THE SOLOVAY KITAEV THEOREM AND GOLDEN GATES

PETER SARNAK.

WATERLOO JUNE 2015.

CLASSICAL COMPUTING:

SINGLE BIT STATE: $\{0,1\}$

GATES FOR CIRCUITS ACHIEVE ANY BOOLEAN $f:\{0,1\}^n \longrightarrow \{0,1\}^m$ VIA $,\ \sim,\ \wedge$ etc, COMPLEXITY = CIRCUIT SIZE.

THEORETICAL QUANTUM COMPUTING:

SINGLE QUBIT STATE:

$$\psi = (\psi_1, \psi_2) \in \mathbb{C}^2, \quad |\psi|^2 = 1.$$

A 1-BIT QUANTUM GATE IS AN ELEMENT $A \in U(2)$ OR BETTER STILL $PU(2) := G$ (NO PHASE)

A UNIVERSAL GATE SET g IS ONE WHICH GENERATES G TOPOLOGICALLY.

$$d_G^2(x,y) = 1 - \frac{|\text{trace}(x^* y)|}{2} = d^2(hx,hy) = d^2(xh,yh)$$
, $h \in G$.

μ Haar measure on G.

$B_r(x)$ the ball centered x radius r

$\mu(B_\varepsilon) \sim c\varepsilon^3$, ε small.

WANT GATE SETS WHICH HAVE SHORT CIRCUITS TO APPROXIMATE A GENERAL $x \in G$.

TEXT BOOK GATES:

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

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

$C = \langle H, S \rangle$ FINITE CLIFFORD GROUP $|C| = 24$

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

$\Gamma = \langle H, T \rangle$ IS UNIVERSAL.

ROSS-SELINGER (2014) (ALGORITHM)

$$d\left(U, \begin{bmatrix} e^{i\pi/128} & 0 \\ 0 & e^{-i\pi/128} \end{bmatrix}\right) < \varepsilon = 10^{-10}$$

WITH

$$U = HTSHTSHT \cdots\cdots\cdots HTH$$

T-COUNT IS 102 (100 IS "OPTIMAL")

$\varepsilon = 10^{-20}$, T-COUNT 200
(OPTIMAL 198)

⋮

$\varepsilon = 10^{-2000}$, T-COUNT 19942

OPTIMAL 19934

(RUN-TIME 383 SECONDS)

$\mathcal{G} = \{ s_1, s_2, \ldots, s_v \}$ GATES

$\Gamma = \langle s_1, \ldots, s_v \rangle \leq G$.

$w : \mathcal{G} \longrightarrow \mathbb{R}_{\geq 0}$, $w(s)$ COST OF PREPARING s.

- $h(\gamma)$; height of $\gamma \in \Gamma$

$$:= \min \left\{ \sum_{k=1}^{l} w(s_{j_k}) : \gamma = s_{j_1} s_{j_2} \cdots s_{j_l} \right\}.$$

$$V(t) := \{ \gamma \in \Gamma : h(\gamma) \leq t \}.$$

(NOTE $|V(t)|$ GROWS EXPONENTIALLY WITH t) IF Γ IS UNIVERSAL.

- FOR $\varepsilon > 0$, t_ε the covering depth, that is the least t such that the balls $B_\varepsilon(\gamma)$, $\gamma \in V(t)$ cover G.

· For $\varepsilon, \delta > 0$, the covering up to ε^δ depth $t_{\varepsilon,\delta}$ is the least t such that $B_\varepsilon(\gamma)$, $\gamma \in V(t)$ cover G except for a set of μ-measure $\leq \varepsilon^\delta$.

CLEARLY $t_{\varepsilon,\delta} \leq t_\varepsilon$ AND

$$|V(t_{\varepsilon,\delta})|\,\mu(B_\varepsilon) \geq \frac{1}{2}.$$

The covering exponent $K(g)$ and typical x covering exponent $K_\mu(g)$ are

$$K(g) = \overline{\lim_{\varepsilon \to 0}} \frac{\log |V(t_\varepsilon)|}{\log(1/\mu(B_\varepsilon))}$$

$$K_\mu(g) = \lim_{\delta \to 0} \overline{\lim_{\varepsilon \to 0}} \frac{\log |V(t_{\varepsilon,\delta})|}{\log(1/\mu(B_\varepsilon))}.$$

$1 \leq K_\mu(g) \leq K(g)$ and $K(g) = 1$ means that every $x \in G$ has an optimally good approximation with γ's of minimal height, while $K_\mu(g) = 1$ says the same for most x.

The mathematical problems are:

(A) How small can we make $K(g)$ and $K_\mu(g)$ by choosing g.

(B) Give a poly $\log(1/\varepsilon)$ time algorithm to find good approximations to short circuits.

• That is something like a continued fraction algorithm for G.

SOLOVAY-KITAEV THEOREM: GIVES FOR ANY UNIVERSAL GATE SET g, AND $\varepsilon > 0$, $x \in G$, A $\gamma \in \Gamma$ WITH $h(\gamma) = O((\log 1/\varepsilon)^c)$ AND SUCH γ CAN BE FOUND IN $O((\log 1/\varepsilon)^c)$ STEPS. ($c = 4$ IS ADMISSIBLE — DAWSON - NIELSON.)

$\Rightarrow$ UNIVERSAL EFFICIENT QUANTUM GATE SETS EXIST.

Note that this is not enough to show that $K(g) < \infty$.

Assume from now on that the entries of $s \in g$ are in $\overline{\mathbb{Q}}$. The coordinates of s's are S-integers in a number field L. Let Λ be the smallest S-arithmetic (unitary) group to contain Γ.

- Either Γ is finite index (better still congruence) in Λ
- Or it is infinite index when we call it "thin".

(•) In either case it follows from the Bourgain-Gamburd spectral gap theorem for such subgroups of G that

$$K(g) < \infty .$$

If Γ is a congruence subgroup of a unitary S-arithmetic group H/L WITH $S = \{p\}$ AND $H(L_p)/H(O_p)$ A $q+1$ REGULAR TREE X AND $h(\gamma)$ BEING ESSENTIALLY THE DISTANCE $d_X(\gamma e, e)$, THEN THE GATE SET IS GOLDEN:

EXAMPLE 1: ([LUBOTZKY-PHILLIPS-S], [BOCHAROV-GUREVICH-SVORE])

$$g = \{s_1, s_1^{-1}, s_2, s_2^{-1}, s_3, s_3^{-1}\}$$

$$s_1 = \frac{1}{\sqrt{5}}\begin{bmatrix} 1+2i & 0 \\ 0 & 1-2i \end{bmatrix}, s_2 = \frac{1}{\sqrt{5}}\begin{bmatrix} 1 & 2i \\ 2i & 1 \end{bmatrix}, s_3 = \frac{1}{\sqrt{5}}\begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}$$

THE WEIGHTS $W(s_j) = 1$; Γ IS FREE ON s_1, s_2, s_3, $h(\gamma)$ IS REDUCED WORD LENGH $|V(t)| \sim c\, 5^t$.

- $1 = K_\mu(g) < \frac{4}{3} \leq K(g) \leq 2$.

• THERE IS A PROBABILISTIC ALGORITHM WITH EXPECTED RUNNING TIME POLY(LOG($1/\varepsilon$)) WHICH FOR $\mathcal{X}$ DIAGONAL PRODUCES (IF IT STOPS) THE γ OF SMALLEST HEIGHT IN $B(x,\varepsilon)$ (ASSUMING ONE HAS A POLYNOMIAL TIME FACTORING ALGORITHM) (ROSS-SELINGER).

EXAMPLE 2: $\frac{\pi}{8}$-GATES [KLIUCHNIKOV, MASLOV, MOSCA] [ROSS-SELINGER]

$$g = \{H, S, T\}, \quad |V_t| = C 2^t$$

T-COUNT

$W(H) = W(S) = 0$

$W(T) = 1$.

$$\bullet\ 1 = K_\mu(g) < \frac{4}{3} \leq K(g) \leq 2 .$$

• THERE IS A PROBABILISTIC ALGORITHM WITH EXPECTED RUNNING TIME POLYLOG($1/\varepsilon$) WHICH FOR $\mathcal{X}$ DIAGONAL PRODUCES (IF IT STOPS) THE γ OF SMALLEST HEIGHT IN $B(x,\varepsilon)$ (AGAIN ASSUMING POLY FACT. ALGORITHM).

COMMENTS:

(i) For these golden gate sets the algorithm to approximate a general $x \in G$ will give a circuit 3-times longer than the optimal that exists according to $K_\mu(g) = 1$. This follows by factoring x as $d_1 d_2 d_3$.

(ii) Example 1 was engineered;
D is the Hamilton quaternions / $\mathbb{Q}$
$S = \{5\}$ (i.e. denominators at 5)

D: $1, \underline{i}, \underline{j}, \underline{k}$, $\underline{i}^2 = \underline{j}^2 = \underline{k}^2 = -1$,
$\underline{i}\underline{j} = \underline{k}$, etc
D is split at $p = 5$ (in fact any $p \neq 2$)

$$D^*\left[\mathbb{Z}\left[\tfrac{1}{5}\right]\right] \xrightarrow[\text{diag}]{} PGL_2(\mathbb{Q}_5)\times(SU(2)\times\mathbb{R}^*)$$

image of $D^*\left(\xi\mathbb{Z}\left[\tfrac{1}{5}\right]\right)$ in $SU(2)$ is Γ.

On the other hand the image in $PGL_2(\mathbb{Q}_5)$ acts isometrically on the 6-regular tree $X := PGL_2(\mathbb{Q}_5)/PGL_2(\mathbb{Z}_5)$.

In fact it acts simply transitively on X and $h(\gamma)$ is simply the distance in X from ξ to $\gamma\xi$ where ξ is the identity coset $e\cdot PGL_2(\mathbb{Z}_5)$.

This allows one to use automorphic forms to analyze the equidistribution in G of V_t as in [L-P-S].

Sharpening the analysis there $\Longrightarrow$ $K(S) \leq 2$ and $K_{\mu}(S) = 1$.

Both make full use of the Ramanujan Conjecture (Deligne's theorem).

(iii) T-gates were not engineered but remarkably give an S-arithmetic group. Γ can be realized as the S-unit group of D/F where $F = \mathbb{Q}(\sqrt{2})$ and $S = \{(\sqrt{2})\} = \{\mathfrak{P}\}$. $(2) = \mathfrak{P}^2$, D is split at $\mathfrak{P}$ (it is ramified at the two archimedian places of F). $\mathcal{O}$ = ring of integers of F, $X := PGL_2(F_{\mathfrak{P}}) / PGL_2(\mathcal{O}_{\mathfrak{P}})$ is a 3-regular tree.

$$\Delta = D^*(\theta[\tfrac{1}{2}]).$$

If $\tilde{H} = \frac{i}{\sqrt{2}} + \frac{k}{\sqrt{2}} \in \Delta$

and $\beta = \frac{2+\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i$,

$N(\beta) = \sqrt{2}(1+\sqrt{2})$, $\beta \in \Delta$.

$$\Delta \hookrightarrow PGL_2(\mathbb{Q}_2) \times (SU(2) \times \mathbb{R}^*)$$

diag

$\tilde{H} \to H$, $\beta \to T$

AND ONE SHOWS THAT Δ is projected onto Π (Δ is generated by H AND T).

MOREOVER UNDER THIS IDENTIFICATION THE T COUNT OF A $\gamma \in \Gamma$ IS AGAIN EXACTLY THE DISTANCE THAT γ MOVES $\mathfrak{Z}$ IN X! THIS ALLOWS FOR A SIMILAR ANALYSIS AS IN EXAMPLE 1.

(iv) THAT $K(g) \geq \frac{4}{3}$ FOR ANY GOLDEN GATE SET CORRESPONDS TO "BIG HOLES" IN THE SET OF POINTS WHICH ARE SUMS OF FOUR SQUARES (A FEATURE THAT GOES BACK TO WRIGHT AND MORE RECENTLY HARMON).

THIS IS THE PRICE OF S-ARITHMETIC GOLDEN GATES, $K(g) \neq 1$ THERE ELEMENTS OF G WHICH REQUIRE LONGER CIRCUITS, BUT THEY ARE RARE, $K_m(g) = 1$.

(V). Another non-engineered gate set was considered by Forest, Gosset, Kliuchnikov and McKinnon: $\mathcal{G}_n$ consists of the Clifford group C_n and the T_n gate $= \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4n} \end{bmatrix}$.

This is naturally a subgroup of the S-arithmetic 2×2 unitary group over $F = \mathbb{Q}(\zeta_{2n} + \zeta_{2n}^{-1})$ and the "CM field" $E = \mathbb{Q}(\zeta_{2n})$ over F, with S being the set of places dividing (2). $\mathcal{G}_n$ is arithmetic for $n = 3, 4, 8, 12$ (F-G-K-M). It is this for all but finitely many n, the above list is probably complete!

(vi) The basic algorithm:

Two steps

(a) First find a global S-integral element in Δ which achieves the desired approximation.

(b) Once we have such, in example 1 it is

$$x_1^2+x_2^2+x_3^2+x_4^2 = 5^h, \quad h \leq t.$$

x_j integers.

With this $x_1 + \underline{i}x_2 + \underline{j}x_3 + \underline{k}x_4$ in Δ we consider its image in $PGL_2(\mathbb{Q}_5)$ and then image of ξ in the tree. The tree tells us how to navigate in terms of the generators to e!

As for (a), want a solution to

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 5^t$$

x_j approximating $\xi_j \in \mathbb{R}$

$$\xi_1^2 + \xi_2^2 + \xi_3^2 + \xi_4^2 = 5^t .$$

The idea is to restrict to $\xi_3 = \xi_4 = 0$ (i.e. $\alpha \in G$ diagonal!)

(seems to appear first in a paper of Petit-Lauter-Quisquater (2008) "Full cryptanalysis of LPS and Morgenstern Hash Functions").

Then take x_1 close to ξ_1
x_2 close to ξ_2

and try solve (two binary problems)

$$5^t - x_1^2 - x_2^2 = x_3^2 + x_4^2 .$$

i.e. sum of two squares ...

(Vii) FOR THE S-ARITHMETIC (GOLDEN GATES) ONE CAN DEFINE THE LOCAL EXPONENT OF APPROXIMATION BY V_t FOR $x \in G$

$$K_i(x) = \overline{\lim_{\varepsilon \to 0}} \frac{\log |V_{t_\varepsilon(x)}|}{\log \varepsilon^{-3}}$$

(Ghosh-Gorodnik-Nevo).

Using the Ramanujan Conjectures they prove that for μ-almost all $x \in G$

$$K(x) = 1.$$

(this is a stronger statement than $K_\mu = 1$).

SOME UNRESOLVED QUESTIONS:

(1) FOR A GOLDEN GATE SET IS $K(S)<2$? PROBABLY $K(S) = 4/3$.

(2) IS THERE A GATE SET WITH $K(S)=1$, PERHAPS WITH A THIN SUBGROUP?

(3). FOR A GOLDEN GATE SET FIND A RANDOM ALGORITHM WHICH FINDS A CIRCUIT WHICH IS ESSENTIALLY OPTIMALLY SHORT (NOT 3-TIMES LONGER) FOR A GENERAL $x \in G$.

IS FINDING THE SHORTEST CIRCUIT TO APPROXMATE A GENERAL $x \in G$ NP COMPLETE?

RECALL: MANDERS-ADLEMAN (1978)

THE PROBLEM OF DECIDING IF

$$ax^2 + by + c = 0$$

has a solution in natural numbers x and y, given a, b, c is NP-complete!

[A-K-S] M. AGRAWAL, N. KAYAL, N. SAXENA
ANN OF MATH, 160 (2004) 781-793

[A-M] K. AMANO, K. MATSUMOTO
arXiv 0806.3834

[B-G] J. BOURGAIN and A. GAMBURD
INVENT. MATH 171 (2008) 83-121

[B-R-S] J. BOURGAIN, Z. RUDNICK, P. SARNAK
arXiv 1204.0134

[B-S] A. BOCHAROV + K. SVORE
arXiv 1206:3223

[B-G-S] A. BOCHAROV, Y. GUREVICH and K. SVORE,
arXiv 1303:1411

[CH] P. CHIU JNL NUMBER THEORY
53, 25-44 (1995)

[D-N] C. DAWSON + M. NIELSEN
QUANT INF COMP 6 (2006)
81-95

[G-G-N] A. GHOSH, A. GORODNIK +
A. NEVO arXiv 1205.4426

[K-M] D. KLEINBOCK and K. MERRILL
arXiv 1301.0989

[HA] G. HARMAN JNL OF NUMBER THEORY 34, 63-81 (1990)

[K-M-M] V. KLIUCHNIKOV, D. MASLOV, M. MOSCA
arXiv 1212.6964.

[L-P-S] A. LUBOTZKY, R. PHILLIPS, P. SARNAK
COMM PURE AND APPLIED MATH
VOL XXXIX 149-186 (1986) and
VOL XL 401-420 (1987).

[R-S] N. ROSS, P. SELINGER
arXiv 1403.2975

[SA] P. SARNAK "NOTES ON THIN MATRIX GROUP"
MSRI PUBL. 61 (2014) 343-362.

[SC] R. SCHOOF MATH COMP 44 (1985) 483-494

[SE] J.P. SERRE "Le groupe quaquaversal, vu comme group S-arithmétique"

P. SARNAK Letter on Solovay Kitaev and Golden Gates
http://publications.ias.edu/sarnak/paper/2637.