Distribution of the trace in the compact group of type G_2 and applications to exponential sums

Gilles Lachaud

CNRS I2M Marseille-Luminy

AGC^{2}T-16

Arithmetic, Geometry, Cryptography and Coding Theory

CIRM, June 19th-23th, 2017

Exponential sums

Sums of degree 7

$k = \mathbb{F}_q$. Assume char $k = p > 14$.
ψ : a nontrivial additive character of k
N. Katz (1990, 2004) introduced the sums

$$S(t) = \sum_{x \in k^\times} \chi_2(x)\psi(x^7 + tx), \qquad t \in k,$$

with the quadratic character (Legendre symbol)

$$\chi_2(x) = \left(\frac{x}{p}\right), \quad x \in \mathbb{F}_p.$$

Then

$$p^{-1/2} S(t) = \sum_{j=1}^{7} \alpha_j$$

with $|\alpha_j| = 1$.

Yoga of equidistribution

By analogy with families of curves, in favorable situations:

As q and t vary, such families of exponential sums satisfy
a generalized equidistribution law,
coming from the trace of elements of a compact Lie group G

In view of its relation to a fundamental group, the group G is called the *monodromy group* of the family

More precisely, the monodromy group G is such that :

1. If $t \in T(\mathbb{F}_p)$,

$$p^{-1/2} S(t) = \mathrm{Tr}(g_t) \quad \text{for some } g_t \in G.$$

2. The $p^{-1/2} S(t)$ are *equidistributed* like the trace of random elements of G:

$$\frac{\left| \left\{ t \in T(\mathbb{F}_p) \mid p^{-1/2} S(t) \le x \right\} \right|}{|T(\mathbb{F}_p)|} = F(x) + O\left(p^{-1/2}\right),$$

with the *cumulative distribution function* (CDF)

$$F(x) = \mathrm{vol}\left\{ g \in G \mid \mathrm{Tr}(g) \le x \right\}$$

The *probability density function* (PDF) is $f(x) = F'(x)$

Normalizing factor

The *quadratic Gauss sum* is

$$g = g(\psi, \chi_2) = \sum_{x \in \mathbb{F}_p^\times} \left(\frac{x}{7}\right) \exp \frac{2i\pi x}{p}.$$

$$g = \begin{cases} \sqrt{p} & if \quad p \equiv 1 \pmod 4 \\ i\sqrt{p} & if \quad p \equiv 3 \pmod 4). \end{cases}$$

Normalization : let

$$\boxed{\widetilde{S}(t) = \left(\frac{p}{7}\right) \frac{S(t)}{g}}$$

Then $\widetilde{S}(t)$ is real and belongs to $[-2, 7]$. We shall see that

$$\widetilde{S}(t) = 1 + \alpha_1 + \alpha_2 + \alpha_1\alpha_2 + \frac{1}{\alpha_1} + \frac{1}{\alpha_2} + \frac{1}{\alpha_1\alpha_2},$$

with α_1, α_2 on the unit circle.

Summary

The normalisation leads to real numbers:

$$\widetilde{S}(t) = \left(\frac{-7}{p}\right) p^{-1/2} \sum_{x\in\mathbb{F}_p^\times} \left(\frac{x}{p}\right) \cos \frac{2\pi(x^7 + tx)}{p} \quad \text{if } p \equiv 1 (\bmod 4),$$

$$= \left(\frac{-7}{p}\right) p^{-1/2} \sum_{x\in\mathbb{F}_p^\times} \left(\frac{x}{p}\right) \sin \frac{2\pi(x^7 + tx)}{p} \quad \text{if } p \equiv 3 (\bmod 4)$$

What is the monodromy group of these families ?

Distribution

Let $\mathbf{UG}_2$ be the compact semi-simple Lie group of exceptional type G_2, and τ_1 the character of the representation of degree 7

Theorem (Katz)

The monodromy group of $\widetilde{S}(t)$ is equal to $\mathbf{UG}_2$. Hence,

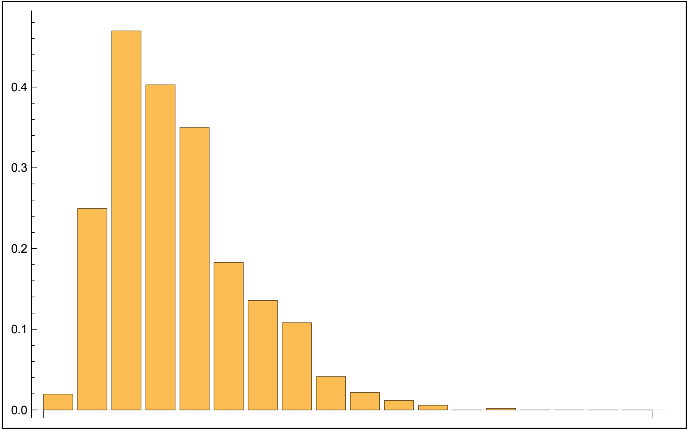
$$\frac{|\{t \in \mathbb{F}_p \mid p^{-1/2}\widetilde{S}(t) \leq x\}|}{p} = \mathrm{vol}\{g \in \mathbf{UG}_2 \mid \tau_1(g) \leq x\} + O\left(p^{-1/2}\right),$$

Katz (2017) generalized this to more general families of degree 7

Question (Katz)

Find an explicit formula for the distribution of τ_1

Histogram



$$f_p(x) = \frac{\left|\left\{t \in \mathbb{F}_p \mid x \le \widetilde{S}(t) \le x + \frac{1}{2}\right\}\right|}{p}, \quad x = -2, \ldots, 6.5$$

$p = 1019$

The group $\mathbf{UG}_2$

The algebra $\mathfrak{g}_2$

$\mathfrak{g}_2$: complex Lie algebra of matrices

$$X = \left(\begin{array}{c|ccc|ccc} 0 & 2d & 2e & 2f & 2a & 2b & 2c \\ \hline a & & & & 0 & f & -e \\ b & & A & & -f & 0 & d \\ c & & & & e & -d & 0 \\ \hline d & 0 & -c & b & & & \\ e & c & 0 & -a & & -\,{}^tA & \\ f & -b & a & 0 & & & \end{array}\right), \quad A \in \mathfrak{sl}_3(\mathbb{C}).$$

$\mathfrak{g}_2$ is a simple Lie subalgebra of an orthogonal Lie algebra $\mathfrak{so}(\Psi)$

Cartan subalgebra $\mathfrak{h}$ of $\mathfrak{g}_2$: diagonal matrices of the form

$$\begin{pmatrix} 0 & & & & & & \\ & \theta_1 & & & & & \\ & & \theta_2 & & & \text{\Large 0} & \\ & & & -\theta_1-\theta_2 & & & \\ & & & & -\theta_1 & & \\ & \text{\Large 0} & & & & -\theta_2 & \\ & & & & & & \theta_1+\theta_2 \end{pmatrix}$$

The group $\mathbf{G}_2$

- There is exactly one connected complex algebraic group $\mathbf{G}_2$ with Lie algebra $\mathfrak{g}_2$
- $\mathbf{G}_2$ is simple , simply connected
- $\mathbf{T}$: Maximal 2-dimensional torus of $\mathbf{G}_2$, with matrices

$$t(a_1, a_2) = \begin{pmatrix} 1 & & & & & & \\ & a & & & & \mathbf{0} & \\ & & a_2 & & & & \\ & & & (a_1 a_2)^{-1} & & & \\ & & & & a_1^{-1} & & \\ & \mathbf{0} & & & & a_2^{-1} & \\ & & & & & & a_1 a_2 \end{pmatrix}.$$

The group $\mathbf{UG}_2$

Compact form of $\mathbf{G}_2$:

$$\mathbf{UG}_2 = \mathbf{G}_2 \cap \mathbf{SU}(H)$$

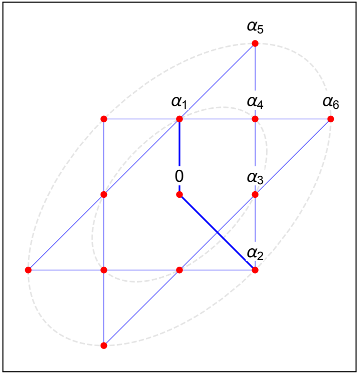
with H a non-degenerate positive hermitian form on $\mathbb{C}^7$
$\mathbf{UG}_2$ is conjugate to a subgroup of $\mathbf{SO}(7)$
T : maximal 2-dimensional torus of $\mathbf{UG}_2$, with matrices

$$u(\theta_1,\theta_2) = \begin{pmatrix} 1 & & & & & & \\ & e^{i\theta_1} & & & & & \\ & & e^{i\theta_2} & & & \mathbf{0} & \\ & & & e^{-i(\theta_1+\theta_2)} & & & \\ & & & & e^{-i\theta_1} & & \\ & \mathbf{0} & & & & e^{-i\theta_2} & \\ & & & & & & e^{i(\theta_1+\theta_2)} \end{pmatrix}$$

Root system

The *root system* $\Phi \subset \mathfrak{h}^*$ of $(\mathfrak{g}_2, \mathfrak{h})$ is of rank 2. Base:

$$\alpha_1 = (0,1), \quad \alpha_2 = (1,-1).$$



Weyl group W of order 12, isomorphic to $S_3 \times C_2 = D_6$

Fundamental representations

$\mathbf{G}_2$ has two fundamental representations:

- The standard representation π_1 of degree 7, defined by the natural imbedding $\mathbf{G}_2 \longrightarrow \mathbf{GL}_7$

$$\tau_1(t) = \operatorname{Tr}\pi_1(t), \qquad t \in \mathbf{T}.$$

- The adjoint representation π_2 of degree 14

$$\tau_2(t) = \operatorname{Tr}\pi_2(t) = \sum_{\alpha\in\Phi} \chi_\alpha(t), \qquad t \in \mathbf{T}.$$

Proposition

If $t(a_1, a_2) \in \mathbf{T}$, then

$$\tau_1 \circ t(a_1, a_2) = u + v + w + 1,$$
$$\tau_2 \circ t(a_1, a_2) = uv + vw + wu + 2,$$

where

$$u = a_1 + \frac{1}{a_1}, \quad v = a_2 + \frac{1}{a_2}, \quad w = a_1 a_2 + \frac{1}{a_1 a_2}.$$

Weyl integration formula

We want to calculate

$$\int_{g \in \mathbf{UG}_2, \tau_1(g) \leq x} dg$$

Theorem (Weyl integration formula for $\mathbf{UG}_2$)

If F *is a piecewise continuous class function, then*

$$\boxed{\int_{\mathbf{UG}_2} \mathsf{F}(g)\, dg = \frac{1}{|W|} \int_{[0,1]^2} \mathsf{F} \circ u(2\pi\theta)\, \delta(2\pi\theta)\, d\theta}$$

with $\theta = (\theta_1, \theta_2)$, $d\theta = d\theta_1 d\theta_2$, *and the Weyl density*

$$\delta(\theta) = (d_1(\theta)\, d_2(\theta))^2$$

$$d_1(\theta) = 2(\sin\theta_1 + \sin\theta_2 - \sin(\theta_1 + \theta_2))$$
$$d_2(\theta) = 2(\sin(\theta_1 - \theta_2) - \sin(2\theta_1 + \theta_2))\sin(2\theta_1 + 2\theta_2))$$

Steinberg map

The *Steinberg map* $\boldsymbol{\tau} : \mathbf{G}_2 \longrightarrow \mathbb{R}^2$ is given by

$$\boldsymbol{\tau}(g) = (\tau_1(g), \tau_2(g))$$

By composition, we define $\boldsymbol{\sigma} : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$

$$\boldsymbol{\sigma}(\theta) = \boldsymbol{\tau} \circ u(2\pi\theta)$$

The Jacobian determinant of $\boldsymbol{\sigma}$ is

$$\operatorname{Jac} \boldsymbol{\sigma}(\theta) = 4\pi^2 \sqrt{\delta(2\pi\theta)}$$

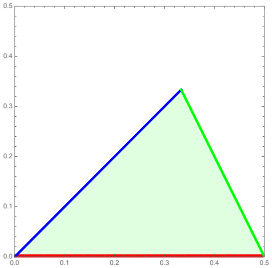
Moreover the Weyl density $\delta(\theta) = D(\boldsymbol{\sigma}(\theta))$, with

$$\boxed{D(x,y) = (4y - x^2 - 2x + 7)((y + 5(x+1))^2 - 4(x+2)^3)}$$

Alcove in the Cartan subalgebra

Fundamental alcove A : fundamental domain for the operation of W on $\mathfrak{h}$: intersection of the half-planes

$$H_1 : \theta_2 > 0, \quad H_2 : 1 - \theta_2 - 2\theta_1 > 0, \quad H_3 : \theta_1 - \theta_2 > 0.$$



A is a triangle with vertices

$$A_1 = \left(\tfrac{1}{3}, \tfrac{1}{3}\right), \quad A_2 = (0,0), \quad A_3 = \left(\tfrac{1}{2}, 0\right).$$

Properties of the Steinberg map

Theorem

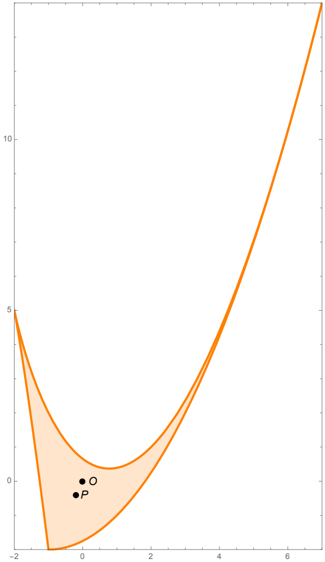
1. *The Steinberg map* $\boldsymbol{\tau}$ *induces an homeomorphism of* $T/W \simeq \mathrm{Cl}\,\mathbf{UG}_2$ *onto a domain* $\Sigma \subset \mathbb{R}^2$.
2. *The map*

$$\boldsymbol{\sigma} = \boldsymbol{\tau} \circ u : A \longrightarrow \Sigma$$

(where A *is the alcove) is a homeomorphism, and* $\partial\Sigma$ *corresponds to the singular classes.*

3. *The restriction to* $\overline{\Sigma}$ *of* $D(x,y)$ *is zero on the boundary and nowhere else.*

Picture of Σ



The boundary of Σ is the curve

$$D(x, y) = 0$$

Vertices:

$$A_1 = (-2, 5),\ A_2 = (7, 14),\ A_3 = (-1, -2)$$

Concentration on the left:

- Maximum of D at $P = (-1/5, -2/5)$
- Center of gravity w.r.t. $D^{1/2}$ at $O = (0, 0)$

Distribution of the trace

Second integral formula

Theorem (Second integration formula for $G = \mathbf{UG}_2$)

If φ is a piecewise continuous function on Σ, then

$$\int_{\mathbf{UG}_2} \varphi \circ \boldsymbol{\tau}(g)\, dg = \frac{1}{4\pi^2} \int_{\Sigma} \varphi(x,y) D(x,y)^{1/2} dx\, dy.$$

Recall that D is defined by $\delta = D(\tau_1 \circ u, \tau_2 \circ u)$

Note : this generalizes (Serre, 2015) to every semisimple simply connected group, thanks to a formula of Steinberg (1965)

Probability density function

Taking for φ the characteristic function of the set $\{x \leq t\}$, we get

$$F(t) = \text{vol}\left\{g \in \mathbf{UG}_2 \mid \tau_1(g) \leq t\right\} = \frac{1}{4\pi^2} \int_{(x,y)\in\Sigma, x\leq t} D(x,y)^{1/2} dx\, dy$$

which is the CDF of τ_1. Hence, the PDF of τ_1 is given by

$$f(x) = F'(x) = \frac{1}{4\pi^2} \int_{\Sigma(x)} D(x,y)^{1/2} dy.$$

where $\Sigma(x) = \left\{y \mid (x,y) \in \Sigma\right\}$

Question

Express this integral with the help of special functions

Gauss' hypergeometric function

Integral representation of Gauss' hypergeometric function:

$$ {}_2F_1(a,b;c;z) = \frac{\Gamma(c)}{\Gamma(b)\Gamma(c-b)} \int_0^1 t^{b-1}(1-t)^{c-b-1}(1-tz)^{-a}\, dt $$

where $a \in \mathbb{C}$ and $\operatorname{Re} c > \operatorname{Re} b > 0$. Analytic function of z in $\mathbb{C} \setminus [1,\infty[$.
The function

$$ \mathsf{H}(z) = {}_2F_1\left(-\frac{1}{2}, \frac{3}{2}, 3; z\right) $$

is also expressible in terms of:

- Legendre function of the first kind $\mathfrak{P}^{-1}_{-5/2}(z)$
- Legendre elliptic integrals $E(z)$ and $K(z)$
- Meijer's G-function, etc.

Main theorem

Theorem (GL)

Let

$$z(x) = \frac{16y^3}{(y+1)(3-y)^3}, \quad y = \sqrt{x+2},$$

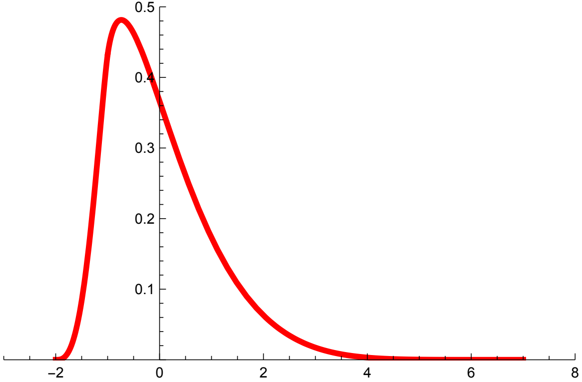
$$f_1(x) = \frac{1}{2\pi} \quad y^6 \quad (3-y)^{3/2}(y+1)^{1/2}\,\mathrm{H}(z(x)),$$
$$f_2(x) = \frac{1}{128\pi} y^{3/2}(3-y)^6 \quad (y+1)^2 \quad \mathrm{H}(\frac{1}{z(x)}).$$

Then the probability density function of the character τ_1 is given by

$$f(x) = \begin{cases} f_1(x) & \text{if} \quad -2 \le x \le -1, \\ f_2(x) & \text{if} \quad -1 \le x \le 7. \end{cases}$$

This is a real analytic function at every point $z \neq 1$.

Graph of PDF

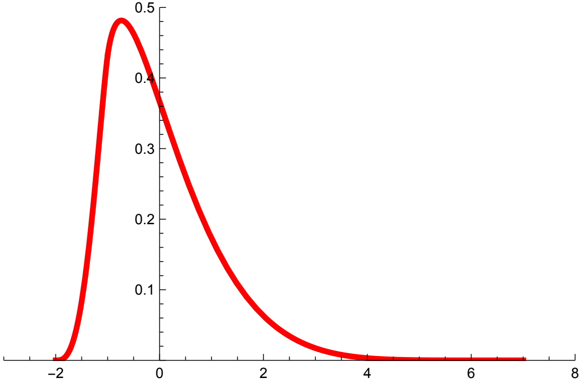


Probability density function $f(x)$

$$x_{max} = -0.736\ldots, \qquad f(x_{max}) = 0.481\ldots$$

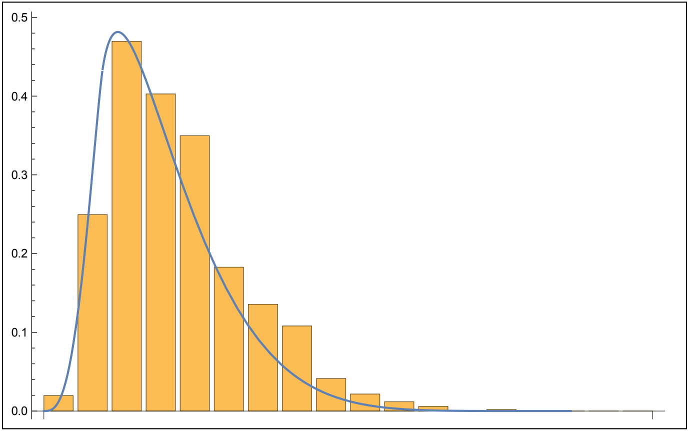
$$f(-2+\varepsilon) \sim \frac{3\sqrt{3}}{2\pi}\,\varepsilon^3, \qquad f(7-\varepsilon) = \frac{1}{2^9\cdot 3^4\cdot\sqrt{3}\cdot\pi}\,\varepsilon^6 + O(\varepsilon)^8.$$

Descriptors of the shape



Skewness (asymétrie) $M_3 = 1 > 0 \Rightarrow$ right tail longer, skewed to the right; mass concentrated on the left.
Kurtosis $M_4 - 3 = 1 > 0 \Rightarrow$ *leptokurtic* curve (high peak).

Relevance of PDF to histogram



$p = 1019$