HARALD BOHR LECTURE
COPENHAGEN JUNE 2017

NAVIGATING $U(2)$ WITH GOLDEN GATES

PETER SARNAK
CLASSICAL COMPUTING CIRCUIT MODEL

SINGLE BIT $x \in \{0, 1\}$

- ONE BIT NOT GATE
  \[ \sim x, \quad x \quad \rightarrow \]

- TWO BIT AND GATE
  \[ x_1 \land x_2, \quad x_1, \quad x_2 \quad \rightarrow \]

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

EG:
\[ x_1 \quad \rightarrow \quad x_4, \quad x_4 = \sim (x_1 \land x_2) \land x_3 \]

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 $\mathbb{C}^2$

$$\psi = (\psi_1, \psi_2)$$

$$|\psi|^2 = \psi_1\overline{\psi_1} + \psi_2\overline{\psi_2} = 1$$

A one bit quantum gate is an element $g \in U(2)$ (or $SU(2)$, $PU(2) = G$) acting on $\psi$’s

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

$U(2)$ is the group of $2 \times 2$ unitary matrices

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

$SU(2)$: 

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

$n$-qubits are vectors in $(\mathbb{C}^2)^n$ vector space of dimension $2^n$

Two bit quantum gate XOR (or CNOT) on basis $e_0 \otimes e_0, e_0 \otimes e_1, e_1 \otimes e_0, e_1 \otimes e_1$

$$XOR = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$|x_1\rangle \xrightarrow{X} |y_1\rangle, \quad |x_2\rangle \xrightarrow{X} |y_2\rangle \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$
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.

**EG:** three bit quantum Fourier transform

\[
\begin{array}{c}
| x_3 \rangle \\
| x_2 \rangle \\
| x_1 \rangle \\
\end{array}
\quad
\begin{array}{c}
H \\
H \\
S \\
\end{array}
\quad
\begin{array}{c}
H \\
X \\
Y \\
Z \\
S \\
\end{array}
\quad
\begin{array}{c}
| y_1 \rangle \\
| y_2 \rangle \\
| y_3 \rangle \\
\end{array}
\]

**Hadamard**

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

**Pauli**

\[ X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \]

\[ Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \]

\[ Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \]

**Phase**

\[ S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \]

These elements generate the Clifford group $C_{24}$ of order 24 in $G$. 
Allowing only a finite set of gates we have to settle with a topologically dense universal gate set.

Distance between elements of $G$

$$d^2_G (g,h) = 1 - \frac{|\text{trace } (g^* h)|}{2}$$

$$d(yg, hy) = d(yg, yh) = d(g, h)$$ for $y \in G$.

We measure approximation in $G$ (or $U(2^m)$) with this distance. We also use the corresponding volume on $G$ which is invariant, $\text{Vol}(A) = \text{Vol}(Ay) = \text{Vol}(yA), y \in G$.

Let $g \in SU(2)$, $g = \begin{bmatrix} x_1 + i x_2 & x_3 + i x_4 \\ -x_3 + i x_4 & x_1 - i x_2 \end{bmatrix}$

$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1$

And the identification $g \leftrightarrow (x_1, x_2, x_3, x_4) \in S^3 \subset \mathbb{R}^4$ of $SU(2)$ and $S^3$ preserves distance and volume.
$C_{24}$ is not dense in $G$.

Most treatments add the "T-Gate"

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

$C_{24}$ plus $T$ generate a dense subgroup and are an example of a Golden Gate set (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.

$\Rightarrow$ 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)

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

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

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

gives a rotation in \((x_2, x_3, x_4)\), call it \(\pi(g)\). \(\pi(g) \in SO(3)\)

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

\[C_2^4 \rightarrow \text{ROTATIONS OF A CUBE}.\]

**SOLOVAY-KITAEGV 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 \(O(\log \frac{1}{\varepsilon})\) 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 (T² = 1) such that F = C \cup \{T\} generates G topologically optimally in terms 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

C₁TC₂T...CₜT, C_j ∈ C

|S_F(t)| = |C|² (|C| - 1)ᵗ⁻¹; t ≥ 1

The properties that we want are
(I) \( S_F(t), t \leq r \) are distinct elements in \( G \).

(II). If \( N_F(k) = \left| \bigcup_{t \leq r} S_F(t) \right| \), then these \( N(k) \) points should cover \( G \) essentially optimally. If \( B \) is a ball centered at \( i \in G \) then 

\[ \bigcup_{t \leq r} \bigcup_{g \in S_F(t)} U_Bg \] 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**
   \[ C_4 = \langle (i,0), (0,i) \rangle, \quad T_4 = \begin{pmatrix} 1 & 1-i \\ 2+i & -1 \end{pmatrix} \]

2. **Minimal Clifford (Octahedron)**
   \[ C_3 = \langle (0,0), (i, i), (1, -i) \rangle, \quad T_3 = \begin{pmatrix} 0 & \sqrt{2} \\ 2+i & 0 \end{pmatrix} \]

3. **Tetrahedron, Hurwitz**
   \[ C_{12} = \langle (i,0), (1, i) \rangle, \quad T_{12} = \begin{pmatrix} 3 & 1-i \\ 1+i & -3 \end{pmatrix} \]
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

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

\[ \phi = \frac{1+\sqrt{5}}{2} \quad \text{(Golden Ratio)}, \quad T_{60} = \begin{pmatrix} 2+\phi & 1-i \\ 1+i & -2-\phi \end{pmatrix} \]
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 \( k = k \) 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.
THE ANALOGOUS ONE DIMENSIONAL PROBLEM.

WHAT IS THE BEST GENERATOR OF $U(1)$?

$U(1) = \{ e^{2\pi i \theta} : 0 \leq \theta < 1 \ \text{mod} \ 1 \}$

$R_\alpha$ the rotation by $\alpha$, for $k \geq 1$,

$S_\alpha(k) = R_\alpha, R_{2\alpha}, \ldots, R_{k\alpha}$ i.e.

$\alpha, 2\alpha, \ldots, k\alpha \ \text{mod} \ 1$.

Want the largest gap between these to be as small as possible.

$L_k(\alpha) := \max |I|$, I interval

$I \cap S_\alpha(k) = \emptyset$ in $U(1)$.
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 $R_\theta$ for $\theta = 4 - \pi$. Iterates are labelled and arcs between consecutive points in each orbit are colored according to their relative length.
THEOREM (R. GRAHAM / VAN LINDT, V. SÖS)

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

WITH EQUALITY IF $\alpha = \phi = \frac{1 + \sqrt{5}}{2}$.

ONE CAN APPLY EUCLID'S ALGORITHM/CONTINUED FRACTIONS TO FIND
THE BEST $n \alpha$, $n \leq k$ APPROXIMATING
ANY GIVEN $\beta \in U(1)$ (EFFICIENTLY
IE $\text{POLY} (\log k)$ STEPS).

SO $R_\phi$ IS THE BEST GENERATOR
OF $U(1)$. 
Some ingredients in the analysis:

We saw that

\[
\text{SU}(2) \xrightarrow{\text{Isometric}} S^3 \subset \mathbb{C} \mathbb{P}^4
\]

\[
x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1
\]

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

\[
x_1^2 + x_2^2 + x_3^2 + x_4^2 = p^t \quad \text{--- } (\star)
\]

Here \( p = 3 \) for \( C_4 \)

\( p = 11 \) for \( C_{12} \)

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

For \( C_{60} \) \((\star)\) is to be solved in \( \mathcal{O} \) the integers in \( \mathcal{O} (\sqrt{5}) \), \( p \) is in \( \mathcal{O} \)

\( \text{n}(p) = 59 \).
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 \( S^3 \)

\[ x \rightarrow \frac{x}{\sqrt{n}} , \quad x \in S(n). \]

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

Optimally in the sense of (III)! ?

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 \( p_j \equiv 3 \pmod{4} \).

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

- For \( p \equiv 1 \pmod{4} \) 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 \( \mathbb{Z} \left[ \sqrt{-1} \right] \).
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-SELINGER ALGORITHM FOR NAVIGATING TO DIAGONAL $\Sigma \in \mathcal{G}$ 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 $\epsilon_1, \ldots, \epsilon_m, \epsilon_j = 0, 1$ S.T.

$$\epsilon_1 t_1 + \ldots + \epsilon_m t_m = l$$

EXPLOIT $n$'S OF THE FORM $p_1 p_2 \ldots p_m$ $p_j$ SMALL.

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

The task is NP-complete, but if \( 3 = (3_1, 3_2, 3_3, 3_4) \) has two of its
coodinates 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 \( \mathbb{P} \) (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

\[ \Pi \longrightarrow \operatorname{PGL}(2, \mathbb{Q}_p) \]

\((p = |C|-1)\) and such that \( \Pi \)

\( \Pi \) acts simply transitively on the edges of the \(|C|-\text{regular tree} \)

\[ X = \operatorname{PGL}(2, \mathbb{Q}_p)/\operatorname{PGL}(2, \mathbb{Z}_p) \]

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.