STRONG APPROXMATION AND GOLDEN GATES

PETER SARNAK

CLASSICAL COMPUTING

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

GATES FOR CIRCUITS ACHIEVE ANY BOOLEAN $f:\{0,1\}^N \longrightarrow \{0,1\}$ VIA $\sim, \wedge$ etc.

COMPLEXITY IS THE SIZE OF THE CIRCUIT.

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 $G = PU(2)$ (NO PHASES).

A UNIVERSAL GATES SET $\mathcal{G}$ IS ONE WHICH GENERATES G TOPOLOGICALLY.

- n-QUBITS, $(\mathbb{C}^2)^{\otimes n}$ AND GATES ARE BUILT FROM THE 1-QUBIT GATES.

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

μ - HAAR MEASURE ON G

$B_r(x)$ BALL CENTERED AT x RADIUS r.

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

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

<u>SOLOVAY / KITAEV THEOREM (95):</u>
<u>EFFICIENT UNIVERSAL GATE SETS</u> EXIST.

TEXT BOOK GATES:

Hadamard	$-\boxed{H}-$	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Pauli-X	$-\boxed{X}-$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y	$-\boxed{Y}-$	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z	$-\boxed{Z}-$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Phase	$-\boxed{S}-$	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$	$-\boxed{T}-$	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

H AND S GENERATE A FINITE SUBGROUP OF G OF ORDER 24 - THE "CLIFFORD GATES".

THESE ALONE CAN BE SIMULATED WITH A CLASSICAL COMPUTER (CHEAP MEMBERS OF A CIRCUIT).

ADDING T TO H AND S GIVE A UNIVERSAL GATE SET.

ROSS-SELINGER (2014): GIVE AN OPTIMALLY EFFICIENT HEURISTIC ALGORITHM TO APPROXIMATE ANY DIAGONAL $A \in G$, WITH MINIMAL T-COUNT.

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

WITH THE CIRCUIT U

$$U = HTSHTSHT \,\ldots\ldots\ldots\ldots\ldots\, HTH$$

T-count is 102 (100 is optimal).

$\varepsilon = 10^{-20}$, T-count 200 (198 optimal).

$\varepsilon = 10^{-2000}$, T-count 19942 (19934 optimal)

"V-GATES" (ALL ARE SPECIAL CASES OF A GENERAL CONSTRUCTION LUBOTZKY-PHILLIPS-S 88)

$$V_1 = \frac{I + 2iX}{\sqrt{5}}, \quad V_2 = \frac{I + 2iY}{\sqrt{5}}, \quad V_3 = \frac{I + 2iZ}{\sqrt{5}}$$

Γ_{V_1, V_2, V_3} THE GROUP (GATES) GENERATED BY IS FREE. THE NUMBER N_t OF (REDUCED) WORDS OF LENGTH $\leq t$ IS

$$N_t = 6 \cdot 5^{t-1} \quad .$$

THE BASIC PROBLEM IS TO APPROXIMATE AN ARBITRARY $g \in G$ BY CIRCUITS OF MINIMAL AND SHORT LENGTH.

- ALGORITHM ; HERE WE SEEK SOMETHING LIKE A CONTINUED FRACTION ALGORITHM IN G

- HOW WELL DO THE GATES DO?

EUCLID AND CONTINUED FRACTIONS:

ACCORDING TO KNUTH AND NOW WIKIPEDIA "THE EUCLIDIAN ALGORITHM TO COMPUTE THE GCD IS ONE OF THE OLDEST ALGORITHMS THAT IS STILL USED"

- CLOSELY RELATED IS THE CONTINUED FRACTION ALGORITHM:

LET $\frac{a}{q} \in [0,1]$, $(a,q)=1$, $q \leq Q$ BE THE FAREY FRACTIONS OF ORDER Q.

THE CONITUED FRACTION ALGORITHM GIVES THE a/q CLOSEST TO $\alpha \in [0,1]$ (WHICH IS GIVEN) AND FAST, POLY(LOG Q).

BASED ON THE PROJECTIVE LINEAR TRANSFORMATIONS

$$S = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

WHICH GENERATE $SL_2(\mathbb{Z})$.

DIOPHANTINE ANALYSIS:

HOW WELL DO THESE Q^2 POINTS DO?

- RATIONALS WITH SMALL DENOMINATOR REPEL

$$\left|\frac{a}{q} - \frac{a'}{q'}\right| \geq \frac{1}{qq'} \qquad \left(\geq \frac{1}{Q^2}\right)$$

- BY DIRICHLET'S BOX PRINCIPLE — SHARP

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{qQ}, \text{ some } q \leq Q.$$

- MOST INTERVALS OF LENGTH $Q^{-2+o(1)}$ HAVE A FAREY POINT.

IT TURNS OUT THAT AT THE HEART OF NAVIGATING $PU(2)$ WITH "GOLDEN GATES" IS STRONG APPROXIMATION FOR QUADRICS IN A^4.

STRONG APPROXIMATION:

CONCERNED WITH THE DENSITY (REAL AND p-ADIC) OF INTEGER POINTS ON AFFINE VARIETIES.

HYPERSURFACES:

$$F(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$$

$$X_m : \qquad F(x) = m.$$

$X_m(\mathbb{Z})$ INTEGER SOLUTIONS.

FOR $q \geq 1$, $X_m(\mathbb{Z}) \xrightarrow{\text{mod } q} X_m(\mathbb{Z}/q\mathbb{Z})$.

DO WE GET ALL SOLUTIONS mod q? (p-ADIC DENSITY).

ARCHIMEDIAN DENSITY, SAY F IS HOMOGENEOUS DEGREE k; project

$$\frac{x}{m^{1/k}} \in X_1(\mathbb{R})$$

CAN WE APPROXMATE $\xi \in X_1(\mathbb{R})$ BY SUCH AS $m \to \infty$.

IN GENERAL THESE ARE HOPELESS PROBLEMS, EVEN WHETHER $X(\mathbb{Z}) \neq \emptyset$ HAS NO DECISION PROCEDURE. THE ONLY GENERAL METHOD TO PRODUCE MANY POINTS AND WITH IT STRONG APPROXIMATION IS THE HARDY-LITTLEWOOD CIRCLE METHOD. HOWEVER IT REQUIRES MANY VARIABLES COMPARED TO THE DEGREES. MUCH EFFORT IS PUT INTO REDUCING THE NUMBER OF VARIABLES (EG WOOLEY'S WORK FOR DIAGONAL F).

BALLS IN BOXES:

WHAT IS THE OPTIMAL FORM OF STRONG APPROXIMATION THAT ONE CAN ACHIEVE?

IF ONE PLACES N BALLS IN N-BOXES ONE HAS TO BE VERY CAREFUL TO HAVE EACH BOX OCCUPIED.

HOWEVER IF $\varepsilon > 0$, THEN PLACING $N^{1+\varepsilon}$ BALLS IN N-BOXES AT RANDOM WILL CAPTURE EACH BOX WITH HIGH PROBABILITY AS $N \to \infty$, AND ALMOST EVERY BOX WITH VERY HIGH PROB.

QUADRICS: $F(x_1, \ldots, x_n)$ IS AN INTEGRAL QUADRATIC FORM (MORE GENERALL "S-INTEGRAL" OVER A NUMBER FIELD K).

NO GO THEOREM (ADLEMAN-MANDERS 78)

(QUADRATIC EQUATIONS ARE COMPUTATIONALLY HARD)

GIVEN a, b, H POSITIVE INTEGERS THE PROBLEM: IS THERE AN INTEGER $0 \leq x \leq H$ SUCH THAT

$$x^2 \equiv a \pmod b$$

IS "NP - COMPLETE"

AND THIS IS SO EVEN IF ONE CAN FACTOR QUICKLY !

(THE LATTER IS SOMETHING WE WILL ASSUME WE CAN DO).

TWO VARIABLES

$$x_1^2 + x_2^2 = m$$

OR INDEFINITE

IE A **TORUS**

$$X : \; x^2 - 2y^2 = 1$$

$X(\mathbb{Z})$ IS IS INFINITE AND A GROUP (CYCLIC)

TORI NEVER OBEY STRONG APPROXIMATION (BASICALLY: 2 IS NOT A PRIMITIVE ROOT MOD MANY P'S).

ALGORITHMIC:

FERMAT: $x_1^2 + x_2^2 = p$, p AN ODD PRIME HAS A SOLUTION IFF $p \equiv 1 (4)$.

CAN WE FIND x_1, x_2 QUICKLY ?

YES! (SCHOOF 85) IN POLY(LOG P) STEPS!

$$x_1^2 + x_2^2 = m$$

FACTOR $m = p_1^{e_1} \cdots p_k^{e_k}$

SOLVE FOR EACH FACTOR $p_j^{e_j}$ THEN MULIPLY IN $\mathbb{Z}[\sqrt{-1}]$.

- HOWEVER IF m HAS MANY PRIME FACTORS THERE CAN BE MORE THAN POLY(LOG m) SOLUTIONS AND THE PROBLEM OF FINDING THE CLOSEST ONE TO A POINT (ξ_1, ξ_2) SUFFERS THE SAME FATE AS WITH A-M.

THREE VARIABLES

$$X_m : \; x_1^2 + x_2^2 + x_3^2 = m > 0$$

$m \neq 4^a(8b+7)$ THEN $X_m(\mathbb{Z}) \neq 0$

GAUSS (1800).

$$N(m) = |X_m(\mathbb{Z})| \qquad \text{SUBTLE}$$

$N(m) \to \infty$ AS $m \to \infty$
HEILBRONN (1934)

$N(m) = m^{\frac{1}{2}+o(1)}$; SIEGEL — INEFFECTIVE!

HOW DO THE PROJECTIONS DISTRIBUTE THEMSELVES (IE $\frac{x}{\sqrt{m}}$) ON S^2?

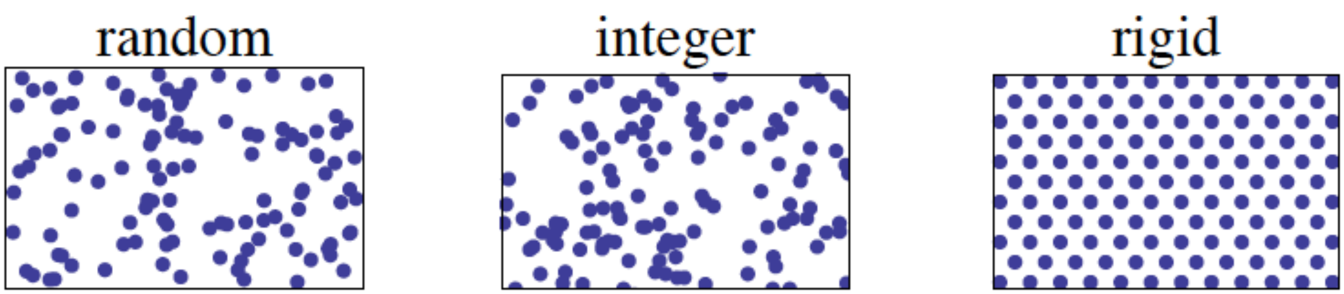

Figure 1. Lattice points coming from the prime $n = 1299709$ (center), versus random points (left) and rigid points (right). The plot displays an area containing about 120 points.

THEOREM (DUKE 87):

THESE $N(m)$ POINTS BECOME DENSE AS $m \to \infty$.

HOW DENSE ?

BOURGAIN - RUDNICK - S (2014):
CONJECTURE WITH SOME EVIDENCE THAT THESE POINTS BEHAVE LOCALLY LIKE RANDOM POINTS (N OF THEM) SO THAT THE COVERING RADIUS IS $N^{-1/2 + o(1)}$ (THE BALL RADIUS ε IN S^2 HAS VOL $c\varepsilon^2$, SO "ε^{-2} BOXES").
IE OPTIMALLY SMALL !

• (B-R-S): ASSUME THE RIEMANN HYPOTHESIS FOR GL_2 AUTOMORPHIC L-FUNCTIONS, THE ALMOST ALL $\xi \in S^2$ HAVE A POINT FROM X_m IN $B(\xi, N^{-1/2+o(1)})$, OPTIMAL !

ALGORITHM: (ADAPTION OF ROSS SELINGER) ROOTS IN WORK OF PETIT, LAUTER, QUASQUATER

FINDING THE POINT IN $X_m(\mathbb{Z})$ CLOSEST TO ANY GIVEN ξ IS HARD (NP COMPLETE), BUT GIVEN $\xi = \frac{a}{|a|}$ WITH $(a_1, a_2, a_3) \in \mathbb{Z}^3$ FIXED OR SMALL ($\log m$ IN SIZE) AND $\varepsilon > 0$ DETERMINES IF THERE IS A POINT OF $X_m(\mathbb{Z})$ IN $B(\xi, \varepsilon)$. IF ONE CAN FACTOR QUICKLY AND ASSUMES SOME HEURISTICS ABOUT PRIMES THE ALGORITHM RUNS IN POLY($\log 1/\varepsilon$).

IDEA: SAY $(a_1, a_2, a_3) = (1, 0, 0)$

$$d^2\left(\frac{(x_1, x_2, x_3)}{\sqrt{m}}, (1, 0, 0)\right) < \varepsilon^2$$

$$\sqrt{m} - x_1 \lessapprox N\varepsilon^2.$$

So for each such x_1 solve

$$m - x_1^2 = x_2^2 + x_3^2 \quad \ldots$$

FOUR VARIABLES

$X_m: \; x_1^2 + x_2^2 + x_3^2 + x_4^2 = m > 0$

Lagrange $\quad X_m(\mathbb{Z}) \neq \phi$

Jacobi: $\; N = |X_m(\mathbb{Z})| \approx m$.

ALGORITHM: (ROSS-SELINGER)

Given $\xi = (\xi_1, \xi_2, 0, 0) \in S^3$ and $\varepsilon > 0$ determines if there is an $x \in X_m$ s.t. $\frac{x}{\sqrt{m}} \in B_\varepsilon(\xi)$ and provides one such x if there is one. Assuming that one can factor quickly and some strong heuristics about primes in certain sets, Their algorithm runs in $\text{poly} \log 1/\varepsilon$ steps.

While the heuristics assumptions are very strong, they are no doubt true for most ξ as above which is why there algorithm works in practice.

DIOPHANTINE ANALYSIS:

(FOLLOWS L-P-S ANALYSIS USING THE RAMANUJAN CONJECTURES)

(i) EVERY BALL B IN S^3 OF RADIUS $N^{-1/6}$ CONTAINS A POINT OF $X_m(\mathbb{Z})$.

(ii) "Almost all points $\xi \in S^3$ have an $x \in X_m(\mathbb{Z})$ in $B_\varepsilon(\xi)$ with

$$\varepsilon = N^{-1/3+o(1)} \quad \text{(OPTIMAL!)}$$

(iii) THERE ARE BIG HOLES IE. POINTS $\eta \in S^3$ FOR WHICH $B_\varepsilon(\eta)$ HAS NO POINTS FROM $X_m(\mathbb{Z})$ WITH $\varepsilon = N^{-1/4}$

CONJECTURE: THE COVERING RADIUS IS $N^{-\frac{1}{4}+o(1)}$.

FIVE OR MORE VARIABLES

N. SARDARI (PRINCETON THESIS 2016) HAS DETERMINED THE EXACT COVERING EXPONENT FOR STRONG APPROXIMATION FOR ANY INTEGRAL QUADRATIC FORM F.

GHOSH - GORODNICK - NEVO HAVE DEVELOPED A THEORY OF DIOPHANTINE APPROXIMATION FOR HOMOGENEOUS VARIETIES FOR LINEAR ALGEBRAIC GROUPS. ("S - ARITHMETIC ORBITS")

CUBICS

FOR HOMOGENEOUS CUBIC FORMS F

$X : F(x) = 0$ (PROJECTIVE)

THE SEARCH FOR RATIONAL POINTS AND STRONG APPROXIMATION IS A VERY ACTIVE TOPIC.

SEE THE 2014 SURVEY BY BROWNING AND IN PARTICULAR WORKS OF HEATH-BROWN, SWINNERTON-DYER, BROWNING, SKOROBOGATOV, ...

OUR INTEREST IS IN INTEGRAL POINTS ON AFFINE CUBIC SURFACES IN $\mathbb{A}^3$

(IN $\mathbb{A}^2$ THERE ARE ONLY FINITELY MANY INTEGRAL POINTS — SIEGEL, IN $\mathbb{A}^3$ WE EXPECT FEW INTEGRAL POINTS IN GENERAL; VOJTA CONJECTURES)

<u>EG</u>: $$X_m \ : \ x_1^3 + x_2^3 + x_3^3 = m \ .$$

IF $m \not\equiv 4$ or $5 \pmod 9$, PERHAPS $|X_m(\mathbb{Z})| = \infty$. HOWEVER THE STRONGEST FORMS OF STRONG APPROXIMATION FAILS (CASSELS, HEATH-BROWN, COLLIOT-THELENE/WITTENBERG)

MARKOFF SURFACES:

$$X_k \ : \ x_1^2 + x_2^2 + x_3^2 - 3x_1 x_2 x_3 = k$$

AFFINE CUBIC SURFACES.

$$X_0 : x_1^2 + x_2^2 + x_3^2 - 3x_1x_2x_3 = 0$$

$X_0(\mathbb{Z})$ IS INFINITE ; THE GROUP Γ OF NONLINEAR AFFINE MORPHISIMS OF A^3 GENERATED BY PERMUTATIONS, VIETA INVOLUTIONS $(x_1, x_2, x_3) \to (x_1, x_2, 3x_1x_2 - x_3)$ AND $(x_1, x_2, x_3) \to (-x_1, -x_2, x_3)$, HAS TWO ORBITS ON $X_0(\mathbb{Z})$, $\{(0,0,0)$, $(1,1,1)$.

<u>CONJECTURE</u> (STRONG APPROXIMATION) BOURGAIN-GAMBURD-S

$X_0(\mathbb{Z}) \longrightarrow X_0(\mathbb{Z}/p\mathbb{Z})$ IS ONTO FOR ALL PRIMES p.

<u>THEOREM</u> (B-G-S 2015): THE SET OF PRIMES $p \leq T$ FOR WHICH STRONG APPROXMATION FAILS IS $O_\varepsilon(T^\varepsilon)$, $\varepsilon > 0$.

- THE TECHNIQUES INVOLVE NONLINEAR DYNAMICS, COMINATORICS, ...

CRITICAL TO THE ANALYSIS IS THE DETERMINATION OF THE FINITE ORBITS OF Γ IN $A^3(\mathbb{C})$. THIS IS CLOSELY CONNECTED TO THE CLASSIFICATION OF ALGEBRAIC PAINLEVE $\overline{\underline{VI}}$!

BACK TO OPTIMAL UNIVERSAL QUANTUM GATES

$\mathbb{H}$ HAMILTON QUATERNIONS

$$x_1 + x_2 \underline{i} + x_3 \underline{j} + x_4 \underline{k}$$

$\alpha \in \mathbb{H}(\mathbb{R})$, $\mathrm{Norm}(\alpha) = \bar{\alpha}\alpha = x_1^2 + x_2^2 + x_3^2 + x_4^2$.

$\mathbb{H}(\mathbb{Z})$ INTEGRAL QUATERNIONS

THESE HAVE UNIQUE FACTORIZATION (NON-COMMUTATIVE!) (HURWITZ).

$v_1 = 1 + 2\underline{i}$, $v_2 = 1 + 2\underline{j}$, $v_3 = 1 + 2\underline{k}$

then up to units the elements of $\mathbb{H}(\mathbb{Z})$ of Norm $= 5$ are $v_1, v_2, v_3, \bar{v}_1, \bar{v}_2, \bar{v}_3$.

$$\alpha \longrightarrow \begin{bmatrix} x_1 + ix_2 & x_2 + ix_3 \\ -x_2 + ix_3 & x_1 - ix_2 \end{bmatrix}$$

is a morphism of $\mathbb{H}_1(\mathbb{R}) \longrightarrow SU(2)$.

$$\frac{1}{\sqrt{5}} v_j \longrightarrow V_j \quad \text{the "V gates".}$$

ALL ELEMENTS OF $H(\mathbb{Z})$ OF NORM 5^k ARE PRODUCTS (ESSENTIALLY UNIQUELY) OF $v_1, v_2, v_3, \bar{v}_1, \bar{v}_2, \bar{v}_3$.

<u>KEY POINT:</u> IF $Nm(\alpha) = 5^k$ THE THE FACTORIZATION OF α AS A PRODUCT OF k OF THE v_j'S CAN BE DETERMINED EFFICIENTLY BY FACTORIZATION IN $H(\mathbb{Z})$!

THE CIRCUITS FORMED FROM $V_1, V_3, \cdot V_3^{-1}$ OF LENGTH k ARE IN BIJECTION WITH

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

$SU(2)$ WITH ITS INVARIANT METRIC IS ISOMETRIC WITH S^3; $\xi_1^2 + \xi_2^2 + \xi_3^2 + \xi_4^2 = 1$.

HENCE GIVEN $g \in SU(2)$ TO BE APPROXIMATED BY CIRCUITS OF LENGTH $\leq t$ AMOUNTS TO FINDING SOLUTIONS x WITH $d\left(\frac{x}{5^{k/2}}, \xi_g\right) < \varepsilon$.

- FOR g DIAGONAL, ROSS-SELINGER GIVES SUCH AN x.

MOREOVER THE DIOPHANTINE ANALYSIS ENSURES THAT MOST g'S HAVE AN OPTIMALLY SHORT CIRCUIT!

FOR A GENERAL $g \in SU(2)$ FIRST FACTOR $g = a_1 a_2 a_3$ IN DIAGONALS (EULER ANGLES) AND APPROXIMATE EACH a_j. THIS YIELDS A CIRCUIT WHICH IS 3-TIMES LONGER THAN OPTIMAL.

- EXCEPT FOR THE LAST THIS GIVES AN OPTIMAL NAVIGATION SCHEME OF SU(2) WITH V-GATES.

THE CLIFFORD + T GATES ARE A VARIANT OF THE ABOVE. THAT THE GROUP (UNITARY) GENERATED BY THEM HAS A NUMBER THEORETIC DEFINITION IS DUE TO KLICHNIKOV-MASLOV-MOSCA (2012)
BOCHAROV-GUREVICH-SVORE (2012)

IT IS ANOTHER SPECIAL CASE OF A CONSTRUCTION VIA INTEGRAL QUATERNIONS.

H HAMILTON QUATERNIONS / K

$K = \mathbb{Q}(\sqrt{2})$, O_K INTEGERS IN K.

THE PRIME 5 IN THE V-GATES IS REPLACED BY THE PRIME $\sqrt{2}$ IN O_K.

AGAIN (REMARKABLY) THE T-COUNT OF CIRCUITS IS k WHERE

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

WITH $x_j \in O_K$!

SO THE ALGORITHMS AND DIOPHANTINE ANALYSIS PROCEED AS BEFORE.

[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 GROUPS" MSRI PUBL. 61 (2014) 343-362.

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

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

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