Equidistribution of Roots of Unity and the Mahler Measure

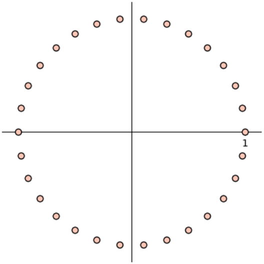
Philipp Habegger

(University of Basel)

Diophantine Problems, Determinism and Randomness
CIRM, November 25, 2020

Joint work with Vesselin Dimitrov

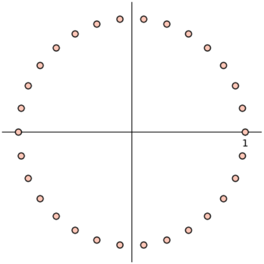
Equidistribution of Roots of Unity



Order dividing 30

$$\left\{ e^{2\pi ik/N} : k \in \mathbb{Z} \right\} \text{ become equdistributed as } N \to \infty.$$

Equidistribution of Roots of Unity



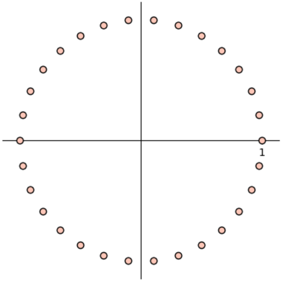
Order dividing 30

$$\left\{e^{2\pi ik/N} : k \in \mathbb{Z}\right\} \text{ become equdistributed as } N \to \infty.$$

If $f\colon S^1 = \{z \in \mathbb{C} : |z| = 1\} \to \mathbb{C}$ is continuous, then

$$\lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} f(e^{2\pi ik/N}) = \int_0^1 f(e^{2\pi it})\mathrm{d}t.$$

Equidistribution of Roots of Unity



Order dividing 30

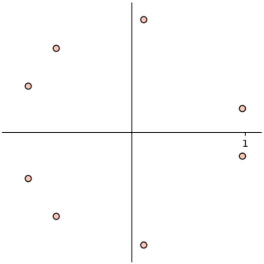
For the test function $f(z) = z^l$ with $l \in \mathbb{Z}$ we have

$$\frac{1}{N}\sum_{k=0}^{N-1} f(e^{2\pi ik/N}) =$$

$$\frac{1}{N}\sum_{k=0}^{N-1} e^{2\pi ikl/N} = \begin{cases} 0 & : N \nmid l, \\ 1 & : N \mid l. \end{cases}$$

$$f(z) = \sum_{l=-L}^{L} a_l z^l \Rightarrow \lim_{N\to\infty} \frac{1}{N}\sum_{k=0}^{N-1} f(e^{2\pi ik/N}) = a_0 = \int_0^1 f(e^{2\pi it})\mathrm{d}t.$$

Equidistribution of Galois Conjugates

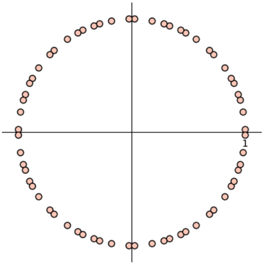


Order (exactly) $N = 30$

Number of roots of unity in $\left\{e^{2\pi ik/N} : k \in \mathbb{Z} \text{ coprime to } N\right\}$ is $\varphi(N)$.
It is the set of $\mathbb{Q}$-Galois conjugates of $e^{2\pi i/N}$. Equidistribution follows from

$$\frac{1}{\varphi(N)} \sum_{\substack{k=1 \\ \gcd(k,N)=1}}^{N} e^{2\pi ikl/N} = \pm\phi\left(\frac{N}{\gcd(N,l)}\right)^{-1}.$$

Equidistribution of Galois Conjugates



Order (exactly) $N = 240$

Number of roots of unity in $\left\{e^{2\pi ik/N} : k \in \mathbb{Z} \text{ coprime to } N\right\}$ is $\varphi(N)$.
It is the set of $\mathbb{Q}$-Galois conjugates of $e^{2\pi i/N}$. Equidistribution follows from

$$\frac{1}{\varphi(N)} \sum_{\substack{k=1 \\ \gcd(k,N)=1}}^{N} e^{2\pi ikl/N} = \pm\phi\left(\frac{N}{\gcd(N,l)}\right)^{-1}.$$

Logarithmic Singularities

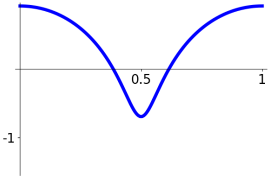
We check equdistribution with **continuous** test functions. What about a weaker hypothesis?

Theorem (M. Baker, Ih, Rumely 2008)

Let $\alpha \in \mathbb{C}$ be algebraic, then

$$\frac{1}{\varphi(N)} \sum_{\substack{k=1 \\ \gcd(k,N)=1}}^{N} \log\left|e^{2\pi i k/N} - \alpha\right| \to \int_0^1 \log\left|e^{2\pi i t} - \alpha\right| \mathrm{d}t$$

as $N = \operatorname{ord}\zeta \to \infty$.



$\alpha = -\frac{3}{2}$

Logarithmic Singularities

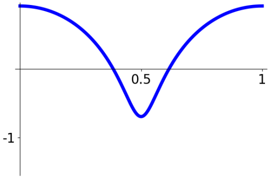
We check equdistribution with **continuous** test functions. What about a weaker hypothesis?

Theorem (M. Baker, Ih, Rumely 2008)

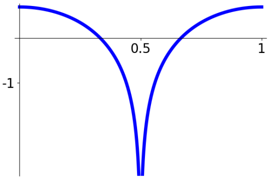
Let $\alpha \in \mathbb{C}$ be algebraic, then

$$\frac{1}{\varphi(N)} \sum_{\substack{k=1 \\ \gcd(k,N)=1}}^{N} \log\left|e^{2\pi i k/N} - \alpha\right| \to \int_0^1 \log\left|e^{2\pi i t} - \alpha\right| \mathrm{d}t$$

as $N = \operatorname{ord}\zeta \to \infty$.



$\alpha = -\frac{3}{2}$



$\alpha = -1$

Logarithmic Singularities

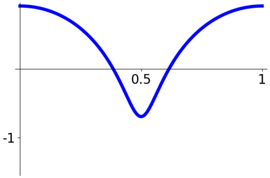
We check equdistribution with **continuous** test functions. What about a weaker hypothesis?

Theorem (M. Baker, Ih, Rumely 2008)

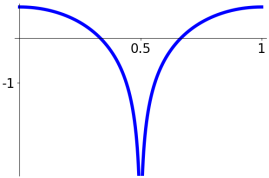
Let $\alpha \in \mathbb{C}$ *be* *algebraic, then*

$$\frac{1}{\varphi(N)} \sum_{\substack{k=1 \\ \gcd(k,N)=1}}^{N} \log\left|e^{2\pi i k/N} - \alpha\right| \to \int_0^1 \log\left|e^{2\pi i t} - \alpha\right| \mathrm{d}t$$

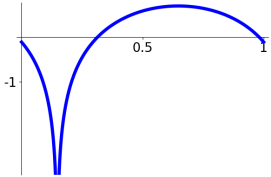
as $N = \operatorname{ord}\zeta \to \infty$.



$\alpha = -\frac{3}{2}$



$\alpha = -1$



$\alpha = \frac{3+4i}{5}$

- $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ with its Haar measure $\mathrm{d}\lambda$
- $\mu_\infty = \{\zeta \in \mathbb{C}$ a root of unity$\}$
- σ denotes an element of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/\operatorname{ord}(\zeta)\mathbb{Z})^\times$

Theorem (M. Baker, Ih, Rumely 2008)

Suppose $P \in \overline{\mathbb{Q}}[T] \smallsetminus \{0\}$, then

$$\frac{1}{[\mathbb{Q}(\zeta):\mathbb{Q}]} \sum_\sigma \log|P(\zeta^\sigma)| \to \int_0^1 \log\left|P(e^{2\pi i t})\right| \mathrm{d}t = \int_{S^1} \log|P| \mathrm{d}\lambda$$

as $\zeta \in \mu_\infty$ and $\operatorname{ord}\zeta \to \infty$.

The <u>Mahler measure</u> of $P = p_d(T-\alpha_1)\cdots(T-\alpha_d) \in \mathbb{C}[T] \smallsetminus \{0\}$ is

$$m(P) \overset{\mathrm{Def}}{=} \int_{S^1} \log|P| \mathrm{d}\lambda = \log|p_d| + \sum_{k=1}^{d} \log\max\{1, |\alpha_k|\}.$$

What about Higher Dimension?

The $\mathbb{Q}$-Galois conjugates of

$$\boldsymbol{\zeta} = (\zeta_1, \ldots, \zeta_d), \qquad \zeta_j = e^{2\pi i a_j / N} \text{ with } a_j \in \mathbb{Z}, \quad \gcd(a_1, \ldots, a_d, N) = 1.$$

are

$$\boldsymbol{\zeta}^k \text{ with } k \in \mathbb{Z} \text{ and } \gcd(k, N) = 1.$$

For $d > 1$ equdistribution does <u>not</u> follow from $N \to \infty$.

Definition

For $\boldsymbol{\zeta} = (\zeta_1, \ldots, \zeta_d) \in \mu_\infty^d$ we define

$$\delta(\boldsymbol{\zeta}) = \min\{|\boldsymbol{b}| : \boldsymbol{b} = (b_1, \ldots, b_d) \in \mathbb{Z}^d \smallsetminus \{0\} \text{ with } \boldsymbol{\zeta}^{\boldsymbol{b}} = \zeta_1^{b_1} \cdots \zeta_d^{b_d} = 1\}.$$

Equidistribution of Galois Conjugates in Dimension d

Fact

Let $f : (S^1)^d \to \mathbb{C}$ be continuous. Then

$$\frac{1}{[\mathbb{Q}(\zeta) : \mathbb{Q}]} \sum_{\sigma} f(\zeta^{\sigma}) \to \int_{(S^1)^d} f \mathrm{d}\boldsymbol{\lambda} \quad \textit{as} \quad \delta(\zeta) \to \infty.$$

Conjecture

Suppose $P \in \overline{\mathbb{Q}}[T_1, \ldots, T_d] \setminus \{0\}$, then

$$\frac{1}{[\mathbb{Q}(\zeta) : \mathbb{Q}]} \sum_{\sigma} \log |P(\zeta^{\sigma})| \to \int_{(S^1)^d} \log |P| \mathrm{d}\boldsymbol{\lambda} \overset{\text{Def}}{=} m(P) \quad \textit{as} \quad \delta(\zeta) \to \infty.$$

Why is the average on the left well-defined for large $\delta(\zeta)$? Laurent's Theorem / the Manin–Mumford Conjecture.

Evidence in Dimension > 1

Theorem (Myerson 1980, Duke 2007)

Let $p \equiv 1 \pmod 3$ be a prime and $G = \{1, a, b\} \subset \mathbb{F}_p^\times$ the subgroup of order 3. Then

$$\frac{1}{p-1}\sum_{\sigma} \log|\zeta^{\sigma} + \zeta^{a\sigma} + \zeta^{b\sigma}| = m(T_1 + T_2 + T_3) + O\left(\frac{\log p}{\sqrt{p}}\right)$$

where $\zeta \in \mu_\infty$ has order p.

Smyth computed $m(T_1 + T_2 + T_3) = L'(-1, \chi_3) = 0.323\ldots$.

Atoral Polynomials

A following definition is similar as in work of Agler–McCarthy–Stankus (2006) and Lind–Schmidt-Verbitskiy (2013).

Say $P \in \mathbb{C}[T_1, \ldots, T_d] \setminus \{0\}$. Consider the **real-algebraic** set

$$A = \left\{ (z_1, \ldots, z_d) \in (S^1)^d : P(z_1, \ldots, z_d) = 0 \right\}.$$

If $(z_1, \ldots, z_d) \in A$, complex conjugation gives 2 relations in Laurent polynomials. They may or may not be coprime.

$$\begin{cases} P(z_1, \ldots, z_d) & = 0 \\ \overline{P}(z_1^{-1}, \ldots, z_d^{-1}) & = 0 \end{cases}$$

Definition

We call P <u>atoral</u> if there exist coprime polynomials R and S such that

$$A \subset R^{-1}(\{0\}) \cap S^{-1}(\{0\}).$$

- $d = 1$: atoral amounts to $P^{-1}(\{0\}) \cap S^1 = \emptyset$.
- $d = 2$: atoral amounts to "$\{(z_1, z_2) \in S^1 \times S^1 : P(z_1, z_2) = 0\}$ finite"
- $T_1 + T_2 + \cdots + T_d$ is atoral
- **Not all polynomials are atoral.** e.g. Blaschke products

Theorem (Lind–Schmidt–Verbitskiy (2013))

Let $P \in \mathbb{Z}[T_1, \ldots, T_d] \smallsetminus \{0\}$ be atoral, then

$$\frac{1}{\# G} \sum_{\substack{\zeta \in G \\ P(\zeta) \neq 0}} \log |P(\zeta)| = m(P) + o(1)$$

as G ranges over finite subgroups of $(\mathbb{C}^{\times})^d$ with $\delta(G) \to \infty$.

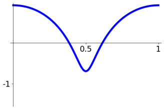
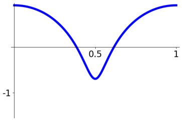
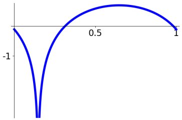
- If $P^{-1}(\{0\}) \cap (S^1)^d$ is empty, then convergences follows from classical equidistribution of tuples of roots of unity.
- Lind–Schmidt–Verbitskiy (2010): convergence if $P^{-1}(\{0\}) \cap (S^1)^d$ is finite
- Dimitrov (2017) dropped the hypothesis on P when averaging over subgroups $G = \{\boldsymbol{\zeta} \in \mu_\infty^d : \boldsymbol{\zeta}^N = 1\}$.

Theorem (Dimitrov–H.)

Suppose $P \in \overline{\mathbb{Q}}[T_1, \ldots, T_d] \setminus \{0\}$ *is* <u>*atoral*</u>, *then*

$$\frac{1}{[\mathbb{Q}(\zeta) : \mathbb{Q}]} \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} \log |P(\zeta^\sigma)| \to m(P) \quad \textit{as} \quad \delta(\zeta) \to \infty.$$

- The convergence rate is $O_P(\delta(\zeta)^{-\epsilon_P})$
- We can generalize to **essentially atoral** P
- $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ can be replaced by $\mathrm{Gal}(K(\zeta)/K)$ with K a fixed number field

$d = 1$			
$d \geq 2$	$\alpha = -\frac{3}{2}$ **atoral**	$\alpha = -1$ **essentially atoral**	$\alpha = \frac{3+4i}{5}$ **(conjectural)**

An Example

$$\boxed{\begin{array}{c} T_1 + T_2 + T_3 + T_4, \\ T_1^{-1} + T_2^{-1} + T_3^{-1} + T_4^{-1} \\ \text{are coprime in } \mathbb{C}[T_1^{\pm 1}, \ldots, T_4^{\pm 1}] \end{array}} \Rightarrow P = T_1 + T_2 + T_3 + T_4 \text{ is atoral}$$

Boyd (1981): $m(P) = \frac{4\zeta(3)}{2\pi^2} = 0.243587656467\ldots > 0.$

Let $\boldsymbol{\zeta} = (\zeta_1, \zeta_2, \zeta_3, \zeta_4) \in \mu_\infty^4$ be a quadruple with

$\zeta_1 + \zeta_2 + \zeta_3 + \zeta_4$ an **algebraic unit**.

$$\frac{1}{[\mathbb{Q}(\boldsymbol{\zeta}) : \mathbb{Q}]} \sum_\sigma \log|\zeta_1^\sigma + \cdots + \zeta_4^\sigma| \overset{\text{Theorem}}{=} \frac{4\zeta(3)}{2\pi^2} + o(1) \text{ as } \delta(\boldsymbol{\zeta}) \to \infty$$

$$\Rightarrow \delta(\boldsymbol{\zeta}) \text{ is bounded.}$$

Conclusion: There exists a constant $B \geq 1$ such that if $\zeta_1 + \zeta_2 + \zeta_3 + \zeta_4$ is an algebraic unit, then

$$\zeta_1^{a_1}\zeta_2^{a_2}\zeta_3^{a_3}\zeta_4^{a_4} = 1 \text{ for some } (a_1, \ldots, a_4) \in \mathbb{Z}^4 \smallsetminus \{0\}$$
$$\text{with } \max\{|a_1|, \ldots, |a_4|\} \leq B.$$

Step A: Univariable Case

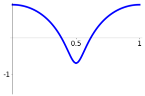
Proposition

Say $Q \in \mathbb{Z}[T] \smallsetminus \{0\}$ has no roots on S^1, $\epsilon > 0$. If $\zeta \in \mu_\infty$ has order N, then

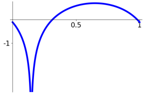
$$\frac{1}{\varphi(N)} \sum_{\sigma} \log|Q(\zeta^\sigma)| = m(Q) + O_\epsilon\left(\frac{(\deg Q)^{1+\epsilon}(1+m(Q))}{N^{1-\epsilon}}\right).$$

We treat first $Q = T - \alpha$. Truncate

$$\frac{1}{\varphi(N)} \sum_{\sigma:|\zeta^\sigma - \alpha| > 1/N^2} \log|\zeta^\sigma - \alpha| + \frac{1}{\varphi(N)} \sum_{\sigma:|\zeta^\sigma - \alpha| \le 1/N^2} \log|\zeta^\sigma - \alpha|$$



average is about $\log \max\{1, |\alpha|\}$



at most one term σ^*

Worst case:

$$\frac{1}{\varphi(N)}\sum_{\sigma}\log|\zeta^{\sigma}-\alpha| = \log\max\{1,|\alpha|\} + \frac{1}{\varphi(N)}\log|\zeta^{\sigma^*}-\alpha| + O(\cdots)$$

with $|\zeta^{\sigma^*}-\alpha|$ very small. NB: $\zeta^{\sigma^*}=e^{2\pi iq}$ with $q\in\mathbb{Q}$.
Temptation: apply Baker's linear forms in logarithms. Dependency on $[\mathbb{Q}(\alpha):\mathbb{Q}]$ not good enough to help, as observed by Duke.

Worst case:

$$\frac{1}{\varphi(N)}\sum_{\sigma}\log|\zeta^{\sigma}-\alpha| = \log\max\{1,|\alpha|\} + \frac{1}{\varphi(N)}\log|\zeta^{\sigma^*}-\alpha| + O(\cdots)$$

with $|\zeta^{\sigma^*}-\alpha|$ very small. NB: $\zeta^{\sigma^*} = e^{2\pi i q}$ with $q \in \mathbb{Q}$.
Temptation: apply Baker's linear forms in logarithms. Dependency on $[\mathbb{Q}(\alpha):\mathbb{Q}]$ not good enough to help, as observed by Duke.

$$|\zeta^{\sigma}-\alpha| \geq |1-|\alpha|| \gg |\alpha-\overline{\alpha}^{-1}| \text{ for } |\alpha| \text{ close to } 1.$$

α and $\overline{\alpha}^{-1}$ are roots of $Q(T)Q(T^{-1})T^d \in \mathbb{Z}[T]$.

Theorem (Mahler 1964)

If $z, w \in \mathbb{C}$ are distinct roots of $F \in \mathbb{Z}[T] \smallsetminus \{0\}$ and $D = \deg F$, then

$$\log|z-w| \geq -\frac{1}{2}(D+2)\log D - Dm(F).$$

$$\Rightarrow \frac{1}{\varphi(N)}\log|\zeta^{\sigma}-\alpha| \gg -\deg(P)\frac{\log\deg(P)+m(P)}{\varphi(N)}.$$

Mignotte (1995): strengthening of Mahler to several pairs of roots

Step B: Reducing to the Univariate Case

Now $P \in \mathbb{Z}[T_1, \dots, T_d] \smallsetminus \{0\}$ is atoral.
Let $\boldsymbol{\zeta} = (\zeta_1, \dots, \zeta_d)$ have order N. There is $\boldsymbol{a} = (a_1, \dots, a_d) \in \mathbb{Z}^d$ with

$$\begin{aligned}
&\boldsymbol{\zeta} = (\zeta^{a_1}, \dots, \zeta^{a_d}) = \zeta^{\boldsymbol{a}} && \text{(for some } \zeta \text{ of order } N) \\
\Rightarrow &\boldsymbol{\zeta}^{\tau} = \zeta^{\tau \boldsymbol{a} + N\boldsymbol{b}} && \text{(for all } \boldsymbol{b} \in \mathbb{Z}^d, \tau \in \mathbb{Z} : \gcd(\tau, N) = 1) \\
\Rightarrow &|P(\boldsymbol{\zeta}^{\tau})| = |Q(\zeta)| && \text{(with } Q(T) = T^{?} P(T^{\tau \boldsymbol{a} + N\boldsymbol{b}}) \in \mathbb{Z}[T]) \\
\Rightarrow &\sum_{\sigma} \log |P(\boldsymbol{\zeta}^{\sigma})| = \sum_{\sigma} \log |Q(\zeta^{\sigma})| && \text{(by the univariate case)}
\end{aligned}$$

Use Erdös–Turán–Koksma to find τ and $\boldsymbol{b}$ with

$$\deg Q = O(|\tau \boldsymbol{a} + N\boldsymbol{b}|) = O\left(\frac{N}{\delta(\boldsymbol{\zeta})^{\kappa_d}}\right).$$

If $\delta(\boldsymbol{\zeta})$ grows at least like a small power of N, the proposition gives

$$\frac{1}{\varphi(N)} \sum_{\sigma} \log |P(\boldsymbol{\zeta}^{\sigma})| = m(Q) + O_{\epsilon}\left(\frac{(\deg P)^{1+\epsilon}(1 + m(Q))}{N^{1-\epsilon}}\right) = m(Q) + o(1).$$

$$\delta(\zeta) \text{ grows polynomially in } N \Rightarrow \frac{1}{\varphi(N)} \sum_{\sigma} \log |P(\zeta^{\sigma})| = m(Q) + o(1)$$

Issues:

- If $\delta(\zeta)$ grows slowly: monomial change of coordinates and induction.
- Need to relate $m(Q)$ to $m(P)$. We require a quantitative version of

Theorem (Lawton 1983)

Let $d \geq 2, P \in \mathbb{C}[T_1, \dots, T_d] \setminus \{0\}$ and $\boldsymbol{a} = (a_1, \dots, a_d) \in \mathbb{Z}^d$, then

$$m(P(T^{a_1}, \dots, T^{a_d})) = m(P) + o(1)$$

as $\min\{|\boldsymbol{b}| : \boldsymbol{b} \in \mathbb{Z}^d \setminus \{0\}$ and $\langle \boldsymbol{a}, \boldsymbol{b} \rangle = 0\} \to \infty$.

This kind of statement helps in showing $m(Q) = m(P) + o(1)$.

- **Warning:** The proposition only applies if $Q(z) \neq 0$ for all $z \in S^1$.

Warning: The proposition only applies if $Q(z) \neq 0$ for all $z \in S^1$. Up-to a power of T:

$$Q(T) = P(T^{\tau \boldsymbol{a} + N\boldsymbol{b}})$$

If $z \in S^1$, then

$$Q(z) = 0 \Rightarrow P(z^{\tau \boldsymbol{a} + N\boldsymbol{b}}) = 0 \Rightarrow z^{\tau \boldsymbol{a} + N\boldsymbol{b}} \in P^{-1}(\{0\}) \cap (S^1)^d$$

Recall that P is atoral. There are coprime polynomials R and S in d variables, fixed in terms of P, with

$$R(z^{\tau \boldsymbol{a} + N\boldsymbol{b}}) = S(z^{\tau \boldsymbol{a} + N\boldsymbol{b}}) = 0.$$

The point $z^{\tau \boldsymbol{a} + N\boldsymbol{b}}$ lies in a 1-dimensional algebraic subgroup of $(\mathbb{C}^{\times})^d$. It is an unlikely intersection.

Theorem (Bombieri–Masser–Zannier 2007)

In the setup above, there exists $B \geq 1$, depending only on (R, S), with

$$\langle \tau \boldsymbol{a} + N\boldsymbol{b}, \boldsymbol{c} \rangle = 0 \quad \textit{for some} \quad \boldsymbol{c} \in \mathbb{Z}^d \smallsetminus \{0\} \textit{ with } |\boldsymbol{c}| \leq B.$$

By the choice of τ and $\boldsymbol{b}$ we have

$$\begin{aligned}\boldsymbol{\zeta} = \zeta^{\tau \boldsymbol{a} + N\boldsymbol{b}} &\Rightarrow \boldsymbol{\zeta}^{\boldsymbol{c}} = \zeta^{\langle \tau \boldsymbol{a} + N\boldsymbol{b}, \boldsymbol{c}\rangle} = 1 \\ &\Rightarrow \delta(\boldsymbol{\zeta}) \leq |\boldsymbol{c}| \leq B.\end{aligned}$$

Thanks for your attention!