Trace functions over finite fields: a study in sums of products

E. Kowalski

ETH Zürich

May 29, 2014
Trace functions over finite fields:
a study in sums of products

E. Kowalski

ETH Zürich

May 29, 2014

[Joint works with É. Fouvry, Ph. Michel (and in part S. Ganguly, G. Ricotta); arXiv:1405.2293]
Trace functions

The trace functions modulo a prime $p$ are functions

$$K : \mathbb{F}_p \to \mathbb{C}$$

which are “special” functions of algebraic nature.
Trace functions

The trace functions modulo a prime $p$ are functions

$$K : F_p \rightarrow C$$

which are “special” functions of algebraic nature.

- Precisely, we consider trace functions of middle-extension $\ell$-adic sheaves $\mathcal{F}$ on the affine line, pointwise pure of weight 0, brought to $\mathbb{C}$ by a fixed $\iota : \bar{\mathbb{Q}}_\ell \rightarrow \mathbb{C}$.
Trace functions

The trace functions modulo a prime $p$ are functions

$$K : \mathbf{F}_p \longrightarrow \mathbf{C}$$

which are “special” functions of algebraic nature.

▶ Precisely, we consider trace functions of middle-extension $\ell$-adic sheaves $\mathcal{F}$ on the affine line, pointwise pure of weight 0, brought to $\mathbf{C}$ by a fixed $\iota : \overline{\mathbb{Q}}_\ell \longrightarrow \mathbf{C}$.

Such a trace function has a “complexity” $c(K)$. 
Trace functions

The trace functions modulo a prime $p$ are functions

$$K : F_p \rightarrow \mathbb{C}$$

which are “special” functions of algebraic nature.

- Precisely, we consider trace functions of middle-extension $\ell$-adic sheaves $\mathcal{F}$ on the affine line, pointwise pure of weight 0, brought to $\mathbb{C}$ by a fixed $\iota : \bar{\mathbb{Q}}_\ell \rightarrow \mathbb{C}$.

Such a trace function has a “complexity” $c(K)$.

- We define $c(K)$ as the minimum of $c(\mathcal{F})$ over sheaves as above with trace function $K$, where

$$c(\mathcal{F}) = \text{rank}(\mathcal{F}) + |(\text{sing. points})| + \sum_{x \text{ sing.}} \text{Swan}_x(\mathcal{F}) \geq 1.$$
Trace functions

The trace functions modulo a prime $p$ are functions

$$K : \mathbb{F}_p \longrightarrow \mathbb{C}$$

which are “special” functions of algebraic nature.

- Precisely, we consider trace functions of middle-extension $\ell$-adic sheaves $\mathcal{F}$ on the affine line, pointwise pure of weight 0, brought to $\mathbb{C}$ by a fixed $\iota : \overline{\mathbb{Q}}_{\ell} \longrightarrow \mathbb{C}$.

Such a trace function has a “complexity” $c(K)$.

- We define $c(K)$ as the minimum of $c(\mathcal{F})$ over sheaves as above with trace function $K$, where

$$c(\mathcal{F}) = \text{rank}(\mathcal{F}) + |\text{(sing. points)}| + \sum_{x \text{ sing.}} \text{Swan}_x(\mathcal{F}) \geq 1.$$  

We typically let $p$ vary, and consider $K_p$ modulo $p$ with bounded conductor: $c(K_p) \leq C$ for all $p$. 
Examples
Examples

- (Characters) $K(x) = e(f(x)/p)$ or $K(x) = \chi(f(x))$, where $\chi \neq 1$ is a multiplicative character, and $f \in \mathbb{F}_p[X]$ is non-constant; the conductor is bounded in terms of $\text{deg}(f)$ only;

- (Hyper)-Kloosterman sums: for $r \geq 1$ integer

\[
K(x) = Kl_r(x) = \frac{1}{p^{r - 1} / 2} \sum_{y_1, \ldots, y_r = x} y_i \in \mathbb{F}_p e(y_1 + \cdots + y_r p);
\]

the conductor is bounded in terms of $r$ only;

- (Point-counting) $K(x) = \sum_{y \in \mathbb{F}_p} f(y) = x^{1 - 1}$, $f \in \mathbb{F}_p[X]$ non-constant

the conductor is bounded in terms of $\text{deg}(f)$ only.
Examples

- (Characters) $K(x) = e(f(x)/p)$ or $K(x) = \chi(f(x))$, where $\chi \neq 1$ is a multiplicative character, and $f \in \mathbf{F}_p[X]$ is non-constant; the conductor is bounded in terms of $\deg(f)$ only;

- (Hyper)-Kloosterman sums: for $r \geq 1$ integer

$$K(x) = K_{1r}(x) = \frac{1}{p^{(r-1)/2}} \sum_{y_1 \cdots y_r = x \atop y_i \in \mathbf{F}_p} e\left(\frac{y_1 + \cdots + y_r}{p}\right);$$

the conductor is bounded in terms of $r$ only;
Examples

▶ (Characters) $K(x) = e(f(x)/p)$ or $K(x) = \chi(f(x))$, where $\chi \neq 1$ is a multiplicative character, and $f \in \mathbb{F}_p[X]$ is non-constant; the conductor is bounded in terms of $\deg(f)$ only;

▶ (Hyper)-Kloosterman sums: for $r \geq 1$ integer

$$K(x) = Kl_r(x) = \frac{1}{p^{(r-1)/2}} \sum_{y_1 \cdots y_r = x \atop y_i \in \mathbb{F}_p} e\left(\frac{y_1 + \cdots + y_r}{p}\right);$$

the conductor is bounded in terms of $r$ only;

▶ (Point-counting)

$$K(x) = \sum_{y \in \mathbb{F}_p \atop f(y) = x} 1 - 1, \quad f \in \mathbb{F}_p[X] \text{ non-constant.}$$

the conductor is bounded in terms of $\deg(f)$ only.
These functions occur in many applications in analytic number theory.
These functions occur in many applications in analytic number theory. Most often, one needs estimates for the “generalized exponential sums” of the type

$$\sum_{x \in F_p} K(x),$$

or more naturally for inner products

$$\sum_{x \in F_p} K_1(x)K_2(x).$$
These functions occur in many applications in analytic number theory. Most often, one needs estimates for the “generalized exponential sums” of the type

$$\sum_{x \in \mathbf{F}_p} K(x),$$

or more naturally for inner products

$$\sum_{x \in \mathbf{F}_p} K_1(x) K_2(x).$$

of trace functions $K_1$ and $K_2$. 
Goals

- Square-root cancellation:

\[
\left| \sum_{x \in \mathbb{F}_p} K_1(x) \overline{K_2(x)} \right| \leq C \sqrt{p},
\]

where \( C \) is under control (depends only on the complexity of \( K_1 \) and \( K_2 \));
Goals

- Square-root cancellation:

\[ \left| \sum_{x \in \mathbb{F}_p} K_1(x) \overline{K_2(x)} \right| \leq C \sqrt{p}, \]

where \( C \) is under control (depends only on the complexity of \( K_1 \) and \( K_2 \));

- Or understanding when this does not hold ("diagonal situations"), e.g., \( K_1(x) = K_2(x) \).
These goals can often be reached, by exploiting the features of the underlying algebraic geometry:
These goals can often be reached, by exploiting the features of the underlying algebraic geometry:

▶ There is a powerful and very flexible formalism for trace functions, including:

1. Stability under algebraic operations;
2. Stability under Fourier transform, convolution(s), etc;
3. The Grothendieck-Lefschetz trace formula
These goals can often be reached, by exploiting the features of the underlying algebraic geometry:

▶ There is a powerful and very flexible formalism for trace functions, including:

1. Stability under algebraic operations;
2. Stability under Fourier transform, convolution(s), etc;
3. The Grothendieck-Lefschetz trace formula

▶ This formalism is compatible with the complexity: operations on trace functions with bounded complexity result in other trace functions with bounded complexity;
These goals can often be reached, by exploiting the features of the underlying algebraic geometry:

- There is a powerful and very flexible formalism for trace functions, including:
  1. Stability under algebraic operations;
  2. Stability under Fourier transform, convolution(s), etc;
  3. The Grothendieck-Lefschetz trace formula

- This formalism is compatible with the complexity: operations on trace functions with bounded complexity result in other trace functions with bounded complexity;

- And we have the general form of Deligne’s Riemann Hypothesis over finite fields.
A version of the Riemann Hypothesis

Theorem (Quasi-orthogonality)

- Suppose $K_1$ and $K_2$ are trace functions modulo $p$ associated to geometrically irreducible sheaves $\mathcal{F}_1, \mathcal{F}_2$. Then

$$\left| \sum_{x \in \mathbb{F}_p} K_1(x) \overline{K_2(x)} \right| \leq C \sqrt{p}$$

where $C$ depends only on $c(K_1), c(K_2)$, unless $\mathcal{F}_1$ and $\mathcal{F}_2$ are geometrically isomorphic.
A version of the Riemann Hypothesis

Theorem (Quasi-orthogonality)

- Suppose $K_1$ and $K_2$ are trace functions modulo $p$ associated to geometrically irreducible sheaves $\mathcal{F}_1, \mathcal{F}_2$. Then

\[
\left| \sum_{x \in \mathbf{F}_p} K_1(x) \overline{K_2(x)} \right| \leq C \sqrt{p}
\]

where $C$ depends only on $c(K_1), c(K_2)$, unless $\mathcal{F}_1$ and $\mathcal{F}_2$ are geometrically isomorphic.

- In this “diagonal” case, there exists $\alpha$ with $|\alpha| = 1$ such that

\[
K_1(x) = \alpha K_2(x)
\]

and

\[
\left| \sum_{x \in \mathbf{F}_p} K_1(x) \overline{K_2(x)} - \bar{\alpha} p \right| \leq C \sqrt{p}.
\]
Examples

- (Weil-Deligne bounds)

\[ |Kl_r(x)| = p^{-(r-1)/2} \left| \sum_{y_1 \cdots y_r = x} e\left( \frac{y_1 + \cdots + y_r}{p} \right) \right| \leq r. \]
Examples

- **(Weil-Deligne bounds)**

  \[ |Kl_r(x)| = p^{-(r-1)/2} \left| \sum_{y_1 \cdots y_r = x} e\left(\frac{y_1 + \cdots + y_r}{p}\right) \right| \leq r. \]

- **(A “non-bound”)** For

  \[ K(x) = \sum_{y \in \mathbb{F}_p} P_2(Kl_2(y^2))e\left(\frac{xy}{p}\right), \quad P_2(X) = X^2 - 1, \]

  we have

  \[ \left| \sum_{\substack{x \in \mathbb{F}_p \\atop \gamma \cdot x \neq \infty}} K(x)\overline{K(\gamma \cdot x)} \right| \geq p + O(1) \]

  if \( \gamma \in \text{PGL}_2(\mathbb{F}_p) \) is

  \( \gamma = \text{Id}, \quad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 16 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 4 & -16 \\ 1 & 4 \end{pmatrix} \) (and 4 others).
The Riemann Hypothesis can be used as a black box in many applications, using known examples of trace functions and their properties;
Philosophy

- The Riemann Hypothesis can be used as a black box in many applications, using known examples of trace functions and their properties;
- But the more one knows, the better (for instance, to identify geometrically irreducible trace functions);
Philosophy

- The Riemann Hypothesis can be used as a black box in many applications, using known examples of trace functions and their properties;
- But the more one knows, the better (for instance, to identify geometrically irreducible trace functions);
- This talk will attempt to explain, in a specific context, how to make the box slightly less dark.
Sums of products

We often find in applications that we need to bound sums like

$$\sum_{x \in \mathbb{F}_p} K_1(x) \cdots K_n(x) \overline{M(x)}$$

where $K_i, 1 \leq i \leq n$, are trace functions, as well as $M$, and often $M(x) = 1$ or $M(x) = e(hx/p)$ for some $h \in \mathbb{F}_p$. 
Sums of products

We often find in applications that we need to bound sums like

$$\sum_{x \in \mathbb{F}_p} K_1(x) \cdots K_n(x) \overline{M(x)}$$

where $K_i$, $1 \leq i \leq n$, are trace functions, as well as $M$, and often $M(x) = 1$ or $M(x) = e(hx/p)$ for some $h \in \mathbb{F}_p$.

In particular, one often has

$$K_i(x) = K(a_ix + b_i)$$

for some other fixed trace function $K$ and $a_i \in \mathbb{F}_p^\times$, $b_i \in \mathbb{F}_p$. The $(a_i, b_i)$ are not necessarily distinct.
Examples

- Proof of the Burgess bound: $k$ even,

\[ K_i(x) = \chi(x + b_i), \quad M(x) = 1. \]
Examples

- Proof of the Burgess bound: $k$ even,

\[ K_i(x) = \chi(x + b_i), \quad M(x) = 1. \]

- (Friedlander–Iwaniec, Heath-Brown, Michel, Zhang, FKM) For $d_3$ in arithmetic progressions, $n = 2$ and

\[ K_1(x) = Kl_3(a_1x), \quad K_2(x) = Kl_3(a_2x), \quad M(x) = e(hx/p). \]

- (Fouvry-Michel-Rivat-Sárközy, FGKM, KR, Irving): $n \geq 1$, and

\[ K_i(x) = Kl_3(a_i x + b_i), \quad M(x) = 1 \text{ or } e(hx/p). \]
Examples

- Proof of the Burgess bound: \( k \) even,

  \[ K_i(x) = \chi(x + b_i), \quad M(x) = 1. \]

- (Friedlander–Iwaniec, Heath-Brown, Michel, Zhang, FKM) For \( d_3 \) in arithmetic progressions, \( n = 2 \) and

  \[ K_1(x) = \text{Kl}_3(a_1x), \quad K_2(x) = \text{Kl}_3(a_2x), \quad M(x) = e(hx/p). \]

- (Fouvry-Michel-Rivat-Sarközy, FGKM, KR, Irving): \( n \geq 1 \), and

  \[ K_i(x) = \text{Kl}_r(a_ix + b_i), \quad M(x) = 1 \text{ or } e(hx/p). \]
Examples

- Proof of the Burgess bound: \( k \) even,
  \[
  K_i(x) = \chi(x + b_i), \quad M(x) = 1.
  \]

- (Friedlander–Iwaniec, Heath-Brown, Michel, Zhang, FKM) For \( d_3 \) in arithmetic progressions, \( n = 2 \) and
  \[
  K_1(x) = K_{l_3}(a_1x), \quad K_2(x) = K_{l_3}(a_2x), \quad M(x) = e(hx/p).
  \]

- (Fouvry-Michel-Rivat-Sarközy, FGKM, KR, Irving): \( n \geq 1 \), and
  \[
  K_i(x) = K_{l_r}(a_ix + b_i), \quad M(x) = 1 \text{ or } e(hx/p).
  \]

- Other examples: Fouvry–Iwaniec, Bombieri–Bourgain, Blomer–Milicevic...
Assumptions

- In general, the $K_i$ are well-understood, and we assume that they are geometrically irreducible (e.g., $Kl_r(a_i x + b_i)$), and are “given”;

Assumptions

- In general, the $K_i$ are well-understood, and we assume that they are geometrically irreducible (e.g., $Kl_r(a_ix+b_i)$), and are “given”;
- We assume also that $M$ is geometrically irreducible, but it might not be known very explicitly.
More precise goal

We wish to classify the “diagonal” cases: for which $M$ does an estimate

$$\left| \sum_{x \in \mathbf{F}_p} K_1(x) \cdots K_n(x) M(x) \right| \leq C \sqrt{p}$$

fail, with $C$ depending only on $\max(c(K_i), c(M))$?
More precise goal

We wish to classify the “diagonal” cases: for which $M$ does an estimate

$$\left| \sum_{x \in \mathbf{F}_p} K_1(x) \cdots K_n(x) M(x) \right| \leq C \sqrt{p}$$

fail, with $C$ depending only on $\max(c(K_i), c(M))$?

**Main difficulty.** For $n \geq 2$, $K_1 \cdots K_n$ has no reason to be geometrically irreducible. Thus quasi-orthogonality can not be applied directly.
Principle of the method

- Each trace function $K_i$ is a restriction to a set of Frobenius conjugacy classes of the character of a finite-dimensional representation of some group $\Pi_1$: there exist

$$\rho_i : \Pi_1 \rightarrow \text{GL}(V_i)$$

such that

$$K_i(x) = \iota\left(\text{Tr} \rho_i(Fr_x,F_{\rho})\right).$$
Principle of the method

- Each trace function $K_i$ is a restriction to a set of Frobenius conjugacy classes of the character of a finite-dimensional representation of some group $\Pi_1$: there exist

$$\rho_i : \Pi_1 \longrightarrow \text{GL}(V_i)$$

such that

$$K_i(x) = \iota \left( \text{Tr} \rho_i(F_{x,F_p}) \right).$$

- Consider the direct sum

$$\rho = \rho_1 \oplus \cdots \oplus \rho_n : \Pi_1 \longrightarrow \text{GL}(V_1 \oplus \cdots \oplus V_n)$$

and the “external” tensor product

$$\pi : \text{GL}(V_1 \oplus \cdots \oplus V_n) \longrightarrow \text{GL}(V_1 \bigotimes \cdots \bigotimes V_n).$$
Then

\[ K_1(x) \cdots K_n(x) = \text{Tr}((\pi \circ \rho)(Fr_x,F_\rho)). \]
Then

\[ K_1(x) \cdots K_n(x) = \text{Tr}((\pi \circ \rho)(\text{Fr}_x, F_p)). \]

Intuitively, we know\(^1\) (Deligne’s Equidistribution Theorem) that this means that the product is distributed like the trace of a “random” matrix in a maximal compact subgroup \( U \) of the Zariski-closure \( G \) of the image of \( \rho \).

\(^1\)With a minor caveat
Then
\[ K_1(x) \cdots K_n(x) = \text{Tr}((\pi \circ \rho)(\text{Fr}_{x,F_p})). \]

Intuitively, we know\(^1\) (Deligne’s Equidistribution Theorem) that this means that the product is distributed like the trace of a “random” matrix in a maximal compact subgroup \( U \) of the Zariski-closure \( G \) of the image of \( \rho \).

This means that (case \( M = 1 \)) we have
\[
\frac{1}{p} \sum_{x \in F_p} K_1(x) \cdots K_n(x) = \int_U \text{Tr}(x) d\mu_{\text{Haar}}(x) + O(p^{-1/2}).
\]

\(^1\)With a minor caveat
Then

\[ K_1(x) \cdots K_n(x) = \text{Tr}((\pi \circ \rho)(\text{Fr}_{x,F_p})). \]

Intuitively, we know\(^1\) (Deligne's Equidistribution Theorem) that this means that the product is distributed like the trace of a “random” matrix in a maximal compact subgroup \(U\) of the Zariski-closure \(G\) of the image of \(\rho\).

This means that (case \(M = 1\)) we have

\[
\frac{1}{p} \sum_{x \in F_p} K_1(x) \cdots K_n(x) = \int_U \text{Tr}(x)d\mu_{\text{Haar}}(x) + O(p^{-1/2}).
\]

So square-root cancellation means exactly that the “main term” vanishes...

\(^1\)With a minor caveat
... which means that the trivial representation is not a component of the “tautological” representation of $U$ on $V_1 \oplus \cdots \oplus V_n$. 

A priori, $G$ (resp. $U$) is a subgroup of the product of the $G_i$ (resp. $U_i$) defined similarly from $\rho_i$. 

If it is so big that $U = U_1 \times \cdots \times U_n$, then 

$$\int_U \text{Tr}(x) \, d\mu_{\text{Haar}}(x) = \prod_{1 \leq i \leq n} \int_{U_i} \text{Tr}(x) \, d\mu_{\text{Haar}}(x).$$ 

If we know that the $\rho_i$ are irreducible and non-trivial, this is zero.
... which means that the trivial representation is not a component of the “tautological” representation of $U$ on $V_1 \oplus \cdots \oplus V_n$.

A priori, $G$ (resp. $U$) is a subgroup of the product of the $G_i$ (resp. $U_i$) defined similarly from $\rho_i$. 
... which means that the trivial representation is not a component of the “tautological” representation of $U$ on $V_1 \oplus \cdots \oplus V_n$.

A priori, $G$ (resp. $U$) is a subgroup of the product of the $G_i$ (resp. $U_i$) defined similarly from $\rho_i$.

If it is so big that $U = U_1 \times \cdots \times U_n$, then

$$\int_U \text{Tr}(x) d\mu_{\text{Haar}}(x) = \prod_{1 \leq i \leq n} \int_{U_i} \text{Tr}(x) d\mu_{\text{Haar}}(x).$$
... which means that the trivial representation is not a component of the “tautological” representation of $U$ on $V_1 \oplus \cdots \oplus V_n$.

A priori, $G$ (resp. $U$) is a subgroup of the product of the $G_i$ (resp. $U_i$) defined similarly from $\rho_i$.

If it is so big that $U = U_1 \times \cdots \times U_n$, then

$$\int_U \text{Tr}(x) d\mu_{\text{Haar}}(x) = \prod_{1 \leq i \leq n} \int_{U_i} \text{Tr}(x) d\mu_{\text{Haar}}(x).$$

If we know that the $\rho_i$ are irreducible and non-trivial, this is zero.
How/when can we get such a “big” group?
How/when can we get such a “big” group?

- Basic information: the projections $U \longrightarrow U_i$ are surjective for each $i$;
Goursat-Kolchin-Ribet, d’après Katz

How/when can we get such a “big” group?

▶ Basic information: the projections $U \rightarrow U_i$ are surjective for each $i$;
▶ A “miracle”: complicated groups are very independent from each other!
How/when can we get such a “big” group?

- Basic information: the projections $U \longrightarrow U_i$ are surjective for each $i$;
- A “miracle”: complicated groups are very independent from each other!
- In particular, if $U_i = SU_{d_i}(\mathbb{C})$, $d_i \geq 2$, and the representations $\rho_i$ are pairwise non-isomorphic,\(^2\) then $U$ is the product of the $U_i$;

\(^2\) More precisely, pairwise unrelated up to twists.
How/when can we get such a “big” group?

- **Basic information:** the projections $U \rightarrow U_i$ are surjective for each $i$;

- **A “miracle”:** complicated groups are very independent from each other!

- In particular, if $U_i = SU_{d_i}(\mathbb{C})$, $d_i \geq 2$, and the representations $\rho_i$ are pairwise non-isomorphic,\(^2\) then $U$ is the product of the $U_i$;

- The same happens with $USp_{2g_i}(\mathbb{C})$, or with mixtures, or with quite a few other groups with simple Lie algebra.

---

\(^2\) More precisely, pairwise unrelated up to twists.
An example

This is already enough for many applications. For instance:

**Theorem (Katz)**

*For* $r$ *even and* $K(x) = \text{Kl}_r(ax + b)$, *we have* $U = \text{USp}_r(C)$, *and the underlying sheaves when* $(a, b) \in F_p^\times \times F_p$ *vary are pairwise non-isomorphic (even up to twist).*
An example

This is already enough for many applications. For instance:

Theorem (Katz)
For r even and $K(x) = Kl_r(ax + b)$, we have $U = USp_r(\mathbb{C})$, and the underlying sheaves when $(a, b) \in F_p^\times \times F_p$ vary are pairwise non-isomorphic (even up to twist).

It follows:

Corollary
If r is even, $n \geq 1$ is fixed, and $(a_i, b_i)_{1 \leq i \leq n}$ are distinct pairs in $F_p^\times \times F_p$, then

$$\sum_{x \in F_p} Kl_r(a_1x + b_1) \cdots Kl_r(a_nx + b_n) \ll p^{1/2}.$$
Diagonal cases

In some applications, not all $K_i$ are distinct. So we may need to consider

$$\sum_{x \in \mathbb{F}_p} K_1(x)^{\nu_1} \cdots K_n(x)^{\nu_n}$$

where the $K_i$ are pairwise non-isomorphic and $\nu_i \geq 1$. 
Diagonal cases

In some applications, not all $K_i$ are distinct. So we may need to consider

$$\sum_{x \in \mathbf{F}_p} K_1(x)^{\nu_1} \cdots K_n(x)^{\nu_n}$$

where the $K_i$ are pairwise non-isomorphic and $\nu_i \geq 1$.

By the previous argument, at least if $(K_1, \ldots, K_n)$ satisfy the same assumptions as before (large “complicated” monodromy), we get square root cancellation if and only if

$$\prod_{1 \leq i \leq n} \int_{U_i} \text{Tr}(x)^{\nu_i} d\mu_{\text{Haar}}(x) = 0.$$
If $U_i = \text{USp}_{2g_i}(\mathbb{C})$, this means that at least some multiplicity $\nu_i$ is odd.

If $U_i = \text{USp}_{2g_i}(\mathbb{C})$, this means that at least some multiplicity $\nu_i$ is odd.

If $U_i = \text{SU}_{d_i}(\mathbb{C})$, this means that at least some multiplicity $\nu_i$ is not divisible by $d_i$. 
If \( U_i = \text{USp}_{2g_i}(\mathbb{C}) \), this means that at least some multiplicity \( \nu_i \) is odd.

If \( U_i = \text{SU}_{d_i}(\mathbb{C}) \), this means that at least some multiplicity \( \nu_i \) is not divisible by \( d_i \).

For instance, if \( r \) is even, we have

\[
\sum_{x \in \mathbb{F}_p} \text{Kl}_r(a_1x + b_1)^{\nu_1} \cdots \text{Kl}_r(a_nx + b_n)^{\nu_n} \ll p^{1/2}
\]

unless each \( \nu_i \) is even.
A comparison

Take $K_i(x) = e((a_i x)^{-1}/p)$ (inverse modulo $p$) for distinct $a_i$'s.
A comparison

Take $K_i(x) = e((a_i x)^{-1}/p)$ (inverse modulo $p$) for distinct $a_i$'s. Then the sum

$$\sum_{x \in \mathbb{F}_p^\times} K_1(x) \cdots K_n(x)$$

has no cancellation for all $(a_1, \ldots, a_n)$ such that

$$\frac{1}{a_1} + \cdots + \frac{1}{a_n} = 0.$$
When $M$ is non-trivial

Now take $M$ any geometrically irreducible trace function and consider

$$\sum_{x \in \mathbb{F}_p} K_1(x)^{\nu_1} \cdots K_n(x)^{\nu_n} \overline{M(x)}.$$
When $M$ is non-trivial

Now take $M$ any geometrically irreducible trace function and consider

$$
\sum_{x \in \mathbb{F}_p} K_1(x)^{\nu_1} \cdots K_n(x)^{\nu_n} \overline{M(x)}.
$$

If there is no square-root cancellation then:

1. $L_n(x)$ is associated to a representation $\Lambda_i \circ \rho_i$ of $\Pi_1$;
2. For each $i$, $\Lambda_i$ is an irreducible subrepresentation of the $\nu_i$-th tensor power of the standard representations of $U_i$. 


When $M$ is non-trivial

Now take $M$ any geometrically irreducible trace function and consider

$$\sum_{x \in \mathbb{F}_p} K_1(x)^{\nu_1} \cdots K_n(x)^{\nu_n} \overline{M(x)}.$$ 

If there is no square-root cancellation then:

- $M$ must correspond to a representation of $\Pi_1$ that factors through $\rho$;
When $M$ is non-trivial

Now take $M$ any geometrically irreducible trace function and consider

$$
\sum_{x \in \mathbb{F}_p} K_1(x)^{\nu_1} \cdots K_n(x)^{\nu_n} M(x).
$$

If there is no square-root cancellation then:

- $M$ must correspond to a representation of $\Pi_1$ that factors through $\rho$;
- If $U$ is the product of the $U_i$, this means that $M = L_1(x) \cdots L_n(x)$ where
  
  1. $L_n(x)$ is associated to a representation $\Lambda_i \circ \rho_i$ of $\Pi_1$;
  2. For each $i$, $\Lambda_i$ is an irreducible subrepresentation of the $\nu_i$-th tensor power of the standard representations of $U_i$. 
For example, we have

$$\sum_{x \in F_p} Kl_2(a_1x + b_1)^{\nu_1} \cdots Kl_2(a_nx + b_n)^{\nu_n} M(x) \ll p^{1/2}$$

for $M$ geometrically irreducible if and only $M$ is not of the form

$$M(x) = \prod_{1 \leq i \leq n} P_{2m_i}(Kl_2(a_i x + b_i))$$

where $P_d$ is a Chebychev polynomial.
An application (FGKM, KR)

Let $k \geq 2$ be an integer, $p$ a prime, $(a, p) = 1$, a real number $X \geq 2$, and $w$ a test function

$$w : [0, +\infty[ \longrightarrow [0, 1]$$

with $w(x) \geq 0$, $w \neq 0$. Let

$$E(X; p, a) = \sum_{n \geq 1} d_k(n) - \frac{1}{p - 1} \sum_{n \geq 1} d_k(n).$$

$$n \equiv a \pmod{p}$$
Theorem
If $X = p^k/\Phi(p)$ with $\Phi(x) \uparrow +\infty$, $\Phi(x) \ll x^\varepsilon$, then

$$a \mapsto E(X; p, a)$$

is approximately normally distributed, if:

1. $a \in I$, $I$ interval of length $p^{1/2+\delta}$, $\delta > 0$
2. $a \in \{F_p\}$ where $F_p \in \mathbb{Z}[X]$ is a fixed non-constant polynomial (KR).
Theorem
If \( X = p^k / \Phi(p) \) with \( \Phi(x) \uparrow +\infty, \Phi(x) \ll x^\varepsilon \), then

\[
a \mapsto E(X; p, a)
\]

is approximately normally distributed, if:

- \( k = 2, a \in F_p^\times \) (FGKM)
Theorem

If $X = p^k / \Phi(p)$ with $\Phi(x) \uparrow +\infty$, $\Phi(x) \ll x^\varepsilon$, then

$$a \mapsto E(X; p, a)$$

is approximately normally distributed, if:

- $k = 2$, $a \in \mathbb{F}_p^\times$ (FGKM)
- $k \geq 3$, $a \in \mathbb{F}_p^\times$ (KR)
Theorem

If \( X = p^k / \Phi(p) \) with \( \Phi(x) \uparrow +\infty, \Phi(x) \ll x^\varepsilon \), then

\[
a \mapsto E(X; p, a)
\]

is approximately normally distributed, if:

- \( k = 2, a \in \mathbf{F}_p^\times \) \((\text{FGKM})\)
- \( k \geq 3, a \in \mathbf{F}_p^\times \) \((\text{KR})\)
- \( k \geq 3, \) and either
  1. \( a \in l, l \text{ interval of length } p^{1/2+\delta}, \delta > 0 \)
  2. \( a \in f(\mathbf{F}_p) \text{ where } f \in \mathbf{Z}[X] \text{ is a fixed non-constant polynomial } \)
     \((\text{KR})\).
Assume one considers \( a \in X_p \) where \( X_p \subset \mathbb{F}_p \). Computing the \( n \)-th moment using the Voronoi summation formula, one ends up dealing with sums

\[
S(a_1, \ldots, a_n) = \sum_{x \in \mathbb{F}_p} Kl_k(a_1x) \cdots Kl_k(a_nx) \overline{M(x)}
\]

for \((a_1, \ldots, a_n) \in \mathbb{F}_p^\times\), \( M \) one of the trace functions arising in a decomposition

\[
1_{X_p}(x) = \sum_j \alpha_j M_j(x), \quad M_1(x) = \frac{|X_p|}{p}.
\]
The key point is that $M$ can not be “diagonal” for too many tuples $(a_1, \ldots, a_n)$:
The key point is that $M$ can not be “diagonal” for too many tuples $(a_1, \ldots, a_n)$: if $M$ is not geometrically trivial, then the number of $a \in (\mathbb{F}_p^\times)^n$ for which there is no square-root cancellation is

$$\ll p^{(n-1)/2}$$

where the implied constant depends only on $r$. 
The key point is that $M$ can not be “diagonal” for too many tuples $(a_1, \ldots, a_n)$: if $M$ is not geometrically trivial, then the number of $a \in (F_p^\times)^n$ for which there is no square-root cancellation is

$$\ll p^{(n-1)/2}$$

where the implied constant depends only on $r$. In contrast, for $M = 1$ and $n$ even, all $(p - 1)^{n/2}$ tuples $(a_1, a_1, \ldots, a_{n/2}, a_{n/2})$ contribute to the main term.
What if the $K_i$ are not pairwise distinct?

One needs some fun algebraic facts. For instance: let $H \subset G$ be a subgroup of a group $G$, $\xi \in G$. Then we have

$$\xi H \xi \subset H$$

if and only if $\xi \in N_G(H)$ and $\xi^2 \in H$. 