The real τ-conjecture & lower bounds for the permanent

Bruno Grenet

LIP — ÉNS de Lyon

Rencontres CoA — 22 novembre 2012

Arithmetic Circuits

$$f(x,y,z) = x^4 + 4\,x^3y + 6\,x^2y^2 + 4\,xy^3 + x^2z + 2\,xyz + y^2z + x^2 + y^4 + 2\,xy + y^2 + z^2 + 2\,z + 1$$

Arithmetic Circuits

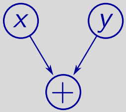
$$f(x, y, z) = (x + y)^4 + (z + 1)^2 + (x + y)^2(z + 1)$$

Arithmetic Circuits

$$f(x, y, z) = (x + y)^4 + (z + 1)^2 + (x + y)^2(z + 1)$$

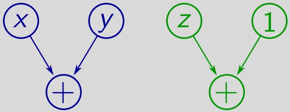
Arithmetic Circuits

$$f(x,y,z) = (x+y)^4 + (z+1)^2 + (x+y)^2(z+1)$$



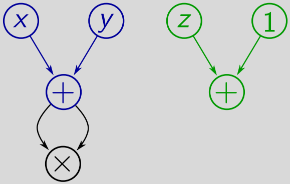
Arithmetic Circuits

$$f(x, y, z) = (x + y)^4 + (z + 1)^2 + (x + y)^2(z + 1)$$



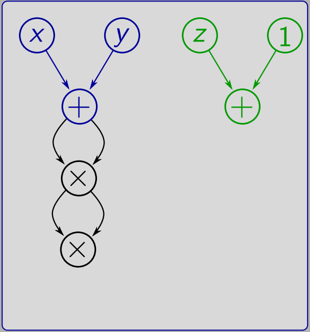
Arithmetic Circuits

$$f(x,y,z) = (x+y)^4 + (z+1)^2 + (x+y)^2(z+1)$$



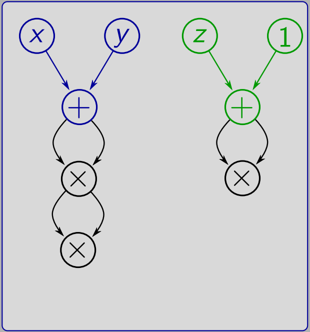
Arithmetic Circuits

$$f(x,y,z) = (x+y)^4 + (z+1)^2 + (x+y)^2(z+1)$$



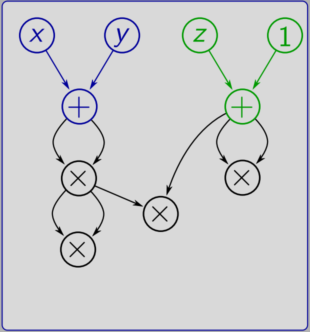
Arithmetic Circuits

$$f(x,y,z) = (x+y)^4 + (z+1)^2 + (x+y)^2(z+1)$$



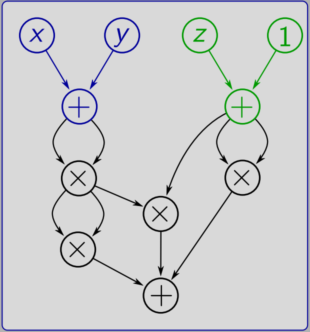
Arithmetic Circuits

$$f(x,y,z) = (x+y)^4 + (z+1)^2 + (x+y)^2(z+1)$$



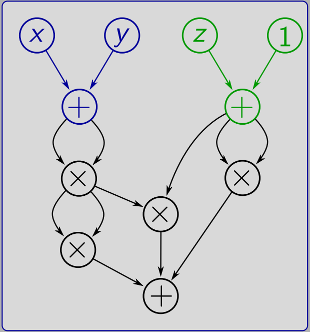
Arithmetic Circuits

$$f(x,y,z) = (x+y)^4 + (z+1)^2 + (x+y)^2(z+1)$$



Arithmetic Circuits

$$f(x,y,z) = (x+y)^4 + (z+1)^2 + (x+y)^2(z+1)$$



Complexity of a polynomial

$\tau(f) =$ size of its smallest circuit representation

The τ-conjecture

Conjecture (Shub & Smale, 1995)

The number of integer roots of any $f \in \mathbb{Z}[X]$ is $\leq \text{poly}(\tau(f))$.

The τ-conjecture

Conjecture (Shub & Smale, 1995)

The number of integer roots of any $f \in \mathbb{Z}[X]$ is $\leq \text{poly}(\tau(f))$.

Theorem (Bürgisser, 2007)

τ-conjecture

$$\implies \textit{super-polynomial lower bound for the permanent}$$

The τ-conjecture

Conjecture (Shub & Smale, 1995)

The number of integer roots of any $f \in \mathbb{Z}[X]$ is $\leq \mathrm{poly}(\tau(f))$.

Theorem (Bürgisser, 2007)

τ-conjecture

$\implies$ *super-polynomial lower bound for the permanent*

$$\mathrm{PER}_n(x_{11}, \ldots, x_{nn}) = \mathrm{per}\begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \cdots & x_{nn} \end{pmatrix} = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^{n} x_{i\sigma(i)}$$

The τ-conjecture

Conjecture (Shub & Smale, 1995)

The number of integer roots of any $f \in \mathbb{Z}[X]$ is $\leq \mathrm{poly}(\tau(f))$.

Theorem (Bürgisser, 2007)

τ-conjecture

$\implies$ *super-polynomial lower bound for the permanent*

$\implies$ $\tau(\mathrm{PER}_n)$ *is not polynomially bounded in n*

$$\mathrm{PER}_n(x_{11}, \ldots, x_{nn}) = \mathrm{per}\begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \cdots & x_{nn} \end{pmatrix} = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^{n} x_{i\sigma(i)}$$

The τ-conjecture

Conjecture (Shub & Smale, 1995)

The number of integer roots of any $f \in \mathbb{Z}[X]$ is $\leq \mathrm{poly}(\tau(f))$.

Theorem (Bürgisser, 2007)

τ-conjecture

$\implies$ *super-polynomial lower bound for the permanent*

$\implies$ $\tau(\textsc{Per}_n)$ *is not polynomially bounded in n*

$\implies$ $\mathsf{VP}^0 \neq \mathsf{VNP}^0$

$$\textsc{Per}_n(x_{11}, \dots, x_{nn}) = \mathrm{per}\begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \cdots & x_{nn} \end{pmatrix} = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^{n} x_{i\sigma(i)}$$

The τ-conjecture is hard

Theorem (Shub & Smale, 1995)

τ-conjecture $\implies \mathsf{P}_{\mathbb{C}} \neq \mathsf{NP}_{\mathbb{C}}$

The τ-conjecture is hard

Theorem (Shub & Smale, 1995)

τ-conjecture $\implies \mathsf{P}_{\mathbb{C}} \neq \mathsf{NP}_{\mathbb{C}}$

Theorem (Cheng, 2003)

Extended τ-conjecture $\implies$ *Merel torsion theorem, ...*

The τ-conjecture is hard

Theorem (Shub & Smale, 1995)

τ-conjecture $\implies \mathsf{P}_{\mathbb{C}} \neq \mathsf{NP}_{\mathbb{C}}$

Theorem (Cheng, 2003)

Extended τ-conjecture $\implies$ Merel torsion theorem, ...

False for real roots (Shub-Smale 95, Borodin-Cook 76)

$T_n = n$-th Chebyshev polynomial

- $\tau(T_n) = \mathcal{O}(\log n)$
- n real roots

Let's make it real!

Real τ-conjecture (Koiran, 2011)

Let $f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}$ where the f_{ij}'s are t-sparse polynomials.

Then f has $\leq \text{poly}(k, m, t)$ real roots.

Let's make it real!

Real τ-conjecture (Koiran, 2011)

Let $f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}$ where the f_{ij}'s are t-sparse polynomials.

Then f has $\leq \text{poly}(k, m, t)$ real roots.

Theorem (Koiran, 2011)

Real τ-conjecture

$\implies$ *Super-polynomial lower bound for the permanent*

Let's make it real!

Real τ-conjecture (Koiran, 2011)

Let $f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}$ where the f_{ij}'s are t-sparse polynomials.

Then f has $\leq$ poly(k, m, t) real roots.

Theorem (Koiran, 2011)

Real τ-conjecture

$\implies$ *Super-polynomial lower bound for the permanent*

- Enough to bound the number of integer roots

Let's make it real!

Real τ-conjecture (Koiran, 2011)

Let $f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}$ where the f_{ij}'s are t–sparse polynomials.

Then f has $\leq \text{poly}(k, m, t)$ real roots.

Theorem (Koiran, 2011)

Real τ-conjecture
$\implies$ *Super-polynomial lower bound for the permanent*

- Enough to bound the number of integer roots
  - $\rightsquigarrow$ Adelic τ-conjecture [Phillipson & Rojas, 2012]

Let's make it real!

Real τ-conjecture (Koiran, 2011)

Let $f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}$ where the f_{ij}'s are t–sparse polynomials.

Then f has $\leq \text{poly}(k, m, t)$ real roots.

Theorem (Koiran, 2011)

Real τ-conjecture

$\implies$ *Super-polynomial lower bound for the permanent*

- Enough to bound the number of integer roots
  - $\rightsquigarrow$ Adelic τ-conjecture [Phillipson & Rojas, 2012]
- Case $k = 1$: Follows from Descartes' rule.

Let's make it real!

Real τ-conjecture (Koiran, 2011)

Let $f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}$ where the f_{ij}'s are t-sparse polynomials.

Then f has $\leq \text{poly}(k, m, t)$ real roots.

Theorem (Koiran, 2011)

Real τ-conjecture

$\implies$ *Super-polynomial lower bound for the permanent*

- Enough to bound the number of integer roots
  - $\rightsquigarrow$ Adelic τ-conjecture [Phillipson & Rojas, 2012]
- Case $k = 1$: Follows from Descartes' rule.
- Case $k = 2$: Open.

Let's make it real!

Real τ-conjecture (Koiran, 2011)

Let $f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}$ where the f_{ij}'s are t-sparse polynomials.

Then f has $\leq \text{poly}(k, m, t)$ real roots.

Theorem (Koiran, 2011)

Real τ-conjecture

$\Longrightarrow$ *Super-polynomial lower bound for the permanent*

- Enough to bound the number of integer roots
  - $\rightsquigarrow$ Adelic τ-conjecture [Phillipson & Rojas, 2012]
- Case $k = 1$: Follows from Descartes' rule.
- Case $k = 2$: Open.
- Toy question: Number of real roots of $fg + 1$?

Descartes' rule without signs

Theorem

If $f \in \mathbb{R}[X]$ has t monomials, then it has $\leq (t-1)$ positive real roots.

Descartes' rule without signs

Theorem

If $f \in \mathbb{R}[X]$ has t monomials, then it has $\leq (t-1)$ positive real roots.

Proof. Induction on t.

- $t = 1$: No positive real root

Descartes' rule without signs

Theorem

If $f \in \mathbb{R}[X]$ has t monomials, then it has $\leq (t-1)$ positive real roots.

Proof. Induction on t.

- $t = 1$: No positive real root
- $t > 1$: Let $c_\alpha X^\alpha$ = lowest degree monomial.

Descartes' rule without signs

Theorem

If $f \in \mathbb{R}[X]$ has t monomials, then it has $\leq (t-1)$ positive real roots.

Proof. Induction on t.

- $t = 1$: No positive real root
- $t > 1$: Let $c_\alpha X^\alpha$ = lowest degree monomial.
  - $g = f/X^\alpha$: same positive roots, nonzero constant coefficient

Descartes' rule without signs

Theorem

If $f \in \mathbb{R}[X]$ has t monomials, then it has $\leq (t-1)$ positive real roots.

Proof. Induction on t.

- $t = 1$: No positive real root
- $t > 1$: Let $c_\alpha X^\alpha$ = lowest degree monomial.
    - $g = f/X^\alpha$: same positive roots, nonzero constant coefficient
    - g' has $(t-1)$ monomials $\implies \leq (t-2)$ positive roots

Descartes' rule without signs

Theorem

If $f \in \mathbb{R}[X]$ has t monomials, then it has $\leq (t-1)$ positive real roots.

Proof. Induction on t.

- $t = 1$: No positive real root
- $t > 1$: Let $c_\alpha X^\alpha =$ lowest degree monomial.
  - $g = f/X^\alpha$: same positive roots, nonzero constant coefficient
  - g' has $(t-1)$ monomials $\Longrightarrow \leq (t-2)$ positive roots
  - There is a root of g' between two consecutive roots of g (Rolle's theorem)

Descartes' rule without signs

Theorem

If $f \in \mathbb{R}[X]$ has t monomials, then it has $\leq (t-1)$ positive real roots.

Proof. Induction on t.

- $t = 1$: No positive real root
- $t > 1$: Let $c_\alpha X^\alpha =$ lowest degree monomial.
  - $g = f/X^\alpha$: same positive roots, nonzero constant coefficient
  - g' has $(t-1)$ monomials $\implies \leq (t-2)$ positive roots
  - There is a root of g' between two consecutive roots of g (Rolle's theorem)

$f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}$: $\leq 2kt^m - 1$ real roots

Real τ-conjecture $\implies$ Permanent is hard

$$\mathrm{SPS}(k,m,t) = \left\{ f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij} : f_{ij}\text{'s are } t\text{-sparse} \right\}$$

Real τ-conjecture $\implies$ Permanent is hard

$$\mathrm{SPS}(k, m, t) = \left\{ f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij} : f_{ij}\text{'s are } t\text{–sparse} \right\}$$

Incorrect proof. Assume the permanent is easy.

Real τ-conjecture $\implies$ Permanent is hard

$$\mathsf{SPS}(k,m,t) = \left\{ f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij} : f_{ij}\text{'s are } t\text{-sparse} \right\}$$

Incorrect proof. Assume the permanent is easy.

- $\prod_{i=1}^{2^n}(X-i)$ has circuits of size poly(n) [Bürgisser, 2007-09]

Real τ-conjecture $\implies$ Permanent is hard

$$\mathrm{SPS}(k, m, t) = \left\{ f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij} : f_{ij}\text{'s are } t\text{-sparse} \right\}$$

Incorrect proof. Assume the permanent is easy.

- $\prod_{i=1}^{2^n}(X - i)$ has circuits of size poly(n) [Bürgisser, 2007-09]
- Reduction to depth 4 $\rightsquigarrow$ SPS polynomial of size $2^{o(n)}$ [Agrawal–Vinay, 2008]

Real τ-conjecture $\implies$ Permanent is hard

$$\mathrm{SPS}(k,m,t) = \left\{ f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij} : f_{ij}\text{'s are } t\text{-sparse} \right\}$$

Incorrect proof. Assume the permanent is easy.

- $\prod_{i=1}^{2^n}(X-i)$ has circuits of size poly(n) [Bürgisser, 2007-09]
- Reduction to depth 4 $\rightsquigarrow$ SPS polynomial of size $2^{o(n)}$ [Agrawal-Vinay, 2008]
- Contradiction with real τ-conjecture

Real τ-conjecture $\Longrightarrow$ Permanent is hard

$$\mathrm{SPS}(k, m, t) = \left\{ f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij} : f_{ij}\text{'s are } t\text{-sparse} \right\}$$

Incorrect proof. Assume the permanent is easy.

- $\prod_{i=1}^{2^n}(X - i)$ has circuits of size poly(n) [Bürgisser, 2007-09]
- Reduction to depth 4 $\rightsquigarrow$ SPS polynomial of size $2^{o(n)}$ [Agrawal–Vinay, 2008]
- Contradiction with real τ-conjecture

Real τ-conjecture $\implies$ Permanent is hard

$$\mathrm{SPS}(k,m,t) = \left\{ f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij} : f_{ij}\text{'s are } t\text{-sparse} \right\}$$

correct proof. Assume the permanent is easy.

- $\prod_{i=1}^{2^n}(X-i)$ has circuits of size poly(n) [Bürgisser, 2007-09]
- Reduction to depth 4 $\rightsquigarrow$ SPS polynomial of size $2^{o(n)}$ [Koiran, 2011]
- Contradiction with real τ-conjecture

$+$ other details…

Reduction to depth 4

Theorem (Koiran, 2011)

Circuit of size t and degree d

$\rightsquigarrow$ *Depth-4 circuit of size* $t^{\mathcal{O}(\sqrt{d}\log d)}$

Reduction to depth 4

Theorem (Koiran, 2011)

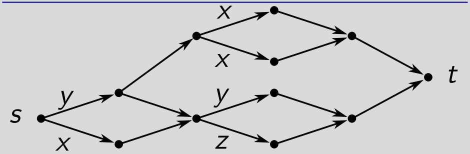
Circuit of size t and degree d

$\rightsquigarrow$ *Depth-4 circuit of size* $t^{\mathcal{O}(\sqrt{d}\log d)}$

Proof idea.

- Construct an equivalent Arithmetic Branching Program
  $\rightsquigarrow$ size $t^{\log 2d} + 1$, depth $\delta = 3d - 1$ [Malod-Portier, 2008]

$(x+y)(y+z) + y(x+x)$



Reduction to depth 4

Theorem (Koiran, 2011)

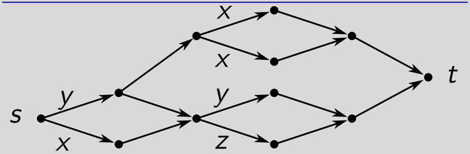
Circuit of size t and degree d

$\rightsquigarrow$ *Depth-4 circuit of size* $t^{\mathcal{O}(\sqrt{d}\log d)}$

Proof idea.

- Construct an equivalent Arithmetic Branching Program
  $\rightsquigarrow$ size $t^{\log 2d} + 1$, depth $\delta = 3d - 1$ [Malod-Portier, 2008]
- ABP $\equiv$ Matrix powering

$(x + y)(y + z) + y(x + x)$



Reduction to depth 4

Theorem (Koiran, 2011)

Circuit of size t and degree d

$\rightsquigarrow$ *Depth-4 circuit of size* $t^{\mathcal{O}(\sqrt{d}\log d)}$

Proof idea.

- Construct an equivalent Arithmetic Branching Program
  $\rightsquigarrow$ size $t^{\log 2d} + 1$, depth $\delta = 3d - 1$ [Malod-Portier, 2008]
- ABP $\equiv$ Matrix powering
- $M^{\delta} = (M^{\sqrt{\delta}})^{\sqrt{\delta}}$

Reduction to depth 4

Theorem (Koiran, 2011)

Circuit of size t and degree d

$\rightsquigarrow$ *Depth-4 circuit of size* $t^{\mathcal{O}(\sqrt{d}\log d)}$

Proof idea.

- Construct an equivalent Arithmetic Branching Program
  $\rightsquigarrow$ size $t^{\log 2d} + 1$, depth $\delta = 3d - 1$ [Malod-Portier, 2008]
- ABP $\equiv$ Matrix powering
- $M^\delta = (M^{\sqrt{\delta}})^{\sqrt{\delta}}$

Consequence. Replace $\mathrm{poly}(k, m, t)$ by $2^{\mathrm{polylog}(k,m,t)}$.

The limited power of powering

$$\mathrm{SPS}(k, m, t, A) = \left\{ \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}} : f_j\text{'s are } t\text{-sparse}, \ \alpha_{ij} \leq A \right\}$$

The limited power of powering

$$\mathrm{SPS}(k,m,t,A) = \left\{ \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}} : f_j\text{'s are } t\text{-sparse, } \alpha_{ij} \leq A \right\}$$

Theorem (G.-Koiran-Portier-Strozecki, 2011)

If $f \in \mathrm{SPS}(k,m,t,A)$, its number of real roots is at most

$$C \cdot \left[e \cdot \left(1 + \frac{t^m}{2^{k-1}-1} \right) \right]^{2^{k-1}-1} \quad \textit{for some } C.$$

The limited power of powering

$$\mathrm{SPS}(k, m, t, A) = \left\{ \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}} : f_j\text{'s are } t\text{-sparse}, \alpha_{ij} \leq A \right\}$$

Theorem (G.–Koiran–Portier–Strozecki, 2011)

If $f \in \mathrm{SPS}(k, m, t, A)$, its number of real roots is at most

$$C \cdot \left[e \cdot \left(1 + \frac{t^m}{2^{k-1} - 1} \right) \right]^{2^{k-1}-1} \quad \textit{for some } C.$$

- Independent of A.

The limited power of powering

$$\mathrm{SPS}(k,m,t,A) = \left\{ \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}} : f_j\text{'s are } t\text{-sparse}, \alpha_{ij} \le A \right\}$$

Theorem (G.–Koiran–Portier–Strozecki, 2011)

If $f \in \mathrm{SPS}(k,m,t,A)$, its number of real roots is at most

$$C \cdot \left[e \cdot \left(1 + \frac{t^m}{2^{k-1}-1} \right) \right]^{2^{k-1}-1} \quad \textit{for some } C.$$

- Independent of A.
- If k and m are fixed, this is polynomial in t.

Case $k = 2$

Proposition

The polynomial

$$f = \prod_{j=1}^{m} f_j^{\alpha_j} + \prod_{j=1}^{m} f_j^{\beta_j}$$

has at most $2mt^m + 4m(t-1)$ *real roots.*

Case $k = 2$

Proposition

The polynomial

$$f = \prod_{j=1}^{m} f_j^{\alpha_j} + \prod_{j=1}^{m} f_j^{\beta_j}$$

has at most $2mt^m + 4m(t-1)$ *real roots.*

Proof sketch. Let $F = f / \prod_j f_j^{\alpha_j} = 1 + \prod_j f_j^{\beta_j - \alpha_j}$.

Case $k = 2$

Proposition

The polynomial

$$f = \prod_{j=1}^{m} f_j^{\alpha_j} + \prod_{j=1}^{m} f_j^{\beta_j}$$

has at most $2mt^m + 4m(t-1)$ *real roots.*

Proof sketch. Let $F = f / \prod_j f_j^{\alpha_j} = 1 + \prod_j f_j^{\beta_j - \alpha_j}$. Then

$$F' = \underbrace{\prod_{j=1}^{m} f_j^{\beta_j - \alpha_j - 1}}_{\leq 2m(t-1) \text{ roots and poles}} \times \underbrace{\sum_{j=1}^{m} (\beta_j - \alpha_j) f_j' \prod_{l \neq j} f_l}_{\leq 2mt^m - 1 \text{ roots}} .$$

Conclusion

- Real τ-conjecture $\implies$ $\mathsf{VP}^0 \neq \mathsf{VNP}^0$

Conclusion

- Real τ-conjecture $\implies \mathsf{VP}^0 \neq \mathsf{VNP}^0$
- Use your favorite real analysis tools!

Conclusion

- Real τ-conjecture $\implies \mathsf{VP}^0 \neq \mathsf{VNP}^0$
- Use your favorite real analysis tools!
- Related:

Conclusion

- Real τ-conjecture $\implies \mathsf{VP}^0 \neq \mathsf{VNP}^0$
- Use your favorite real analysis tools!
- Related:
  - Adelic formulation: number of p-adic roots [Phillipson-Rojas]

Conclusion

- Real τ-conjecture $\implies \mathsf{VP}^0 \neq \mathsf{VNP}^0$
- Use your favorite real analysis tools!
- Related:
  - Adelic formulation: number of p-adic roots [Phillipson-Rojas]
  - Random f_{ij}: Work in progress [Briquel-Bürgisser]

Conclusion

- Real τ-conjecture $\implies \mathsf{VP}^0 \neq \mathsf{VNP}^0$
- Use your favorite real analysis tools!
- Related:
  - Adelic formulation: number of p-adic roots [Phillipson-Rojas]
  - Random f_{ij}: Work in progress [Briquel-Bürgisser]
  - Consequences on repartition of complex roots [Hrubes]

Conclusion

- Real τ-conjecture $\implies \mathsf{VP}^0 \neq \mathsf{VNP}^0$
- Use your favorite real analysis tools!
- Related:
  - Adelic formulation: number of p-adic roots [Phillipson-Rojas]
  - Random f_{ij}: Work in progress [Briquel-Bürgisser]
  - Consequences on repartition of complex roots [Hrubes]

Embarrassing Open Problem

Let f, g be t-sparse polynomials.

$\rightsquigarrow$ What is the maximum number real of roots of $fg + 1$?

Conclusion

- Real τ-conjecture $\implies \mathsf{VP}^0 \neq \mathsf{VNP}^0$
- Use your favorite real analysis tools!
- Related:
  - Adelic formulation: number of p-adic roots [Phillipson-Rojas]
  - Random f_{ij}: Work in progress [Briquel-Bürgisser]
  - Consequences on repartition of complex roots [Hrubes]

Embarrassing Open Problem

Let f, g be t-sparse polynomials.

$\rightsquigarrow$ What is the maximum number real of roots of $fg + 1$?

Thank you for your attention!