Optimal topological generators of U(1) and Short paths in SU(2)

Zachary Stier

Princeton e-University

May 11, 2020

Topological generators

Say $S \subset G$ is a set of topological generators for the infinite group G.

Question: How good is a given set of topological generators?

Question: What does it mean for a set of topological generators to be "good"?

We'll work in $G \leqslant \mathrm{U}(n)$, a compact metric space.

Topological generators

Assign to each generator $s \in S$ a weight $w(s)$. The weight of a word is just the sum of its elements' weights.

Question: For each n, what is the radius of the largest ball in G whose translates by all words of weight $\leqslant n$ fail to cover G?

i.e., $$\sup \left\{ r \mid \exists x : \bigcup_{g \in S(n)} B_r(x) g \neq G \right\}$$

Loosely speaking, the "goodness" of S correlates with the asymptotics of that radius as $n \to \infty$ (smaller is better).

Topological generators

There are two intertwined questions that arise:

- Can we find particularly good topological generators?
- Given good topological generators, how well can we navigate?

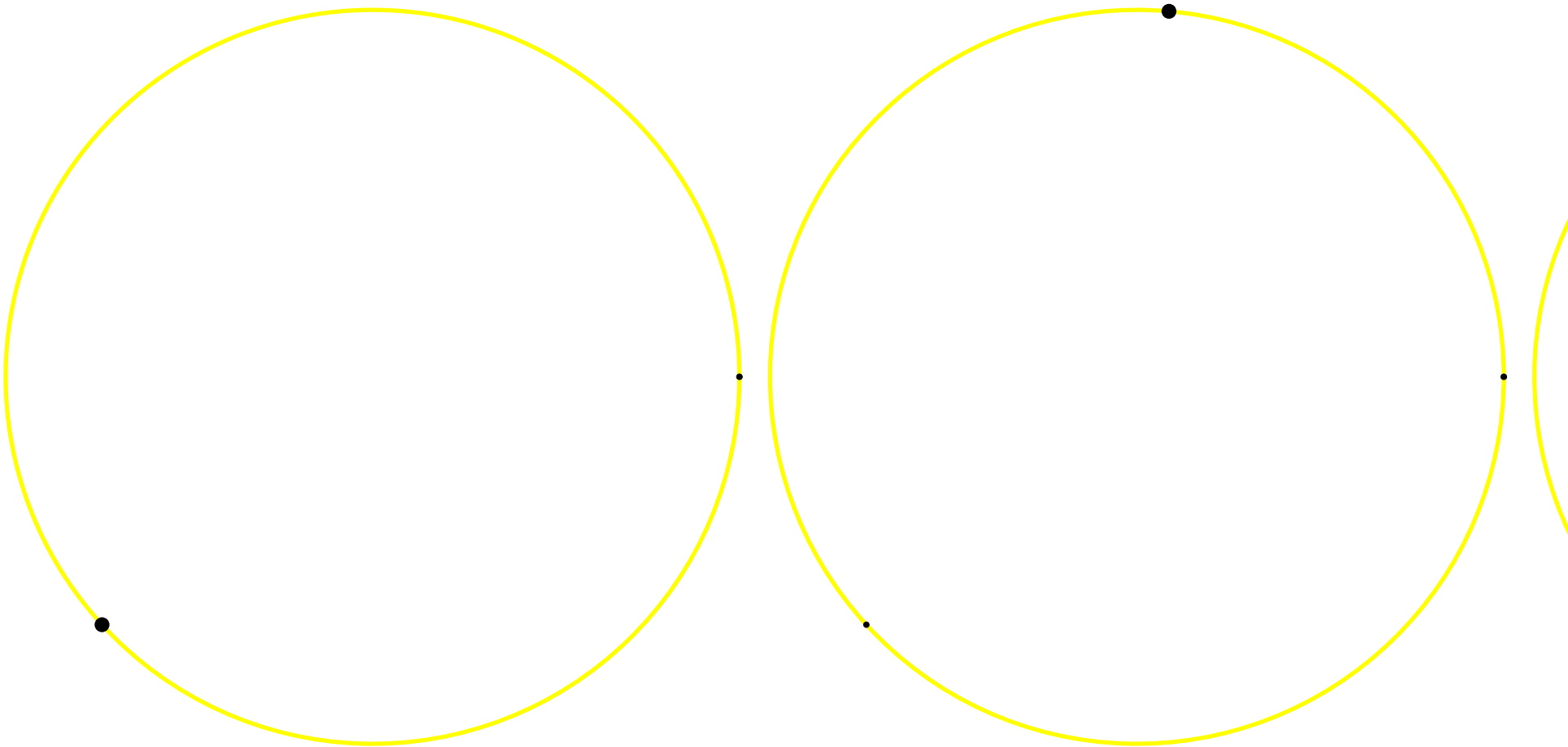
Outline

1. Optimal topological generators of U(1)
   - "Good" U(1)-generators
   - The "best" U(1)-generators

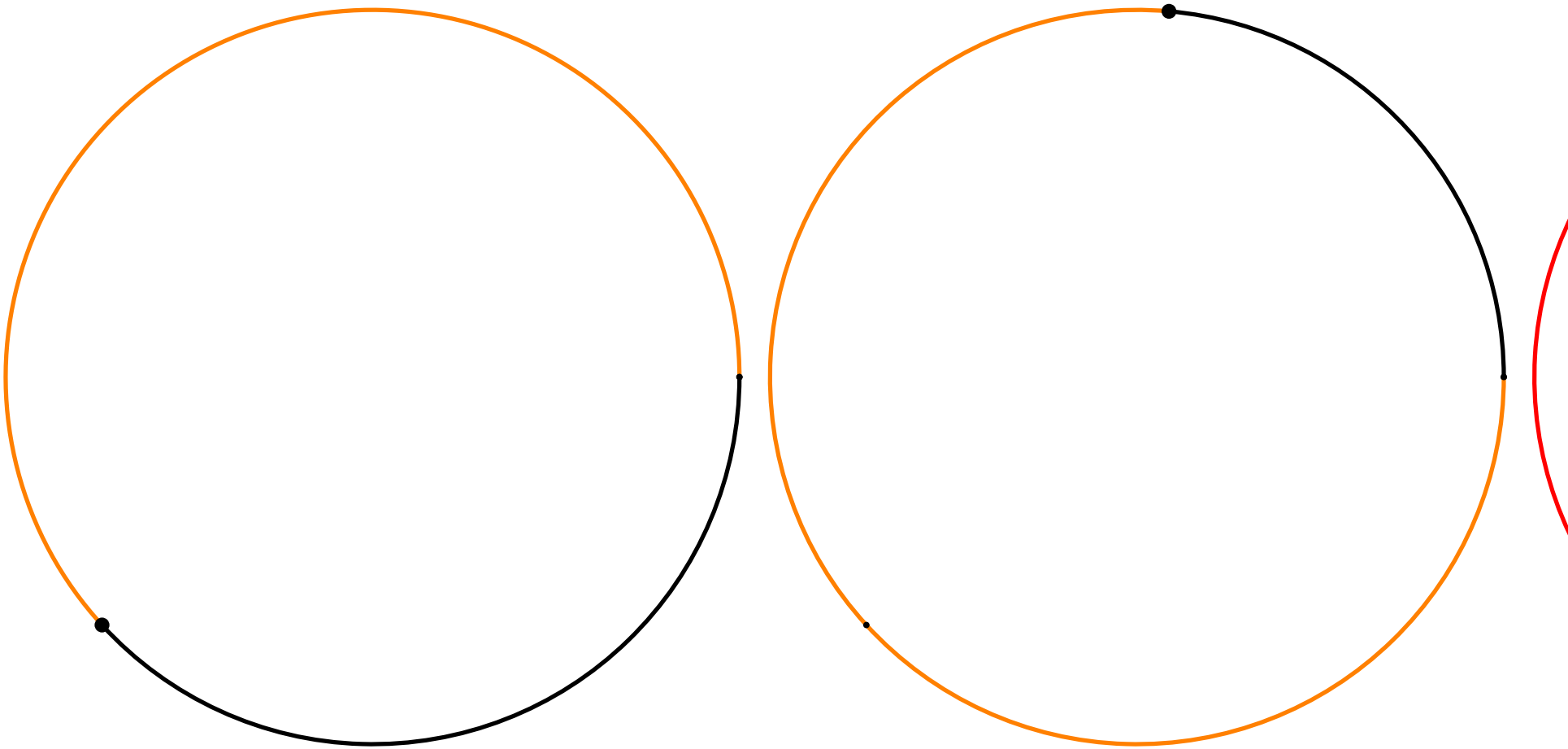
2. Short paths in SU(2)
   - Motivation
   - Context
   - Path-finding for one qubit

Outline

Topological generators of U(1)



Topological generators of U(1)



Topological generators of U(1)

Say θ is an irrational angle. Here are some facts about this setting:

- θ generates a dense subgroup of S^1.
- There are at most three distinct distances marked off by any number of multiples of θ.
- θ cannot generate U(1) "too well."

The discrepancy function

Mark off the first m multiples of θ on S^1. Let $d_\theta(m)$ equal the length of the longest resulting arc.

Theorem (Graham–van Lint, 1966)

For any θ,

$$\limsup_{m\to\infty} m d_\theta(m) \geqslant 1 + \frac{2}{\sqrt{5}} \approx 1.89$$

with equality if and only if $\theta \asymp \varphi$.

Continued fractions notation

Every irrational number θ has an **(infinite) continued fraction**

$$\theta = [a_0, a_1, \dots] = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \cdots}}$$

with **convergents** denoted

$$[a_0, a_1, \dots, a_n] = \frac{h_n}{k_n} = \frac{a_n h_{n-1} + h_{n-2}}{a_n k_{n-1} + k_{n-2}}.$$

Define the useful values

$$x_n = x_n(\theta) = [a_{n+1}, \dots, a_1], \qquad \theta_n = [a_n, a_{n+1}, \dots],$$

the convention

$$[a_0, a_1, \dots, a_{n-1}, \dot{1}] = [a_0, a_1, \dots, a_{n-1}, 1, 1, 1, \dots],$$

and say $\mu \asymp \sigma$ when there exist $m, n \in \mathbb{N}$ for which $\mu_m = \sigma_n$. Fix the constants $\varphi = [\dot{1}] = \frac{1+\sqrt{5}}{2}$ and $\rho = 1 + \frac{2}{\sqrt{5}}$.

Continued fractions facts

Lemma (corollary from Hardy–Wright, Slater/Sós)

If $\alpha < a_{n+2}$ *and* $k_n + (\alpha+1)k_{n+1} - 1 \leqslant m \leqslant k_n + (\alpha+2)k_{n+1} - 2$, *then*

$$d_\theta(m) = \frac{\theta_{n+2} - \alpha}{k_n + k_{n+1}\theta_{n+2}}.$$

Proposition (Mozzochi, 2019)

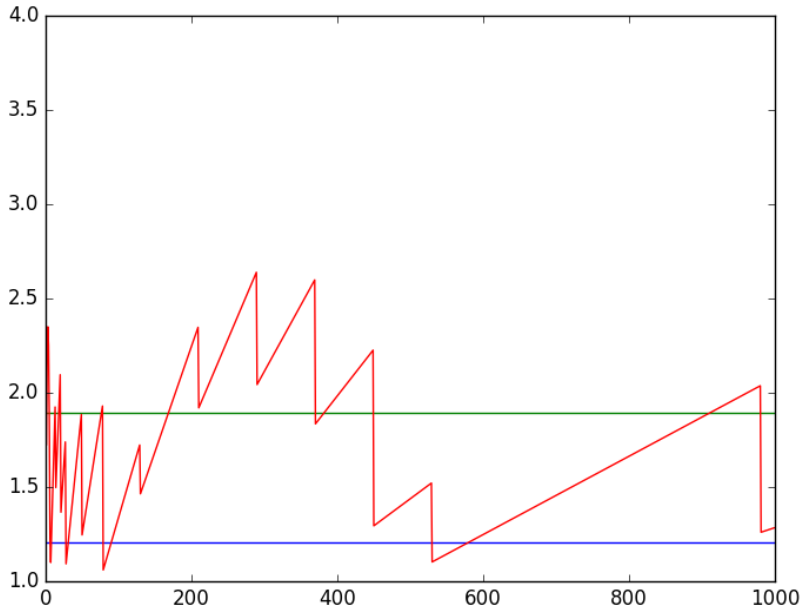
If $\theta \asymp \varphi$, $a_k = 1$ *for* $k \geqslant n$, *and* $k_n + k_{n+1} - 1 \leqslant m \leqslant k_n + 2k_{n+1} - 2$, *then*

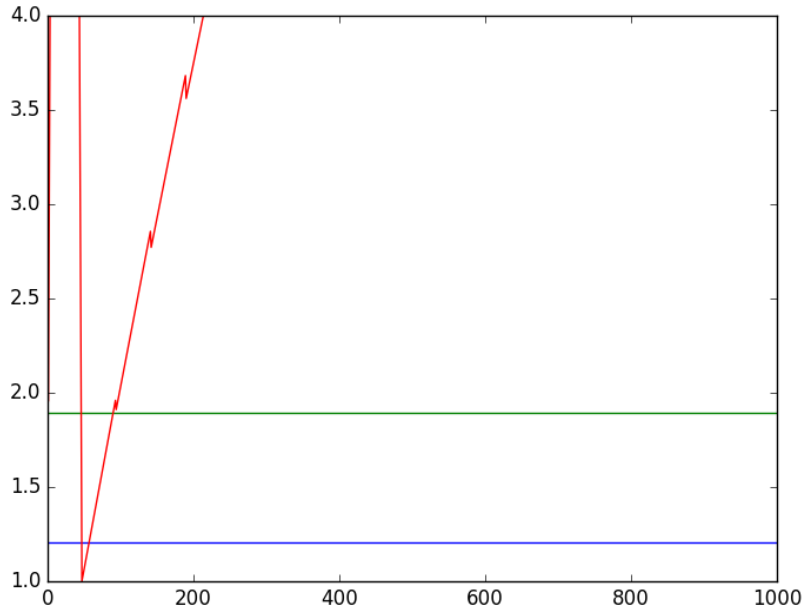
$$\max m d_\theta(m) = \frac{2x_n + 1 - \frac{1}{k_n}}{x_n + \varphi - 1}.$$

Outline

What we're looking for

Say $\theta \asymp \varphi$. When does $md_\theta(m)$ reach its lim sup, ρ, from below?





Put differently:

Question: When does there exist $M_\theta \in \mathbb{N}$ satisfying

$$m \geqslant M_\theta \implies md_\theta(m) \leqslant \rho?$$

Answer: Always!

Good U(1)-generators

Theorem

For all $\theta = [a_0, a_1, \ldots, a_N, \dot{1}] \asymp \varphi$, *there exists an* $M_\theta \in \mathbb{N}$ *satisfying*

$$m \geqslant M_\theta \implies m d_\theta(m) \leqslant \rho,$$

and an upper bound on M_θ *is computable.*

Proof outline. For each $n = N + d$, take m between $k_n + k_{n+1} - 1$ and $k_n + 2k_{n+1} - 2$, where

$$\max m d_\theta(m) = \frac{2x_n + 1 - \frac{1}{k_n}}{x_n + \varphi - 1}.$$

By bounding convergents, $m d_\theta(m) \leqslant \max m d_\theta(m) \leqslant \rho$ if

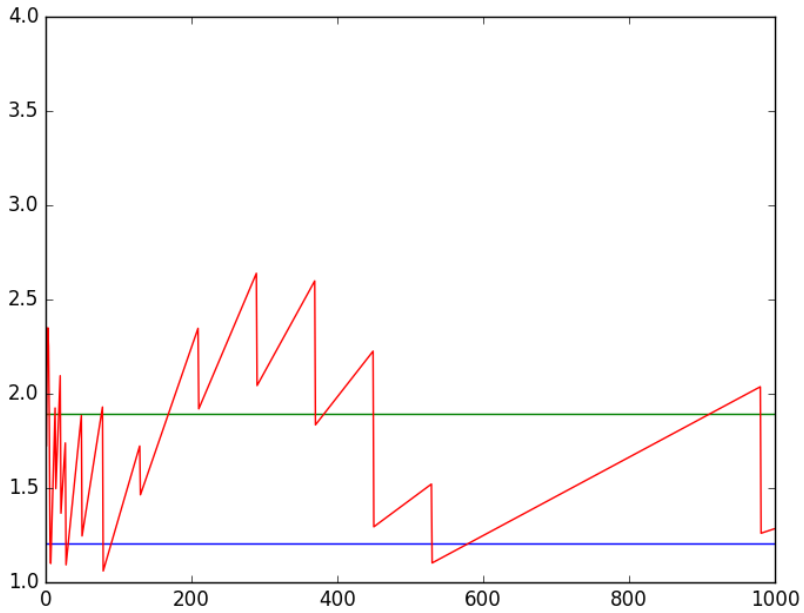
$$F_{d+1} > \frac{k_N + k_{N-1}}{5 + 2\sqrt{5}}$$

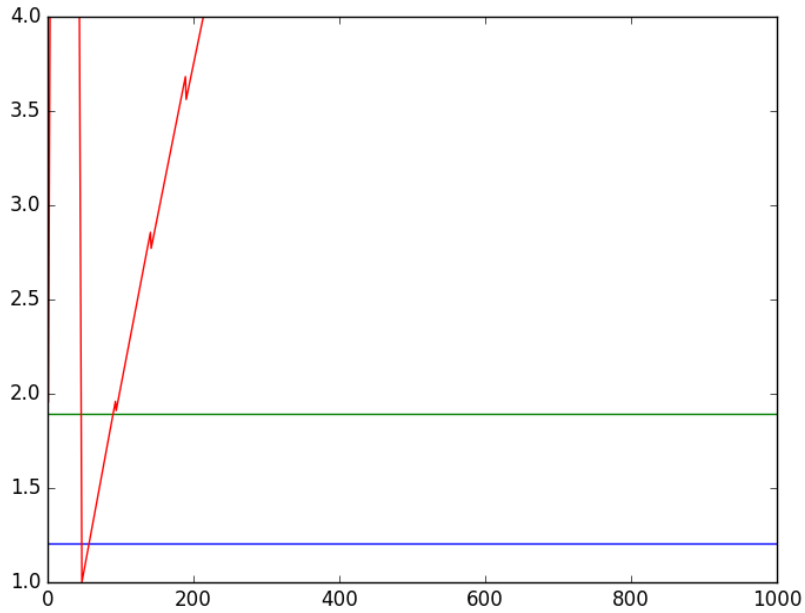
which obviously holds for all d, hence all m, beyond a certain value. ■

Outline

How can we do better?

Recall that $md_\theta(m)$ can behave strangely for small m.





The natural question then is which values of θ avoid this behavior.

Theorem (Sarnak's golden mean conjecture; Mozzochi, 2019)

For all $m \in \mathbb{N}$,

$$md_\varphi(m) \leqslant \rho.$$

The main result of this paper

Theorem

There are eight distinct generators of U(1) *with that property.*

We call this set $\mathcal{S}$ and $\mathcal{S}/\bowtie$ has these representatives:

	1	2	3	4	5	exact	num. val.
η_7	2	1	1	1	i	$\frac{3-\sqrt{5}}{2}$	0.381...
η_6	2	1	2	1	i	$\frac{25-\sqrt{5}}{62}$	0.367...
η_8	2	2	1	1	i	$\frac{7+\sqrt{5}}{22}$	0.419...
η_4	3	1	1	1	i	$\frac{5-\sqrt{5}}{10}$	0.276...
η_5	3	2	1	1	i	$\frac{9+\sqrt{5}}{38}$	0.295...
η_2	4	1	1	1	i	$\frac{7-\sqrt{5}}{22}$	0.216...
η_3	4	2	1	1	i	$\frac{11+\sqrt{5}}{58}$	0.228...
η_1	5	2	1	1	i	$\frac{13+\sqrt{5}}{82}$	0.185...

Proof of the theorem I

Proof outline. Let $\theta = [a_0, a_1, \ldots, a_N, \dot{1}]$ where $a_N \geqslant 2$. We first argue that $N < 6$. Take $m = k_N + 2k_{N+1} - 1$, where

$$md_\theta(m) = \varphi \frac{2k_{N+1} + k_N - 1}{\theta_{N+1}k_N + k_{N-1}}$$

and $md_\theta(m) \leqslant \rho$ is equivalent to

$$((2-\rho)a_N + 1 + \rho - \rho\varphi)k_N + (2-\rho)k_{N-1} \leqslant 1$$

which is false when $k_N \geqslant 13$ and $k_{N-1} \geqslant 8$ as is the case with $N \geqslant 6$.

Proof of the theorem II

Proof outline, cont. Now we argue that there exist finite bounds on each a_n, $n \in [5]$ by finding necessary conditions for $\theta \in \mathcal{S}$. Take m between $k_{n-1} + k_n - 1 \leqslant m \leqslant k_{n-1} + 2k_n - 2$, where

$$\max m d_\theta(m) = \frac{k_{n-1} + 2k_n - 1}{k_{n-2} + k_{n-1}\theta}$$

which manipulates to

$$a_n \leqslant \frac{\rho - 1}{2 - \rho} + 1 + \frac{1}{(2 - \rho)F_n}$$

hence using numerical values gives

$$a_1 \leqslant 18, \qquad a_2 \leqslant 18, \qquad a_3 \leqslant 14, \qquad a_4 \leqslant 12, \qquad a_5 \leqslant 11.$$

Proof of the theorem III

Proof outline, cont. How can we check the remaining $18 \times 18 \times 14 \times 12 \times 11 \approx 600000$ irrationals? We return to the intervals for each n given by Slater/Sós, where we compute a local maximum for n up to $29 = N + d$. 29 arises from the k-terms of θ being bounded by those of

$$[0, 18, 18, 14, 12, 11, \dot{1}],$$

at which point $d = 24$ is guaranteed to be the point where θ approaches from below. (Recall the previous Theorem.) ■

Is there a bias? alternation?

Chebyshev and Littlewood lead us to wonder about the asymptotic relevance of each generator.

On a bounded interval $[M]$, let

$$w(M) = \operatorname*{argmin}_{\theta \in \mathcal{S}} \max_{m \in [M]} m d_m(\theta).$$

Does each $[\theta] \in \mathcal{S}$ arise as $w(M)$ infinitely often? with positive density?

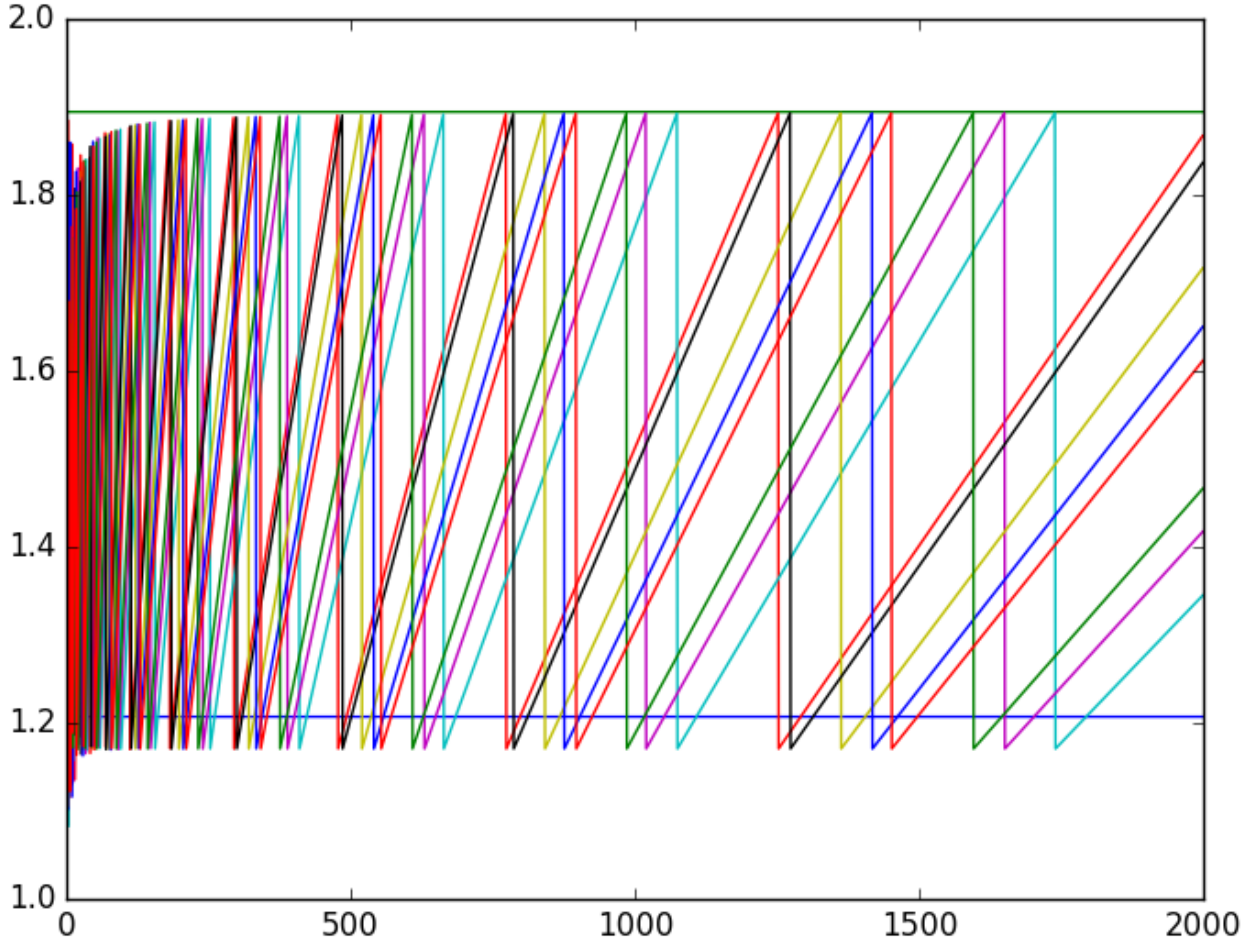
Theorem

Let $W_\theta(M)$ be the number of times for $m \in [M]$ that $[\theta] = w(m)$. Then,

$$\liminf_{M \to \infty} \frac{W_\theta(M)}{M} \geqslant 2.7\%$$

for all $\theta \in \mathcal{S}$.

Empirical evidence



Outline

1. Optimal topological generators of U(1)
   - "Good" U(1)-generators
   - The "best" U(1)-generators

2. Short paths in SU(2)
   - Motivation
   - Context
   - Path-finding for one qubit

Outline

Why unitary groups?

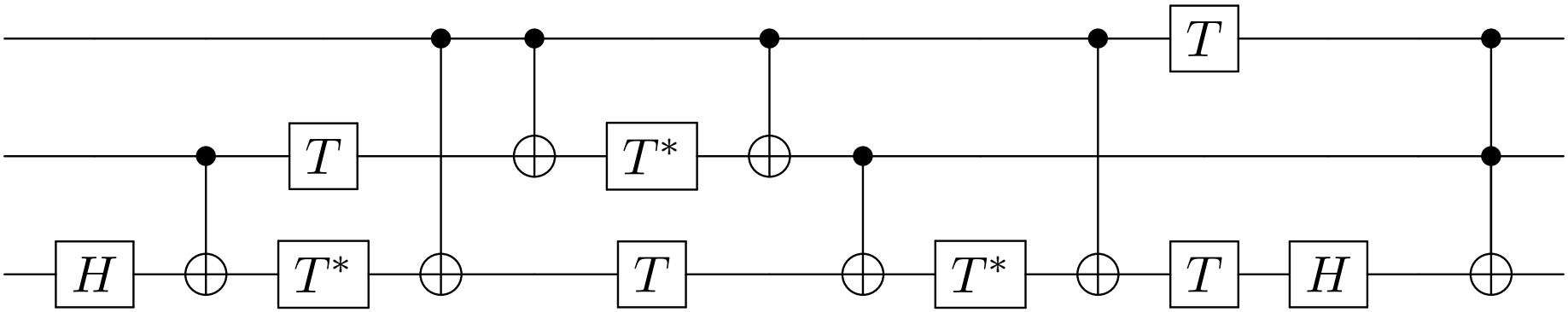
Single qubits are norm-1 $\mathbb{C}^2$ vectors equivalent under scalar multiplication by $\mathbb{C}^\times$. Qubits in general are inside $(\mathbb{C}^2)^{\otimes n}$. Linear operators sending qubits to qubits (i.e., gates) are unitary matrices.

Any n-qubit gate can be synthesized with one-qubit gates and some copies of a fixed two-cubit gate.

What can we do if we only have a finite set of one-qubit gates?

Exact and approximate synthesis

Say we only have $CNOT = I_2 \oplus i \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$, $H = \frac{i}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and $T = R_{\pi/4}$.
We can exactly get some nice circuits.



However, all we can say is that $\langle H, T \rangle$ is dense in $SU(2)$.

Outline

Previous results I

Theorem (Ross–Selinger, 2016)

There is a $\operatorname{poly}\log\frac{1}{\varepsilon}$ *algorithm to factor almost any diagonal element of* $\mathrm{SU}(2)$ *in* $\langle H, T\rangle$ *to precision* ε *using at most* $(3 + o(1))\log_2\frac{1}{\varepsilon}$ *copies of* T*.*

Theorem (Parzanchevski–Sarnak, 2018)

Suppose S *is a finite set topologically generating* $\mathrm{SU}(2)$ *whose entries are in* $\mathbb{Z}[i, \sqrt{p}]$*, where* $\mathcal{O}_{\mathbb{Q}[\sqrt{p}]}$ *is a UFD. Then Ross–Selinger's algorithm holds with* S *to give total path length at most* $(3 + o(1))\log_p\frac{1}{\varepsilon}$*.*

Previous results II

Theorem (Parzanchevski–Sarnak, 2018)

Taking S and p as before, almost any element of $\mathrm{SU}(2)$ may be approximated to within ε by decomposing using Euler angles, obtaining total path length at most $(9 + o(1)) \log_p \frac{1}{\varepsilon}$.

This is the result that we resolve to improve. To do so, we seek inspiration from the study of LPS Ramanujan graphs $X^{p,q}$.

Theorem (Carvalho Pinto–Petit, 2018; Sardari, 2019)

There is a Ross–Selinger analogue for exact factorization in $X^{p,q}$ of length at most $(3 + o(1)) \log_p q$ almost always.

Theorem (Carvalho Pinto–Petit, 2018)

There is an algorithm for exact factorization in $X^{p,q}$ of length at most $(7 + o(1)) \log_p q$ almost always.

Outline

1. Optimal topological generators of U(1)
   - "Good" U(1)-generators
   - The "best" U(1)-generators
2. Short paths in SU(2)
   - Motivation
   - Context
   - Path-finding for one qubit

Setup and roadmap

Implicitly, "approximating x within ε" has meant finding $y \in \mathrm{SU}(2)$ where

$$\varepsilon > d(x, y) = 1 - \frac{1}{2} \left| \operatorname{tr} x^* y \right| .$$

We work with "V-gates": set $\Gamma = \langle s_1, s_2, s_3 \rangle$, $S = \{s_1^{\pm 1}, s_2^{\pm 1}, s_3^{\pm 1}\}$,

$$s_1 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1+2i & \\ & 1+2i \end{pmatrix}, \quad s_2 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}, \quad s_3 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}.$$

We approximate given $g \in \mathrm{SU}(2)$ as $\delta_1 \gamma \delta_2$ where δ_i are diagonal and $\gamma \in \Gamma$ has short factorization.

Theorem

There is a $\operatorname{poly} \log \frac{1}{\varepsilon}$ *algorithm to approximate almost any element of* $\mathrm{SU}(2)$ *in path length at most* $(7 + o(1)) \log_5 \frac{1}{\varepsilon}$.

The approximation algorithm

Given $g = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}$, we seek $\gamma = \frac{1}{5^{\frac{1}{2}k}} \begin{pmatrix} x_0 + x_1 i & x_2 + x_3 i \\ -x_2 + x_3 i & x_0 - x_1 i \end{pmatrix} \in \mathrm{SU}(2)$ (since then $\gamma \in \Gamma$) with $|x_0 + x_1 i|$ near $|\alpha| < \sqrt{1 - \varepsilon_0^2}$.

Solve in $\mathbb{Z}$ with minimal k:

$$\left| (x_0^2 + x_1^2) - |\alpha|^2 \, 5^k \right| \leqslant |\alpha| \, \varepsilon 5^k,$$
$$(x_0^2 + x_1^2) + (x_2^2 + x_3^2) = 5^k.$$

We heuristically expect this to be solved when $5^k \varepsilon \in O(1)$, so γ's factorization is of length about $\log_5 \frac{1}{\varepsilon}$.
Using technical results, appropriate diagonals δ_1 and δ_2 are easily computable such that we can piece together the approximation of g: $d(g, \delta_1 \gamma \delta_2) < \frac{4}{\varepsilon_0} \varepsilon$ and δ_1 and δ_2 are each approximable to within ε in length $3 \log_5 \frac{1}{\varepsilon}$, for a total length of $7 \log_5 \frac{1}{\varepsilon}$.

Acknowledgements

I am grateful to my advisor Peter Sarnak for his guidance, support, and insight through these projects.
Thank you to Matt Tyler and Sagar Garg for helpful comments on this presentation.
This beamer color scheme is by Michael Gintz.

Partial bibliography


E. Carvalho Pinto and C. Petit. "Better path-finding algorithms in LPS Ramanujan graphs." In: *Journal of Mathematical Cryptology* 12(4) (2018).


R. L. Graham and J. H. van Lint. "On the Distribtion of $n\theta$ modulo 1." In: *Canadian Journal of Mathematics* 20 (1966), pp. 1020–1024.


C. J. Mozzochi. "A Proof of Sarnak's Golden Mean Conjecture." In: *Journal of Number Theory* (2020), to appear.


O. Parzanchevski and P. Sarnak. "Super-Golden-Gates for $PU(2)$." In: *Advances in Mathematics* 327 (2018), pp. 869–901.


N. Ross and P. Selinger. "Optimal ancilla-free Clifford+T approximation of z-rotations." In: *Quantum Information & Computation* (2016).


P. Sarnak. "Letter to Scott Aaronson and Andy Pollington on the Solovay–Kitaev Theorem and Golden Gates." (2015).


Z. Stier. "Optimal topological generators of U(1)." In: *Journal of Number Theory* (2020), to appear.