NAVIGATING $\mathbb{PU}(2)$ WITH GOLDEN GATES

PETER SARNAK

FIELD OF DREAMS

NOV | 2018
A practice problem \( U(1) \)

\[
G = U(1) = \left\{ z \in \mathbb{C}^* : z\bar{z} = z^*z = 1 \right\}
\]

\[
\cong \mathbb{R}/\mathbb{Z} ; \quad \theta \rightarrow e^{2\pi i \theta}
\]

Seek the best topological generator of \( G \).

\( R_\alpha : \theta \mapsto \theta + \alpha \), rotation by \( \alpha \)

\[ \langle R_\alpha \rangle \text{ the group generated by } R_\alpha \]

\[ R_\alpha^j = R_{j\alpha} , \quad j = 1, 2, \ldots , k , \]

\[ \langle R_\alpha \rangle = G \quad \text{iff } \alpha \text{ is irrational.} \]

How well does \( R_\alpha^j , j = 1, \ldots , k \) cover \( G \)?

\[ L_k(\alpha) := \max_{I \in G} |I| \quad \text{I-interval} \]

\[ I \cap \{ \alpha, 2\alpha, \ldots , k\alpha \} = \emptyset \]

Clearly \( L_k(\alpha) \geq 1/k \)
Figure 1. (a) The first 45 iterates of $x = 0$ under $R_\phi$ for $\phi = \left(\sqrt{5} - 1\right)/2$. (b) The first 45 iterates of $x = 0$ under $R_\phi$ for $\theta = 4 - \pi$. Iterates are labelled and arcs between consecutive points in each orbit are colored according to their relative length.
Theorem (Graham Ivan Lindt, V. Sós):

$$\lim_{k \to \infty} k L_x(k) \geq 1 + \frac{2}{\sqrt{5}}$$

With equality if $F$ is $\phi = \frac{1+\sqrt{5}}{2}$.

Moreover given $I \subset \mathbb{R}/\mathbb{Z}$ an interval determine if there is $1 \leq j \leq k$ with $j \phi \in I$?

One can use Euclid's algorithm for GCD's to answer this in polylog$(k)$ steps!

$\Rightarrow R_\phi$ is the optimal topological generator of $U(1)$ and one can navigate efficiently with $R_\phi$. 
Our problem is to do the same for \( G = \text{SU}(2) \) or \( \text{PU}(2) \).

\[ G = \text{SU}(2) = \left\{ g \in \text{GL}_2 : g g^* = I, \det g = 1 \right\} \]

(\( \text{PU}(2) = \text{U}(2) / \text{SCALAR MATRICES} \))

\( G \) is a topological (compact) group with bi-invariant metric

\[ d_G^2 (g, h) = 1 - \frac{|\text{trace}(g^* h)|}{2} \]

\[ d_G (gy, hy) = d_G (yg, yh) = d_G (g, h) \quad g, h, y \in G. \]

\( \text{Vol}_G \) is the corresponding invariant haar measure on \( G \)

\[ \text{Vol}(G) = 1, \quad \text{Vol}(Ag) = \text{Vol}(gA) = \text{Vol}(A). \]

Our aim is to give optimal topological generators of \( G \) and to navigate efficiently.
CLASSICAL COMPUTING CIRCUIT MODEL

SINGLE BIT \( x \in \{0, 1\} \)

- ONE BIT NOT GATE
  \[ \sim x \]

- TWO BIT AND GATE
  \[ x_1 \land x_2 \]
  \[ x_1 \]
  \[ x_2 \]

An \( n \)-BIT CIRCUIT IS A BOOLEAN FUNCTION
\[ f : \{0, 1\}^n \rightarrow \{0, 1\} \]

EG:

- \( x_1 \)
- \( x_2 \)
- \( x_3 \)
- \( x_4 = \sim(x_1 \land x_2) \land x_3 \)

The gates \{not, and\} are universal; every \( f \) can be expressed as a circuit using these gates.

- The size of a circuit is its complexity.
THEORETICAL QUANTUM COMPUTING

A SINGLE QUBIT STATE IS A UNIT VECTOR $\psi$ IN $\mathbb{C}^2$

$$\psi = (\psi_1, \psi_2), \quad |\psi|^2 = \psi_1 \overline{\psi_1} + \psi_2 \overline{\psi_2} = 1$$

A ONE BIT QUANTUM GATE IS AN ELEMENT $g \in U(2)$ (or $SU(2)$, $PU(2) = G$) acting on $\psi$'s

$$|x\rangle \quad \xrightarrow{[g]} \quad |y\rangle$$

$U(2)$ is the group of 2x2 unitary matrices

$$g = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \quad g^* = \begin{bmatrix} \overline{\alpha} & \overline{\beta} \\ \overline{\gamma} & \overline{\delta} \end{bmatrix}; \quad gg^* = I$$

$SU(2)$:

$$g = \begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix}, \quad |\alpha|^2 + |\beta|^2 = 1$$

$m$-QUBITS ARE VECTORS IN $(\mathbb{C}^2)^\otimes_m$

VECTOR SPACE OF DIMENSION $2^m$

* TWO BIT QUANTUM GATE XOR (OR CNOT) ON BASIS $e_0 \otimes e_0, e_0 \otimes e_1, e_1 \otimes e_0, e_1 \otimes e_1$

$$XOR = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}; \quad |x\rangle \quad \xrightarrow{X} \quad |y\rangle$$

$$X = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$
The one bit gates $g \in G$, together with XOR are universal for quantum computing. That is any $g \in U(2^n)$ can be expressed as a circuit in these.

**Example:** Three bit quantum Fourier transform

\[
\begin{align*}
|x_3\rangle & \quad |y_1\rangle & \\
|x_2\rangle & \quad |y_2\rangle & \\
|x_1\rangle & \quad |y_3\rangle & \\
\end{align*}
\]

**Hadamard:*** \[ H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \]

**Pauli:**
- $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
- $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
- $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
- $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$

These elements generate the Clifford group $C_{24}$ of order 24 in $G$. 
$C_{24}$ is not dense in $G$.

Most treatments add the "T-gate"

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \quad \frac{\pi}{8} - \text{gate}$$

$C_{24} \oplus T$ generate a dense subgroup and are an example of a golden gate set ($\text{Kliuchnikov-Maslov-Mosca}$).

$F = \{ C_{24}, T, \text{XOR} \}$ is universal and has some optimal properties.

The T-gate is considered expensive in circuits in $G$ from various points of view including fault tolerance.

⇒ The complexity of a circuit in $C_{24} + T$ is the T-count, i.e., number of applications of $T$. 
**SU(2) Double Covers SO(3)**

\[ g \in SU(2), \quad g = \begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix}, \quad \text{trace}(g) = 0 \iff g = \begin{bmatrix} ix_2 & x_3 + ix_4 \\ -x_3 + ix_4 & -ix_2 \end{bmatrix} \]

\[(x_2, x_3, x_4) \leftrightarrow \text{trace}(g) = 0 \quad x_2^2 + x_3^2 + x_4^2 = 1\]

\[(x_2, x_3, x_4) \rightarrow \begin{bmatrix} ix_2 & x_3 + ix_4 \\ -x_3 + ix_4 & -ix_2 \end{bmatrix}^* g \]

Gives a rotation in \((x_2, x_3, x_4)\), call it \(\pi(g)\). \(\pi(g) \in \text{SO}(3)\)

\[SU(2) \xrightarrow{\pi} \text{SO}(3).\]

\(C_2^4 \rightarrow \text{Rotations of a Cube.}\)

**Solovay-Kitaev Theorem:**

Given \(A, B\) topological generators of \(G\), for \(\varepsilon > 0\) and \(g \in G\) one can find a word \(W(A,B)\) of length \(O(\log \frac{1}{\varepsilon} C)\) and in as many steps s.t. \(d(W, g) < \varepsilon\) (Here \(C \approx 4\)).

This gives a crude but reasonably efficient algorithm to navigate \(G\).
Basic Problem: Optimal Generators for $G$

Given a finite subgroup $C$ of $G$ to find an involution $T$ ($T^2 = 1$) such that $F = C U \{ T \}$ generates $G$ topologically optimally in term of covering $G$ with small $T$-count, and with an efficient navigation algorithm.

The circuits $S_F(t)$ in the gates $F$ with $T$-count $t$ are of the form

$$C_1 T C_2 T \ldots C_t T$$

where $c_j \in C$

$$|S_F(t)| = |C|^2 (|C|-1)^{t-1}; t \geq 1$$

The properties that we want are
(I) $S_f(t), t \leq k$ are distinct elements in $G$.

(II) If $N_f(k) = \left| \bigcup_{t \leq k} S_f(t) \right|$, then these $N_f(k)$ points should cover $G$ essentially optimally. If $B$ is a ball centered at $I \in G$ then

$$\bigcup_{t \leq k} \bigcup_{g \in S_f(t)} B_g$$

covers $G$. For this to happen we need

$$\text{Vol}(B) N_f(k) \geq 1.$$ 

We relax this a little, requiring that if $\text{Vol}(B) N_f(k) \to \infty$ very slowly then we (almost) cover $G$.

(III) Navigation: Given $x \in G$ and a ball $B$ centered at $x$, find efficiently (i.e., in poly $k$) a $g \in \bigcup_{t \leq k} S_f(t) \cap B$, if such exists.
The (interesting) finite subgroups of \( G \) arise as the rotational symmetries of the platonic solids.

- **Tetrahedron**, \( A_4 \), \( |A_4| = 12 \)
- **Cube/Octahedron**, \( S_4 \), \( |S_4| = 24 \)
- **Dodecahedron/Icosahedron**, \( A_5 \), \( |A_5| = 60 \)

**Super-Golden Gates (Parzanchevski-S):**

1. **Cube**, Pauli Group
   
   \[ C_4 = \langle \left( \begin{array}{cc} i & 0 \\
                 0 & -i \end{array} \right), \left( \begin{array}{cc} 0 & 1 \\
                 1 & 0 \end{array} \right) \rangle, \quad T_4 = \left( \begin{array}{cc} 1 & 1-i \\
                          2+i & -1 \end{array} \right) \]

2. **Minimal Clifford (Octahedron)**
   
   \[ C_3 = \{ \left( \begin{array}{cc} 1 & 0 \\
                 0 & i \end{array} \right), \left( \begin{array}{cc} i & 1 \\
                1 & i \end{array} \right), \left( \begin{array}{cc} 1 & -i \\
                 i & i \end{array} \right) \}, \quad T_3 = \left( \begin{array}{cc} 0 & \sqrt{2} \\
                          2+i & 0 \end{array} \right) \]

3. **Tetrahedron**, Hurwitz
   
   \[ C_{12} = \langle \left( \begin{array}{cc} i & 0 \\
                 0 & -i \end{array} \right), \left( \begin{array}{cc} 1 & 1 \\
                i & -i \end{array} \right) \rangle, \quad T_{12} = \left( \begin{array}{cc} 3 & 1-i \\
                          1+i & -3 \end{array} \right) \]
4) Octahedron, Clifford

\[ C_{24} = \langle 5, H \rangle, \quad T_{24} = \begin{pmatrix} -1-\sqrt{2} & 2-\sqrt{2}+i \\ 2-\sqrt{2}-i & 1+\sqrt{2} \end{pmatrix} \]

5) Icosahedron, Klein Group

\[ C_{60} = \langle \begin{pmatrix} 1 & 0 \\ i & -i \end{pmatrix}, \begin{pmatrix} 1 & \phi-i/\phi \\ \phi+i/\phi & -1 \end{pmatrix} \rangle \]

\[ \phi = \frac{1+\sqrt{5}}{2} \quad (Golden \ Ratio), \quad T_{60} = \begin{pmatrix} 2+\phi & 1-i \\ 1+i & -2-\phi \end{pmatrix} \]
THEOREM:

These super gate sets satisfy (I), (II) and part of (III).

More precisely concerning navigation (III), if \( G \) is diagonal and one can factor integers efficiently, then there is a heuristic efficient algorithm (Ross-Selinger) which finds the shortest circuit with \( R \) as \( k \) best approximating \( G \). On the other hand if \( G \) is a general element in \( G \) then finding the shortest circuit approximating \( G \) is essentially NP-complete!

Nevertheless a circuit 3-times longer than the shortest one can be found efficiently.
Some ingredients in the analysis:

We saw that
\[ \text{SU}(2) \xrightarrow{\text{Isometric}} S^3 \subset \mathbb{R}^4 \]
\[ x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1 \]

The arithmetic set up for these golden gates is so that the words in \( F \) of \( t \)-count \( t \) correspond to solutions in integers to
\[ x_1^2 + x_2^2 + x_3^2 + x_4^2 = p^t \quad \text{--- (*)} \]

Here \( p = 3 \) for \( C_4 \)
\( p = 11 \) for \( C_{12} \)

For \( C_{24} \) (**) is to be solved in integers in \( \theta = \mathbb{Z} \left[ \sqrt{2} \right] \) and \( \mathbb{Z} \left[ \sqrt{5} \right] \); \( \text{norm}(p) = 23 \) \( p \in \theta \)

For \( C_{60} \) (**) is to be solved in \( \theta \) the integers in \( \mathbb{Q}(\sqrt{5}) \), \( p \) is in \( \theta \)
\( \text{norm}(p) = 59 \).
Problem (II) becomes one of very strong approximation for
\[ x_1^2 + x_2^2 + x_3^2 + x_4^2 = n \]

Let the integer solutions be \( S(n) \), \( |S(n)| = N(n) \) (\( \approx n \))

Project these \( N(n) \) points onto \( S^3 \)
\[ x \rightarrow x \frac{1}{\sqrt{n}} , \ x \in S(n) \]

How well do these \( N(n) \) points cover \( S^3 \)?

Optimally in the sense of (II)?

Relies on the Ramanujan Conjectures = Deligne's Theorem.
For the navigation we need to find solutions to sums of squares

\[ x_1^2 + x_2^2 = n \]  \hspace{1cm} (1)

It is solvable iff \( n = p_1^{e_1} \cdots p_k^{e_k} \) with \( e_j \) even when \( p_j \equiv 3 \, (4) \).

Can we find a solution efficiently, ie in \( \text{poly}(\log n) \) steps?

- For \( p \equiv 1 \, (4) \) a prime, Schoof gives a \((\log p)^9\) algorithm to find \( x_1 \) and \( x_2 \).

Hence if we can factor \( n \) efficiently we can solve (1) efficiently by simply multiplying the solutions in \( \mathbb{Z} [\sqrt{-1}] \).
NOTE: WHILE FACTORING IS NOT KNOWN TO BE EFFICIENT (I.E. IN \( P \)) THERE IS NO THEORETICAL EVIDENCE THAT IT IS NOT IN \( P \). A QUANTUM COMPUTER CAN FACTOR EFFICIENTLY (SHOR'S THEOREM) SO WE MIGHT WANT TO AVOID FACTORING IN BUILDING EFFICIENT GATES. THE ROSS-SLINGER ALGORITHM FOR NAVIGATING TO DIAGONAL \( \Sigma G \) WILL YIELD A SOLUTION WHICH HAS A \( (1 + o(1)) \) TIMES LONGER T-COUNT THAN THE OPTIMAL, WITHOUT APPEALING TO FACTORING.

IF WE ADD TO THE QUADRATIC DIOPHANTINE PROBLEM (1) A SIMPLE APPROXIMATION CONDITION THINGS CHANGE DRAMATICALLY.
THE TASK: GIVEN \( n \in \mathbb{N} \), \( \alpha, \beta \in \mathbb{Q} \) FIND INTEGERS \( x_1, x_2 \) S.T.

\[
x_1^2 + x_2^2 = n \\
\alpha \leq x_1 / x_2 \leq \beta
\]

IS NP-COMPLETE!

IDEA OF PROOF: REDUCE TO SUBSUM PROBLEM GIVEN \( t_1, \ldots, t_m, l \) INTEGERS IS THERE \( \varepsilon_1, \ldots, \varepsilon_m, \varepsilon_j = 0,1 \) S.T.

\[
\varepsilon_1 t_1 + \ldots + \varepsilon_m t_m = l
\]

EXPLOIT \( n^\prime \)'S OF THE FORM \( p_1 p_2 \ldots p_m \) \( p_j \)'S SMALL.

THE MOST DIFFICULT PART OF THE NAVIGATION ALGORITHM IS TO SOLVE:
Task: Given \( n \in \mathbb{N}, \mathbf{z} \in \mathbb{S}^3 \) and a ball \( B \) centered at \( \mathbf{z} \), find \( \mathbf{x} \in \mathbb{S}(n) \) (if such exists) such that \( \mathbf{z} = \frac{\mathbf{x}}{\sqrt{n}} \in B \).

The task is NP-complete, but if \( \mathbf{z} = (z_1, z_2, z_3, z_4) \) has two of its co-ordinates equal to 0 ("diagonal") then assuming that one can factor efficiently the above task can be done efficiently.

The algorithm uses a convex integer program in fixed dimension (2 and 4) which is in \( \mathcal{P} \) (Lenstra) and also Schoof's algorithm.
The last step in the algorithm involves factoring an element
\[ \gamma \in \Pi = \langle C, T \rangle \]
into a word with minimal T-count.

The key point is that these super gates are set up so that there is an explicit homomorphism
\[ \Pi \rightarrow \text{PGL}(2, \mathbb{Q}_p) \]
(\( p = |C|-1 \)) and such that \( \Pi \)
acts simply transitively on the edges of the \( |C| \)-regular tree,
\[ X = \text{PGL}(2, \mathbb{Q}_p) / \text{PGL}(2, \mathbb{Z}_p). \]

The T-count corresponding to distance moved on the tree.

The miracle of these gates is this simple transitive action and there are only finitely many such \( \Pi \)'s.