ARITHMETIC GOLDEN GATES: PROBLEM SESSION

Problem 1. For the V-basis $\left\{\frac{1 \pm 2i}{\sqrt{5}} P : P = X, Y, Z\right\}$ with X, Y, Z the Pauli spin matrices, is there an algorithm that takes as input:

- $U \in SU(2)$ to some precision, and
- $\epsilon > 0$,

produces as output a sequence of elements $U_1, \ldots, U_\ell$ from the V-basis such that

$$\|U - U_1 \cdots U_\ell\|_2 < \epsilon$$

and $\ell \leq \beta \log_5(1/\epsilon) + c$ (for a fixed constant c) with $\beta = 4$ in the worst case and $\beta = 3$ in the average case.

(1) In order to not lose precision, we should work with the elements of the V-basis over $\mathbb{Q}(i, \sqrt{5})$ using exact arithmetic.
(2) Does input preceision for the input matrix $U \in SU(2)$ matter? An oracle model for complex arithmetic may work. Perhaps all of the ways of working with real numbers are equivalent: errors in the entries of the matrix would affect the norm by a bounded amount, so one can specify the entries of the matrix to enough precision.
(3) The norm $\| \|_2$ could be replaced by a different norm, but this would surely only affect the constant c.
(4) There is a provable lower bound for the average case: for almost all U, the constant is $\beta = 3$. There are examples with a worst case with constant $\beta = 4$ ("large holes", see also below).
(5) For U general, there is an algorithm by Lubotzky–Phillips–Sarnak with constant $\beta = 6$ and a heuristic algorithm for constant $\beta = 9$.
(6) The basis is chosen for simplicity (and is natural for quantum spin states), but the question makes sense for other bases. Does there exist a basis where we can take the constant $\beta = 3$ as worst case? These would be optimal: a random set of generators would likely allow us to write elements with this constant, but probably without an explicit algorithm. (From this point of view, what are the "worst generators"?)
(7) In general, we should also include cost functions that depend on the expense (measured by quantum physics) for the gates used. These factors would depend on quantum engineering, which may change over time—so we may want to leave this as variable.
(8) The constant 3 arises as the dimension of the sphere, and the base of the logarithm 5 comes from counting the rate of growth of the number of distinct group elements with bounded length. The number 4 comes the meniscus: in the worst case, the meniscus could be parallel to the lattice, and this is more restrictive. The constants 3 and 4 are perhaps "universal" for $SU(2)$?

Problem 2. A "hole" is a region where the approximation in terms of generators is worse than the average. For Clifford+T, where are the large holes? These would require $4\log_2(1/\epsilon)$ matrices to estimate.

Is it true that outside these holes, the constant is 3 (as $1/\epsilon \to \infty$).

For diagonal entries (rotation by θ), are the holes are when the angle θ is such that $\tan(\theta/2) \in \mathbb{Q}(\sqrt{2})$?

(1) The set of holes have measure zero, but they are still dense.
(2) In terms of Ramanujan graphs, this question asks: how many vertices are far from a given vertex? Computing shortest vectors gives distance to the identity; this distance is related to the distribution of points on quadrics.
(3) Can we prove that random sets of generators have no holes?
(4) What are the "best generators", those without holes? The best possible result would be "no holes": then the answer to Problem 1 for these generators would have $\beta = 3$ in all cases. Perhaps this holds for random generators! How close can you get with deterministically constructed generators?
(5) How do we measure the quality of the generators (measurement of "best")?
(6) In the short length words, for some reason they are repelling—so the sequence approaches these points more slowly than other points. For example, on the circle, zero is such a point; points with small denominator repel other rationals. So whatever is happening here is very reminiscent of what begins in the circle method. This is a more general phenomenon with small height algebraic numbers repel large height algebraic numbers. It's not clear if this phenomenon holds for all groups.
(7) Here we care first about existence; then later, algorithmic issues.

Problem 3. What is the best exponent for strong approximation for integral quadratic forms in 4 variables?

To be more precise, let Q be a positive definite integral quadratic form in 4 variables. Let $x_1, \dots, x_4 \in \mathbb{R}$ be such that $Q(x_1, \dots, x_4) = n$. We seek $u_1, \dots, u_4 \in \mathbb{Z}$ such that $Q(u_1, \dots, u_4) = n$ such that $|x - u| = n^\alpha$ is minimal. What is the minimum exponent α?

(1) The exponent $\alpha = 1/4$ is a lower bound, due to Wright from 1937. The basic problem arises for Clifford+T: can you write an integer n as the sum of four squares with all entries approximately $n^{1/2}$? What is the smallest interval where the diophantine equation has a solution? If more generally, we ask the same question for an integral quadratic form $f(x_1, \dots, x_d) = n$, we may ask about repulsion of integral points. If the gradient has a small integral vector norm, then you have holes. Whenever the orbits are described by quadratic forms, this phenomenon will arise.
(2) There are existence and deterministic algorithm versions of this problem.
(3) Under a conjecture on quadratic forms like this one, what is the precise relationship towards the constant in Problem 1? (Sarnak's letter addresses aspects of this.)
(4) For applications, we only care about n a power of a fixed prime element (or several, for the S-arithmetic groups). Perhaps this special case has a better answer than the general case. The answer is probably also different if n is restricted to be a prime versus a product of elements of a fixed size.

Problem 4. Turning this setup around, can you specify sets of generators that guarantee hard instances for the approximation problem? In other words, can you find a family of finite groups (or an S-arithmetic group and its finite quotients) and a set of generators such that finding short paths in the Cayley graph is provably hard?

(1) LPS is now known to be not hard ($\mathrm{SL}_2(\mathbb{F}_p)$ with specified generators); but there are still proposals for Cayley graphs that are supposedly still hard.
(2) An instance: supersingular ℓ-isogeny graphs; this graph is known to be isomorphisc to the LPS graph, but it is not known if this isomorphism is efficiently computable. Can it be found? Can we translate LPS to this case? The issue is to efficiently associate a given maximal order to a supersingular curve.
(3) We would put ourselves in the situation where theoretically there is a solution (short path) known, but algorithmically it would be hard to find.

Problem 5. Find better algorithms for exact synthesis ("efficiently finding a short word, with respect to some metric") for S-arithmetic gate sets for *two or more* qubits. And same question for approximate synthesis (again, with two or more qubits).

Problem 6. What is the connection between approximate synthesis and diophantine approximation, continued fractions, and versions of the Euclidean algorithm? Relating questions in each world might be useful.

(1) Is there an analogue of the Euclidean algorithm in more general settings? These approaches seem also to work in cryptographic contexts?
(2) The sphere or the unitary group is only one example: the theory of diophantine approximation thinks more generally about rational or S-arithmetic groups for homogeneous algebraic varieties associated to a (semi-)simple group. There are cases where the *almost sure* exponent is provably correct, and twice this exponent is universal. (These are existential aspects.) See for example `https://arxiv.org/abs/1401.6581`.
(3) A closest approximation to a rational number is given by convergents in the continued fraction, with very good approximations obtained by cutting off with large terms. Is there a similar thing for words in $SU(2)$, are there "repelling words" (their neighborhoods fill less quickly?)? This is related to the issues with holes: algebraic numbers of small height cannot be close together?

Problem 7. There are heuristic assumptions involved in the distribution of integers arising in exact synthesis and their prime factorizations. Can these be proven, or reduced to a standard conjecture?

Problem 8. What is the relationship to synthesis for "repeat-until-success" computational model? If you allow in a quantum circuit certain steps of measurement, then you can shorten the circuit and number-theoretic methods (should) again apply.

Problem 9. What is the generalization of optimal strong approximation for an arbitrary Hermitian lattice? In particular, with four or more variables over a number field?

Problem 10. Are the super golden gates physically feasible as transversal operation on a suitably designed quantum code? What specific conditions are required for fault-tolerant gate sets?

Problem 11. Consider more generally S-arithmetic groups where the places at infinity are split (but the group is still S-indefinite)? How well do hyperbolic generators in a ball distribute when they are considered in the unitary setting?

(1) For the generators obtained in this way, the connection to physics (e.g., costs of gates) is not clear, so they would be much farther off in the future.