# Item: **Solovay-Kitaev Theorem**

John D Mangual

Can you make a living solving diophantine equations? There is Peter Sarnak.

What can the rest of us do? How about showing an integer is the sum of four squares:

$$n = a^2 + b^2 + c^2 + d^2$$

and in recent work Mr. Sarnak makes a connection to quantum computing. Even if, out of curiosity, you read Nielsen and Chuang, I got sort of shy that maybe my arithmetic questions were stupid or something. These titles like the **quantum fourier transform** sound rather enticing, but the number theory in the textbook is rather limited. There is Shor's algorithm.

If I read correctly their gates are unitary operators act on a copy of $\mathbb{C}^2 \otimes \mathbb{C}^2$ a copy of two "qubits". And we get the basis operators:

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

Then we check there are 2 basis elements $\times$ 2 basis elements for a total of 4 "states":

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \simeq \mathbb{C}^4$$

I took a course on "alternative modes of computation" and I found the discussion lacking. Nielsen-Chuang make the common-sense derivation:

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \simeq \mathbb{C}^4 \quad \text{therefore} \quad U\Big((\mathbb{C}^2)^{\otimes 2}\Big) \simeq U\big(\mathbb{C}^4\big) \text{ or } U(4)$$

In an abstract algebra class (maybe 3rd year undergrad or again in graduate school[1]) there is also the special unitary group, where we factor out the various copies of $S^1$. Sarnak has chosen not to.

Solovay-Kitaev theorem says we can approximate every state, with a product of basic operators. For me it's the simple $\otimes$ which makes me wonder about it's cousins (that I know much less about)

Ext Tor

This is the part of abstract algebra class I blanked out on. However, the more backflips I see Nielsen and Chuang do, makes me wonder if Ext and Tor are not far behind.

[1] or forever...

What exactly did Sarnak do? Picking two matrices in $SO(3)$ out and we just multiply them at random, they will get close to all matrices, this is called **density**.

$$F : \langle A, B \rangle \to SO(3) \simeq SU(2)$$

and the image of $F$ will be a dense in group. Since he is talking about quantum computation, he will use $U(2)$. There is a homomorphism:

$$\det : U(2) \to S^1$$

and this leads to an exact sequence of matrix groups, where $SU(2)$ is the kernel:

$$1 \to SU(2) \to U(2) \to S^1 \to 1$$

Then - the part I got stuck on - how to make a good choice of generators. Using the platonic solids, Sarnak and I went two different routes:

- move each of the vertices slightly, e.g. $\begin{pmatrix} 0+\epsilon & 1+\epsilon \\ -1+\epsilon & 0+\epsilon \end{pmatrix}$
- adjoin a single element $\begin{pmatrix} 1 & 0 \\ 0 & e^{\pi i/8} \end{pmatrix}$ as in all the textbooks

It doesn't look like adjoining something that well-behaved (by itself it behaves like $\frac{1}{8}$) on it's own could be enough to produce chaos.

Then, using measures like the Prime Number Theorem and GRH he gets various estimates for various situations[2] (strong approximation) and sort of trails off...

For someone who is not that experience, I think it's important to learn the various benchmarking techniques (such as the circle method or geometry of numbers) and try to get as far along.

# References


(1) John Cremona **The L-functions and modular forms database project** `arXiv:1511.04289` `http://www.lmfdb.org/`

(2) Sofia Lindqvist **Weak approximation results for quadratic forms in four variables** `arXiv:1704.00502`

(3) Ori Parzanchevski, Peter Sarnak. **Super-Golden-Gates for PU(2)** `arXiv:1704.02106`

Peter Sarnak. **Letter to Aaronson and Pollington on the Solvay-Kitaev Theorem and Golden Gates** `https://publications.ias.edu/sarnak/paper/2637`

(4) Michael Nielsen, Isaac Chaung.
**Quantum computation and quantum information** Cambridge University Press , 2010

(5) Leonard Susskind, Art Friedman.
**Quantum Mechanics: The Theoretical Minimum** Basic Books, 2015


[2] cuspidal representations and Adeles, etc. if we knew what those were