

UNIVERSAL QUANTUM GATES

ABHINAV KUMAR

ABSTRACT. I discuss the question of when the set of gates $\{R_x(\pi\alpha), R_y(\pi\alpha), R_z(\pi\alpha)\}$ generates a dense subset of $SU(2)$ and is universal for quantum computation on 1 qubit. I prove that any two elements of the above set are universal for all $\alpha \in (0, 1) \setminus \{1/2\}$.

1. INTRODUCTION

In this paper I will discuss some possible examples of universal finite sets of quantum gates. In other words, we are looking for a finite set $S \subset SU(N)$ such that S generates a dense subset of $SU(N)$. The fact that dense subsets lead to efficient quantum computation is the fundamental Solovay-Kitaev theorem [1] which states that we can approximate any gate to accuracy ϵ using $O(\log^c(1/\epsilon))$ gates, where $c \approx 4$.

This leads us to search for simple sets of gates which generate dense subsets of $SU(N)$. One such set is made up of the Hadamard, phase, C-NOT, and $\pi/8$ gates. In fact, if we can perform the CNOT-gate and approximate single-qubit gates to any degree of accuracy, then it is possible to generate any gate in $SU(N)$. So we want to explore finite small sets of gates which generate $SU(2)$. In particular, this paper focuses on the set $\{R_x(\pi\alpha), R_y(\pi\alpha), R_z(\pi\alpha)\}$.

In section 2, I will discuss some concepts and formulae needed from quantum computing and from number theory. In section 3, I will discuss when $\{R_x(\pi\alpha), R_y(\pi\alpha), R_z(\pi\alpha)\}$ is universal for $SU(2)$. The main result of the paper is the following:

Theorem 1.1. *If α is not a half-integer (i.e. $2\alpha \notin \mathbb{Z}$), then the subgroup generated by any two elements of $S_\alpha = \{R_x(\pi\alpha), R_y(\pi\alpha), R_z(\pi\alpha)\}$ is dense in $SU(2)$.*

It will be proved in section 3.

2. PRELIMINARIES

2.1. Quantum Mechanics. Before we discuss the problem at hand, a few preliminaries: $SU(2)$ is the set of 2×2 matrices U such that $UU^\dagger = 1$. Such a U can be written as

$$U = \begin{bmatrix} a & b \\ -e^{i\phi}b^* & e^{i\phi}a^* \end{bmatrix}, |a|^2 + |b|^2 = 1$$

Any such matrix can be written in the form $e^{i\alpha}R_{\hat{n}}(\phi)$, where $\alpha \in \mathbb{R}$ is a global phase and $R_{\hat{n}}(\phi)$ is rotation by ϕ about the \hat{n} axis. An expression for this rotation is given by:

$$R_{\hat{n}}(\phi) = \exp(-i\hat{n} \cdot \vec{\sigma}/2) = \cos(\phi/2)I - i \sin(\phi/2)(n_x X + n_y Y + n_z Z)$$

where X, Y, Z are the Pauli matrices given by:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

The product of two rotations is now easily computed, and is given by [2]

$$R_{\hat{n}_1}(\phi_1)R_{\hat{n}_2}(\phi_2) = R_{\hat{n}_{12}}(\phi_{12})$$

where

$$\cos(\phi_{12}/2) = \cos(\phi_1/2) \cos(\phi_2/2) - \hat{n}_1 \cdot \hat{n}_2 \sin(\phi_1/2) \sin(\phi_2/2)$$

$$\sin(\phi_{12}/2)\hat{n}_{12} = \sin(\phi_1/2) \cos(\phi_2/2)\hat{n}_1 + \sin(\phi_2/2) \cos(\phi_1/2)\hat{n}_2 + \sin(\phi_1/2) \sin(\phi_2/2)\hat{n}_1 \times \hat{n}_2$$

2.2. Number Theory. We let \mathbb{Q} be the set of rational numbers, \mathbb{Z} be the set of integers, and \mathbb{N} the set of positive integers. $\mathbb{Q}(z)$ is the set of polynomials with rational coefficients, with similar notation for $\mathbb{Z}(z)$.

An *algebraic number* ζ is a complex number which is root of a polynomial in $\mathbb{Q}(z)$. An *algebraic integer* is a complex number which is a root of a polynomial in $\mathbb{Z}(z)$ with highest coefficient 1 (such a polynomial is called monic).

A polynomial $f(z)$ is called irreducible if there is no non-trivial factorization. For $f(z) \in \mathbb{Q}(z)$ this means it is not possible to write $f(z) = g(z)h(z)$ with $h(z), g(z) \in \mathbb{Q}(z)$ both nonconstant. For $f(z) \in \mathbb{Z}(z)$ this means that if we write $f(z) = g(z)h(z)$ with $h(z), g(z) \in \mathbb{Z}(z)$ then $h(z)$ or $g(z)$ must equal ± 1 .

For every algebraic number ζ there is a unique monic polynomial with rational coefficients $f(z)$ such that $f(\zeta) = 0$, and if ζ is a root of some polynomial $g(z)$ with rational coefficients, then $f(z)|g(z)$ (that is, $f(z)$ divides $g(z)$ in $\mathbb{Q}(z)$.) If ζ is an algebraic integer, then $f(z)$ may be taken to have integer coefficients. The polynomial $f(z)$ is irreducible and is called the irreducible polynomial of ζ . It is the polynomial of lowest degree of which ζ is a root.

Finally, there is a result of algebra called Gauss' lemma, which states the following:

Lemma 2.1. (*Gauss*) *If $f(z) \in \mathbb{Z}(z)$ factors into two polynomials with rational coefficients, $f(z) = g(z)h(z)$, then there exist multipliers $c, d \in \mathbb{Q}$ such that $cg(z) \in \mathbb{Z}(z)$ and $dh(z) \in \mathbb{Z}(z)$, and $cd = 1$. That is, $f(z) = (cg(z)) \cdot (dh(z))$ is a factorization into polynomials with integer coefficients.*

For details and proofs I refer the reader to [3].

3. GENERATING $SU(2)$ FROM ROTATIONS ABOUT THE THREE AXES

Now we want the set of α for which $S_\alpha = \{R_x(\pi\alpha), R_y(\pi\alpha), R_z(\pi\alpha)\}$ is universal. We have the following elementary result.

Lemma 3.1. *If α is irrational, then S_α is dense in $SU(2)$.*

Proof. Notice $R_x(\pi\alpha)^n = R_x(n\pi\alpha)$. Since α is irrational, the set of $\{n\pi\alpha : n \in \mathbb{N}\}$ is dense in the interval $[0, 2\pi)$ (modulo 2π). Since $R_x(2\pi) = (-1)I$, we can generate a dense subset of rotations about the x -axis. Similarly, we can generate a dense subsets of rotations about the z -axis. These are enough to generate $SU(2)$ densely. \square

Notice that we needed only $R_x(\pi\alpha)$ and $R_y(\pi\alpha)$ for our purposes. So we have a strengthening of our proposition: if α is irrational, any two elements of the set S_α above suffice to generate $SU(2)$ densely.

So now we wish to investigate the case when α is rational. There are clearly some values for α such as the trivial $\alpha = 0, 1$ for which S_α isn't universal. A nontrivial value is $\alpha = 1/2$ in which case S_α turns out to consist of rotations of $\pi/2$ about the x, y, z axes. But the group these generate are the symmetries of a cube, which is a finite group. So it cannot be dense in $SU(2)$.

The surprising thing is that for all other values S_α is universal. In fact, we have the following stronger result.

Theorem 3.2. *If α is not a half-integer (i.e. $2\alpha \notin \mathbb{Z}$), then the subgroup generated by any two elements of $S_\alpha = \{R_x(\pi\alpha), R_y(\pi\alpha), R_z(\pi\alpha)\}$ is dense in $SU(2)$.*

Proof. We have already dealt with the case of irrational α . So assume α is rational now. Write $\alpha = \frac{p}{q}$ in reduced terms. Since α is not a half-integer, either $4|q$ or $q = 2s$ or $q = s$ with s odd and greater than 1.

Case 1: We assume $4|q$. We can find integers a, b such that $ap + bq = 1$. Furthermore we can assume that b is even, (otherwise we can replace (a, b) by $(a - q, b + p)$, and p is odd since $\gcd(p, q) = 1$ and 4 divides q). Then

$$R_x(\pi\alpha)^a = R_x\left(\frac{ap}{q}\pi\right) = R_x\left(\frac{1 - bq}{q}\pi\right) = (-1)^{b/2} R_x\left(\frac{\pi}{q}\right)$$

So we might as well take $\alpha = 1/q$. Then $R_x(\pi\alpha)^{q/4} = R_x(\pi/4)$ is in the subgroup generated by S_α . Similarly $R_y(\pi/4)$ and $R_z(\pi/4)$ are in that subgroup too.

Consider the following computation:

$$\begin{aligned} R_x(\pi/4)R_y(\pi/4) &= R_{\hat{n}}(\theta) \\ \cos(\theta/2) &= \cos(\pi/8)\cos(\pi/8) - \hat{x} \cdot \hat{y} \sin(\pi/8)^2 \\ &= \cos(\pi/8)^2 = \frac{1 + \cos(\pi/4)}{2} \\ &= \frac{\sqrt{2} + 1}{2\sqrt{2}} \end{aligned}$$

and

$$\sin(\theta/2)\hat{n} = \sin(\pi/8)\cos(\pi/8)(\hat{x} + \hat{y}) + \sin(\pi/8)^2\hat{z}$$

I claim that θ cannot be a rational multiple of π . Once I prove this, it will follow that $R_{\hat{n}}(\theta)$ generates densely all the rotations about the \hat{n} axis. After that, we'll consider the product $R_y(\pi/4)R_x(\pi/4) = R_{\hat{n}'}(\theta)$ (same θ , by the above cosine formula!) with \hat{n}' given by

$$\sin(\theta/2)\hat{n}' = \sin(\pi/8)\cos(\pi/8)(\hat{x} + \hat{y}) - \sin(\pi/8)^2\hat{z}$$

We see that \hat{n}' and \hat{n} are along different axes and since S_α densely generates rotations about these axes, it is dense in $SU(2)$. So now it remains to prove that θ is not a rational multiple of π .

For arbitrary θ , let $z = 2\cos(\theta)$. Let $z_n = 2\cos(n\theta)$. We will show that $z_n = P_n(z)$ where P_n is a monic polynomial with integer coefficients and degree n . First

$2 \cos(0\theta) = 2$ so we can take $P_0(z) = 2$. Similarly $P_1(z) = z$ is obvious. We will define $P_n(z)$ inductively using the formula

$$\cos(n\theta) + \cos((n-2)\theta) = 2 \cos((n-1)\theta) \cos(\theta)$$

This implies $z_n + z_{n-2} = z_{n-1}z$ after multiplying both sides by 2. So we just define $P_n(z) := zP_{n-1}(z) - P_{n-2}(z)$. By induction it follows that P_n is monic with integer coefficients and degree n . The first few values are listed below.

$$\begin{aligned} P_0(z) &= 2 \\ P_1(z) &= z \\ P_2(z) &= z^2 - 2 \\ P_3(z) &= z^3 - 3z \\ P_4(z) &= z^4 - 4z^2 + 2 \end{aligned}$$

Now, if $\theta/2 = a/b\pi$ is a rational multiple of π , then $z = 2 \cos(\theta/2)$ satisfies $P_b(z) = 2 \cos(a\pi) = \pm 2$, so it's the root of a monic polynomial with integer coefficients, say $G(z)$. But $z = 2 \cos(\theta/2)$ for the θ above satisfies $z = 1 + \cos(\pi/4)$, or $(z-1)^2 = 1/2$, or $z^2 - 2z + 1/2$. This is the irreducible polynomial for $z = 2 \cos(\theta/2)$ over \mathbb{Q} , so it must divide $G(z)$. But $G(z)$ has integer coefficients and is monic, and it follows from Gauss' lemma that if such a polynomial factors over $\mathbb{Q}(z)$, then the same factorization gives rise to a factorization over $\mathbb{Z}(z)$ with monic factors. However, $z^2 - 2z + 1/2$ does not have integer coefficients and if we try to make it have integer coefficients by multiplying by 2, then it's not monic any more. So we see that $z^2 - 2z + 1/2$ can't divide $G(z)$, and therefore θ can't be a rational multiple of π . This takes care of Case 1, but the techniques we used here are also useful in Case 2.

Case 2: $q = 2s$ or $q = s$, with s odd, and greater than 1. Then we can compute $R_x(\pi\alpha)^2$ (if $q = 2s$) to get $R_x(\frac{2\pi}{s})$. Now, we find integers a, b such that $ap + bs = 1$. Then

$$R_x(\pi\frac{p}{s})^{2a} = R_x\left(\frac{2ap}{s}\pi\right) = R_x\left(\frac{2-2bs}{s}\pi\right) = (-1)^b R_x\left(\frac{2\pi}{s}\right)$$

So we can just assume $p = 2$. Since s is odd and greater than 1, it has an odd prime divisor, say r . By raising $R_x(2\pi/s)$ to s/r , we can get $R_x(2\pi/r)$. Therefore, for the purposes of argument, let's just assume s is prime. So we compute $R_x(2\pi/s)R_y(2\pi/s) = R_{\hat{n}}(\theta)$ with

$$\cos(\theta/2) = \cos(\pi/s)^2$$

$$\sin(\theta/2)\hat{n} = \sin(\pi/s)\cos(\pi/s)(\hat{x} + \hat{y}) + \sin(\pi/s)^2\hat{z}$$

The plan, as before, is to prove that θ is not a rational multiple of π . Once we show that, the above rotation generates a dense subgroup of rotations about \hat{n} . Then we use the opposite product $R_y(\pi\alpha)R_x(\pi\alpha)$ which will have the same θ but a different axis \hat{n}' give by

$$\sin(\theta/2)\hat{n}' = \sin(\pi/s)\cos(\pi/s)(\hat{x} + \hat{y}) - \sin(\pi/s)^2\hat{z}$$

So we have dense subgroups of rotations about \hat{n} and \hat{n}' which together generate $SU(2)$. All that remains now is to show that θ is an irrational multiple of π .

Proof. We know $\cos(\theta/2) = \cos(\pi/s)^2 = \frac{1+\cos(2\pi/s)}{2}$. So let $u = 2\cos(\theta/2)$, then we have $2u - 2 = 2\cos(2\pi/s)$. So $2u - 2$ is a root of $P_s(z) = 2\cos(2\pi/s) = 2$, or a root of the polynomial $P_s(z) - 2$. Also, $2u - 2$ is not a root of the polynomial $z - 2$, because $(2u - 2) - 2 \neq 0$ because $u \neq 1$ because $\cos(\pi/s)^2 \neq 1$ because $s > 1$. Therefore $2u - 2$ is a root of the polynomial $G(z) = \frac{P_s(z) - 2}{z - 2}$ (which is easily seen to be a monic polynomial of degree $s - 1$. Note that $z - 2$ divides $P_s(z) - 2$ because 2 is a root of $P_s(z) - 2$ because $P_s(2) - 2 = P_s(2\cos(0)) - 2 = 2\cos(s \cdot 0) - 2 = 2 - 2 = 0$.) I'm going to claim that $G(z)$ is the square of an irreducible polynomial. I use the following theorem from number theory, which is easily proved using cyclotomic polynomials.

Theorem 3.3. [4] (*D. H. Lehmer*) *If $n > 2$ and $\text{g.c.d}(k, n) = 1$ then $2\cos(2\pi k/n)$ is an algebraic integer of degree $\phi(n)/2$.*

Note: $\phi(n)$ is the Euler phi-function, the number of positive integers less than or equal to n that are relatively prime to n .

To use this theorem, we set $k = 1, n = s$ and see that $\phi(n) = \phi(s) = s - 1$ since s is prime. So the theorem is saying that $2\cos(2\pi/s)$ has a monic irreducible polynomial of degree $(s - 1)/2$. I will show that $G(z) = H(z)^2$, whence $H(z)$ is monic and of degree $(s - 1)/2$, and $2\cos(\pi/2)$ is a root of $G(z)$, therefore a root of $H(z)$. Hence $H(z)$ is the unique irreducible polynomial of $2\cos(\pi/s)$.

So, note that $P_s(2\cos(\theta)) = 2\cos(s\theta)$, therefore

$$\frac{P_s(2\cos(\theta)) - 2}{2\cos(\theta) - 2} = \frac{\sin(s\theta/2)^2}{\sin(\theta/2)^2}$$

has roots at $\theta = m\pi/s$, where m is even and ranges from $2\pi/s - 1$. Also, each of these roots is a double root. So $G(z) = \frac{P_s(z) - 2}{z - 2}$ has double roots at $2\cos(m\pi/s)$ at the $(s - 1)/2$ even values of m . This immediately shows that $G(z)$ is a square. We know $G(z)$ has coefficients in \mathbb{Q} and is monic, so the square root algorithm for a polynomial shows that $G(z)$ is in fact a square in $\mathbb{Q}(z)$. Further, since $G(z)$ has integer coefficients it follows that its square root has integer coefficients too. Thus $H(z)$ has integer coefficients and $G(z) = H(z)^2$. Now we're almost at the end of our proof.

If $\theta/2$ is a rational multiple of π , say $\theta/2 = a\pi/b$, then $u = 2\cos(\theta/2)$ satisfies $P_{2b}(u) = 2$. But also $H(2u - 2) = 0$, since $G(2u - 2) = 0$. Since $H(z)$ is irreducible over $\mathbb{Q}(z)$, so is $H(2z - 2)$ (since if $H(2z - 2) = P(z)Q(z)$, then $H(z) = P(z/2 + 1)Q(z/2 + 1)$ is a factorization over $\mathbb{Q}(z)$.) Now, $G(z) = \frac{P_s(z) - 2}{z - 2}$ has constant term 1 (this is easily seen by induction: first we show that $P_s(z)$ has no constant term when s is odd, follows from $P_1 = z$ and $P_{n+2}(z) = -P_n(z) + zP_{n-1}(z)$ and both of the terms on the RHS have zero constant term. Then the constant term of $G(z)$ is $G(0) = \frac{P_s(0) - 2}{0 - 2} = \frac{0 - 2}{0 - 2} = 1$.) So $H(z)$ constant term ± 1 . Therefore $H(2z - 2)$ must have odd constant term. On the other hand, we already know that since the degree of $H(z)$ is $(s - 1)/2$ and $H(z)$ is monic, it follows that the coefficient of $z^{(s-1)/2}$ (the highest term) in $H(2z - 2)$ must be $2^{(s-1)/2}$, a power of 2. Therefore the polynomial $H(2z - 2)$ is primitive, that is, the g.c.d. of its coefficients is 1. Therefore $H(2z - 2)$ is irreducible over $\mathbb{Z}(z)$. But u is a root of both $H(2z - 2)$ and $P_{2b}(z) - 2$. Therefore, it follows that $H(2z - 2)$ divides P_{2b} in $\mathbb{Z}(z)$, which is

impossible since $P_{2b}(z)$ is monic and $H(2z-2)$ has highest coefficient $2^{(s-1)/2} > 1$. This contradiction proves that θ cannot be a rational multiple of π . \square

Notice that we have indeed proved that we only need rotations of α about two axes, say x and y , to generate a dense subgroup of $SU(2)$. This concludes the proof of the main result. \square

4. ACKNOWLEDGEMENTS

This question was posed as part of a possible final project in Isaac Chang's course on Quantum Information Science at MIT. I am also thankful to Aram Harrow and Andrew Childs for suggestions on the problem.

REFERENCES

- [1] A. Y. Kitaev, *Quantum computations: algorithms and error correction*, Russ. Math. Surv., **(52) 6**: 1191-1249, 1997.
- [2] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
- [3] H. S. Zuckerman, H. L. Montgomery, I. M. Niven, A. Niven, *An Introduction to the Theory of Numbers*, Fifth edition, Wiley, 1991.
- [4] I. Niven, *Irrational Numbers*, Mathematical Association of America, 1956. The cited theorem is Theorem 3.9 in the book.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA 02139
E-mail address: abhinavk@mit.edu