HARALD BOHR LECTURE

COPENHAGEN JUNE 2017

NAVIGATING U(2) WITH GOLDEN GATES

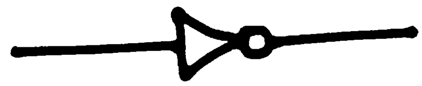
PETER SARNAK

CLASSICAL COMPUTING CIRCUIT MODEL

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

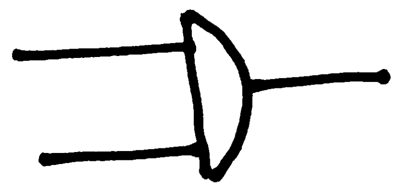
- ONE BIT NOT GATE

$\sim x$, x



- TWO BIT AND GATE

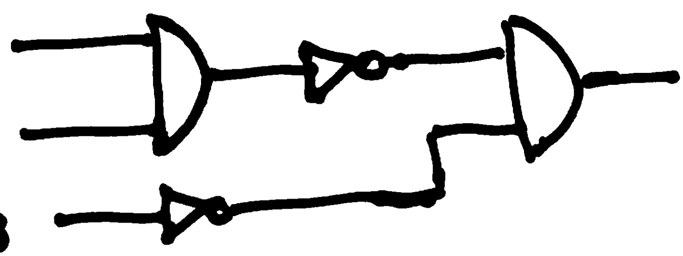
$x_1 \wedge x_2$, x_1, x_2



AN n-BIT CIRCUIT IS A BOOLEAN FUNCTION

$$f : \{0,1\}^n \longrightarrow \{0,1\}$$

EG: x_1, x_2, x_3



x_4 , $x_4 = \sim(x_1 \wedge x_2) \wedge \sim x_3$

THE GATES {NOT, AND} ARE UNIVERSAL; EVERY f CAN BE EXPRESSED AS A CIRCUIT USING THESE GATES.

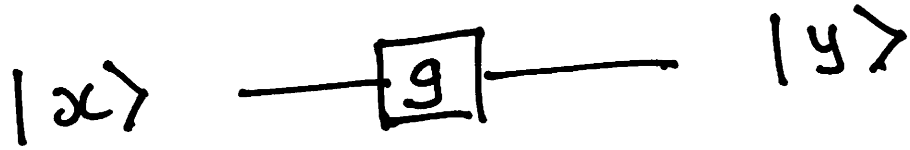
- THE SIZE OF A CIRCUIT IS ITS COMPLEXITY.

THEORETICAL QUANTUM COMPUTING

A SINGLE QUBIT STATE IS A UNIT VECTOR ψ 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 ψ'S



$U(2)$ IS THE GROUP OF 2×2 UNITARY MATRICES

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

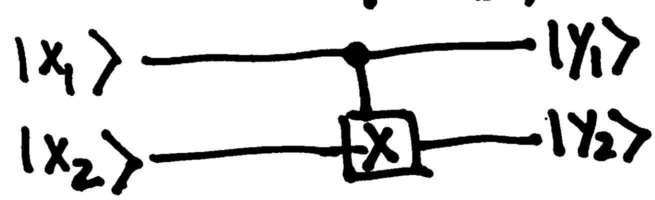
$$SU(2): \quad g = \begin{bmatrix} \alpha & \beta \\ -\bar\beta & \bar\alpha \end{bmatrix}, \quad |\alpha|^2 + |\beta|^2 = 1$$

n - QUBITS ARE VECTORS IN $(\mathbb{C}^2)^{\otimes n}$
VECTOR SPACE OF DIMENSION 2^n

- TWO BIT QUANTUM GATE

XOR (OR CNOT) ON BASIS $e_0 \otimes e_0, e_0 \otimes e_1, e_1 \otimes e_0, e_1 \otimes e_1$

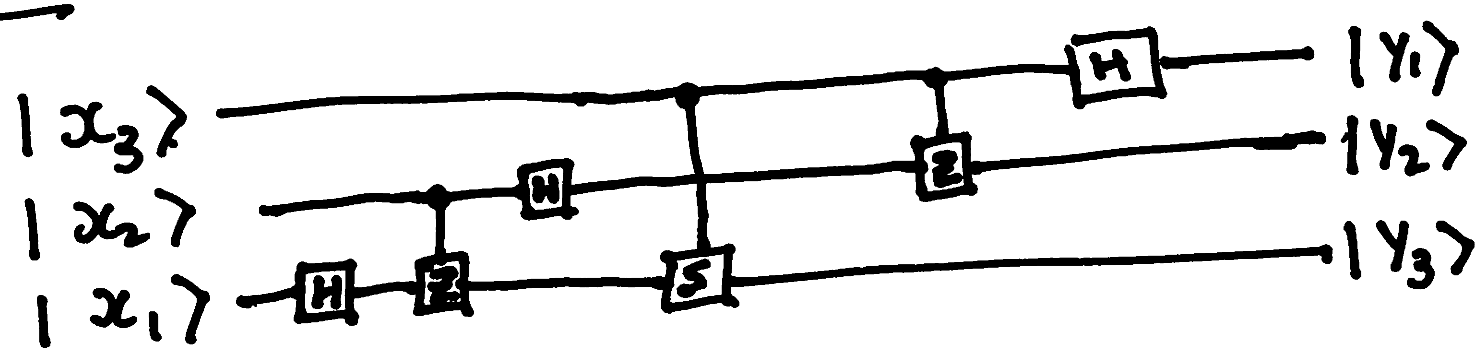
$$XOR = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix};$$



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

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.

<u>EG:</u> THREE BIT QUANTUM FOURIER TRANSFORM



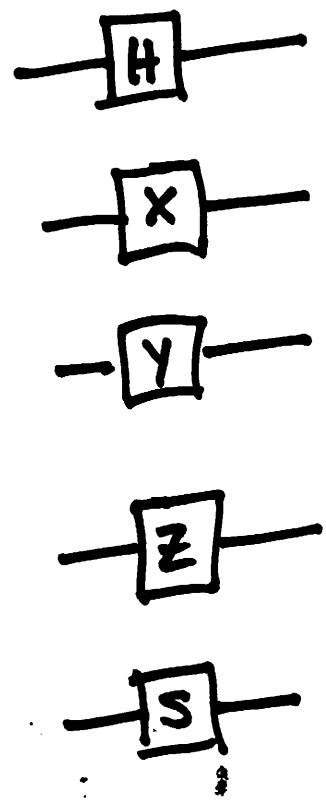
HADAMARD $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

PAULI $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

PAULI $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

PAULI $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

PHASE $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$



THESE ELEMENT 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

$$d_G^2(g,h) = 1 - \frac{|\mathrm{TRACE}\,(g^* h)|}{2}$$

$$d(gy, hy) = d(yg, yh) = d(g,h) \quad \text{FOR } y \in G.$$

WE MEASURE APPROXIMATION IN G (OR $U(2^n)$) WITH THIS DISTANCE. WE ALSO USE THE CORRESPONDIG VOLUME ON G WHICH IS INVARIANT, $\mathrm{VOL}(A) = \mathrm{Vol}(Ay) = \mathrm{Vol}(yA), y \in G.$

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

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

AND THE IDENTIFICATION

$$g \longleftrightarrow (x_1, x_2, x_3, x_4) \in S^3 \subset \mathbb{R}^4$$

OF SU(2) AND S^3 PRESERVES DISTANCE AND VOLUME.

C_{24} IS NOT DENSE IN G.

MOST TREATMENTS ADD THE "T-GATE"

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

C_{24} PLUS T GENERATE A DENSE SUBGROUP AND ARE AN EXAMPLE OF A GOLDEN GATE SET (KLIUCHNIKOV-MASLOV-MOSCA).

$F = \{C_{24}, T, XOR\}$ 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, IE NUMBER OF APPLICATIONS OF T.

SU(2) DOUBLE COVERS SO(3)

$g \in SU(2)$, $g = \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix}$, TRACE$(g) = 0 \Longleftrightarrow$

$$g = \begin{bmatrix} ix_2 & x_3 + ix_4 \\ -x_3 + ix_4 & -ix_2 \end{bmatrix}$$

$(x_2, x_3, x_4) \longleftrightarrow \mathrm{trace}(g) = 0$

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

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

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

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

$C_{24} \rightarrow$ 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 $O((\log 1/\varepsilon)^c)$ 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 $F = C \cup \{T\}$ 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

$$c_1 T c_2 T \dots c_t T \quad , \; c_j \in C$$

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

THE PROPERTIES THAT WE WANT ARE

(I) $S_F(t)$, $t \le k$ ARE DISTINCT ELEMENTS IN G.

(II). IF $N_F(k) = \left| \bigcup_{t \le k} S_F(t) \right|$, THEN THESE $N(k)$ POINTS SHOULD COVER G ESSENTIALLY OPTIMALLY. IF B IS A BALL CENTERED AT $I \in G$ THEN

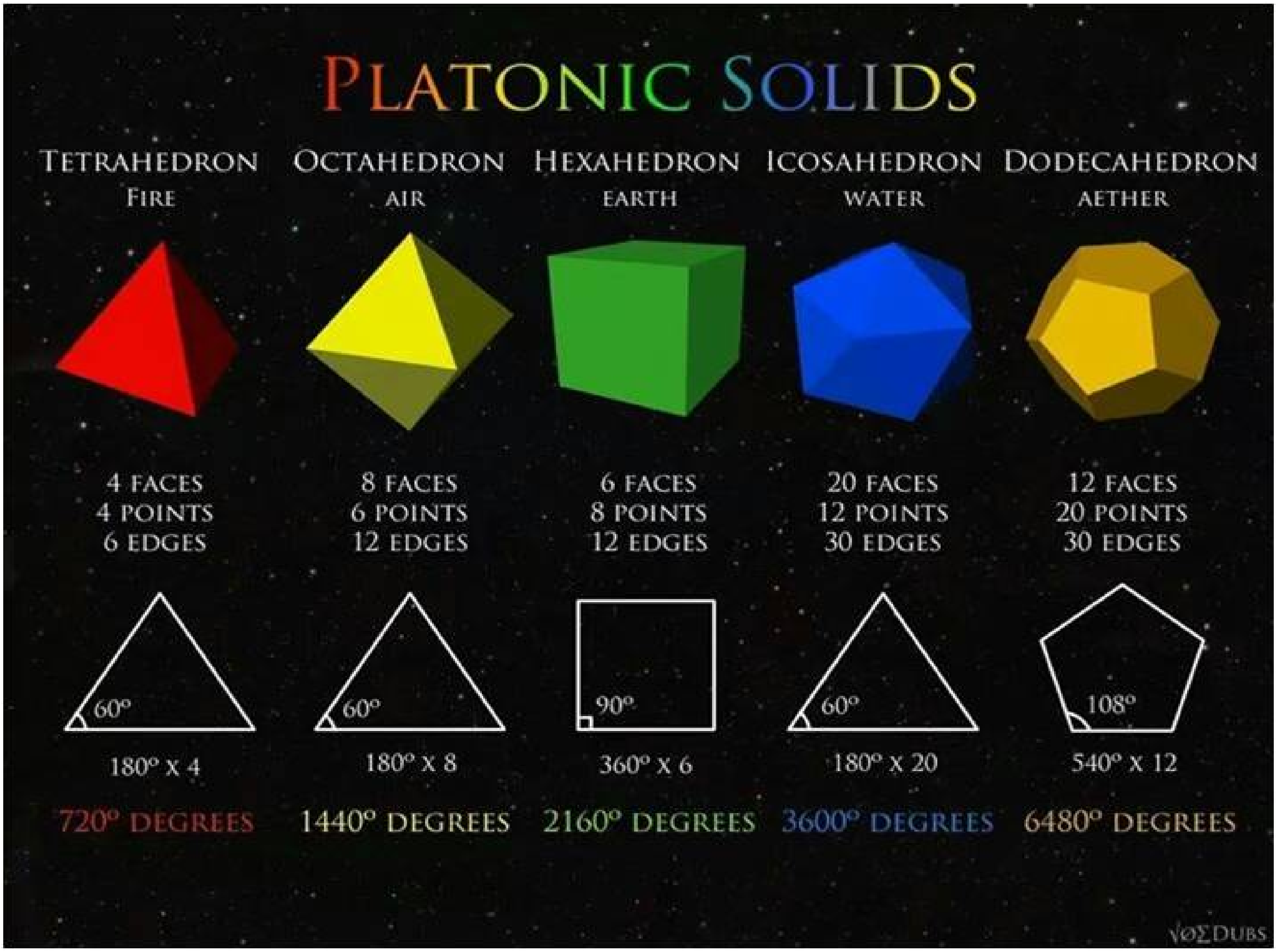
$$\bigcup_{t \le k} \bigcup_{g \in S_F(t)} Bg \quad \text{COVERS } G.$$

FOR THIS TO HAPPEN WE NEED

$$\mathrm{Vol}(B)\, N_F(k) \ge 1 .$$

WE RELAX THIS A LITTLE, REQUIRING THAT IF $\mathrm{Vol}(B) N_F(k) \longrightarrow \infty$ VERY SLOWLY THEN WE (ALMOST) COVER G.

(III) NAVIGATION: GIVEN $x \in G$ AND A BALL B CENTERED AT x, FIND EFFICIENTLY (IE IN POLY k) A $g \in \left[\bigcup_{t \le k} S_F(t) \right] \cap B$, IF SUCH EXISTS.


PLATONIC SOLIDS
TETRAHEDRON
FIRE
OCTAHEDRON
AIR
HEXAHEDRON
EARTH
ICOSAHEDRON
WATER
DODECAHEDRON
AETHER
4 FACES
4 POINTS
6 EDGES
8 FACES
6 POINTS
12 EDGES
6 FACES
8 POINTS
12 EDGES
20 FACES
12 POINTS
30 EDGES
12 FACES
20 POINTS
30 EDGES
60°
60°
90°
60°
108°
180° X 4
180° X 8
360° X 6
180° X 20
540° X 12
720° DEGREES
1440° DEGREES
2160° DEGREES
3600° DEGREES
6480° DEGREES
√ØΣDUBS

THE (INTERESTING) FINITE SUBGROUPS OF G ARISE AS THE ROTATIONAL SYMMETRIES OF THE 5 PLATONIC SOLIDS.

TETRAHEDRON	,	A_4	$\lvert A_4\rvert = 12$
CUBE / OCTAHEDRON	,	S_4	$\lvert S_4\rvert = 24$
DODECAHEDRON / ICOSAHEDRON.	,	A_5	$\lvert A_5\rvert = 60$.

SUPER-GOLDEN GATES (PARZANCHEVSKI-S):

(1) CUBE, PAULI GROUP.

$$C_4 = \left\langle \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle, \quad T_4 = \begin{pmatrix} 1 & 1-i \\ 1+i & -1 \end{pmatrix}$$

(2) MINIMAL CLIFFORD (OCTAHEDRON).

$$C_3 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}, \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix} \right\}, \quad T_3 = \begin{pmatrix} 0 & \sqrt{2} \\ 1+i & 0 \end{pmatrix}$$

(3) TETRAHEDRON, HURWITZ

$$C_{12} = \left\langle \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \right\rangle, \quad T_{12} = \begin{pmatrix} 3 & 1-i \\ 1+i & -3 \end{pmatrix}$$

4) OCTAHEDRON, CLIFFORD

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

5) ICOSAHEDRON, KLEIN GROUP.

$$C_{60} = \left\langle \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}, \begin{pmatrix} 1 & \phi - i/\phi \\ \phi + i/\phi & -1 \end{pmatrix} \right\rangle$$

$$\phi = \frac{1+\sqrt{5}}{2} \text{ (GOLDEN RATIO)}, \quad T_{60} = \begin{pmatrix} 2+\phi & 1-i \\ 1+i & -2-\phi \end{pmatrix}$$

THEOREM:

THESE SUPER GATE SETS SATISFY (I), (II) AND PART OF (III).

MORE PRECISELY CONCERNING NAVIGATION (III)

IF $g \in G$ IS DIAGONAL AND ONE CAN FACTOR INTEGERS EFFICIENTLY, THEN THERE IS A HEURISTIC EFFICIENT ALGORITHM (ROSS-SELINGER) WHICH FINDS THE SHORTEST CIRCUIT WITH $k \leq K$ 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!

NEVER-THE-LESS A CIRCUIT 3-TIMES LONGER THAN THE SHORTEST ONE CAN BE FOUND EFFICIENTLY.

THE ANALOGOUS ONE DIMENSIONAL PROBLEM:

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

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

R_α THE ROTATION BY α, FOR $k \geq 1$,

$S_\alpha(k) = R_\alpha, R_\alpha^2, \dots, R_\alpha^k$ I.E.

$\alpha, 2\alpha, \dots, k\alpha \mod 1$.

WANT THE LARGEST GAP BETWEEN THESE TO BE AS SMALL AS POSSIBLE.

$$L_k(\alpha) := \max_{I \cap S_\alpha(k) = \phi} |I| \quad , \quad I \text{ INTERVAL IN } U(1).$$

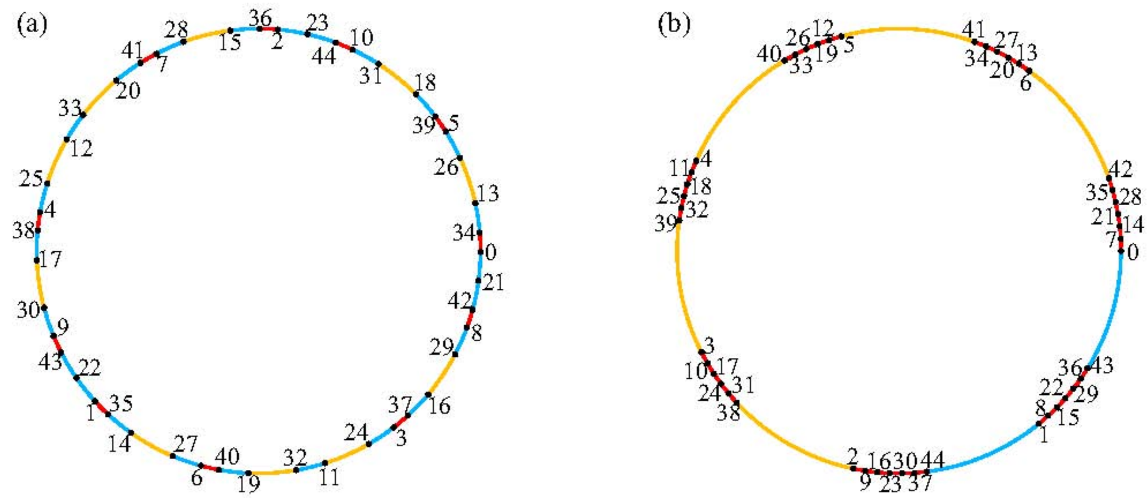


Figure 1. (a) The first 45 iterates of $x = 0$ under R_ϕ for $\phi = \left(\sqrt{5}-1\right)/2$. (b) The first 45 iterates of $x = 0$ under R_θ for $\theta = 4 - \pi$. Iterates are labelled and arcs between consecutive points in each orbit are colored according to their relative length.

THEOREM (R. GRAHAM / VAN LINDT , V. SÓS).

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

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 POLY(LOG k) STEPS).

SO R_ϕ IS THE BEST GENERATOR OF $U(1)$.

SOME INGREDIENTS IN THE ANALYSIS :

WE SAW THAT

$$SU(2) \xleftrightarrow{\text{ISOMETRIC}} S^3 \subset \mathbb{R}^4$$

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

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 $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$ AND $\cancel{\underline{P} = \sqrt{2}}$; NORM $(\underline{P}) = 23$
$\underline{P} \in \mathcal{O}$

FOR C_{60} $(*)$ IS TO BE SOLVED IN $\mathcal{O}$ THE INTEGERS IN $\mathbb{Q}(\sqrt{5})$, $\underline{P}$ IS IN $\mathcal{O}$
$N(\underline{P}) = 59$.

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

$$x \to \frac{x}{\sqrt{n}}, \quad x \in S(n).$$

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

$$x_1^2 + x_2^2 = n \quad \text{——— (1)}$$

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 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 MULTIPYING THE SOLUTIONS IN $\mathbb{Z}[\sqrt{-1}]$.

<u>NOTE:</u> WHILE FACTORING IS NOT KNOWN TO BE EFFICIENT (I.E. IN $\mathbb{P}$) THERE IS NO THEORETICAL EVIDENCE THAT IT IS NOT IN $\mathbb{P}$. 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 $\mathfrak{Z} \in G$ 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.

$$\left.\begin{aligned} x_1^2 + x_2^2 &= n \\ \alpha \le x_1/x_2 &\le \beta \end{aligned}\right\}$$

IS NP-COMPLETE!

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

$$\varepsilon_1 t_1 + \cdots + \varepsilon_m t_m = \ell.$$

EXPLOIT n's OF THE FORM $p_1 p_2 \cdots p_m$
p_js SMALL.

THE MOST DIFFICULT PART OF THE NAVIGATION ALGORITHM IS TO SOLVE:

TASK: GIVEN $n \in \mathbb{N}$, $\xi \in S^3$ AND A BALL B CENTERED AT ξ, FIND $x \in S(n)$ (IF SUCH EXISTS) SUCH THAT $\tilde{x} = \frac{x}{\sqrt{n}} \in B$.

THE TASK IS NP-COMPLETE, BUT IF $\xi = (\xi_1, \xi_2, \xi_3, \xi_4)$ 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

$$\gamma \in \Gamma = \langle C, T \rangle$$

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

$$\Gamma \longrightarrow PGL(2, \mathbb{Q}_p)$$

$(p = |C| - 1)$ AND SUCH THAT Γ

Γ ACTS SIMPLY TRANSITIVELY ON THE EDGES OF THE $|C|$-REGULAR TREE

$$X = PGL(2, \mathbb{Q}_p) / PGL(2, \mathbb{Z}_p).$$

THE T-COUNT CORRESPONDING TO DISTANCE MOVED ON THE TREE.

THE MIRACLE OF THESE GATES IS THIS SIMPLE TRANSITIVE ACTION AND THE ARE ONLY FINITELY MANY SUCH Γ'S.