Advances in Mathematics ••• (••••) •••–•••

Contents lists available at ScienceDirect

Advances in Mathematics

www.elsevier.com/locate/aim

Super-Golden-Gates for $PU(2)$

Ori Parzanchevski *, Peter Sarnak

ARTICLE INFO

Article history:
Available online xxxx

To David Kazhdan with admiration

Keywords:
Ramanujan conjectures
Strong approximation
Unitary groups
Quantum computing

ABSTRACT

To each of the symmetry groups of the Platonic solids we adjoin a carefully designed involution yielding topological generators of $PU(2)$ which have optimal covering properties as well as efficient navigation. These are a consequence of optimal strong approximation for integral quadratic forms associated with certain special quaternion algebras and their arithmetic groups. The generators give super efficient 1-qubit quantum gates and are natural building blocks for the design of universal quantum gates.

1. Introduction

The n-qubit circuits used for quantum computation are unitaries in $U\left(\left(\mathbb{C}^2\right)^{\otimes n}\right) = U(2^n)$ which are products of elementary unitaries, each of which operates on a fixed (typically at most 3) number of qubits. The standard universal gate set for quantum computing consists of all 1-qubit unitaries i.e. $U(2)$ (which can be applied to any of the single qubits) and the 2-bit XOR gate, together these generate $U(2^n)$ ([32]). In a classical computer the only operations on a single bit are to leave it or flip it. In the quantum setting we can rotate by these 2×2 unitaries.

* Corresponding author.
E-mail addresses: parzan@math.huji.ac.il (O. Parzanchevski), sarnak@math.princeton.edu (P. Sarnak).

http://dx.doi.org/10.1016/j.aim.2017.06.022

To further reduce to a finite universal gate set one has to settle for a topologically dense set, and since overall phases do not matter it suffices to find "good" topological generators of $G = PU(2)$. The Solovay–Kitaev algorithm [32] ensures that any fixed topological generators of G have reasonably short words (i.e. circuits) to approximate any $x \in G$ (with respect to the bi-invariant metric $d^2(x,y) = 1 - \frac{|\mathrm{trace}(x^*y)|}{2}$). From the point of view of general polynomial type complexity classes this is sufficient, however there is much interest ([32,21,20]) both theoretical and practical, to optimize the choice of such generators.

Golden-Gates ([45]) which correspond to special arithmetic subgroups of unit quaternions and which were introduced as optimal generating rotations in [30], yield variants of optimal generators. A particular case is the "Clifford plus T" gates described below and which appear in most textbooks. The Clifford gates form a finite subgroup C_{24} of order 24 in G and to make the set universal one needs to add an extra element of G. The popular choice is the order 8 element $T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{smallmatrix}\right)$. That these generate an S-arithmetic group was shown in [21], see also [45].

Considerations of fault-tolerance when applying these to make circuits in $U(2^n)$, require among other things that the universal gate set consists of elements of finite order. Moreover for the Clifford plus T gates, the applications of the c gates with $c \in C_{24}$ in a circuit are considered to be of small cost compared to T ([6,3]). This leads to the "T-count" being the measure of complexity of a word and to the problem that we consider in this note:

To find universal gate sets (i.e. ones that are topological generators of G) which are of the form a finite group C in G together with an extra element τ, which we take to be an involution, so that C plus τ is optimal with respect to covering G with a small τ-count, and at the same time to be a able to navigate G efficiently with these gates.

The key feature that was needed for a Golden-Gate construction[1] was that the corresponding S-arithmetic unit quaternion group act transitively on the vertices of the corresponding $(q+1)$-regular tree (here q is a prime power). The extra "miracle" that is needed here is that the group act transitively on the edges. With this extra requirement there are only finitely many such "Super-Golden-Gates", see Section 3. We list some of them; in each case the finite group C is naturally a subgroup of the symmetries of a platonic solid:

(1) Pauli plus τ (Cube)

$$C_4 = \left\langle \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle, \text{ the 4-group of Pauli matrices}$$

$$\tau_4 = \begin{pmatrix} 1 & 1-i \\ 1+i & -1 \end{pmatrix}.$$

[1] See (3.11) in Section 3 for the precise definition of a Golden Gate set.

Please cite this article in press as: O. Parzanchevski, P. Sarnak, Super-Golden-Gates for $PU(2)$, Adv. Math. (2017), http://dx.doi.org/10.1016/j.aim.2017.06.022