On Golden Gates and Discrepancy

Examining the Efficiency of Universal Gate Sets

Brent Mode

University of Louisville

August 6, 2017

Advisor: Dr. Steven Damelin

UNIVERSITY OF MICHIGAN

Quantum Computation v. Classical Computation

Classical Computation

- Classical computers, or just computers, rely on Boolean logic gates to execute programs.

Quantum Computation v. Classical Computation

Classical Computation

- Classical computers, or just computers, rely on Boolean logic gates to execute programs.
- All classical programs are formed from a combination of AND, OR, and NOT gates.

Quantum Computation v. Classical Computation

Classical Computation

- Classical computers, or just computers, rely on Boolean logic gates to execute programs.
- All classical programs are formed from a combination of AND, OR, and NOT gates.
- These programs are synthesized exactly, since the spectrum of possible programs is discrete.

Quantum Computation v. Classical Computation

Classical Computation

- Classical computers, or just computers, rely on Boolean logic gates to execute programs.
- All classical programs are formed from a combination of AND, OR, and NOT gates.
- These programs are synthesized exactly, since the spectrum of possible programs is discrete.
- In other words, if you can dream it, it can be done exactly.

Quantum Computation v. Classical Computation

Quantum Computation

- Quantum computing utilizes a quantum system consisting of two discrete states, $|0\rangle$ and $|1\rangle$.

Quantum Computation v. Classical Computation

Quantum Computation

- Quantum computing utilizes a quantum system consisting of two discrete states, $|0\rangle$ and $|1\rangle$.
- Thus, a single qubit is in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

Quantum Computation v. Classical Computation

Quantum Computation

- Quantum computing utilizes a quantum system consisting of two discrete states, $|0\rangle$ and $|1\rangle$.
- Thus, a single qubit is in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.
- While a classical logic gate takes one or two inputs and returns a single output, a quantum logic gate acts as a linear map on $|\psi\rangle$.

Quantum Computation v. Classical Computation

Quantum Computation

- Quantum computing utilizes a quantum system consisting of two discrete states, $|0\rangle$ and $|1\rangle$.
- Thus, a single qubit is in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.
- While a classical logic gate takes one or two inputs and returns a single output, a quantum logic gate acts as a linear map on $|\psi\rangle$.
- A 1-qubit quantum gate X acts on $|\psi\rangle$ to produce $|\psi'\rangle$.

Quantum Computation v. Classical Computation

Quantum Computation

- Quantum computing utilizes a quantum system consisting of two discrete states, $|0\rangle$ and $|1\rangle$.
- Thus, a single qubit is in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.
- While a classical logic gate takes one or two inputs and returns a single output, a quantum logic gate acts as a linear map on $|\psi\rangle$.
- A 1-qubit quantum gate X acts on $|\psi\rangle$ to produce $|\psi'\rangle$.
- While classical logic gates are discrete, X can be any 2×2 matrix such that, since $|\psi|^2 = 1$, then $|\psi'|^2 = 1$.

An Unfortunate Number of Definitions

- *Unitary Group* - The group of all 1-qubit quntum gates is defined as: $U(2) = \{X \in GL_2(\mathbb{C}) | X^\dagger X = I\}$.

An Unfortunate Number of Definitions

- *Unitary Group* - The group of all 1-qubit quntum gates is defined as: $U(2) = \{X \in GL_2(\mathbb{C}) | X^\dagger X = I\}$.
- *Special Unitary Group* - This can be simplified by the mapping $\dfrac{X}{\sqrt{|X|}}$ to be: $SU(2) = \{X \in U(2) | \det X = 1\}$.

An Unfortunate Number of Definitions

- *Unitary Group* - The group of all 1-qubit quntum gates is defined as: $U(2) = \{X \in GL_2(\mathbb{C}) | X^\dagger X = I\}$.
- *Special Unitary Group* - This can be simplified by the mapping $\frac{X}{\sqrt{|X|}}$ to be: $SU(2) = \{X \in U(2) | \det X = 1\}$.
- *Projective Special Unitary Group* - Further, for quantum gates it is also valid to view the gates X and $-X$ as the same, which leads us to: $PSU(2) = SU(2)/Z(SU(2))$.

An Unfortunate Number of Definitions

- *Unitary Group* - The group of all 1-qubit quntum gates is defined as: $U(2) = \{X \in GL_2(\mathbb{C}) | X^\dagger X = I\}$.
- *Special Unitary Group* - This can be simplified by the mapping $\dfrac{X}{\sqrt{|X|}}$ to be: $SU(2) = \{X \in U(2) | \det X = 1\}$.
- *Projective Special Unitary Group* - Further, for quantum gates it is also valid to view the gates X and $-X$ as the same, which leads us to: $PSU(2) = SU(2)/Z(SU(2))$.
- *Metric on* $SU(2)$ - We need to define a notion of distance on $SU(2)$, so we use the invariant metric, $d^2_{SU(2)}(X, Y) = 1 - \dfrac{Tr|X^\dagger Y|}{2}$, where $d : SU(2) \to \mathbb{R}_{\geqslant 0}$.

The Problem at Hand

- The difficulty in quantum computing is the overwhelming number of possible programs available to us as quantum logic gate circuits.

Quantum Computation Theory

The Problem at Hand

- The difficulty in quantum computing is the overwhelming number of possible programs available to us as quantum logic gate circuits.
- Unlike in classical computing, it is impossible to exactly synthesize every possible program using a handful of gates.

Quantum Computation Theory

The Problem at Hand

- The difficulty in quantum computing is the overwhelming number of possible programs available to us as quantum logic gate circuits.
- Unlike in classical computing, it is impossible to exactly synthesize every possible program using a handful of gates.
- This is the same problem that occurs when comparing the rational numbers to the real numbers.

Quantum Computation Theory

The Problem at Hand

- The difficulty in quantum computing is the overwhelming number of possible programs available to us as quantum logic gate circuits.
- Unlike in classical computing, it is impossible to exactly synthesize every possible program using a handful of gates.
- This is the same problem that occurs when comparing the rational numbers to the real numbers.
- What is needed is a way to approximate every element of $SU(2)$ using a circuit built from a small set of specially chosen quantum gates.

The Problem at Hand

- The difficulty in quantum computing is the overwhelming number of possible programs available to us as quantum logic gate circuits.
- Unlike in classical computing, it is impossible to exactly synthesize every possible program using a handful of gates.
- This is the same problem that occurs when comparing the rational numbers to the real numbers.
- What is needed is a way to approximate every element of $SU(2)$ using a circuit built from a small set of specially chosen quantum gates.
- The problem is then two-fold: Find a good gate set and come up with an approximation algorithm.

An Example Universal Gate Set

- A universal gate set is a 'good' gate set: The group generated by the elements in the set is dense in $SU(2)$.

An Example Universal Gate Set

- A universal gate set is a 'good' gate set: The group generated by the elements in the set is dense in $SU(2)$.
- My work has focused on the set T that is defined below: $T = \{s_1, s_2, s_3, s_1^{-1}, s_2^{-1}, s_3^{-1}, I, iX, iY, iZ\}$, where $s_1 = \dfrac{1}{\sqrt{5}}(I + 2iX), s_2 = \dfrac{1}{\sqrt{5}}(I + 2iY), s_3 = \dfrac{1}{\sqrt{5}}(I + 2iZ)$, and X, Y, and Z are the Pauli matrices.

An Example Universal Gate Set

- A universal gate set is a 'good' gate set: The group generated by the elements in the set is dense in $SU(2)$.
- My work has focused on the set T that is defined below: $T = \{s_1, s_2, s_3, s_1^{-1}, s_2^{-1}, s_3^{-1}, I, iX, iY, iZ\}$, where $s_1 = \frac{1}{\sqrt{5}}(I + 2iX), s_2 = \frac{1}{\sqrt{5}}(I + 2iY), s_3 = \frac{1}{\sqrt{5}}(I + 2iZ)$, and X, Y, and Z are the Pauli matrices.
- These elements are combined to form reduced words of increasing length, with iX, iY, and iZ then inserted at the front to quadruple the number of elements of a certain length.

An Example Universal Gate Set

- A universal gate set is a 'good' gate set: The group generated by the elements in the set is dense in $SU(2)$.
- My work has focused on the set T that is defined below: $T = \{s_1, s_2, s_3, s_1^{-1}, s_2^{-1}, s_3^{-1}, I, iX, iY, iZ\}$, where $s_1 = \frac{1}{\sqrt{5}}(I + 2iX), s_2 = \frac{1}{\sqrt{5}}(I + 2iY), s_3 = \frac{1}{\sqrt{5}}(I + 2iZ)$, and X, Y, and Z are the Pauli matrices.
- These elements are combined to form reduced words of increasing length, with iX, iY, and iZ then inserted at the front to quadruple the number of elements of a certain length.
- We say that $\Omega = \langle T \rangle$ is the group generated by T.

An Example Universal Gate Set

- A universal gate set is a 'good' gate set: The group generated by the elements in the set is dense in $SU(2)$.
- My work has focused on the set T that is defined below: $T = \{s_1, s_2, s_3, s_1^{-1}, s_2^{-1}, s_3^{-1}, I, iX, iY, iZ\}$, where $s_1 = \frac{1}{\sqrt{5}}(I + 2iX), s_2 = \frac{1}{\sqrt{5}}(I + 2iY), s_3 = \frac{1}{\sqrt{5}}(I + 2iZ)$, and X, Y, and Z are the Pauli matrices.
- These elements are combined to form reduced words of increasing length, with iX, iY, and iZ then inserted at the front to quadruple the number of elements of a certain length.
- We say that $\Omega = \langle T \rangle$ is the group generated by T.
- Then $V(t)$ is defined as the set of elements in Ω of length at most t.

Connection to Discrepancy

A Different Way to Approach the Problem

- Recall that $PSU(2)$ is just as valid a group for representing gates as $SU(2)$.

A Different Way to Approach the Problem

- Recall that $PSU(2)$ is just as valid a group for representing gates as $SU(2)$.
- It is interestingly the case that $PSU(2) \approx SO(3)$ and that $SU(2) \approx S^3$, where the $SO(3)$ is the rotation group of the sphere S^2, the first relation is by isomorphism, and the second relation is by diffeomorphism.

Connection to Discrepancy

A Different Way to Approach the Problem

- Recall that $PSU(2)$ is just as valid a group for representing gates as $SU(2)$.
- It is interestingly the case that $PSU(2) \approx SO(3)$ and that $SU(2) \approx S^3$, where the $SO(3)$ is the rotation group of the sphere S^2, the first relation is by isomorphism, and the second relation is by diffeomorphism.
- Thus, it follows that elements of Ω correspond to solutions to: $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 5^t$, and can be projected onto the sphere.

Connection to Discrepancy

A Different Way to Approach the Problem

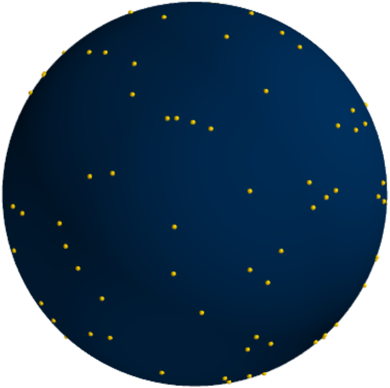
- Recall that $PSU(2)$ is just as valid a group for representing gates as $SU(2)$.
- It is interestingly the case that $PSU(2) \approx SO(3)$ and that $SU(2) \approx S^3$, where the $SO(3)$ is the rotation group of the sphere S^2, the first relation is by isomorphism, and the second relation is by diffeomorphism.
- Thus, it follows that elements of Ω correspond to solutions to: $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 5^t$, and can be projected onto the sphere.
- This is a well-studied problem in number theory and lends itself to being studied numerically.

Connection to Discrepancy

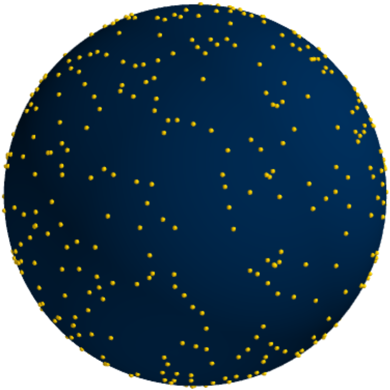
A Different Way to Approach the Problem

- Recall that $PSU(2)$ is just as valid a group for representing gates as $SU(2)$.
- It is interestingly the case that $PSU(2) \approx SO(3)$ and that $SU(2) \approx S^3$, where the $SO(3)$ is the rotation group of the sphere S^2, the first relation is by isomorphism, and the second relation is by diffeomorphism.
- Thus, it follows that elements of Ω correspond to solutions to: $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 5^t$, and can be projected onto the sphere.
- This is a well-studied problem in number theory and lends itself to being studied numerically.
- In many ways, we can change the quantum problem to a study of how well this point set is distributed on the sphere.

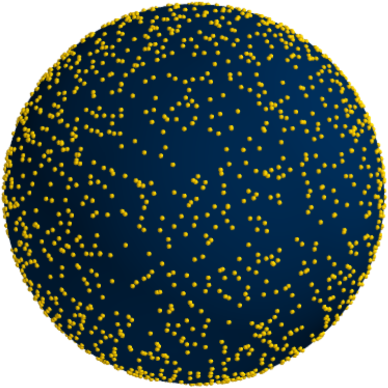
The Points of $V(2)$



The Points of $V(3)$



The Points of $V(4)$



Efficiency and Discrepancy

Solovay-Kitaev and Efficiency

- The Solovay-Kitaev Theorem states that for $X \in SU(2)$ and a symmetric universal set of quantum gates, for a given $\varepsilon > 0$, there exists some $\omega \in \Omega$ of length $O\left(\log^c\left(\frac{1}{\varepsilon}\right)\right)$ approximating X within distance ε.

Efficiency and Discrepancy

Solovay-Kitaev and Efficiency

- The Solovay-Kitaev Theorem states that for $X \in SU(2)$ and a symmetric universal set of quantum gates, for a given $\varepsilon > 0$, there exists some $\omega \in \Omega$ of length $O\left(\log^c\left(\frac{1}{\varepsilon}\right)\right)$ approximating X within distance ε.
- This guarantees that an approximation exists, but does not robustly address the relative efficiency of different choices of gate set.

Solovay-Kitaev and Efficiency

- The Solovay-Kitaev Theorem states that for $X \in SU(2)$ and a symmetric universal set of quantum gates, for a given $\varepsilon > 0$, there exists some $\omega \in \Omega$ of length $O\left(\log^c\left(\frac{1}{\varepsilon}\right)\right)$ approximating X within distance ε.
- This guarantees that an approximation exists, but does not robustly address the relative efficiency of different choices of gate set.
- To that end, Sarnak introduces the covering exponent, defined below, to serve this purpose:

$$K(T) \equiv \limsup_{\varepsilon \to 0} \frac{\log|V(t_\varepsilon)|}{\log(\frac{1}{\mu(B(\varepsilon))})},$$

where t_ε is the smallest t such that for the given ε, $V(t_\varepsilon)$ approximates all of $SU(2)$ within a distance ε, $B(\varepsilon)$ is an arbitrary ball of radius ε in $SU(2)$ and μ is a Haar measure on $SU(2)$.

Efficiency and Discrepancy

Bounds on K

- From the definition, it follows that if T approximates all of $SU(2)$ with optimal efficiency, then $K(T) = 1$.

Efficiency and Discrepancy

Bounds on K

- From the definition, it follows that if T approximates all of $SU(2)$ with optimal efficiency, then $K(T) = 1$.
- This is not the case: Sarnak has proven that $\frac{4}{3} \leqslant K(T) \leqslant 2$.

Efficiency and Discrepancy

Bounds on K

- From the definition, it follows that if T approximates all of $SU(2)$ with optimal efficiency, then $K(T) = 1$.
- This is not the case: Sarnak has proven that $\frac{4}{3} \leqslant K(T) \leqslant 2$.
- However, T is optimally efficiency *almost everywhere*.

Efficiency and Discrepancy

Bounds on K

- From the definition, it follows that if T approximates all of $SU(2)$ with optimal efficiency, then $K(T) = 1$.
- This is not the case: Sarnak has proven that $\frac{4}{3} \leqslant K(T) \leqslant 2$.
- However, T is optimally efficiency *almost everywhere*.
- It is suspected that $K(T) = \frac{4}{3}$; what remains is for this to be proven or refuted.

Conjecture on K

- We conjecture $\varepsilon \leq f(t_\varepsilon)5^{-t_\varepsilon/4}$ for a function $f:(0,\infty)\to(1,\infty)$ satisfying:

$$\lim_{t_\varepsilon\to\infty} log(f(t_\varepsilon))/t_\varepsilon$$

exists with value 0.

Efficiency and Discrepancy

Conjecture on K

- We conjecture $\varepsilon \leq f(t_\varepsilon)5^{-t_\varepsilon/4}$ for a function $f : (0, \infty) \to (1, \infty)$ satisfying:

$$\lim_{t_\varepsilon \to \infty} log(f(t_\varepsilon))/t_\varepsilon$$

  exists with value 0.

- Let $\nu(5^{t_\varepsilon})$ denote the set of integer solutions of the quadratic form: $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 5^{t_\varepsilon}$.

Efficiency and Discrepancy

Conjecture on K

- We conjecture $\varepsilon \leq f(t_\varepsilon)5^{-t_\varepsilon/4}$ for a function $f : (0, \infty) \to (1, \infty)$ satisfying:
  $$\lim_{t_\varepsilon \to \infty} log(f(t_\varepsilon))/t_\varepsilon$$
  exists with value 0.
- Let $\nu(5^{t_\varepsilon})$ denote the set of integer solutions of the quadratic form: $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 5^{t_\varepsilon}$.
- Let $M \equiv M_{S^3}(\mathcal{N})$ denote the covering radius of the points $\mathcal{N} = \nu(5^{t_\varepsilon}) \cup \nu(5^{t_\varepsilon - 1})$ on the sphere S^3 in $\mathbb{R}^4$.

Efficiency and Discrepancy

Conjecture on K

- We conjecture $\varepsilon \leq f(t_\varepsilon)5^{-t_\varepsilon/4}$ for a function $f:(0,\infty)\to(1,\infty)$ satisfying:

$$\lim_{t_\varepsilon\to\infty} log(f(t_\varepsilon))/t_\varepsilon$$

  exists with value 0.
- Let $\nu(5^{t_\varepsilon})$ denote the set of integer solutions of the quadratic form: $x_1^2+x_2^2+x_3^2+x_4^2=5^{t_\varepsilon}$.
- Let $M\equiv M_{S^3}(\mathcal{N})$ denote the covering radius of the points $\mathcal{N}=\nu(5^{t_\varepsilon})\cup\nu(5^{t_\varepsilon-1})$ on the sphere S^3 in $\mathbb{R}^4$.
- Then $M\sim f(\log N)N^{-1/4}$. Here $N\equiv N(\varepsilon)=6\cdot 5^{t_\varepsilon}-2$.

Conjecture on K

- We conjecture $\varepsilon \leq f(t_\varepsilon)5^{-t_\varepsilon/4}$ for a function $f : (0, \infty) \to (1, \infty)$ satisfying:

$$\lim_{t_\varepsilon \to \infty} log(f(t_\varepsilon))/t_\varepsilon$$

  exists with value 0.
- Let $\nu(5^{t_\varepsilon})$ denote the set of integer solutions of the quadratic form: $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 5^{t_\varepsilon}$.
- Let $M \equiv M_{S^3}(\mathcal{N})$ denote the covering radius of the points $\mathcal{N} = \nu(5^{t_\varepsilon}) \cup \nu(5^{t_\varepsilon - 1})$ on the sphere S^3 in $\mathbb{R}^4$.
- Then $M \sim f(\log N)N^{-1/4}$. Here $N \equiv N(\varepsilon) = 6 \cdot 5^{t_\varepsilon} - 2$.
- Assuming this conjecture implies that $K(T) \leqslant \frac{4}{3}$ and then also that $K(T) = \frac{4}{3}$.

A Valid Example

With $t_\varepsilon \sim \log(N)$, consider:

$$f(t_\varepsilon) = t_\varepsilon^{\left(\log\left(t_\varepsilon^{\log\left(t_\varepsilon^{\cdot^{\cdot^{\cdot}}}\right)}\right)\right)}$$

where the term $\log(t_\varepsilon)$ is nested n times. Then easily we have

$$\log(f(t_\varepsilon))/t_\varepsilon \sim \frac{(\log(\log N))^{n+1}}{\log N}$$

which decays to 0 for large enough N.

An Invalid Example

On the other hand for a function which grows faster, say

$$f(t_\varepsilon) = t_\varepsilon^{t_\varepsilon}$$

we easily have

$$\log(f(t_\varepsilon))/t_\varepsilon \sim (\log(\log N))$$

which diverges for large enough N.

References

1. S.B. Damelin, Q. Liang, B.A.W. Mode, "On Golden Gates and Discrepancy," arxiv:1506.05785 (2017) preprint. Submitted to J. Complex.
2. A. Bocharov, Y. Gurevich, and K. Svore. "Efficient decomposition of single-qubit gates into V basis circuits," Phys. Rev. A 88.1 (2013): 012313.
3. J. Bourgain, P. Sarnak, and Z. Rudnick, "Local statistics of lattice points on the sphere," arXiv preprint arXiv:1204.0134 (2012).
4. C.M. Dawson, M.A. Nielsen, "The Solovay-Kitaev Algorithm," QIC, Vol 6, No 1 (2006), pp 081-095.
5. P. Sarnak, "Letter to Scott Aaronson and Andy Pollington on the Solovay-Kitaev Theorem and Golden Gates," `http://publications.ias.edu/sarnak/paper/2637` (2015).
6. N. Ross and P. Selinger, "Optimal ancilla-free Clifford+T approximation of z-rotations," QIC. **16**(2016) (11-12), pp 901-953.

Acknowledgments

- Thanks to Dr. Damelin for his collaboration and insights.
- Research for this REU was supported by funding from the National Science Foundation.