem (Poisson summation with local conditions)

For $\Phi_q : V(\mathbb{Z}/q\mathbb{Z}) \to \mathbb{C}$, we have

$$\sum_{v \in V(\mathbb{Z})} \Phi_q(v)\phi(v) = \sum_{w \in \widehat{V(\mathbb{Z})}} \widehat{\Phi_q}(w)\widehat{\phi}(w/q).$$

The Fouvry-Katz Theorem

Let Y be a (locally closed) subscheme of $\mathbb{A}^n_{\mathbb{Z}}$, of dimension d. Take $V = \mathbb{A}^n$, p prime, and Φ_p the the characteristic function of $Y(\mathbb{F}_p)$.

Theorem (Fouvry-Katz, 2001)

There exists a filtration of subschemes

$$\mathbb{A}^n_{\mathbb{Z}} \supseteq X_1 \supseteq \cdots \supseteq X_j \supseteq \cdots \supseteq X_n$$

with X_j of codimension j, so that

$$|\widehat{\Phi_p}(y)| \leq Cp^{-n+\frac{d}{2}+\frac{j-1}{2}}$$

away from $X_j(\mathbb{F}_p)$.

Example: Fouvry-Katz

Corollary (Fouvry-Katz, 2001)

There exist $\gg \frac{X}{\log X}$ *primes* $p \leq X$ *with*

$$\#\mathrm{Cl}(\mathbb{Q}(\sqrt{p+4}))[3] = 1.$$

Example: Fouvry-Katz

Corollary (Fouvry-Katz, 2001)

There exist $\gg \frac{X}{\log X}$ *primes* $p \leq X$ *with*

$$\#\mathrm{Cl}(\mathbb{Q}(\sqrt{p+4}))[3] = 1.$$

(Here $p + 4 \equiv 1 \pmod 4$ and squarefree.)

Example 2: Davenport-Heilbronn

Let $V = \mathrm{Sym}^3(\mathbb{Z}/p^2\mathbb{Z})^2$, with:

Example 2: Davenport-Heilbronn

Let $V = \mathrm{Sym}^3(\mathbb{Z}/p^2\mathbb{Z})^2$, with:

$\Phi_{p^2}(v) =$ char. fn. of v with a $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$-translate

$$ax^3 + bx^2y + cxy^2 + dy^3$$

with $p^2 \mid a$ and $p \mid b$.

Example 2: Davenport-Heilbronn

Let $V = \mathrm{Sym}^3(\mathbb{Z}/p^2\mathbb{Z})^2$, with:

$\Phi_{p^2}(v) =$ char. fn. of v with a $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$-translate

$$ax^3 + bx^2y + cxy^2 + dy^3$$

with $p^2 \mid a$ and $p \mid b$.

This is the Davenport-Heilbronn condition for nonmaximality at p.

An explicit evaluation

Theorem (Taniguchi-T., 2011)

We have

$$\widehat{\Phi_{p^2}}(v) = \begin{cases} p^{-2} + p^{-3} - p^{-5} & v/p \text{ : of type } (0), \\ p^{-3} - p^{-5} & v/p \text{ : of type } (1^3), (1^2 1), \\ -p^{-5} & v/p \text{ : of type } (111), (21), (3). \\ p^{-3} - p^{-5} & v \text{ : of type } (1^3_{**}), \\ -p^{-5} & v \text{ : of type } (1^3_{*}),\ (1^3_{\max}), \\ 0 & \text{otherwise.} \end{cases}$$

An explicit evaluation

Theorem (Taniguchi-T., 2011)

We have

$$\widehat{\Phi_{p^2}}(v) = \begin{cases} p^{-2} + p^{-3} - p^{-5} & v/p : \textit{ of type } (0), \\ p^{-3} - p^{-5} & v/p : \textit{ of type } (1^3), (1^2 1), \\ -p^{-5} & v/p : \textit{ of type } (111), (21), (3). \\ p^{-3} - p^{-5} & v : \textit{ of type } (1^3_{**}), \\ -p^{-5} & v : \textit{ of type } (1^3_{*}),\ (1^3_{\max}), \\ 0 & \textit{otherwise.} \end{cases}$$

So:

$$\frac{1}{p^8} \sum_{v \in V(\mathbb{Z}/p^2\mathbb{Z})} |\widehat{\Phi_{p^2}}(v)| \ll p^{-7}.$$

Consequence – Improved Davenport-Heilbronn

Theorem (Bhargava-Taniguchi-T.)

We have

$$N_3(X) = CX + C'X^{\frac{5}{6}} + O(X^{\frac{3}{5}+\epsilon}) + O(X^{1-\frac{1}{8-7+2}+\epsilon}).$$

The bilinear form

Proposition

"Typical cases" enjoy a symmetric bilinear form $[-,-]$ satisfying identically

$$[gv, g^{-T} w] = [v, w].$$

The bilinear form

Proposition

"Typical cases" enjoy a symmetric bilinear form $[-,-]$ satisfying identically

$$[gv, g^{-T}w] = [v, w].$$

Example: For forms

$$v = ax^3 + bx^2y + cxy^2 + dy^3, \quad w = a'x^3 + b'x^2y + c'xy^2 + d'y^3,$$

we have

$$[v, w] = aa' + \frac{bb'}{3} + \frac{cc'}{3} + dd'.$$

The bilinear form

Proposition

"Typical cases" enjoy a symmetric bilinear form $[-,-]$ satisfying identically

$$[gv, g^{-T}w] = [v, w].$$

Example: For forms

$$v = ax^3 + bx^2y + cxy^2 + dy^3, \quad w = a'x^3 + b'x^2y + c'xy^2 + d'y^3,$$

we have

$$[v, w] = aa' + \frac{bb'}{3} + \frac{cc'}{3} + dd'.$$

(Assume that $p \neq 3$, or otherwise as needed.)

The bilinear form

Proposition

"Typical cases" enjoy a symmetric bilinear form $[-,-]$ satisfying identically

$$[gv, g^{-T}w] = [v, w].$$

Example: For forms

$$v = ax^3 + bx^2y + cxy^2 + dy^3, \quad w = a'x^3 + b'x^2y + c'xy^2 + d'y^3,$$

we have

$$[v, w] = aa' + \frac{bb'}{3} + \frac{cc'}{3} + dd'.$$

(Assume that $p \neq 3$, or otherwise as needed.)

Obtain a G-equivariant isomorphism $\widehat{V}(\mathbb{F}_p) \to V(\mathbb{F}_p)$.

G-invariance

Proposition

If $\Phi : V(\mathbb{F}_p) \to \mathbb{C}$ is G-invariant, then so is $\widehat{\Phi}$.

Proof.

.

G-invariance

Proposition

If $\Phi : V(\mathbb{F}_p) \to \mathbb{C}$ is G-invariant, then so is $\widehat{\Phi}$.

Proof.

$$\widehat{\Phi}(gw) = \sum_{v \in V(\mathbb{F}_p)} \Phi(v) \langle [v, gw] \rangle$$

.

G-invariance

Proposition

If $\Phi : V(\mathbb{F}_p) \to \mathbb{C}$ is G-invariant, then so is $\widehat{\Phi}$.

Proof.

$$\begin{aligned} \widehat{\Phi}(gw) &= \sum_{v \in V(\mathbb{F}_p)} \Phi(v)\langle [v, gw]\rangle \\ &= \sum_{v \in V(\mathbb{F}_p)} \Phi(v)\langle [g^T v, w]\rangle \end{aligned}$$

.

G-invariance

Proposition

If $\Phi : V(\mathbb{F}_p) \to \mathbb{C}$ is G-invariant, then so is $\widehat{\Phi}$.

Proof.

$$\begin{aligned}
\widehat{\Phi}(gw) &= \sum_{v \in V(\mathbb{F}_p)} \Phi(v) \langle [v, gw] \rangle \\
&= \sum_{v \in V(\mathbb{F}_p)} \Phi(v) \langle [g^T v, w] \rangle \\
&= \sum_{v \in V(\mathbb{F}_p)} \Phi(g^T v) \langle [g^T v, w] \rangle
\end{aligned}$$

.

G-invariance

Proposition

If $\Phi : V(\mathbb{F}_p) \to \mathbb{C}$ is G-invariant, then so is $\widehat{\Phi}$.

Proof.

$$\begin{aligned}
\widehat{\Phi}(gw) &= \sum_{v \in V(\mathbb{F}_p)} \Phi(v) \langle [v, gw] \rangle \\
&= \sum_{v \in V(\mathbb{F}_p)} \Phi(v) \langle [g^T v, w] \rangle \\
&= \sum_{v \in V(\mathbb{F}_p)} \Phi(g^T v) \langle [g^T v, w] \rangle \\
&= \sum_{v \in V(\mathbb{F}_p)} \Phi(v) \langle [v, w] \rangle .
\end{aligned}$$

Three proof methods for explicit formulas

- The group decomposition method (Mori, Taniguchi-T., Hough);

Three proof methods for explicit formulas

- The group decomposition method (Mori, Taniguchi-T., Hough);
- The subspace method (Taniguchi-T.; Ishimoto);

Three proof methods for explicit formulas

- The group decomposition method (Mori, Taniguchi-T., Hough);
- The subspace method (Taniguchi-T.; Ishimoto);
- The morphism method (Ishitsuka, Ito, Taniguchi, T., Xiao).

Group decomposition (Hough, 2018)

Theorem 2. *The Fourier transform of the maximal set is supported on the mod p orbits $\mathcal{O}_0, \mathcal{O}_{D1^2}, \mathcal{O}_{D11}$ and $\mathcal{O}_{D2}$. It is given explicitly in the following tables.*

(1) *Case $\mathcal{O}_0$, $\xi = p\xi_0$.*

(6.1)

Orbit	$p^{-12}\widehat{\mathbf{1}_{\max}}(p\xi_0)$	*Orbit size*
$\mathcal{O}_0$	$(p-1)^4p(p+1)^2(p^5+2p^4+4p^3+4p^2+3p+1)$	1
$\mathcal{O}_{D1^2}$	$-(p-1)^3p(p+1)^4$	$(p-1)(p+1)(p^2+p+1)$
$\mathcal{O}_{D11}$	$-(p-1)^3p(2p^3+6p^2+4p+1)$	$(p-1)p(p+1)^2(p^2+p+1)/2$
$\mathcal{O}_{D2}$	$(p-1)^2p(2p^2+3p+1)$	$(p-1)^2p(p+1)(p^2+p+1)/2$
$\mathcal{O}_{Dns}$	$(p-1)^2p(2p^2+3p+1)$	$(p-1)^2p^2(p+1)(p^2+p+1)$
$\mathcal{O}_{Cs}$	$-p^7+5p^5-3p^4-3p^3+p^2+p$	$(p-1)^2p(p+1)^2(p^2+p+1)$
$\mathcal{O}_{Cns}$	$(p-1)^2p(2p^2+3p+1)$	$(p-1)^2p^3(p+1)(p^2+p+1)$
$\mathcal{O}_{B11}$	$(p-1)^2p(2p^2+3p+1)$	$(p-1)^2p^2(p+1)^2(p^2+p+1)/2$
$\mathcal{O}_{B2}$	$(p-1)^2p(2p^2+3p+1)$	$(p-1)^3p^2(p+1)(p^2+p+1)/2$
$\mathcal{O}_{1^4}$	$p(p^3-3p^2+p+1)$	$(p-1)^3p^2(p+1)^2(p^2+p+1)$
$\mathcal{O}_{1^31}$	$p(p^3-3p^2+p+1)$	$(p-1)^3p^3(p+1)^2(p^2+p+1)$
$\mathcal{O}_{1^21^2}$	$(p-1)^2p(3p+1)$	$(p-1)^2p^4(p+1)^2(p^2+p+1)/2$
$\mathcal{O}_{2^2}$	$-(p-1)p(p+1)^2$	$(p-1)^3p^4(p+1)(p^2+p+1)/2$
$\mathcal{O}_{1^211}$	$p(p^3-3p^2+p+1)$	$(p-1)^3p^4(p+1)^2(p^2+p+1)/2$
$\mathcal{O}_{1^22}$	$p(p^3-3p^2+p+1)$	$(p-1)^3p^4(p+1)^2(p^2+p+1)/2$
$\mathcal{O}_{1111}$	$-p^3+p^2+p$	$(p-1)^4p^4(p+1)^2(p^2+p+1)/24$
$\mathcal{O}_{112}$	$-p^3+p^2+p$	$(p-1)^4p^4(p+1)^2(p^2+p+1)/4$
$\mathcal{O}_{22}$	$-p^3+p^2+p$	$(p-1)^4p^4(p+1)^2(p^2+p+1)/8$
$\mathcal{O}_{13}$	$-p^3+p^2+p$	$(p-1)^4p^4(p+1)^2(p^2+p+1)/3$
$\mathcal{O}_4$	$-p^3+p^2+p$	$(p-1)^4p^4(p+1)^2(p^2+p+1)/4$

Binary cubic forms – singularity

On $V = \mathrm{Sym}^3(\mathbb{F}^2)$, let Φ_p be the characteristic function of the singular locus:

$$\Phi_p(v) := \begin{cases} 1 & \text{if } \mathrm{Disc}(\mathsf{v}) = 0 \ , \\ 0 & \text{otherwise} \ . \end{cases}$$

Theorem (Mori 2010)

We have

$$\widehat{\Phi_p}(v) = \begin{cases} p^{-1} + p^{-2} - p^{-3} & (v = 0), \\ p^{-2} - p^{-3} & (v \textit{ has splitting type } (1^3) \textit{ or } (1^2 1)), \\ -p^{-3} & (\textit{otherwise}). \end{cases}$$

[The above corrects a mistake pointed out in the talk.]

Binary cubic forms

Recall that $\mathrm{PGL}(2)$ acts triply transitively on $\mathbb{P}^1$.

Binary cubic forms

Recall that $\mathrm{PGL}(2)$ acts triply transitively on $\mathbb{P}^1$.

Therefore, the action of $\mathrm{GL}(2)$ on $\mathrm{Sym}^3(\mathbb{F}^2)$ has six orbits:

Binary cubic forms

Recall that $\mathrm{PGL}(2)$ acts triply transitively on $\mathbb{P}^1$.

Therefore, the action of $\mathrm{GL}(2)$ on $\mathrm{Sym}^3(\mathbb{F}^2)$ has six orbits:

$$(0), (1^3), (1^2 1), (111), (12), (3)$$

Singularity and subspaces

Proposition

A form $v \in \mathrm{Sym}^3(\mathbb{F}^2)$ is:

Proposition

A form $v \in \mathrm{Sym}^3(\mathbb{F}^2)$ is:

- $(1^2 1), (1^3)$, or (0) if it is G-equivalent to some $(0, 0, *, *)$;

Proposition

A form $v \in \mathrm{Sym}^3(\mathbb{F}^2)$ is:

- $(1^2 1), (1^3)$, or (0) if it is G-equivalent to some $(0, 0, *, *)$;
- (1^3), or (0) if it is G-equivalent to some $(0, 0, 0, *)$;

Singularity and subspaces

Proposition

A form $v \in \mathrm{Sym}^3(\mathbb{F}^2)$ is:

- $(1^21), (1^3)$, or (0) if it is G-equivalent to some $(0, 0, *, *)$;
- (1^3), or (0) if it is G-equivalent to some $(0, 0, 0, *)$;
- (0) if it is G-equivalent to $(0, 0, 0, 0)$.

Singularity and subspaces

Proposition

A form $v \in \mathrm{Sym}^3(\mathbb{F}^2)$ is:

- $(1^2 1), (1^3)$, or (0) if it is G-equivalent to some $(0, 0, *, *)$;
- (1^3), or (0) if it is G-equivalent to some $(0, 0, 0, *)$;
- (0) if it is G-equivalent to $(0, 0, 0, 0)$.

Moral:

G-orbits of subspaces distinguish the orbits.

Sketch Proof of FT formula

Consider

$$f := \sum_{v \in (0,0,*,*)} \sum_{g \in \mathrm{GL}_2(\mathbb{F}_p)} \mathbf{1}_{gv}.$$

Then

Sketch Proof of FT formula

Consider

$$f := \sum_{v \in (0,0,*,*)} \sum_{g \in \mathrm{GL}_2(\mathbb{F}_p)} \mathbf{1}_{gv}.$$

Then

$$f(v) = \begin{cases} (p^2-1)(p^2-p) & (v = 0), \\ p^2 - p & (v \text{ has splitting type } (1^3)), \\ p - 1 & (v \text{ has splitting type } (1^2 1)), \\ 0 & \text{otherwise}, \end{cases}$$

Sketch Proof of FT formula

Consider

$$f := \sum_{v \in (0,0,*,*)} \sum_{g \in \mathrm{GL}_2(\mathbb{F}_p)} \mathbf{1}_{gv}.$$

Then

$$f(v) = \begin{cases} (p^2-1)(p^2-p) & (v = 0), \\ p^2 - p & (v \text{ has splitting type } (1^3)), \\ p - 1 & (v \text{ has splitting type } (1^2 1)), \\ 0 & \text{otherwise}, \end{cases}$$

a weighted version of our counting formula.

Sketch Proof of FT formula (2)

$$p^4 \widehat{f}(w) = \sum_{v \in (0,0,*,*)} \sum_{g \in G(\mathbb{F}_p)} \langle [gv, w] \rangle$$

Sketch Proof of FT formula (2)

$$p^4 \widehat{f}(w) = \sum_{v \in (0,0,*,*)} \sum_{g \in G(\mathbb{F}_p)} \langle [gv, w] \rangle$$
$$= \sum_{v \in (0,0,*,*)} \sum_{g \in G(\mathbb{F}_p)} \langle [v, g^T w] \rangle$$

Sketch Proof of FT formula (2)

$$
\begin{aligned}
p^4 \widehat{f}(w) &= \sum_{v \in (0,0,*,*)} \sum_{g \in G(\mathbb{F}_p)} \langle [gv, w] \rangle \\
&= \sum_{v \in (0,0,*,*)} \sum_{g \in G(\mathbb{F}_p)} \langle [v, g^T w] \rangle \\
&= p^2 \# \{ G(\mathbb{F}_p) - \text{translates of } w \text{ in } (*, *, 0, 0) \}
\end{aligned}
$$

Sketch Proof of FT formula (2)

$$\begin{aligned}
p^4 \widehat{f}(w) &= \sum_{v \in (0,0,*,*)} \sum_{g \in G(\mathbb{F}_p)} \langle [gv, w] \rangle \\
&= \sum_{v \in (0,0,*,*)} \sum_{g \in G(\mathbb{F}_p)} \langle [v, g^T w] \rangle \\
&= p^2 \# \{ G(\mathbb{F}_p) - \text{translates of } w \text{ in } (*,*,0,0) \} \\
&= p^2 \sum_{g \in G(\mathbb{F}_p)} \sum_{w \in (*,*,0,0)} \mathbf{1}_{gw}.
\end{aligned}$$

Other prehomogeneous cases (Taniguchi-T.)

Other prehomogeneous cases (Taniguchi-T.)

- $V = \mathrm{Sym}^2(2)$, $G = \mathrm{GL}_1 \times \mathrm{GL}_2$.

Other prehomogeneous cases (Taniguchi-T.)

- $V = \mathrm{Sym}^2(2)$, $G = \mathrm{GL}_1 \times \mathrm{GL}_2$.
- $V = \mathrm{Sym}^2(3)$, $G = \mathrm{GL}_1 \times \mathrm{GL}_3$.

Other prehomogeneous cases (Taniguchi-T.)

- $V = \mathrm{Sym}^2(2)$, $G = \mathrm{GL}_1 \times \mathrm{GL}_2$.
- $V = \mathrm{Sym}^2(3)$, $G = \mathrm{GL}_1 \times \mathrm{GL}_3$.
- $V = 2 \otimes \mathrm{Sym}^2(2)$, $G = \mathrm{GL}_2 \times \mathrm{GL}_2$.

Other prehomogeneous cases (Taniguchi-T.)

- $V = \mathrm{Sym}^2(2)$, $G = \mathrm{GL}_1 \times \mathrm{GL}_2$.
- $V = \mathrm{Sym}^2(3)$, $G = \mathrm{GL}_1 \times \mathrm{GL}_3$.
- $V = 2 \otimes \mathrm{Sym}^2(2)$, $G = \mathrm{GL}_2 \times \mathrm{GL}_2$.
- $V = 2 \otimes \mathrm{Sym}^2(3)$, $G = \mathrm{GL}_2 \times \mathrm{GL}_3$.

Binary quartic forms

Let V be the space of binary quartic forms, where $\mathrm{GL}(1) \times \mathrm{GL}(2)$ acts by

$$\left(\alpha, \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \cdot f(x, y) = \alpha f(ax + cy, bx + dy).$$

Binary quartic forms

Let V be the space of binary quartic forms, where $\mathrm{GL}(1) \times \mathrm{GL}(2)$ acts by

$$\left(\alpha, \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \cdot f(x,y) = \alpha f(ax+cy, bx+dy).$$

Associate to $f = a_0x^4 + a_1x^3y + a_2x^2y^2 + a_3xy^3 + a_4y^4$:

$$\begin{aligned} I(f) &= 12a_0a_4 - 3a_1a_3 + a_2^2, \\ J(f) &= 72a_0a_2a_4 + 9a_1a_2a_3 - 27(a_0a_3^2 + a_1^2a_4) - 2a_2^3. \end{aligned}$$

Binary quartic forms

Let V be the space of binary quartic forms, where $\mathrm{GL}(1) \times \mathrm{GL}(2)$ acts by

$$\left(\alpha, \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \cdot f(x,y) = \alpha f(ax+cy, bx+dy).$$

Associate to $f = a_0x^4 + a_1x^3y + a_2x^2y^2 + a_3xy^3 + a_4y^4$:

$$I(f) = 12a_0a_4 - 3a_1a_3 + a_2^2,$$
$$J(f) = 72a_0a_2a_4 + 9a_1a_2a_3 - 27(a_0a_3^2 + a_1^2a_4) - 2a_2^3.$$

Let Φ_p be the characteristic function of the singular locus:

$$\Phi_p(v) := \begin{cases} 1 & \text{if } \mathrm{Disc}(v) = 0 \,, \\ 0 & \text{otherwise} \,. \end{cases}$$

Main Theorem for Quartic Forms

Theorem (Ishitsuka, Ito, Taniguchi, T., Xiao)

For a prime $p > 3$, we have

$$\widehat{\Phi_p}(v) = \begin{cases} p^{-1} + p^{-2} - p^{-3} & (v = 0), \\ p^{-2} - p^{-3} & (v \textit{ has splitting type } (1^4) \textit{ or } (1^3 1)), \\ \chi_{12}(p)(p^{-4} - p^{-3}) & (v \textit{ has splitting type } (1^2 1^2)), \\ \chi_{12}(p)(p^{-4} + p^{-3}) & (v \textit{ has splitting type } (2^2)), \\ \chi_{12}(p) p^{-4} & (v \textit{ has splitting type } (1^2 11) \textit{ or } (1^2 2)), \\ \chi_3(p) \left(\frac{I(v)}{p} \right) \cdot p^{-4} & (J(v) = 0, I(v) \neq 0), \\ a(E'_v) p^{-4} & (J(v) \neq 0, \mathrm{Disc}(v) \neq 0). \end{cases}$$

Here E'_v is the elliptic curve defined by

$$y^2 = x^3 - 3I(v)x^2 + J(v)^2,$$

with $a(E'_v) := p + 1 - \#E'_v(\mathbb{F}_p)$.

If $w \neq 0$, we have

$$\sum_{\substack{w \in \overline{w} \\ w \neq 0}} \langle [w, v] \rangle = \begin{cases} p - 1 & ([w, v] = 0) \\ -1 & ([w, v] \neq 0), \end{cases}$$

where $\overline{w}$ is the line through w and 0. So,

$$\begin{aligned} \widehat{\Phi_p}(v) &= 1 + (p-1) \sum_{\overline{w} \in \mathbb{P}(V), [\overline{w}, v] = 0} \Phi_p(\overline{w}) - \sum_{\overline{w} \in \mathbb{P}(V), [\overline{w}, v] \neq 0} \Phi_p(\overline{w}) \\ &= 1 + p \# X_v(\mathbb{F}_p) - \# X(\mathbb{F}_p), \end{aligned}$$

where

$$X := \{ w \in \mathbb{P}(V) \mid \mathrm{Disc}(w) = 0 \},$$
$$X_v := \{ w \in \mathbb{P}(V) \mid \mathrm{Disc}(w) = [w, v] = 0 \}.$$

Three morphisms

Consider projective morphisms

$$\psi_1 \colon \mathbb{P}(\mathbb{F}_p^2) \times \mathbb{P}(\mathrm{Sym}^2\mathbb{F}_p^2) \to \mathbb{P}(\mathrm{Sym}^4\mathbb{F}_p^2) = \mathbb{P}(V)$$
$$(s_0x + s_1y, t_0x^2 + t_1xy + t_2y^2) \mapsto (s_0x + s_1y)^2(t_0x^2 + t_1xy + t_2y^2).$$

$$\psi_2 \colon \mathbb{P}(\mathrm{Sym}^2\mathbb{F}_p^2) \to \mathbb{P}(\mathrm{Sym}^4\mathbb{F}_p^2) = \mathbb{P}(V)$$
$$t_0x^2 + t_1xy + t_2y^2 \mapsto (t_0x^2 + t_1xy + t_2y^2)^2$$

$$\psi_3 \colon \mathbb{P}(\mathbb{F}_p^2) \times \mathbb{P}(\mathbb{F}_p^2) \to \mathbb{P}(\mathrm{Sym}^4\mathbb{F}_p^2) = \mathbb{P}(V)$$
$$(s_0x + s_1y, t_0x + t_1y) \mapsto (s_0x + s_1y)^2(t_0x + t_1y)^2.$$

Then, the cardinalities of each $\psi_i(v)$ are:

Spitting type	$\#\psi_1^{-1}$	$\#\psi_2^{-1}$	$\#\psi_3^{-1}$
non-degenerate	0	0	0
(1^4)	1	1	1
$(1^3 1)$	1	0	0
$(1^2 1^2)$	2	1	2
(2^2)	0	1	0
$(1^2 11)$	1	0	0
$(1^2 2)$	1	0	0

Three morphisms – inverse images

Then, the cardinalities of each $\psi_i(v)$ are:

Spitting type	$\#\psi_1^{-1}$	$\#\psi_2^{-1}$	$\#\psi_3^{-1}$
non-degenerate	0	0	0
(1^4)	1	1	1
$(1^3 1)$	1	0	0
$(1^2 1^2)$	2	1	2
(2^2)	0	1	0
$(1^2 11)$	1	0	0
$(1^2 2)$	1	0	0

So,

$$\Phi_p(\overline{w}) = \#\psi_1^{-1}(\overline{w}) + \#\psi_2^{-1}(\overline{w}) - \#\psi_3^{-1}(\overline{w}).$$

The elliptic curve

We have

$$\sum_{\overline{w} \in \mathbb{P}(V), [\overline{w}, v] = 0} \#\psi_3^{-1}(\overline{w}) = \# C_3(v),$$

where

$$C_3(v) = \left\{ (l_1, l_2) \in \mathbb{P}(\mathbb{F}_p^2) \times \mathbb{P}(\mathbb{F}_p^2) \mid [l_1^2 l_2^2, v] = 0 \right\}.$$

The elliptic curve

We have

$$\sum_{\overline{w}\in\mathbb{P}(V),[\overline{w},v]=0} \#\psi_3^{-1}(\overline{w}) = \#C_3(v),$$

where

$$C_3(v) = \left\{(l_1, l_2) \in \mathbb{P}(\mathbb{F}_p^2) \times \mathbb{P}(\mathbb{F}_p^2) \mid [l_1^2 l_2^2, v] = 0\right\}.$$

Proposition (Bhargava-Ho)

If $\mathrm{Disc}(v) \neq 0$ and $J(v) \neq 0$, then $C_3(v)$ is of genus one, isomorphic to

$$E'_v \;:\; y^2 = x^3 - 3I(v)x^2 + J(v)^2.$$

Some Closing Questions

Some Closing Questions

- Can we do $\mathbb{F}^4 \otimes \wedge^2(\mathbb{F}^5)$ (the "quintic case")?

Some Closing Questions

- Can we do $\mathbb{F}^4 \otimes \wedge^2(\mathbb{F}^5)$ (the "quintic case")?
- Can one explain the regularity of these results?

Some Closing Questions

- Can we do $\mathbb{F}^4 \otimes \wedge^2(\mathbb{F}^5)$ (the "quintic case")?
- Can one explain the regularity of these results?
- What else are these formulas related to?

Some Closing Questions

- Can we do $\mathbb{F}^4 \otimes \wedge^2(\mathbb{F}^5)$ (the "quintic case")?
- Can one explain the regularity of these results?
- What else are these formulas related to?
- Can one exploit the oscillation in sign?