Universal Gate Sets, Unitary Gate Decompositions and Quantum Computing

Zoltán Zimborás

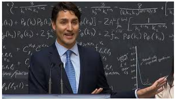
Theoretical Physics Department, Wigner Research Center for Physics
Hungarian Academy of Sciences

Z. Zimborás, R. Zeier, T. Schulte-Herbrueggen, D. Burgarth, *Symmetry criteria for quantum simulability of effective interactions*, Phys. Rev. A 92, 042309 (2015).
R. Zeier, Z. Zimborás, *On squares of representations of compact Lie algebras*, J. Math. Phys. 56, 081702 (2015).
M. Oszmaniec, Z. Zimborás, *Universal extensions of restricted classes of quantum operations*,
Phys. Rev. Lett. 119, 220502 (2017).

Szeged, 18 April 2019

Recent buzz around quantum computing

- Quantum Computing is very popular nowadays:
  - Everybody talks about this from the Canadian Prime Minister to EU officials.



  - Recent Nobel prize given to related research (Haroche, Wineland).

  - Many physicists specializing in this field get jobs in Multinational Companies.
  - EU Quantum Technology Flagship, US Quantum Technology Strategy.

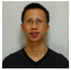
Google created already two types of Quantum Engineer positions

PI

John M. Martinis
Professor at UC Santa Barbara since 2004
Research Scientist at Google since 2014
martinis (at) physics (dot) ucsb (dot) edu
jmartinis (at) google (dot) com

Quantum Electronics Engineers, Google

Rami Barends
Post Doctoral Fellow, 2010-2014
Quantum Electronics Engineer at Google since 2014
rbarends (at) physics (dot) ucsb (dot) edu
barends (at) google (dot) com



Yu Chen
Post Doctoral Fellow, 2010-2014
Quantum Electronics Engineer at Google since 2014
ychen (at) physics (dot) ucsb (dot) edu
bryanchen (at) google (dot) com

Austin Fowler
Staff Scientist, 2013-2014
Quantum Electronics Engineer at Google since 2014
agfowler (at) google (dot) com

Ryan Babbush
August 4, 2015 ·

Waited a long time for these cards (like 2 whole days).

Like Comment Share

You, Borzumehr Toloui, Jonathan Romero Fontalvo and 104 others

View 13 more comments

Richard Swensson Don't make me poach you.
Like · Reply · August 5, 2015 at 5:43pm

Lots of quantum start-ups

Company	Date initiated	Area	Affiliate University or Research Institute	Headquarters
1QBit	1 December 2012	Computing		Vancouver, Canada
Accenture[1]	14 June 2017	Computing		
imec[2]		Silicon Quantum Computing		Belgium
Airbus[3]	2015	Computing		Blagnac, France
Aliyun (Alibaba Cloud)[4]	30 July 2015	Computing/Communication[4][5]	Chinese Academy of Sciences [6][5][7]	Hangzhou, China
AT&T[8]	2011	Communication		Dallas, TX, USA
Atos[9]		Communication		Bezons, France
Booz Allen Hamilton[10]		Computing		Tysons Corner, VA, USA
BT[11]		Communication		London, UK
Carl Zeiss AG[12]			University College London	Oberkochen, Germany
Cambridge Quantum Computing Limited[13]		Communication		Cambridge, UK
D-Wave	1 January 1999	Computing		Burnaby, Canada
Fujitsu[14]	28 September 2015	Communication	University of Tokyo	Tokyo, Japan
Google QuAIL[15]	16 May 2013	Computing	UCSB	Mountain View, CA, USA
HP[16][17]		Computing[16]/Communication[17]		Palo Alto, CA, USA
Hitachi		Computing	University of Cambridge, University College London	Tokyo, Japan
Honeywell[18][19]		Computing	Georgia Tech,[18] University of Maryland[19]	Morris Plains, NJ, USA
HRL Laboratories		Computing		Malibu, CA, USA
Huawei Noah's Ark Lab[20]		Communication	Nanjing University	Shenzhen, China
IBM[21]	10 September 1990[22]	Computing	MIT[23]	Armonk, NY, USA
ID Quantique	1 July 2001	Communication		Geneva, Switzerland
ionQ[24][25]		Computing	University of Maryland, Duke University	College Park, MD, USA
Intel[26]	3 September 2015	Computing	TU Delft	Santa Clara, CA, USA
KPN[27]		Communication		The Hague, Netherlands
Lockheed Martin		Computing	University of Southern California, University College London	Bethesda, MD, USA
MagiQ		Communication		Somerville, MA, USA
Microsoft Research QuArC	19 December 2011	Computing	TU Delft, Niels Bohr Institute, University of Sydney, Purdue University, University of Maryland, ETH Zurich, UCSB	Redmond, WA, USA
Microsoft Research Station Q	22 April 2005	Computing	UCSB	Santa Barbara, CA, USA
Mitsubishi[28]		Communication		Tokyo, Japan
NEC Corporation[29]	29 April 1999[30]	Communication	University of Tokyo	Tokyo, Japan
Nokia Bell Labs[31][32]		Computing	University of Oxford	Murray Hill, NJ, USA
Northrop Grumman		Computing		West Falls Church, VA, USA
NTT Laboratories[33]		Computing	Bristol University	Tokyo, Japan
Q-Ctrl[34][35][36]	2017	Computing[note 1]		Sydney, Australia

Early opinions

QUANTUM COMPUTING: DREAM OR NIGHTMARE?

Recent experiments have deepened our insight into the wonderfully counterintuitive quantum theory. But are they really harbingers of quantum computing? We doubt it.

Serge Haroche and Jean-Michel Raimond

The principles of quantum computing were laid out about 15 years ago by computer scientists applying the superposition principle of quantum mechanics to computer operation. Quantum computing has recently become a hot topic in physics, with the recognition that a two-level system can be presented as a quantum bit, or "qubit," and that an interaction between such systems could lead to the building of quantum gates obeying nonclassical logic. (See PHYSICS TODAY, October 1995, page 24 and March 1996, page 21.)

two interacting qubits: a "control" bit and a "target" bit. The control remains unchanged, but its state determines the evolution of the target: If the control is 0, nothing happens to the target; if it is 1, the target undergoes a well-defined transformation.

Quantum mechanics admits additional options. If the control is in some coherent superposition of 0 and 1, the output of the gate is entangled. That is to say, the two qubits are strongly correlated in a nonseparable state, analogous to the particle pairs of the Einstein–Podolsky–Rosen paradox. The

Early opinions

brothers. How can we get kids excited about becoming scientists, engineers, or technological entrepreneurs if they are taught a form of history in which role models are removed?

Under the Dole administration, I look forward to working with you in an era where good science will be consistently supported.

Robert J. Dole
Washington, DC

Future of Quantum Computing Proves to Be Debatable

In presenting their opinions in the article "Quantum Computing: Dream or Nightmare?" (August, page 51), Serge Haroche and Jean-Michel Raimond conclude that large-scale quantum computation will remain merely a dream of computer theorists. Their principal argument is that, for a quantum computer to be would be useful only if R is of order 10^{11}, or that any application requiring more than 3×10^6 optical operations would be fundamentally disallowed.

Experimentally, our laboratory has demonstrated a "controlled-NOT" quantum logic gate with a single trapped ion,[4] following the ideas of Ignacio Cirac and Peter Zoller.[5] (See PHYSICS TODAY, March, page 21.) In the experiment, R was about 10^1 and the gate time was about 50 s. However, as is often the case in experimental physics, this apparatus was assembled with the least effort necessary to exhibit the desired behavior and should not be taken to represent the technological limit. Although the task of scaling this system to large numbers of ions and gates involving massively entangled quantum states is daunting, the pitfalls are technical, not fundamental.

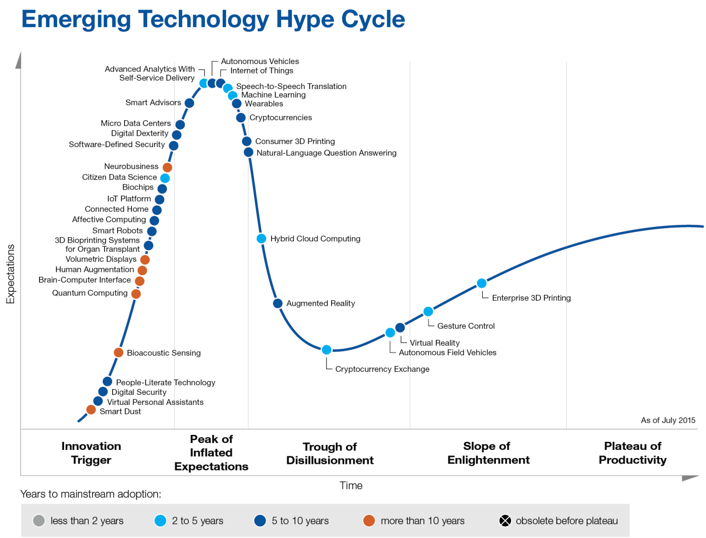
It is too early to make absolute assertions regarding the viability of quantum computation when such a large degree of uncertainty in both

Early opinions

Early opinions

A harmadik évezred elején azonban a kvantumszámítógép egy mesebeli eszköz, létező néhány qubites modellekkel. A mese az elméleti kvantumszámítástudomány; a létező kísérleti valóság annyiféle, ahányféle módon kétállapotú koherens rendszereket definiálni és néhány számolási lépésen keresztül koherensnek tartani képesek vagyunk. A továbblépés azért hihetetlenül nehéz, mert az összefonódásba kéretlen partnerként belép a környezet,

The (trivial) emerging technology hype cycle



International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

1. INTRODUCTION

On the program it says this is a keynote speech—and I don't know what a keynote speech is. I do not intend in any way to suggest what should be in this meeting as a keynote of the subjects or anything like that. I have my own things to say and to talk about and there's no implication that anybody needs to talk about the same thing or anything like it. So what I want to talk about is what Mike Dertouzos suggested that nobody would talk about. I want to talk about the problem of simulating physics with computers and I mean that in a specific way which I am going to explain. The reason for doing this is something that I learned about from Ed Fredkin, and my entire interest in the subject has been inspired by him. It has to do with learning something about the possibilities of computers, and also something about possibilities in physics. If we suppose that we know all the physical laws perfectly, of course we don't have to pay any attention to computers. It's interesting anyway to entertain oneself with the idea that we've got something to learn about physical laws; and if I take a relaxed view here (after all I'm here and not at home) I'll admit that we don't understand everything.

The first question is, What kind of computer are we going to use to simulate physics? Computer theory has been developed to a point where it realizes that it doesn't make any difference; when you get to a *universal computer*, it doesn't matter how it's manufactured, how it's actually made. Therefore my question is, Can physics be simulated by a universal computer? I would like to have the elements of this computer *locally interconnected*, and therefore sort of think about cellular automata as an example (but I don't want to force it). But I do want something involved with the

locality of interaction. I would not like to think of a very enormous computer with arbitrary interconnections throughout the entire thing.

Now, what kind of physics are we going to imitate? First, I am going to describe the possibility of simulating physics in the classical approximation, a thing which is usually described by local differential equations. But the physical world is quantum mechanical, and therefore the proper problem is the simulation of quantum physics—which is what I really want to talk about, but I'll come to that later. So what kind of simulation do I mean? There is, of course, a kind of approximate simulation in which you design numerical algorithms for differential equations, and then use the computer to compute these algorithms and get an approximate view of what physics ought to do. That's an interesting subject, but is not what I want to talk about. I want to talk about the possibility that there is to be an *exact* simulation, that the computer will do *exactly* the same as nature. If this is to be proved and the type of computer is as I've already explained, then it's going to be necessary that *everything* that happens in a finite volume of space and time would have to be exactly analyzable with a finite number of logical operations. The present theory of physics is not that way, apparently. It allows space to go down into infinitesimal distances, wavelengths to get infinitely great, terms to be summed in infinite order, and so forth; and therefore, if this proposition is right, physical law is wrong.

So good, we already have a suggestion of how we might modify physical law, and that is the kind of reason why I like to study this sort of problem. To take an example, we might change the idea that space is continuous to the idea that space perhaps is a simple lattice and everything is discrete (so that we can put it into a finite number of digits) and that time jumps discontinuously. Now let's see what kind of a physical world it would be or what kind of problem of computation we would have. For example, the first difficulty that would come out is that the speed of light would depend slightly on the direction, and there might be other anisotropies in the physics that we could detect experimentally. They might be very small anisotropies. Physical knowledge is of course always incomplete, and you can always say we'll try to design something which beats experiment at the present time, but which predicts anistropies on some scale to be found later. That's fine. That would be good physics if you could predict something consistent with all the known facts and suggest some new fact that we didn't explain, but I have no specific examples. So I'm not objecting to the fact that it's anistropic in principle, it's a question of how anistropic. If you tell me it's so-and-so anistropic, I'll tell you about the experiment with the lithium atom which shows that the anistropy is less than that much, and that this here theory of yours is impossible.

You cannot even describe the state of 100 quantum dipole moments (spins) with any future classical computer. What should we do?

Feynman's question and vision

Richard Feynman (1981):

"...trying to find a computer simulation of physics, seems to me to be an excellent program to follow out...and I'm not happy with all the analyses that go with just the classical theory, because *nature isn't classical*, dammit, and if you want to make a simulation of nature, you'd better *make it quantum mechanical*, and by golly it's a wonderful problem because it doesn't look so easy."

"How can you simulate the quantum mechanics? ... Can you do it with a new type of computer - a quantum computer? It is not a Turing machine, but a machine of a different kind".

This opened the way for the idea of quantum algorithms (Deutsch '85, Deutsch-Jozsa '87, Bernstein-Vazirani '88, Shor '94)

Feynman's question and vision

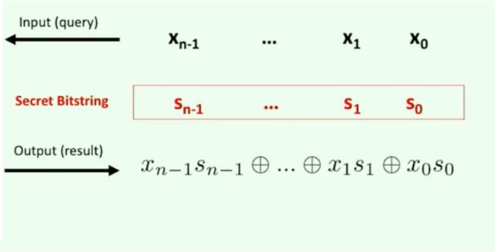
Richard Feynman (1981):

"...trying to find a computer simulation of physics, seems to me to be an excellent program to follow out...and I'm not happy with all the analyses that go with just the classical theory, because *nature isn't classical*, dammit, and if you want to make a simulation of nature, you'd better *make it quantum mechanical*, and by golly it's a wonderful problem because it doesn't look so easy."

"How can you simulate the quantum mechanics? ... Can you do it with a new type of computer - a quantum computer? It is not a Turing machine, but a machine of a different kind".

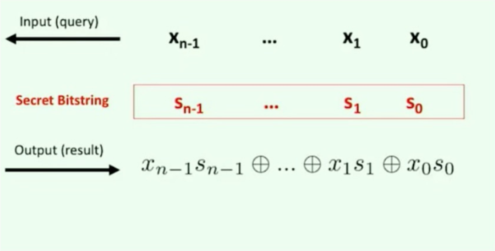
This opened the way for the idea of quantum algorithms (Deutsch '85, Deutsch-Jozsa '87, Bernstein-Vazirani '88, Shor '94)

Bernstein-Vazirani Algorithm



Bernstein-Vazirani Algorithm

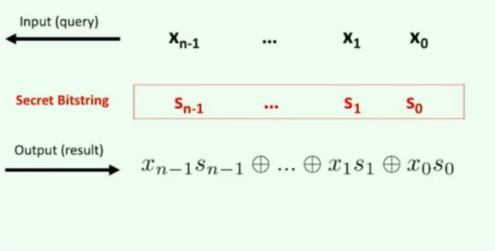
Oracle



optimal classical strategy: n tries

Bernstein-Vazirani Algorithm

Oracle

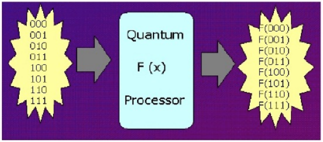


optimal classical strategy: n tries

Bernstein-Vazirani Algorithm

The general hope of quantum computing

the (naive) quantum parallelism

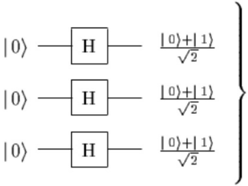


$$\sum_{x=0}^{2^n-1} |x\rangle\,|y\rangle \longrightarrow \sum_{x=0}^{2^n-1} |x\rangle\,|f(x) \oplus y\rangle$$

The Quantum Oracle

Bernstein-Vazirani Algorithm

Creating a uniform superpositions with Hadamard Gates



IN BINARY

$$= \frac{1}{2^{3/2}} \left\{ \begin{array}{l} |000\rangle + |001\rangle + |010\rangle + |011\rangle + \\ + |100\rangle + |101\rangle + |110\rangle + |111\rangle \end{array} \right\}$$

$$= \frac{1}{2^{3/2}} \left\{ \begin{array}{l} |0\rangle + |1\rangle + |2\rangle + |3\rangle + \\ + |4\rangle + |5\rangle + |6\rangle + |7\rangle \end{array} \right\}$$

IN DECIMAL

n qubit computational qubit basis:

$$|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes \cdots \otimes |x_n\rangle$$

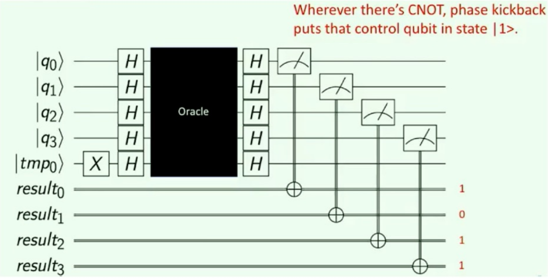
$|x\rangle \quad x \in \{0,1\}^n$ n bit string

$$|x\rangle \quad x \in \{0,1,2,\ldots,2^n-1\}$$

n qubit Hadamard:

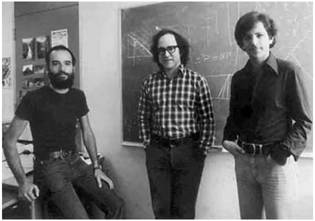
$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{y \cdot x} |y\rangle$$

Bernstein-Vazirani Algorithm



Finding the prime factors of integers is hard

- The most popular public-key cryptosystem, the RSA (Rivest-Shamir-Adleman) encryption, which was developed already in 1978, uses the observation that multiplying integers is easy, factoring integers into prime factors is hard.



- For example, let us have a look at the factors of the following 232 decimal digits (768 bits) number

```
RSA-768 = 12301866845301177551304949583849627207728535695953347921973224521517264005
          07263657518745202199786469389956474942774063845925192557326303453731548268
          50791702612214291346167042921431160222124047927473779408066535141959745985
          6902143413
```

```
RSA-768 = 33478071698956898786044169848212690817704794983713768568912431388982883793
          878002287614711652531743087737814467999489
        × 36746043666799590428244633799627952632279158164343087642676032283815739666
```

The RSA Factoring Challenge

- What about the following 230 decimal digits (762 bits) number?

```
RSA-232 = 1009881397871923546909564894309468582818233821955573955141120516205831021338
          5285453743661097571543636649133800849170651699217015247332943892702802343809
          6090980497644054071120196541074755382494867277137407501157718230539834060616
          2079
```

RSA number	Decimal digits	Binary digits	Cash prize offered	Factored on	Factored by
RSA-100	100	330	US$1,000[4]	April 1, 1991[5]	Arjen K. Lenstra
RSA-110	110	364	US$4,429[4]	April 14, 1992[5]	Arjen K. Lenstra and M.S. Manasse
RSA-120	120	397	$5,898[4]	July 9, 1993[6]	T. Denny *et al.*
RSA-129 [**]	129	426	$100 USD	April 26, 1994[5]	Arjen K. Lenstra *et al.*
RSA-130	130	430	US$14,527[4]	April 10, 1996	Arjen K. Lenstra *et al.*
RSA-140	140	463	US$17,226	February 2, 1999	Herman te Riele *et al.*
RSA-150	150	496		April 16, 2004	Kazumaro Aoki *et al.*
RSA-155	155	512	$9,383[4]	August 22, 1999	Herman te Riele *et al.*
RSA-160	160	530		April 1, 2003	Jens Franke *et al.*, University of Bonn
RSA-170 [*]	170	563		December 29, 2009	D. Bonenberger and M. Krone [***]
RSA-576	174	576	$10,000 USD	December 3, 2003	Jens Franke *et al.*, University of Bonn
RSA-180 [*]	180	596		May 8, 2010	S. A. Danilov and I. A. Popovyan, Moscow State University[7]
RSA-190 [*]	190	629		November 8, 2010	A. Timofeev and I. A. Popovyan
RSA-640	193	640	$20,000 USD	November 2, 2005	Jens Franke *et al.*, University of Bonn
RSA-200 [*] ?	200	663		May 9, 2005	Jens Franke *et al.*, University of Bonn
RSA-210 [*]	210	696		September 26, 2013[8]	Ryan Propper
RSA-704 [*]	212	704	$30,000 USD	July 2, 2012	Shi Bai, Emmanuel Thomé and Paul Zimmermann
RSA-220 [*]	220	729		May 13, 2016	S. Bai, P. Gaudry, A. Kruppa, E. Thomé and P. Zimmermann
RSA-230	230	762			
RSA-232	232	768			
RSA-768 [*]	232	768	$50,000 USD	December 12, 2009	Thorsten Kleinjung *et al.*
RSA-240	240	795			
RSA-250	250	829			
RSA-260	260	862			
RSA-270	270	895			
RSA-896	270	896	$75,000 USD		
RSA-280	280	928			
RSA-290	290	962			
RSA-300	300	995			
RSA-309	309	1024			
RSA-1024	309	1024	$100,000 USD		
RSA-310	310	1028			
RSA-320	320	1061			
RSA-330	330	1094			
RSA-340	340	1128			
RSA-350	350	1161			
RSA-360	360	1194			
RSA-370	370	1227			
RSA-380	380	1261			
RSA-390	390	1294			
RSA-400	400	1327			
RSA-410	410	1360			
RSA-420	420	1393			
RSA-430	430	1427			
RSA-440	440	1460			
RSA-450	450	1493			
RSA-460	460	1526			
RSA-1536	463	1536	$150,000 USD		
RSA-470	470	1559			
RSA-480	480	1593			
RSA-490	490	1626			
RSA-500	500	1659			
RSA-617	617	2048			
RSA-2048	617	2048	$200,000 USD		

An algorithm to factor numbers

1. Pick a random number $a < N$.
2. Compute **gcd**(a,N), the greatest common divisor of a and N.
3. If **gcd**(a,N)$\neq$1, then this number is a nontrivial factor of N, so we are done.
4. Otherwise, use a period-finding subroutine to find r which denotes the period of the following function:

$$f(x) = a^x \bmod N$$

5. If r is odd, or a to the power of $r/2$ gives $N-1$ modulo N, then go back to step 1.
6. Otherwise, we have a nontrivial factor of N:

$$\gcd(a^{r/2} - 1, N) \quad \gcd(a^{r/2} + 1, N)$$

Modular multiplication and period finding

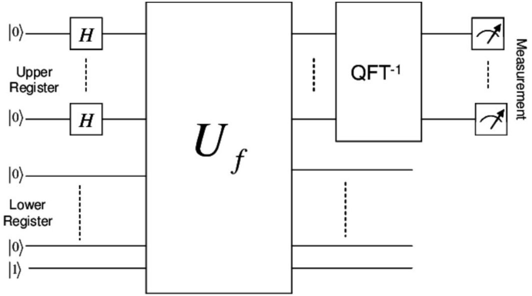
$$\begin{array}{ccccccccc} |1\rangle & \rightarrow & |7\rangle & \rightarrow & |4\rangle & \rightarrow & |13\rangle & \rightarrow & |1\rangle \\ |2\rangle & \rightarrow & |14\rangle & \rightarrow & |8\rangle & \rightarrow & |11\rangle & \rightarrow & |2\rangle \end{array}$$

Multiplication by 7 modulo 15

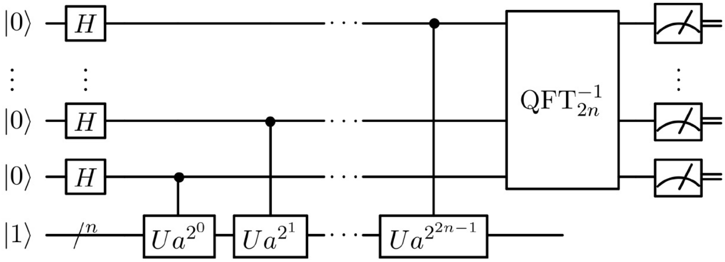
$$\begin{aligned} 7^2 &= 4 \pmod{15} \\ 7^3 &= 4 \cdot 7 = 13 \pmod{15} \\ 7^4 &= 13 \cdot 7 = 1 \pmod{15} \end{aligned}$$

$$\gcd(a^{r/2} - 1, N) \quad \gcd(a^{r/2} + 1, N)$$

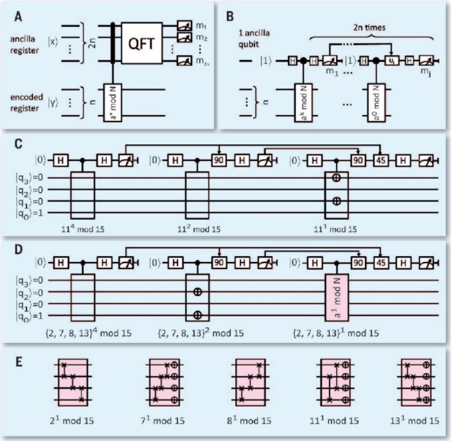
Shor's Algorithm



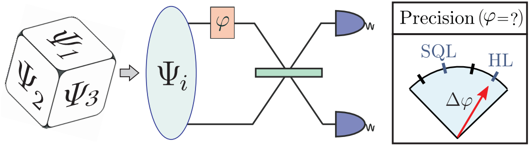
Shor's Algorithm



Shor's Algorithm



Random bosonic circuits (I)



Universal extensions of bosonic linear optics can be used to generate random bosonic circuits which generate states useful in quantum computing and quantum metrology[1].

[1] M.O, R. Augusiak, C. Gogolin, J. Kołodyński, A. Acin, and M. Lewenstein Phys. Rev. X **6**, 041044 (2016)

Random bosonic circuits (II)

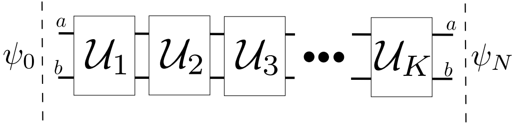
- Can states mimicking the properties of Haar-random states on $\mathcal{H}_b$ be **generated efficiently**?

Construction of the universal set of gates in $\mathcal{H}_b$:

- **Three linear gates** generating whole linear optics [Sarnak 1986]

$$V_1 = \frac{1}{\sqrt{5}}\begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}, V_2 = \frac{1}{\sqrt{5}}\begin{pmatrix} 1 & -2 \\ -2 & 1 \end{pmatrix},$$
$$V_3 = \frac{1}{\sqrt{5}}\begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix},$$

- Supplement this set of gates by **cross-Kerr like** transformation $V_{\mathsf{CK}} = \exp\left(-i\frac{\pi}{3}n_1 n_2\right)$.



In each step the gate $\mathcal{U}_i$ is chosen uniformly at random from a possibly universal gate-set. Is this universal?

Basic problem (I)

- Transformations allowed to perform on a quantum system belong **the unitary group** $\mathrm{U}(\mathcal{H})$, where $\mathcal{H}$ - Hilbert space of the system.
- **Full controllability:** ability to perform any $U \in \mathrm{U}(\mathcal{H})$.
- **Pure state controllability:** ability to perform any $U \in \mathrm{U}(\mathcal{H})$ or $U \in USp(\mathcal{H})$.
- **Limited resources**: only a subset $G \subset \mathrm{U}(\mathcal{H})$ is available.

Basic problem (I)

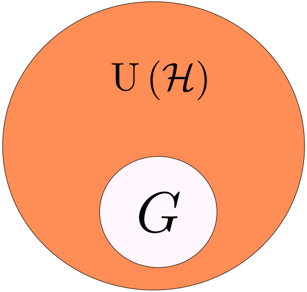
- Transformations allowed to perform on a quantum system belong **the unitary group** $\mathrm{U}(\mathcal{H})$, where $\mathcal{H}$ - Hilbert space of the system.
- **Full controllability:** ability to perform any $U \in \mathrm{U}(\mathcal{H})$.
- **Pure state controllability:** ability to perform any $U \in \mathrm{U}(\mathcal{H})$ or $U \in USp(\mathcal{H})$.
- **Limited resources**: only a subset $G \subset \mathrm{U}(\mathcal{H})$ is available.

Basic problem (I)

- Transformations allowed to perform on a quantum system belong **the unitary group** $\mathrm{U}(\mathcal{H})$, where $\mathcal{H}$ - Hilbert space of the system.
- **Full controllability:** ability to perform any $U \in \mathrm{U}(\mathcal{H})$.
- **Pure state controllability:** ability to perform any $U \in \mathrm{U}(\mathcal{H})$ or $U \in USp(\mathcal{H})$.
- **Limited resources**: only a subset $G \subset \mathrm{U}(\mathcal{H})$ is available.

Basic problem (I)

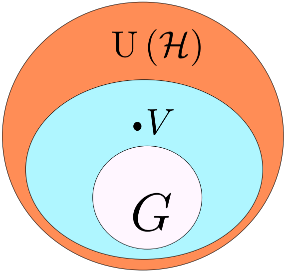
- Transformations allowed to perform on a quantum system belong **the unitary group** $\mathrm{U}(\mathcal{H})$, where $\mathcal{H}$ - Hilbert space of the system.
- **Full controllability:** ability to perform any $U \in \mathrm{U}(\mathcal{H})$.
- **Pure state controllability:** ability to perform any $U \in \mathrm{U}(\mathcal{H})$ or $U \in USp(\mathcal{H})$.
- **Limited resources**: only a subset $G \subset \mathrm{U}(\mathcal{H})$ is available.



Basic problem (II)

In **our works**:

- What gates can be generated when G is **supplemented with and additional gate** $V \notin G$?
- Physical scenarios considered: restricted gate sets for **bosonic and fermionic** systems



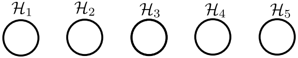
$$\langle G, V \rangle = ?$$

Formal definition of universality

- A collection of quantum gates $\mathcal{S} \subset \mathrm{U}(\mathcal{H})$ is called **universal** in $\mathcal{H}$ iff every element $U \in \mathrm{U}(\mathcal{H})$ can be **approximated arbitrarily well** with elements $U_i \in \mathcal{S}$:

$$\forall \epsilon \; \exists U_{i_k} \in \mathcal{S} \text{ such that } \|U - U_{i_1} U_{i_2} \cdots U_{i_N}\| \leq \epsilon$$

Example 1: distinguishable particles



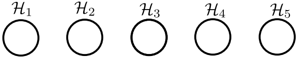
- **Local qubit gates** $\mathrm{LU} = \mathrm{U}(2) \times \mathrm{U}(2) \times \ldots \times \mathrm{U}(2)$ plus any entangling gate is universal in $(\mathbb{C}^2)^{\otimes N}$.[2]

- **Clifford gates** (important for quantum error-correction) are universal in $(\mathbb{C}^2)^{\otimes N}$, when supplemented with any extra gate.[3]

[2] J. L. Brylinski and R. Brylinski, Math. Quant. Comp. **79** (2002)

[3] G. Nebe *et al.*, Designs, Codes and Cryptography **24**, 99 (2001)

Example 1: distinguishable particles



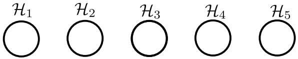
- **Local qubit gates** $\mathrm{LU} = \mathrm{U}(2) \times \mathrm{U}(2) \times \ldots \times \mathrm{U}(2)$ plus any entangling gate is universal in $(\mathbb{C}^2)^{\otimes N}$.[2]
- **Clifford gates** (important for quantum error-correction) are universal in $(\mathbb{C}^2)^{\otimes N}$, when supplemented with any extra gate.[3]

---

[2] J. L. Brylinski and R. Brylinski, Math. Quant. Comp. **79** (2002)

[3] G. Nebe *et al.*, Designs, Codes and Cryptography **24**, 99 (2001)

Example 1: distinguishable particles



- **Local qubit gates** $\mathrm{LU} = \mathrm{U}(2) \times \mathrm{U}(2) \times \ldots \times \mathrm{U}(2)$ plus any entangling gate is universal in $(\mathbb{C}^2)^{\otimes N}$.[2]
- **Clifford gates** (important for quantum error-correction) are universal in $(\mathbb{C}^2)^{\otimes N}$, when supplemented with any extra gate.[3]

OUR WORK: Analogous analysis for non-distinguishable particles

[2] J. L. Brylinski and R. Brylinski, Math. Quant. Comp. **79** (2002)
[3] G. Nebe *et al.*, Designs, Codes and Cryptography **24**, 99 (2001)

SETTING

(A) N **Bosons** in d modes + *passive* linear optics

$$\mathcal{H}_b = \mathrm{Sym}^N(\mathbb{C}^d)\ ,\ \mathrm{LO}_b = \left\{ U^{\otimes N} \ \middle|\ U \in \mathrm{U}(d) \right\}\ .$$

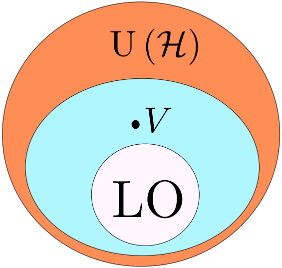
(B) N **Fermions** in d modes + *passive* linear optics

$$\mathcal{H}_f = \bigwedge^N(\mathbb{C}^d)\ ,\ \mathrm{LO}_f = \left\{ U^{\otimes N} \ \middle|\ U \in \mathrm{U}(d) \right\}\ .$$

(C) **Fermions** in d modes in the positive parity subspace
+ *active* fermionic linear optics

$$\mathcal{H}^+_{\mathrm{Fock}} = \bigoplus_{m=0}^{\lfloor \frac{d}{2} \rfloor} \bigwedge^{2m}(\mathbb{C}^d)\ ,\ \mathrm{FLO}\text{ - pp. Bogoliubov transformations}\ .$$

What gates can be generated when bosonic/fermionic linear optics is **supplemented with an additional gate** $V \notin \mathrm{LO}$?



$$\langle \mathrm{LO}, V \rangle = ?$$

The answer must depend on: **type of particles**, **number of modes** and **number of particles**.

More general physical context and motivation

(A) **Bosons**: photonic linear optics[4], interferometry and metrology[5].

(B) **Passive fermionic linear optics**: fermionic interferometry, restricted model of quantum computation[6].

(C) **Active fermionic linear optics**: restricted model of quantum computation[8], Ising anyons[7].

---

[4] E. Knill, R. Laflamme, and G. J. Milburn, Nature **409**, 46 (2001).
[5] V. Giovannetti, *et al.*, Phys. Rev. Lett. **96**, 010401 (2006)
[6] D. P. DiVincenzo and B. M. Terhal, Found. Phys. **35**, 1967 (2005)
[7] S. Bravyi, Phys. Rev. A **73**, 042313 (2006)

Mathematical detour (I): membership problems

- Hamiltonian and group **membership problem**:
  - Is there an efficient way to determine whether $i\tilde{H} \in \langle iH_1, iH_2, \ldots, iH_n \rangle_{Lie}$?
  - Discrete case: $\{U_1, U_2, \ldots U_n\}$ set of unitaries; G is the discrete (finite or infinite) group generated by this set. Is there an efficient way of determining whether $\tilde{U} \in G$?

Mathematical tools (I): simple symmetries

- For Unitary Gates:
  - If there exists a non-trivial symmetry S, such that $[S, U_i] = 0$ for all $\{U_1, U_2, \ldots, U_n\}$, but $[S, U] \neq 0$, then U cannot be generated.
- For Hamiltonians:
  - If there exists a non-trivial symmetry S, such that $[S, H_i] = 0$ for all $\{iH_1, iH_2, \ldots, iH_n\}$, but $[S, iH] \neq 0$, then iH cannot be generated.
- However, this is only a necessary, but not sufficient, condition.

Mathematical tools (II): higher-order symmetries

- For Unitary Gates:
  - A non-trivial second-order symmetry $S^{(2)}$ on $\mathcal{H}^{\otimes 2}$ or a third-order symmetry $S^{(3)}$ on $\mathcal{H}^{\otimes 3}$ are operators that satisfy $[S^{(2)}, U_i \otimes U_i] = 0$ and $[S^{(3)}, U_i \otimes U_i \otimes U_i] = 0$ for all $\{U_1, U_2, \ldots, U_n\}$.
  - If for some n-th order symmetry $[S^{(n)}, U^{\otimes n}] \neq 0$, then U cannot be generated. However, only by checking it for all n is this known to be a sufficient an necessary condition.
- For Hamiltonians:
  - Second-order and third-order symmetries: $[S^{(2)}, iH_\ell \otimes \mathbb{I} + \mathbb{I} \otimes iH_\ell] = 0$ and $[S^{(3)}, iH_\ell \otimes \mathbb{I} \otimes \mathbb{I} + \mathbb{I} \otimes iH_\ell \otimes \mathbb{I} + \mathbb{I} \otimes \mathbb{I} iH_\ell] = 0$ for all $\{iH_1, iH_2, \ldots, iH_n\}$.
  - $[S^{(2)}, iH \otimes \mathbb{I} + \mathbb{I} \otimes iH] \neq 0 \Leftrightarrow iH \notin \langle iH_1, \ldots, iH_m \rangle_{\mathrm{Lie}}$ (morally).[8]

[8] Z. Zimborás, R. Zeier, T. Schulte-Herbrueggen, D. Burgarth, *Symmetry criteria for quantum simulability of effective interactions*, Phys. Rev. A 92, 042309 (2015). R. Zeier, Z. Zimborás, *On squares of representations of compact Lie algebras*, J. Math. Phys. 56, 081702 (2015).

Mathematical tools (II): higher-order symmetries

- For Unitary Gates:
  - A non-trivial second-order symmetry $S^{(2)}$ on $\mathcal{H}^{\otimes 2}$ or a third-order symmetry $S^{(3)}$ on $\mathcal{H}^{\otimes 3}$ are operators that satisfy $[S^{(2)}, U_i \otimes U_i] = 0$ and $[S^{(3)}, U_i \otimes U_i \otimes U_i] = 0$ for all $\{U_1, U_2, \ldots, U_n\}$.
  - If for some n-th order symmetry $[S^{(n)}, U^{\otimes n}] \neq 0$, then U cannot be generated. However, only by checking it for all n is this known to be a sufficient an necessary condition.
- For Hamiltonians:
  - Second-order and third-order symmetries: $[S^{(2)}, iH_\ell \otimes \mathbb{I} + \mathbb{I} \otimes iH_\ell] = 0$ and $[S^{(3)}, iH_\ell \otimes \mathbb{I} \otimes \mathbb{I} + \mathbb{I} \otimes iH_\ell \otimes \mathbb{I} + \mathbb{I} \otimes \mathbb{I} iH_\ell] = 0$ for all $\{iH_1, iH_2, \ldots, iH_n\}$.
  - $[S^{(2)}, iH \otimes \mathbb{I} + \mathbb{I} \otimes iH] \neq 0 \Leftrightarrow iH \notin \langle iH_1, \ldots, iH_m \rangle_{\mathrm{Lie}}$ (morally).[8]

[8] Z. Zimborás, R. Zeier, T. Schulte-Herbrueggen, D. Burgarth, *Symmetry criteria for quantum simulability of effective interactions*, Phys. Rev. A 92, 042309 (2015). R. Zeier, Z. Zimborás, *On squares of representations of compact Lie algebras*, J. Math. Phys. 56, 081702 (2015).

Mathematical tools (II): higher-order symmetries

- For Unitary Gates:
  - A non-trivial second-order symmetry $S^{(2)}$ on $\mathcal{H}^{\otimes 2}$ or a third-order symmetry $S^{(3)}$ on $\mathcal{H}^{\otimes 3}$ are operators that satisfy $[S^{(2)}, U_i \otimes U_i] = 0$ and $[S^{(3)}, U_i \otimes U_i \otimes U_i] = 0$ for all $\{U_1, U_2, \ldots, U_n\}$.
  - If for some n-th order symmetry $[S^{(n)}, U^{\otimes n}] \neq 0$, then U cannot be generated. However, only by checking it for all n is this known to be a sufficient an necessary condition.
- For Hamiltonians:
  - Second-order and third-order symmetries: $[S^{(2)}, iH_\ell \otimes \mathbb{I} + \mathbb{I} \otimes iH_\ell] = 0$ and $[S^{(3)}, iH_\ell \otimes \mathbb{I} \otimes \mathbb{I} + \mathbb{I} \otimes iH_\ell \otimes \mathbb{I} + \mathbb{I} \otimes \mathbb{I} iH_\ell] = 0$ for all $\{iH_1, iH_2, \ldots, iH_n\}$.
  - $[S^{(2)}, iH \otimes \mathbb{I} + \mathbb{I} \otimes iH] \neq 0 \Leftrightarrow iH \notin \langle iH_1, \ldots, iH_m \rangle_{\mathrm{Lie}}$ (morally).[8]

[8] Z. Zimborás, R. Zeier, T. Schulte-Herbrueggen, D. Burgarth, *Symmetry criteria for quantum simulability of effective interactions*, Phys. Rev. A 92, 042309 (2015). R. Zeier, Z. Zimborás, *On squares of representations of compact Lie algebras*, J. Math. Phys. 56, 081702 (2015).

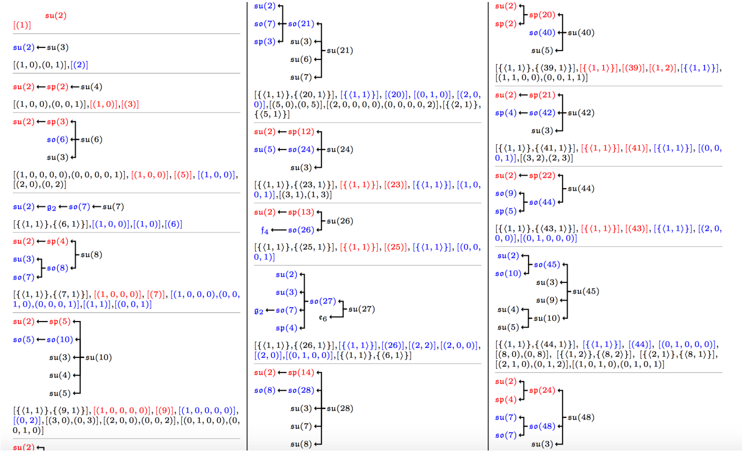
Mathematical tools (III): Dynkin's classification of irreducible Lie-subalgebras

TABLE VIII. Irreducible simple subalgebras not maximal in $\mathfrak{su}(\dim)$, $\mathfrak{sp}(\dim/2)$, or $\mathfrak{so}(\dim)$.

Subalgebra	Type	Highest weight(s)	Algebra	Highest weight(s)	dim
$\mathfrak{su}(\ell+1)$[a]	u	$(1,0,1,0,\ldots,0)$, $(0,\ldots,0,1,0,1)$	$\mathfrak{su}[\ell(\ell+1)/2]$	$(0,1,0,\ldots,0)$, $(0,\ldots,0,1,0)$	$3\binom{\ell+2}{4}$
$\mathfrak{su}(\ell+1)$[b]	u	$(2,1,0,\ldots,0)$, $(0,\ldots,0,1,2)$	$\mathfrak{su}[\ell(\ell+3)/2+1]$	$(0,1,0,\ldots,0)$, $(0,\ldots,0,1,0)$	$3\binom{\ell+3}{4}$
$\mathfrak{su}(2)$	o	(6)	$\mathfrak{g}_2$	$(1,0)$	7
$\mathfrak{su}(6)$	o	$(0,1,0,1,0)$	$\mathfrak{sp}(10)$	$(0,1,0,\ldots,0)$	189
$\mathfrak{so}(4k+3)$[c]	s/o[d]	$(0,\ldots,0,m)$	$\mathfrak{so}(4k+4)$	$(0,\ldots,0,m,0)$, $(0,\ldots,0,0,m)$	[e]
$\mathfrak{so}(9)$	o	$(1,0,0,1)$	$\mathfrak{so}(16)$	$(0,\ldots,0,1,0)$, $(0,\ldots,0,0,1)$	128
$\mathfrak{sp}(3)$	o	$(0,2,0)$	$\mathfrak{sp}(7)$	$(0,1,0,0,0,0,0)$	90
$\mathfrak{sp}(3)$	s	$(0,2,1)$	$\mathfrak{sp}(7)$	$(0,0,1,0,0,0,0)$	350
$\mathfrak{so}(10)$	u	$(0,1,0,1,0)$, $(0,1,0,0,1)$	$\mathfrak{su}(16)$	$(0,0,1,0,\ldots,0)$, $(0,\ldots,0,1,0,0)$	560
$\mathfrak{so}(12)$	o	$(0,0,0,1,0,0)$	$\mathfrak{sp}(16)$	$(0,1,0,0,\ldots,0)$	495
$\mathfrak{so}(12)$	s	$(0,0,1,0,1,0)$, $(0,0,1,0,0,1)$	$\mathfrak{sp}(16)$	$(0,0,1,0,\ldots,0)$	4928
$\mathfrak{e}_6$	u	$(0,0,1,0,0,0)$, $(0,0,0,0,1,0)$	$\mathfrak{su}(27)$	$(0,1,0,0,0,\ldots,0)$	351
$\mathfrak{e}_6$	u	$(0,1,1,0,0,0)$, $(0,1,0,0,1,0)$	$\mathfrak{su}(27)$	$(0,0,0,1,0,\ldots,0)$	17550
$\mathfrak{e}_7$	o	$(0,0,0,0,0,1,0)$	$\mathfrak{sp}(28)$	$(0,1,0,\ldots,0)$	1539
$\mathfrak{e}_7$	s	$(0,0,0,0,1,0,0)$	$\mathfrak{sp}(28)$	$(0,0,1,0,\ldots,0)$	27664
$\mathfrak{e}_7$	o	$(0,0,0,1,0,0,0)$	$\mathfrak{sp}(28)$	$(0,0,0,1,0,\ldots,0)$	365750
$\mathfrak{e}_7$	s	$(0,1,1,0,0,0,0)$	$\mathfrak{sp}(28)$	$(0,0,0,0,1,0,\ldots,0)$	3792096
$\mathfrak{g}_2$[f]	o	$(m,0)$	$\mathfrak{so}(7)$	$(m,0,0)$	$\frac{2m+5}{5}\binom{m+4}{4}$

[a] $\ell \geq 4$.
[b] $\ell \geq 3$.
[c] $k \geq 1$, $m \geq 1$; but not $k = m = 1$ (corrected) as $\mathfrak{so}(7)\subset\mathfrak{so}(8)\subset\mathfrak{su}(8)$.
[d] If $(k+1)m$ is odd then s else o.
[e] $\prod_{s=1}^{2k+1}\left[\binom{m+2s-1}{m}/\binom{m+s-1}{m}\right]$ (corrected).
[f] $m \geq 2$.

Constructing complete Lie-subalgebra tables



Passive bosonic linear optics (I)

For $d = 2$ we define $\mathbb{L}_b = |\Psi_b\rangle\langle\Psi_b|$, where

$$|\Psi_b\rangle = \sum_{k=0}^{N} (-1)^k |D_k\rangle|D_{N-k}\rangle \in \mathcal{H}_b \otimes \mathcal{H}_b \ ,$$

and $|D_k\rangle$ are two-mode Dicke states.

THEOREM

Let $V \notin \mathrm{LO}_b$ be a gate acting on Hilbert space of N bosons in d modes (with $N \neq 6$).
We have the following possibilities:

(i) If $d > 2$, then $\langle \mathrm{LO}_b, V\rangle = \mathrm{U}\left(\mathcal{H}_b\right)$.

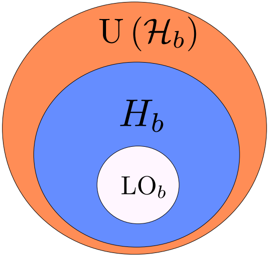
(ii) If $d = 2$ and $[V \otimes V, \mathbb{L}_b] = 0$, then

$$\langle \mathrm{LO}_b, V\rangle = H_b = \{U \in \mathrm{U}\left(\mathcal{H}_b\right) |\, [U \otimes U, \mathbb{L}_b] = 0\ \}.$$

(iii) If $[V \otimes V, \mathbb{L}_b] \neq 0$, then $\langle \mathrm{LO}_b, V\rangle = \mathrm{U}\left(\mathcal{H}_b\right)$.

Passive bosonic linear optics (II)

Extensions of LO_b for two modes and $N \neq 6$ particles.



- When N - even, then $H_b = \langle \mathrm{SO}(\mathcal{H}_b), \exp(i\phi)\mathbb{I} \rangle$ and we have **no transitivity for pure states**;
- When N - odd, then $H_b = \langle \mathrm{USp}(\mathcal{H}_b), \exp(i\phi)\mathbb{I} \rangle$ and we have **transitivity for pure states**;
- Extra Hamiltonian $H_{in} = n_1^3 - n_2^3$ promotes LO_b to H_b.

Passive fermionic linear optics

For $d = 2N$ (half-filling) we define $\mathbb{L}_f = |\Psi_f\rangle\langle\Psi_f|$, where

$$|\Psi_f\rangle = |1\rangle \wedge |2\rangle \wedge \ldots \wedge |2N\rangle \in \mathcal{H}_f \otimes \mathcal{H}_f .$$

Theorem

Let $V \notin \mathrm{LO}_f$ be a gate acting on Hilbert space of N fermions in d modes. We have the following possibilities:

(i) If $d \neq 2N$, then $\langle \mathrm{LO}_f, V\rangle = \mathrm{U}(\mathcal{H}_f)$.

(ii) If $d = 2N$ and $V = Wg$, for $g \in \mathrm{LO}_f$ and $W = \prod_{i=1}^{d}(a_i + a_i^\dagger)$, then

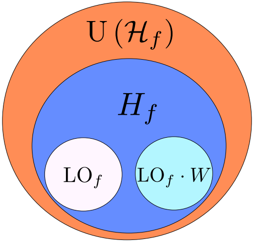
$$\langle \mathrm{LO}_f, V\rangle = \mathrm{LO}_f \cup \mathrm{LO}_f \cdot W \ .$$

(iii) If $d = 2N$, $V \neq gW$, for $g \in \mathrm{LO}_f$, and $[V \otimes V, \mathbb{L}_f] = 0$, then

$$\langle \mathrm{LO}_f, V\rangle = H_f = \{ U \in \mathrm{U}(\mathcal{H}_f) |\ [V \otimes V, \mathbb{L}_f] = 0 \ \}.$$

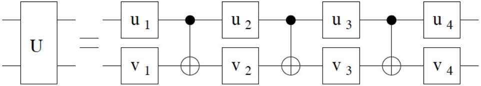
Passive fermionic linear optics

Extensions of LO_f for the case of half-filling $N = d/2$.

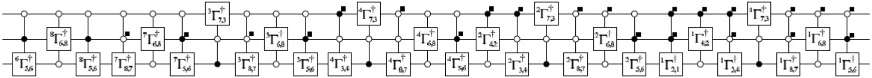


- When N - even, then $H_f = \langle \mathrm{SO}(\mathcal{H}_f), \exp(i\phi)\mathbb{I} \rangle$ and we have **no transitivity for pure states**;
- When N - odd, then $H_f = \langle \mathrm{USp}(\mathcal{H}_f), \exp(i\phi)\mathbb{I} \rangle$ and we have **transitivity for pure states**;
- An extra Hamiltonian with correlated hopping terms $H'_{in} = \sum_j i \left(a_j n_{j+1} a^\dagger_{j+2} - \mathrm{h.c} \right)$ promotes LO_f to H_f.

Generic two-qubit gate decomposition

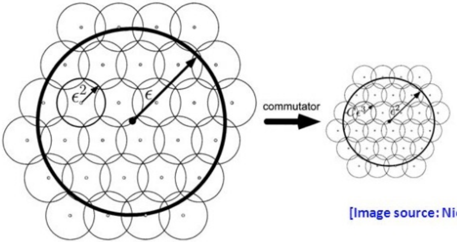


Generic three-qubit gate decomposition



Solovay-Kitaev algorithm

Goal: Approximate unitaries by elements of dense subgroup $G \leq U(N)$
Basic idea: Successive refining of a "net" using commutators



[Image source: Nielsen/Chuang, CUP 2000]

Implementations:

- **[Kitaev, Shen, Vyialyi, AMS 2002]:** $\log^{3+\delta}(1/\varepsilon)$ time, $\log^{3+\delta}(1/\varepsilon)$ length
- **[Dawson, Nielsen, quant-ph/0505030]:** $\log^{2.71}(1/\varepsilon)$ time, $\log^{3.97}(1/\varepsilon)$ length
- **[Harrow, Recht, Chuang, quant-ph/0111031]:** non-constructive, $\log(1/\varepsilon)$ length