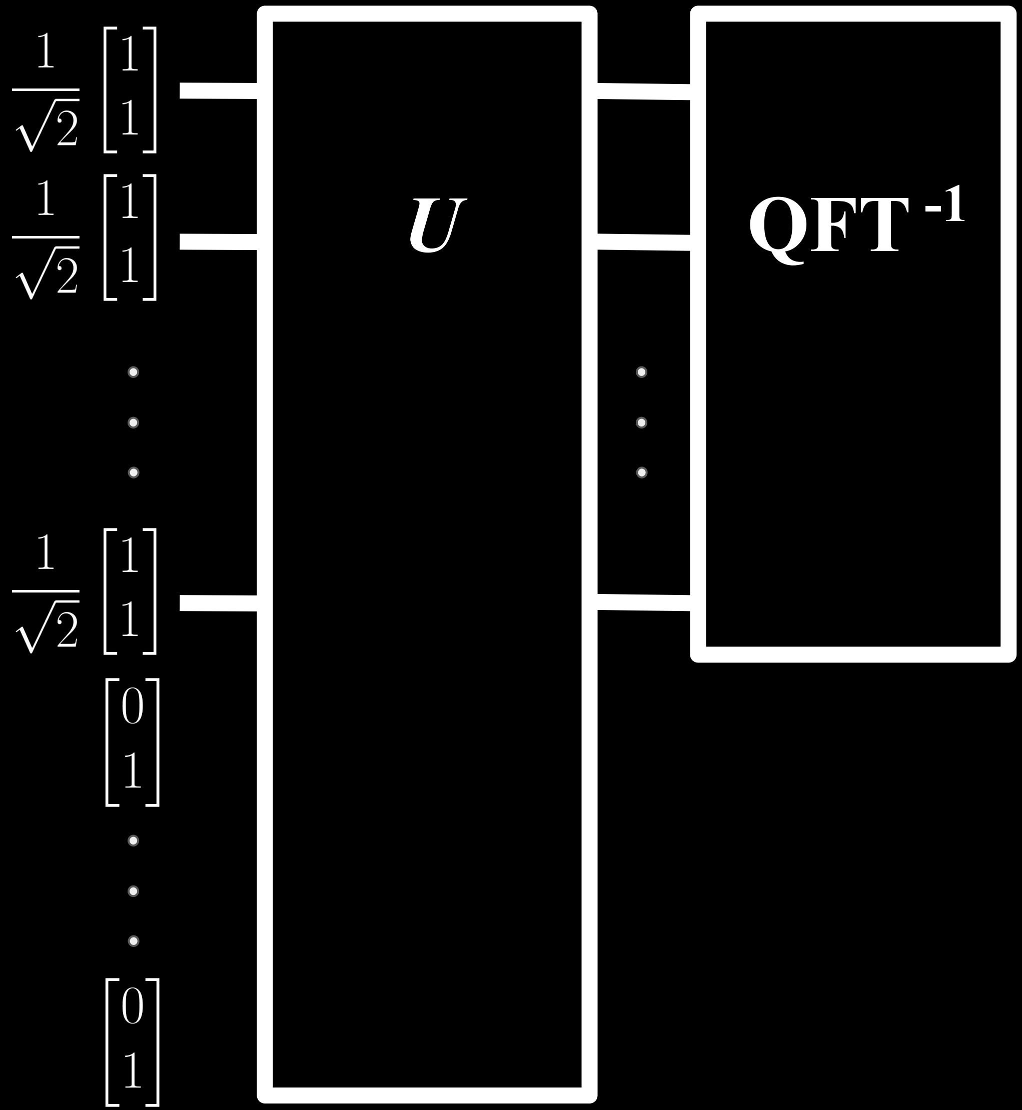
Adiabatic Quantum Computing
Lecture 2

Nike Dattani
nike@hpqc.org

HPQC Labs

2022 11 28

Largest number factored with Shor's algorithm?



<u>**Number factored**</u>	<u>**Year**</u>
15	2001
	2007
	2007
	2009
	2012
21	2012

Number factored	**Year**
15	2001
	2007
	2007
	2009
	2012
21	2012

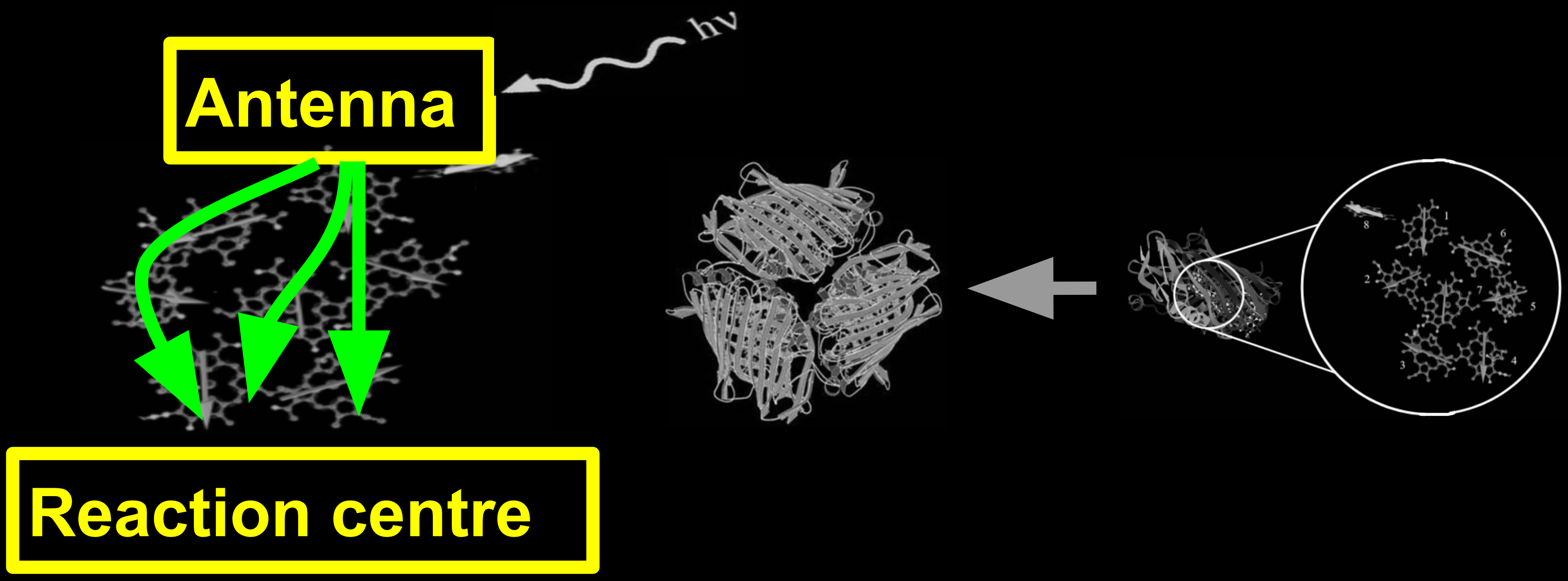
None of these used more than 7 qubits!

Number factored	Year
15	2001
	2007
	2007
	2009
	2012
21	2012

None of these used more than 7 qubits!

At around the same time…

Quantum effects in photosynthesis



Approximate quantum dynamics for the FMO:

2008 Jang et. al : Small polaron
2008 Piilo, Maniscalco, Härkönen, Suominen: NMQJ
2009 Palmieri, Abramavicius, Mukamel : Extended Lindblad approach
2009 Ishizaki & Fleming : Redfield equation
2009 Ishizaki & Fleming : Doctor equations
2009 Roden, Eisfeld, Strunz: Quantum state diffusion
2009 Rebentrost & Aspuru-Guzik: NMQJ
2010 Huo & Coker : Linearized Feynman integral
2010 Huo & Coker : Iterative Linearized Feynman integral
2010 Tao & Miller : Semi-classical Feynman integral
2010 Prior, Chin, Huelga, Plenio: t-DMRG - for 2 site sub-system
2010 Wu, ... , Silbey: generalized Bloch-Redfield
2011 Zhu, Kais, Rebentrost, Aspuru-Guzik: Scaled doctor equations
2011 Lloyd : time non-local quantum master equation
2011 Nalbach & Thorwart : Quasiadiabatic Feynman integral – for 7 site sub-system
2011 Ritschel, Roden, Strunz, Eisfeld : NMQSD-ZOFE , 7-level, arb. Temp. , arb. J(w)
2011 Pachon & Brumer : NIBA, 2-level, ohmic J(w)
2011 Alicki & Miklaszewski : Wigner-Weisskopf-type model (not a typical model)
2012 Reichman, Markland, Berkelbach : RDM-hybrid
2012 Markland, Berkelbach, Reichman : Ehrenfest Trajectories

.... and more (stochastic Liouville equations, generalized master equations, etc.)

Approximate quantum dynamics for the FMO:

2008 Jang et. al : Small polaron
2008 Piilo, Maniscalco, Härkönen, Suominen: NMQJ
2009 Palmieri, Abramavicius, Mukamel :
2009 Ishizaki & Fleming : Redfield equati
2009 Ishizaki & Fleming : Doctor equation
2009 Roden, Eisfeld, Strunz: Quantum sta
2009 Rebentrost & Aspuru-Guzik: NMQJ
2010 Huo & Coker : Linearized Feynman
2010 Huo & Coker : Iterative Linearized
2010 Tao & Miller : Semi-classical Feynma
2010 Prior, Chin, Huelga, Plenio: t-DMRG
2010 Wu, ... , Silbey: generalized Bloch-Re
2011 Zhu, Kais, Rebentrost, Aspuru-Guzik
2011 Lloyd : time non-local quantum master equation
2011 Nalbach & Thorwart : Quasiadiabatic Feynman integral – for 7 site sub-system
2011 Ritschel, Roden, Strunz, Eisfeld : NMQSD-ZOFE , 7-level, arb. Temp. , arb. J(w)
2011 Pachon & Brumer : NIBA, 2-level, ohmic J(w)
2011 Alicki & Miklaszewski : Wigner-Weisskopf-type model (not a typical model)
2012 Reichman, Markland, Berkelbach : RDM-hybrid
2012 Markland, Berkelbach, Reichman : Ehrenfest Trajectories

.... and more (stochastic Liouville equations, generalized master equations, etc.)

Numerically exact quantum dynamics:

***Feyn**man **Dyn**amics on GPUs* (https://github.com/ndattani)

Contents lists available at ScienceDirect

Computer Physics Communications

journal homepage: www.elsevier.com/locate/cpc

ELSEVIER

COMPUTER PHYSICS COMMUNICATIONS

CrossMark

FeynDyn: A MATLAB program for fast numerical Feynman integral calculations for open quantum system dynamics on GPUs☆

Nikesh S. Dattani *

Physical and Theoretical Chemistry Laboratory, Department of Chemistry, Oxford University, Oxford, OX1 3QZ, UK

Why Quantum Coherence Is Not Important in the Fenna–Matthews–Olsen Complex

David M. Wilkins*,
Physical and Theoretical Chemistry Laboratory, Oxford University, South Parks Road, Oxford, OX1 3QZ, United Kingdom
Nikesh S. Dattani*
Quantum Chemistry Laboratory, Department of Chemistry, Kyoto University, 606-8502, Kyoto, Japan
School of Materials Science and Engineering, Nanyang Technological University, Block N4.1, Nanyang Avenue, Singapore 639798

J. Chem. Theory Comput., **2015**, *11* (7), pp 3411–3419
DOI: 10.1021/ct501066k
Publication Date (Web): March 4, 2015

*E-mail: david.wilkins@chem.ox.ac.uk (D. M. Wilkins)., *E-mail: dattani.nike@gmail.com (N. S. Dattani).

Why Quantum Coherence Is Not Important in the Fenna–Matthews–Olsen Complex

David M. Wilkins*,
Physical and Theoretical Chemistry Laboratory, Oxford University, South Parks Road, Oxford, OX1 3QZ, United Kingdom
Nikesh S. Dattani*
pan
nyang Avenue, Singapore

QUEEN'S UNIVERSITY BELFAST

Home Profiles Organisations Research output Projects Impact Datasets

View Scopus Profile

David Wilkins

Dr
Vice-Chancellor Illuminate Fellow, **School of Mathematics and Physics**
Atomistic Simulation Centre (ASC)
https://orcid.org/0000-0003-3739-5512

Phone
+44 (0)28 9097 3643

Email
D.Wilkins@qub.ac.uk

Room LG.022 - New Physics
United Kingdom

Accepting PhD Students

Feynman dynamics

Feynman (1959)

Leggett & Caldeira (1983): 2 levels

Makri *et. al.* (1995): 3 levels

Sim & Kim (2006): 5 levels

Kim & Sim (2010): 10 levels

Wilkins, Dattani (2011): 24 levels - FMO (quantum effects in photosynthesis)

Strumpfer, Schulten (2012): 50 levels

Tsuchimoto, Tanimura (2014): 512 levels

Jones, Dattani (2014): 600 levels

Dattani, Chen, Gelin, Domcke (2014): 800 levels

Dattani, Bryans (2014): 1024 levels - 10 qubit quantum computer

<u>Number factored</u>	<u>Year</u>
15	2001
	2007
	2007
	2009
	2012
21	2012

None of these used more than <u>7 qubits</u>!

At around the same time...

Methods developed for numerically exact quantum dynamics could simulate up to <u>10 qubits</u> with decoherence.

Factoring 143

	b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0	
Multiplier					1	p_2	p_1	1	p
					1	q_2	q_1	1	x q
Binary-multiplication					1	p_2	p_1	1	
				q_1	p_2q_1	p_1q_1	q_1		
			q_2	p_2q_2	p_1q_2	q_2			
		1	p_2	p_1	1				
Carry	z_{67}	z_{56}	z_{45}	z_{34}	z_{23}	z_{12}			
	z_{57}	z_{46}	z_{35}	z_{24}					
Product	1	0	0	0	1	1	1	1	143

Factoring 143

	b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0
Multiplier					1	p_2	p_1	1
					1	q_2	q_1	1
Binary-multiplication					1	p_2	p_1	1
				q_1	p_2q_1	p_1q_1	q_1	
			q_2	p_2q_2	p_1q_2	q_2		
		1	p_2	p_1	1			
Carry	z_{67}	z_{56}	z_{45}	z_{34}	z_{23}	z_{12}		
	z_{57}	z_{46}	z_{35}	z_{24}				
Product	1	0	0	0	1	1	1	1

p

x q

143

$$
\begin{aligned}
p_1 + q_1 &= 1 + 2z_{12} \\
p_2 + p_1q_1 + q_2 + z_{12} &= 1 + 2z_{23} + 4z_{24} \\
1 + p_2q_1 + p_1q_2 + 1 + z_{23} &= 1 + 2z_{34} + 4z_{35} \\
q_1 + p_2q_2 + p_1 + z_{34} + z_{24} &= 0 + 2z_{45} + 4z_{46} \\
q_2 + p_2 + z_{45} + z_{35} &= 0 + 2z_{56} + 4z_{57} \\
1 + z_{56} + z_{46} &= 0 + 2z_{67} \\
z_{67} + z_{57} &= 1.
\end{aligned}
$$

Deductions !!!

$$a + b = 1 + 2c$$

What is c ?

Compile your code before you run it:

$$\begin{aligned}
p_1 + q_1 &= 1 + 2z_{12} \\
p_2 + p_1 q_1 + q_2 + z_{12} &= 1 + 2z_{23} + 4z_{24} \\
1 + p_2 q_1 + p_1 q_2 + 1 + z_{23} &= 1 + 2z_{34} + 4z_{35} \\
q_1 + p_2 q_2 + p_1 + z_{34} + z_{24} &= 0 + 2z_{45} + 4z_{46} \\
q_2 + p_2 + z_{45} + z_{35} &= 0 + 2z_{56} + 4z_{57} \\
1 + z_{56} + z_{46} &= 0 + 2z_{67} \\
z_{67} + z_{57} &= 1.
\end{aligned}$$

$$\downarrow$$

$$\begin{aligned}
p_1 + q_1 &= 1 \\
p_2 + q_2 &= 1 \\
p_2 q_1 + p_1 q_2 &= 1
\end{aligned}$$

$$(p_1 + q_1 - 1)^2$$

The solution to:

$$p_1 + q_1 = 1$$

Is the same as the input that minimizes the function:

$$(p_1 + q_1 - 1)^2$$

The solution to:

$$\begin{aligned} p_1 + q_1 &= 1 \\ p_2 + q_2 &= 1 \\ p_2 q_1 + p_1 q_2 &= 1 \end{aligned}$$

Is the same as the minimum of the function:

$$(p_1 + q_1 - 1)^2 + (p_2 + q_2 - 1)^2 + (p_2 q_1 + p_1 q_2 - 1)^2$$

The solution to:

$$\begin{aligned} p_1 + q_1 &= 1 \\ p_2 + q_2 &= 1 \\ p_2 q_1 + p_1 q_2 &= 1 \end{aligned}$$

Is the same as the minimum of the function:

$$(p_1 + q_1 - 1)^2 + (p_2 + q_2 - 1)^2 + (p_2 q_1 + p_1 q_2 - 1)^2$$

$$5 - 3p_1 - p_2 - q_1 + 2p_1 q_1 - 3p_2 q_1 + 2p_1 p_2 q_1 - 3q_2 + p_1 q_2 + 2p_2 q_2 + 2p_2 q_1 q_2$$

$$5 - 3p_1 - p_2 - q_1 + 2p_1q_1 - 3p_2q_1 + 2p_1p_2q_1 - 3q_2 + p_1q_2 + 2p_2q_2 + 2p_2q_1q_2$$

p_1	p_2	q_1	q_2	F	
0	0	0	0	5	
0	0	0	1	2	
0	0	1	0	4	
0	0	1	1	1	
0	1	0	0	4	
0	1	0	1	3	
0	**1**	**1**	**0**	**0**	$\rightarrow p = 11, q = 13$
0	1	1	1	1	
1	0	0	0	2	
1	**0**	**0**	**1**	**0**	$\rightarrow p = 13, q = 11$
1	0	1	0	3	
1	0	1	1	1	
1	1	0	0	1	
1	1	0	1	1	
1	1	1	0	1	
1	1	1	1	3	

$$5 - 3p_1 - p_2 - q_1 + 2p_1q_1 - 3p_2q_1 + 2p_1p_2q_1 - 3q_2 + p_1q_2 + 2p_2q_2 + 2p_2q_1q_2$$

p_1	p_2	q_1	q_2	F
0	0	0	0	5
0	0	0	1	2
0	0	1	0	4
0	0	1	1	1
0	1	0	0	4
0	1	0	1	3
0	**1**	**1**	**0**	**0**
0	1	1	1	1
1	0	0	0	2
1	**0**	**0**	**1**	**0**
1	0	1	0	3
1	0	1	1	1
1	1	0	0	1
1	1	0	1	1
1	1	1	0	1
1	1	1	1	3

$$\rightarrow p = 11, q = 13$$

$$\rightarrow p = 13, q = 11$$

4 variables:

Search through 2^4 possibilities

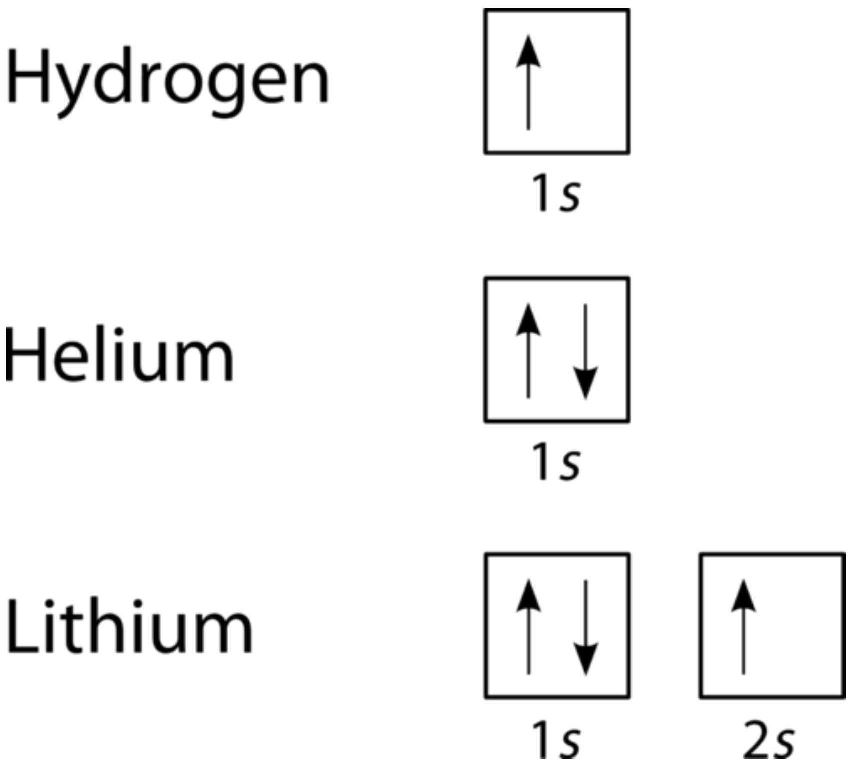
5000 variables:

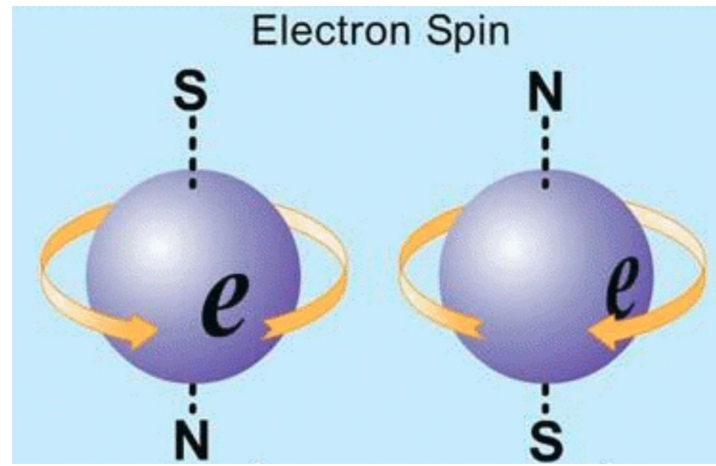
Search through 2^{5000} possibilities

$$5 - 3p_1 - p_2 - q_1 + 2p_1q_1 - 3p_2q_1 + 2p_1p_2q_1 - 3q_2 + p_1q_2 + 2p_2q_2 + 2p_2q_1q_2$$
$$5 - 3b_1 - b_2 - b_3 + 2b_1b_3 - 3b_2b_3 + 2b_1b_2b_3 - 3b_3 + b_1b_4 + 2b_2b_4 + 2b_2b_3b_4$$

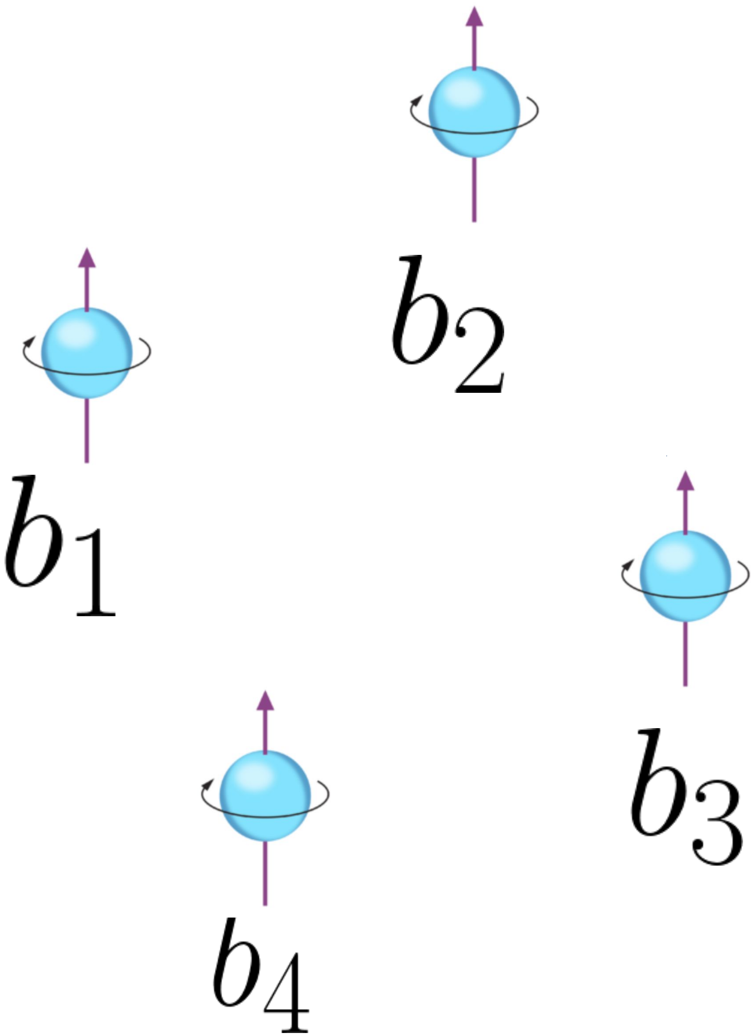
$$5 - 3p_1 - p_2 - q_1 + 2p_1q_1 - 3p_2q_1 + 2p_1p_2q_1 - 3q_2 + p_1q_2 + 2p_2q_2 + 2p_2q_1q_2$$

$$5 - 3b_1 - b_2 - b_3 + 2b_1b_3 - 3b_2b_3 + 2b_1b_2b_3 - 3b_3 + b_1b_4 + 2b_2b_4 + 2b_2b_3b_4$$



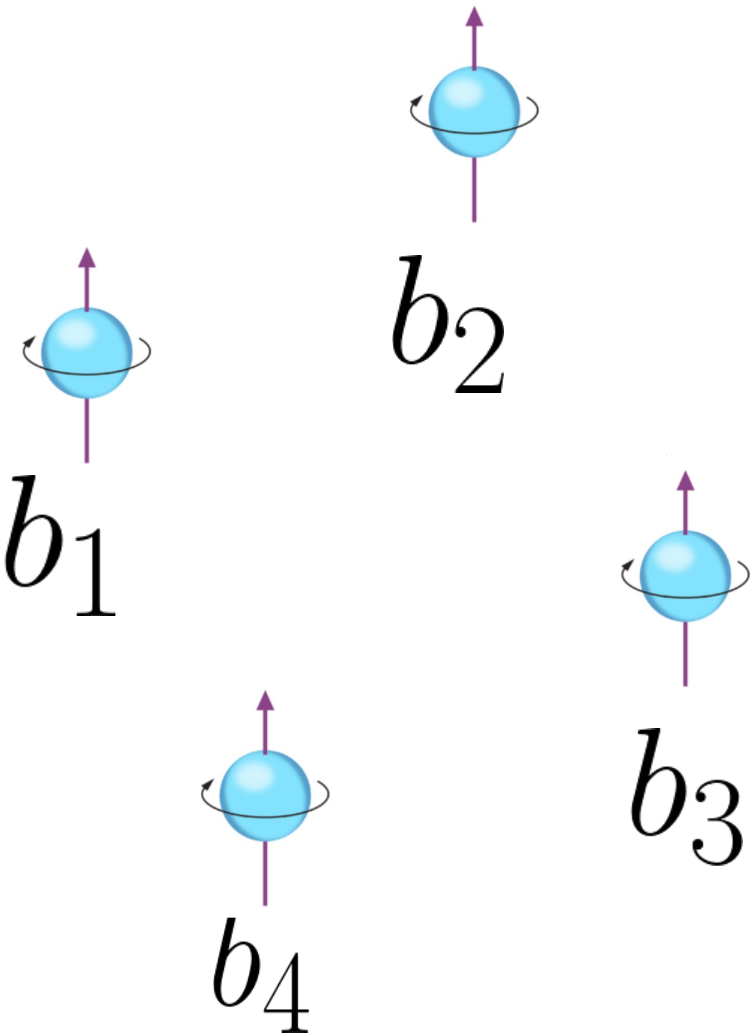


$$5 - 3p_1 - p_2 - q_1 + 2p_1q_1 - 3p_2q_1 + 2p_1p_2q_1 - 3q_2 + p_1q_2 + 2p_2q_2 + 2p_2q_1q_2$$
$$5 - 3b_1 - b_2 - b_3 + 2b_1b_3 - 3b_2b_3 + 2b_1b_2b_3 - 3b_3 + b_1b_4 + 2b_2b_4 + 2b_2b_3b_4$$



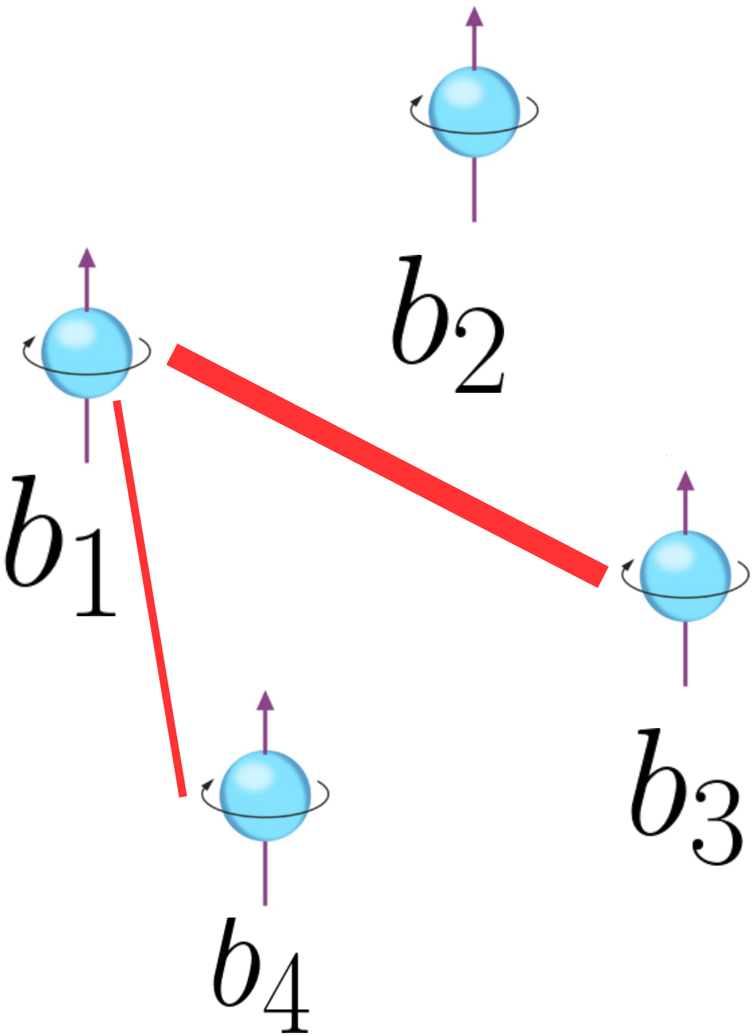
$$5 - 3p_1 - p_2 - q_1 + 2p_1q_1 - 3p_2q_1 + 2p_1p_2q_1 - 3q_2 + p_1q_2 + 2p_2q_2 + 2p_2q_1q_2$$

$$5 - 3b_1 - b_2 - b_3 + 2b_1b_3 - 3b_2b_3 + 2b_1b_2b_3 - 3b_3 + b_1b_4 + 2b_2b_4 + 2b_2b_3b_4$$



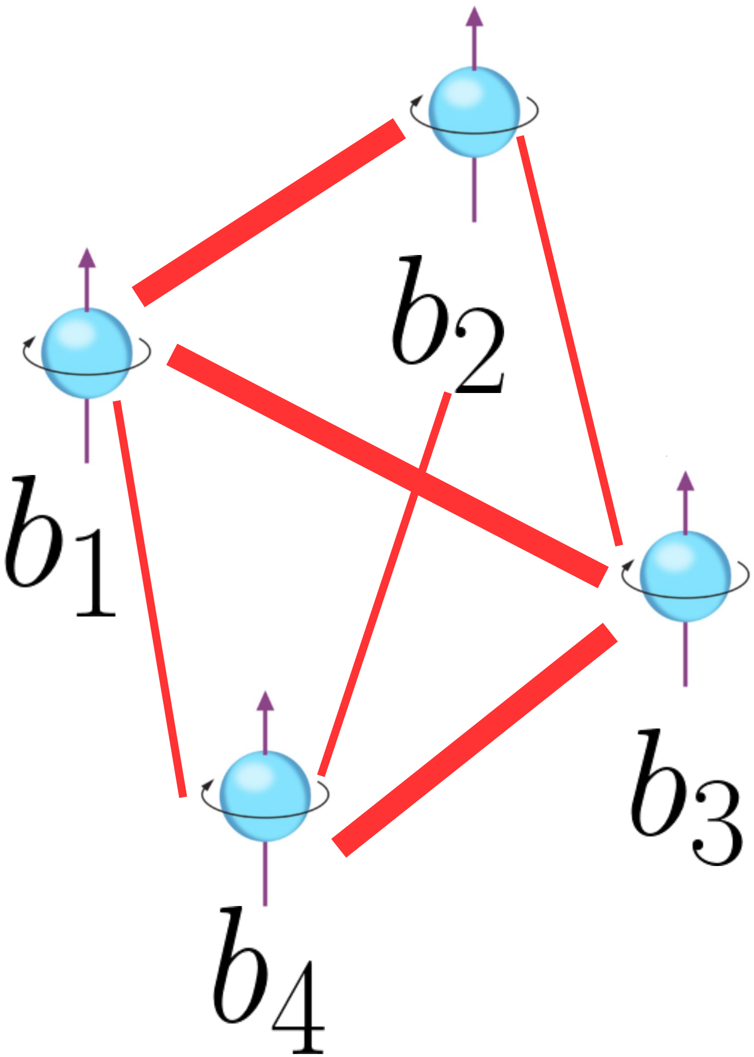
$$5 - 3p_1 - p_2 - q_1 + 2p_1q_1 - 3p_2q_1 + 2p_1p_2q_1 - 3q_2 + p_1q_2 + 2p_2q_2 + 2p_2q_1q_2$$

$$5 - 3b_1 - b_2 - b_3 + 2b_1b_3 - 3b_2b_3 + 2b_1b_2b_3 - 3b_3 + b_1b_4 + 2b_2b_4 + 2b_2b_3b_4$$



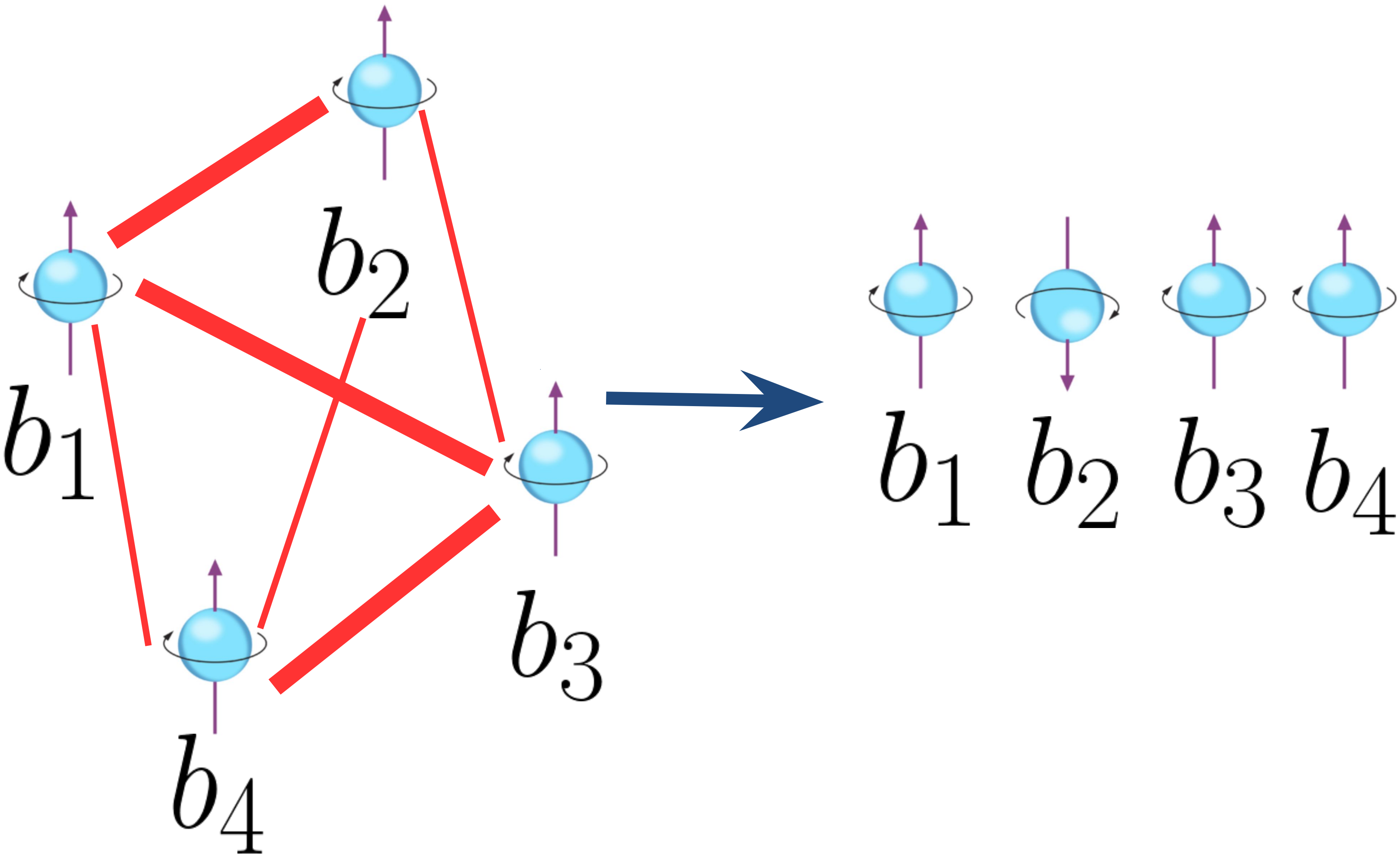
$$5 - 3p_1 - p_2 - q_1 + 2p_1q_1 - 3p_2q_1 + 2p_1p_2q_1 - 3q_2 + p_1q_2 + 2p_2q_2 + 2p_2q_1q_2$$

$$5 - 3b_1 - b_2 - b_3 + 2b_1b_3 - 3b_2b_3 + 2b_1b_2b_3 - 3b_3 + b_1b_4 + 2b_2b_4 + 2b_2b_3b_4$$



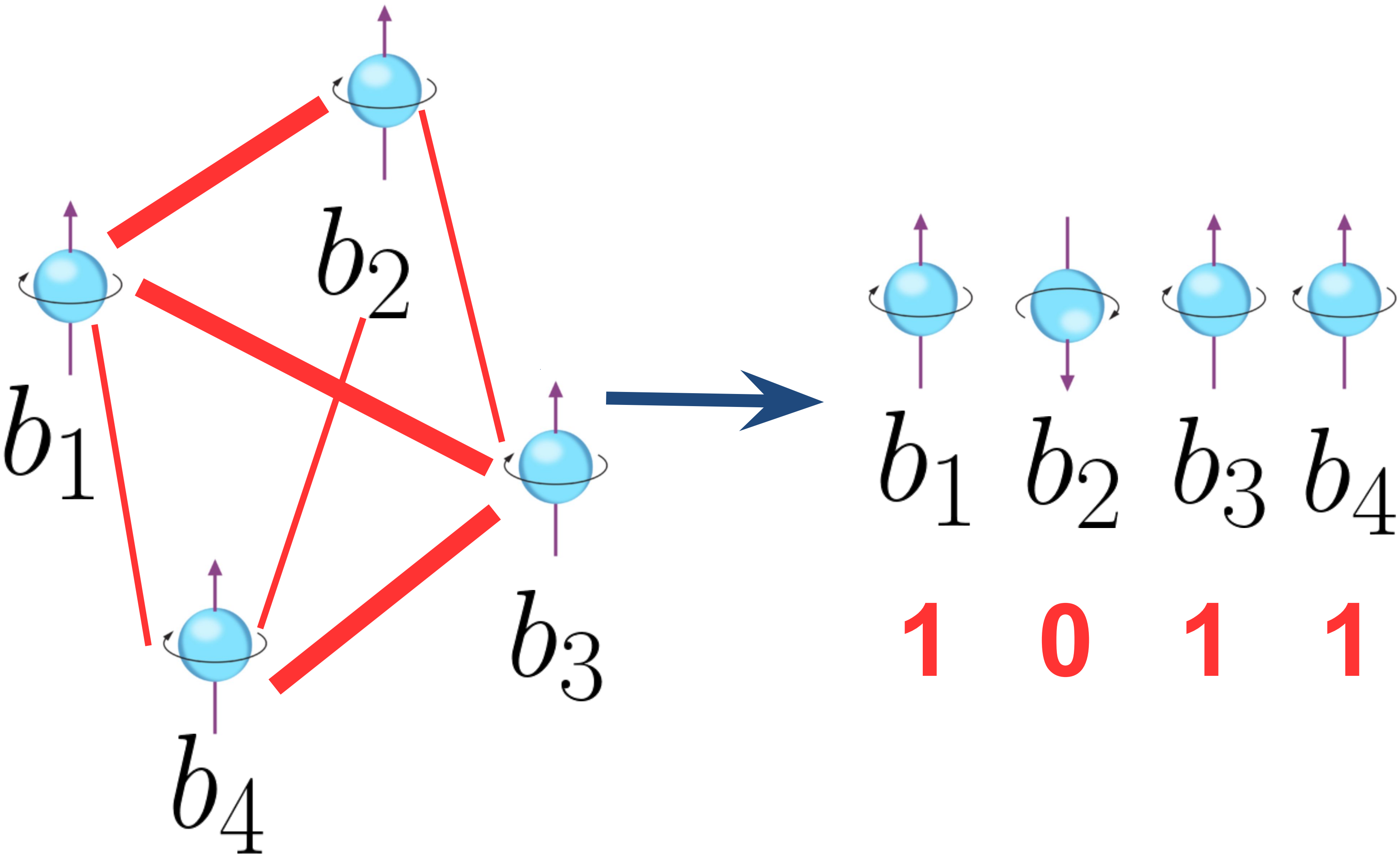
$$5 - 3p_1 - p_2 - q_1 + 2p_1q_1 - 3p_2q_1 + 2p_1p_2q_1 - 3q_2 + p_1q_2 + 2p_2q_2 + 2p_2q_1q_2$$

$$5 - 3b_1 - b_2 - b_3 + 2b_1b_3 - 3b_2b_3 + 2b_1b_2b_3 - 3b_3 + b_1b_4 + 2b_2b_4 + 2b_2b_3b_4$$



$$5 - 3p_1 - p_2 - q_1 + 2p_1q_1 - 3p_2q_1 + 2p_1p_2q_1 - 3q_2 + p_1q_2 + 2p_2q_2 + 2p_2q_1q_2$$

$$5 - 3b_1 - b_2 - b_3 + 2b_1b_3 - 3b_2b_3 + 2b_1b_2b_3 - 3b_3 + b_1b_4 + 2b_2b_4 + 2b_2b_3b_4$$

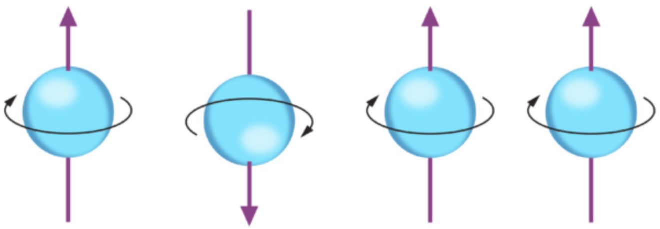


4 variables:

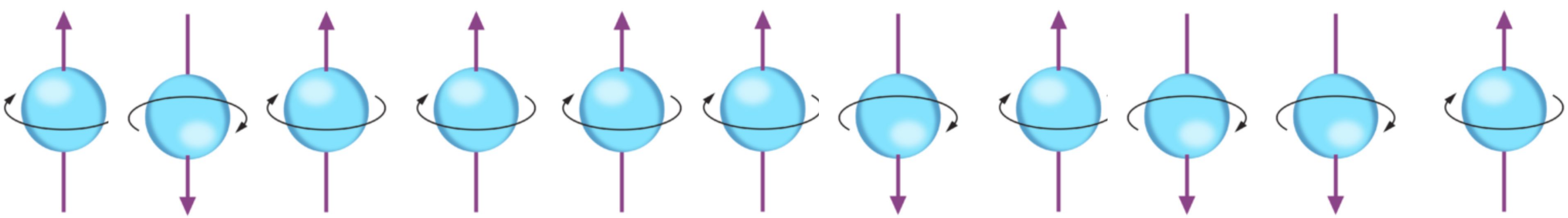
Search through 2^4 possibilities

5000 variables:

Search through 2^{5000} possibilities



$b_1 \quad b_2 \quad b_3 \quad b_4$



$b_1 \quad b_2 \quad b_3 \quad b_4 \quad b_5 \quad b_6 \quad b_7 \quad b_8 \quad b_9 \quad b_{10}$

Adiabatic Quantum Computing

- Encode the solution to your problem in the ground state of a Hamiltonian.

- Find the ground state of that Hamiltonian

Quantum Chemistry

$$H = \sum_{p,q} h_{pq} a_p^\dagger a_q + \frac{1}{2} \sum_{p,q,r,s} h_{pqrs} a_p^\dagger a_q^\dagger a_r a_s$$

Jordan-Wigner Transform

$$a_j \Leftrightarrow \mathbf{1}^{\otimes j-1} \otimes \sigma^+ \otimes \sigma^{z \otimes N-j-1}$$

$$a_j^\dagger \Leftrightarrow \mathbf{1}^{\otimes j-1} \otimes \sigma^- \otimes \sigma^{z \otimes N-j-1}$$

$$\sigma^y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad \sigma^x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma^+ \equiv \frac{\sigma^x + i\sigma^y}{2} \qquad \sigma^- \equiv \frac{\sigma^x - i\sigma^y}{2}$$

H_2 molecule

$$
\begin{aligned}
H &= -0.812261\mathbf{1} + 0.171201 Z_0 + 0.171201 Z_1 - 0.2227965 Z_2 - 0.2227965 Z_3 \\
&= +0.16862325 Z_1 Z_0 + 0.12054625 Z_2 Z_0 + 0.165868 Z_2 Z_1 + 0.165868 Z_3 Z_0 \\
&= +0.12054625 Z_3 Z_1 + 0.17434925 Z_3 Z_2 - 0.04532175 X_3 X_2 Y_1 Y_0 \\
&= +0.04532175 X_3 Y_2 Y_1 X_0 + 0.04532175 Y_3 X_2 X_1 Y_0 - 0.04532175 Y_3 Y_2 X_1 X_0
\end{aligned}
$$

```
1111000001
                                          1    p3    p2    p1     1
                                          1    q3    q2    q1     1
------------------------------------------------------------------------
                                          1    p3    p2    p1     1
                                    q1 p3q1  p2q1  p1q1    q1
                              q2 p3q2  p2q2  p1q2    q2
                        q3 p3q3  p2q3  p1q3    q3
                 1      p3    p2    p1     1
------------------------------------------------------------------------
   z89   z78   z67   z56   z45   z34   z23   z12
   z79   z68   z57   z46   z35   z24
         z58   z47
------------------------------------------------------------------------
     1     1     1     1     0     0     0     0     0     1

1  =  1
p1 + q1  =  0 + 2z12
p2 + p1q1 + q2 + z12  =  0 + 2z23 + 4z24
p3 + p2q1 + p1q2 + q3 + z23  =  0 + 2z34 + 4z35
1 + p3q1 + p2q2 + p1q3 + 1 + z34 + z24  =  0 + 2z45 + 4z46 + 8z47
q1 + p3q2 + p2q3 + p1 + z45 + z35  =  0 + 2z56 + 4z57 + 8z58
q2 + p3q3 + p2 + z56 + z46  =  1 + 2z67 + 4z68
q3 + p3 + z67 + z57 + z47  =  1 + 2z78 + 4z79
1 + z78 + z68 + z58  =  1 + 2z89
z89 + z79  =  1
------------------------------------
Solved for all carries after 31 iterations!
z12  1
z23  0
z24  1
z34  0
z35  1
z45  1
z46  1
z47  0
z56  1
z57  1
z58  0
z67  0
z68  1
z78  1
z79  0
z89  1

1 = 1
p1 + q1 = 0 + 2 x z12
p2 + p1q1 + q2 + z12 = 0 + 2 x z23 + 4 x z24
p3 + p2q1 + p1q2 + q3 + z23 = 0 + 2 x z34 + 4 x z35
1 + p3q1 + p2q2 + p1q3 + 1 + z34 + z24 = 0 + 2 x z45 + 4 x z46 + 8 x z47
q1 + p3q2 + p2q3 + p1 + z45 + z35 = 0 + 2 x z56 + 4 x z57 + 8 x z58
q2 + p3q3 + p2 + z56 + z46 = 1 + 2 x z67 + 4 x z68
q3 + p3 + z67 + z57 + z47 = 1 + 2 x z78 + 4 x z79
1 + z78 + z68 + z58 = 1 + 2 x z89
z89 + z79 = 1
```

Quantum factorization of 56153 with only 4 qubits

Nikesh S. Dattani,[1,2,*] ***Nathaniel Bryans***[3,†]
[1]Quantum Chemistry Laboratory, Kyoto University, 606-8502, Kyoto, Japan, [2]Physical & Theoretical Chemistry Laboratory, Oxford University, OX1 3QZ, Oxford, UK, [3]University of Calgary, T2N 4N1, Calgary, Canada. *dattani.nike@gmail.com, †nbryans1@gmail.com

December 1, 2014

The largest number factored on a quantum device reported until now was 143 [1]. That quantum computation, which used only 4 qubits at 300K, actually also factored much larger numbers such as 3599, 11663, and 56153, without the awareness of the authors of that work. Furthermore, unlike the implementations of Shor's algorithm performed thus far [2–8], these 4-qubit factorizations do not need to use prior knowledge of the answer. However, because they only use 4 qubits, these factorizations can also be performed trivially on classical computers. We discover a class of numbers for which the power of quantum information actually comes into play. We then demonstrate a 3-qubit factorization of 175, which would be the first quantum factorization of a triprime.

and no prior knowledge of the answer to the problem. To provide context, factoring the number 15 with Shor's algorithm and no prior knowledge of the answer to the problem, requires a minimum of 8 qubits (and more if error correction is attempted); and this has still never been done.

Quantum factorization of 143

The NMR factorization of 143 in 2012 [1] began with the multiplication table:

Table 1: *Multiplication table for* $11 \times 13 = 143$ *in binary.*

	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
p					1	p_2	p_1	1
q					1	q_2	q_1	1
					1	p_2	p_1	1
				q_1	p_2q_1	p_1q_1	q_1	

Nathaniel Bryans

Director, Artificial Intelligence at ATB Financial

Nathaniel Bryans is a Director, Artificial Intelligence at ATB Financial based in Calgary, Alberta. Previously, Nathaniel was a Test Software Deve... Read More

New largest number factored on a quantum device is 56,153

Nov 28, 2014 by Lisa Zyga report

- **http://phys.org/news/2014-11-largest-factored-quantum-device.html**

PHYS.ORG

Sign In + Register

Physics · Nanotechnology · Earth · Astronomy & Space · Chemistry · Biology · Technology · Other Sciences · Medicine & Health

Home > Physics > Quantum Physics > November 28, 2014

New largest number factored on a quantum device is 56,153

Nov 28, 2014 by Lisa Zyga report

- http://phys.org/news/2014-11-largest-factored-quantum-device.html

Mathematical Trick Helps Smash Record For the Largest Quantum Factorization

Posted by **Soulskill** on Wednesday December 03, 2014 @11:02AM
from the still-slower-than-a-12-year-old dept.

- http://science.slashdot.org/story/14/12/03/1551239/mathematical-trick-helps-smash-record-for-the-largest-quantum-factorization

Wrednych Fizyków Dwóch komentuje wydarzenia naukowe i doniesienia

Magazine · Strona główna · Wredny Fizyk Jeden · Jeszcze Wredniejszy Fizyk · Wredny Facebook

NOV 30

Nowy rekord faktoryzacji liczb algorytmem kwantowym. Tylko nie wiadomo jaki... 56153? 44929?

- http://fizycy.blogspot.sg/2014/11/nowy-rekord-faktoryzacji-liczb.html7. International exchange achieved through the research

The Mathematical Trick That Helped Smash The Record For The Largest Number Ever Factorised By A Quantum Computer: 56153 = 233 x 241

- https://medium.com/the-physics-arxiv-blog/the-mathematical-trick-that-helped-smash-the-record-for-the-largest-number-ever-factorised-by-a-77fde88499

NSA Plans for a Post-Quantum World

Quantum computing is a novel way to build computers — one that takes advantage of the quantum properties of particles to perform operations on data in a very different way than traditional computers. In some cases, the algorithm speedups are extraordinary.

Specifically, a quantum computer using something called Shor's algorithm can efficiently factor numbers, breaking RSA. A variant can break Diffie-Hellman and other discrete log-based cryptosystems, including those that use elliptic curves. This could potentially render all modern public-

RSA (cryptosystem)

From Wikipedia, the free encyclopedia

RSA (**Rivest–Shamir–Adleman**) is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. The acronym **RSA** comes from the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who publicly described the algorithm in 1977. An equivalent system was

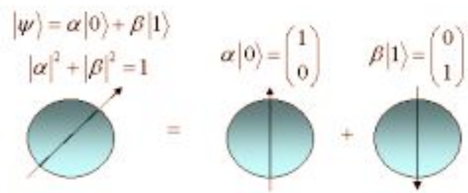
On the growth of cryptography[1]

Ronald L. Rivest

Vannevar Bush Professor of EECS
MIT, Cambridge, MA

Simons Institute Cryptography Program
Historical Papers Seminar Series
U.C. Berkeley
June 3, 2015

Factoring on a Quantum Computer?



In 1994, Peter Shor invented a fast factorization algorithm that runs on a (hypothetical) *quantum computer* and works by determining multiplicative period of elements mod *n*.

- In 2001, researchers at IBM used this algorithm on a (real) quantum computer to factor $15 = 3 \times 5$.
- Recently (Dattani, 2014): 291311 = 557 x 523

Factoring 291311 with NMR

High-fidelity adiabatic quantum computation using the intrinsic Hamiltonian of a spin system: Application to the experimental factorization of 291311

Zhaokai Li,[1,2] Nikesh S. Dattani,[3,4] Xi Chen,[1] Xiaomei Liu,[1] Hengyan Wang,[1]
Richard Tanburn,[3] Hongwei Chen,[5] Xinhua Peng,[1,2,6,*] and Jiangfeng Du[1,2,6,†]

[1] *CAS Key Laboratory of Microscale Magnetic Resonance and Department of Modern Physics, University of Science and Technology of China (USTC), Hefei 230026, China*
[2] *Synergetic Innovation Center of Quantum Information and Quantum Physics, USTC, Hefei, China*
[3] *Oxford University, Hertford College, Oxford, OX1 3BW, UK*
[4] *Fukui Institute for Fundamental Chemistry, Kyoto University, Kyoto, 606-8103, Japan*
[5] *High Magnetic Field Laboratory, Chinese Academy of Sciences, Hefei 230031, China*
[6] *Hefei National Laboratory for Physical Sciences at the Microscale, USTC, Hefei, China*

High-fidelity adiabatic quantum computation using the intrinsic Hamiltonian of a spin system: Application to the experimental factorization of 291311

Zhaokai Li, Nikesh S. Dattani, Xi Chen, Xiaomei Liu, Hengyan Wang, Richard Tanburn, Hongwei Chen, Xinhua Peng, Jiangfeng Du

(Submitted on 25 Jun 2017)

High-fidelity adiabatic quantum computation using the intrinsic Hamiltonian of a spin system: Application to the experimental factorization of 291311

Zhaokai Li,[1,2] Nikesh S. Dattani,[3,4] Xi Chen,[1] Xiaomei Liu,[1] Hengyan Wang,[1]
Richard Tanburn, Hongwei Chen,[5] Xinhua Peng,[1,2,6,*] and Jiangfeng Du[1,2,6,†]
[1] *CAS Key Laboratory of Microscale Magnetic Resonance and Department of Modern Physics,*

Article | Open Access | Published: 01 December 2021

Advancing mathematics by guiding human intuition with AI

Alex Davies, Petar Veličković, Lars Buesing, Sam Blackwell, Daniel Zheng, Nenad Tomašev, Richard Tanburn, Peter Battaglia, Charles Blundell, András Juhász, Marc Lackenby, Geordie Williamson, Demis Hassabis & Pushmeet Kohli

Nature **600**, 70–74 (2021) | Cite this article

mathoverflow

Home

PUBLIC

Breakthroughs in mathematics in 2021

Asked 2 months ago Active 1 month ago Viewed 9k times

51

Advancing mathematics by guiding human intuition with AI, Nature **600**, 70 (2021), stands out because it represents the first significant advance in pure mathematics generated by artificial intelligence.

Carlo Beenakker

Article | Open Access | Published: 01 December 2021

Advancing mathematics by guiding human intuition with AI

Alex Davies, Petar Veličković, Lars Buesing, Sam Blackwell, Daniel Zheng, Nenad Tomašev, Richard Tanburn, Peter Battaglia, Charles Blundell, András Juhász, Marc Lackenby, Geordie Williamson, Demis Hassabis & Pushmeet Kohli

Nature **600**, 70–74 (2021) | Cite this article

Shor's Algorithm	**Year**
15	2001
	2007
	2007
	2009
	2012
21	2012
Adiabatic Algorithm	**Year**
143	2012
56153	2014
291311	2017

Thank you!

Next lecture:

Compiling AQC algorithms to run on real hardware

nike@hpqc.org