Towards useful quantum computation

Damian Markham

Plan

1. What is quantum?

2. What is quantum computing?

3. What can we do with quantum computers?

4. What's so hard about building a quantum computer?

5. Near term quantum computing

6. Going beyond big algorithms: quantum networks

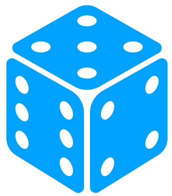
1. What is quantum?

1. What is quantum?

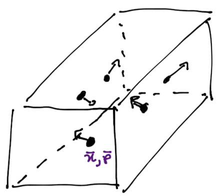
Quantum randomness is different from classical 'randomness'

Classical randomness = ignorance!

E.g. - rolling a die



- Boltzmann distribution of particles in a box



If we *know* the initial conditions, outcome is **deterministic**

Quantum randomness $\neq$ ignorance!

Quantum randomness ≠ ignorance!

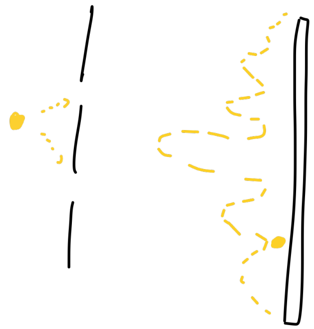
Polarisation filter measurements

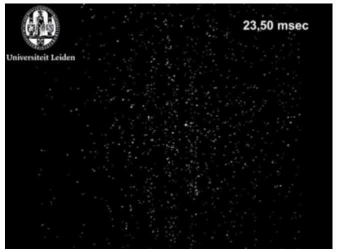
Sunglasses, photographic plates….

The tilting head game: (try looking at your phone / tablette
through polarised sunglasses and tilt you head)

Polarisation filter measurements

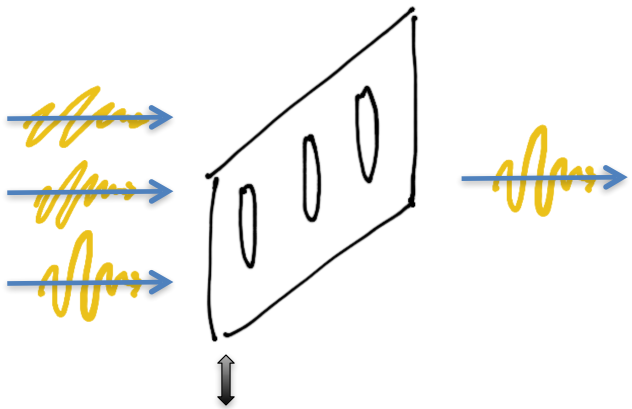
- Light comes in single photons



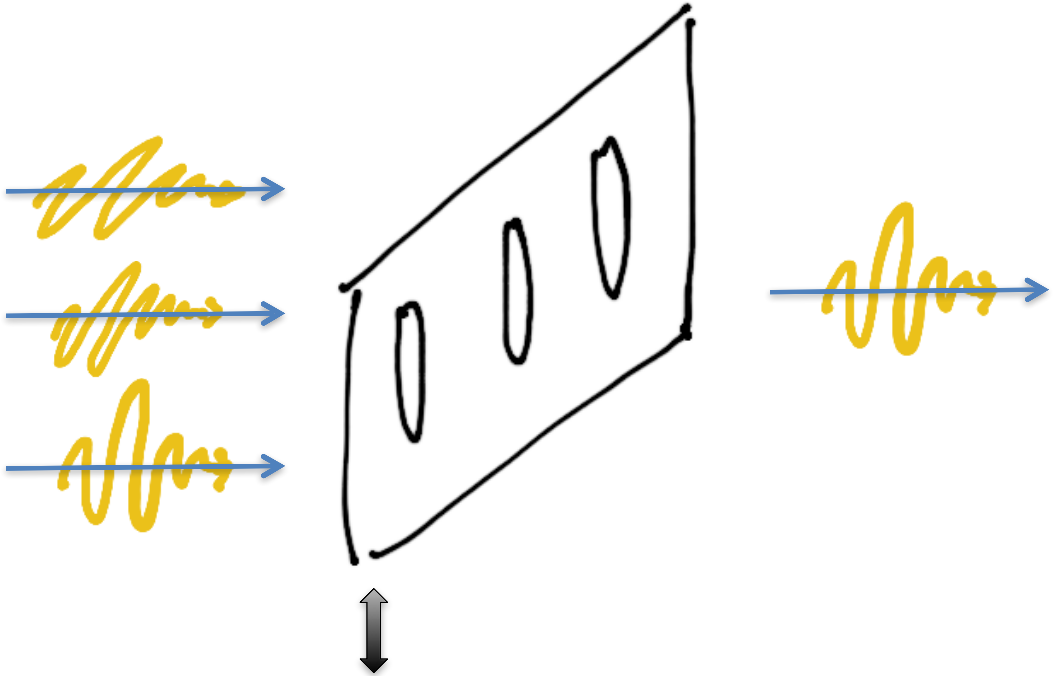


https://physicsworld.com/a/frog-photoreceptor-counts-photons/

- Polarizing filters: only aligned photons pass

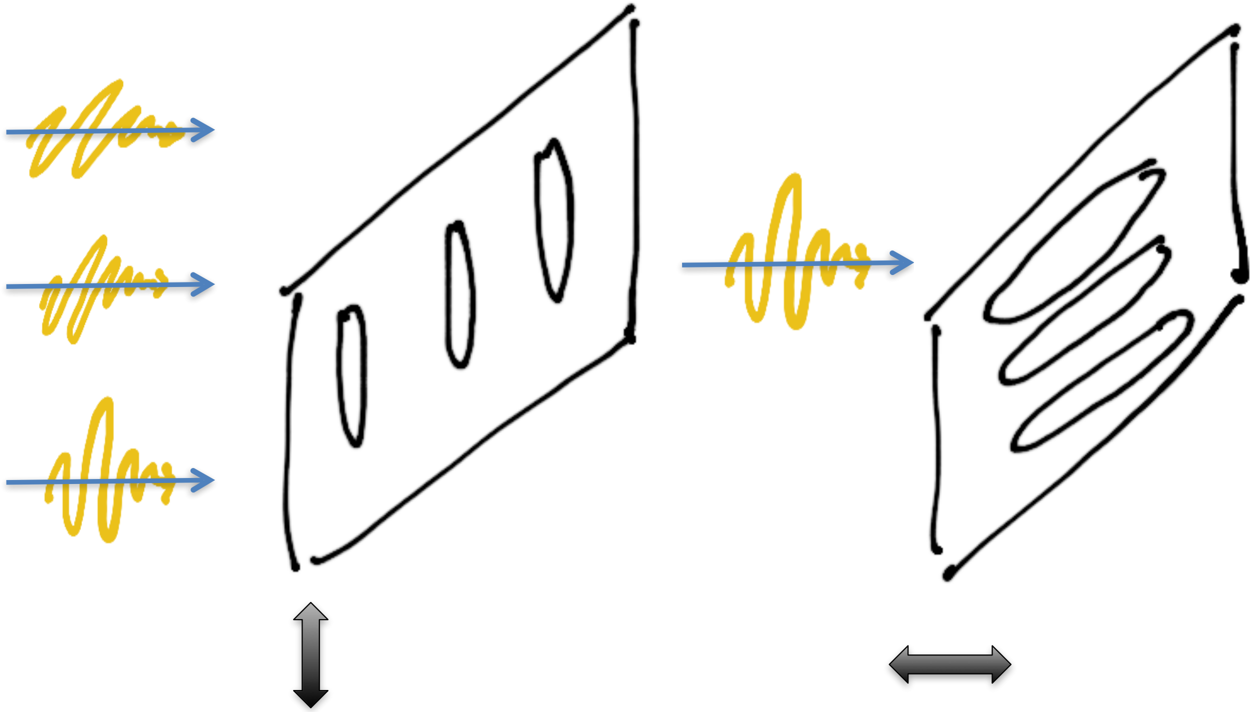


Polarisation filter measurements



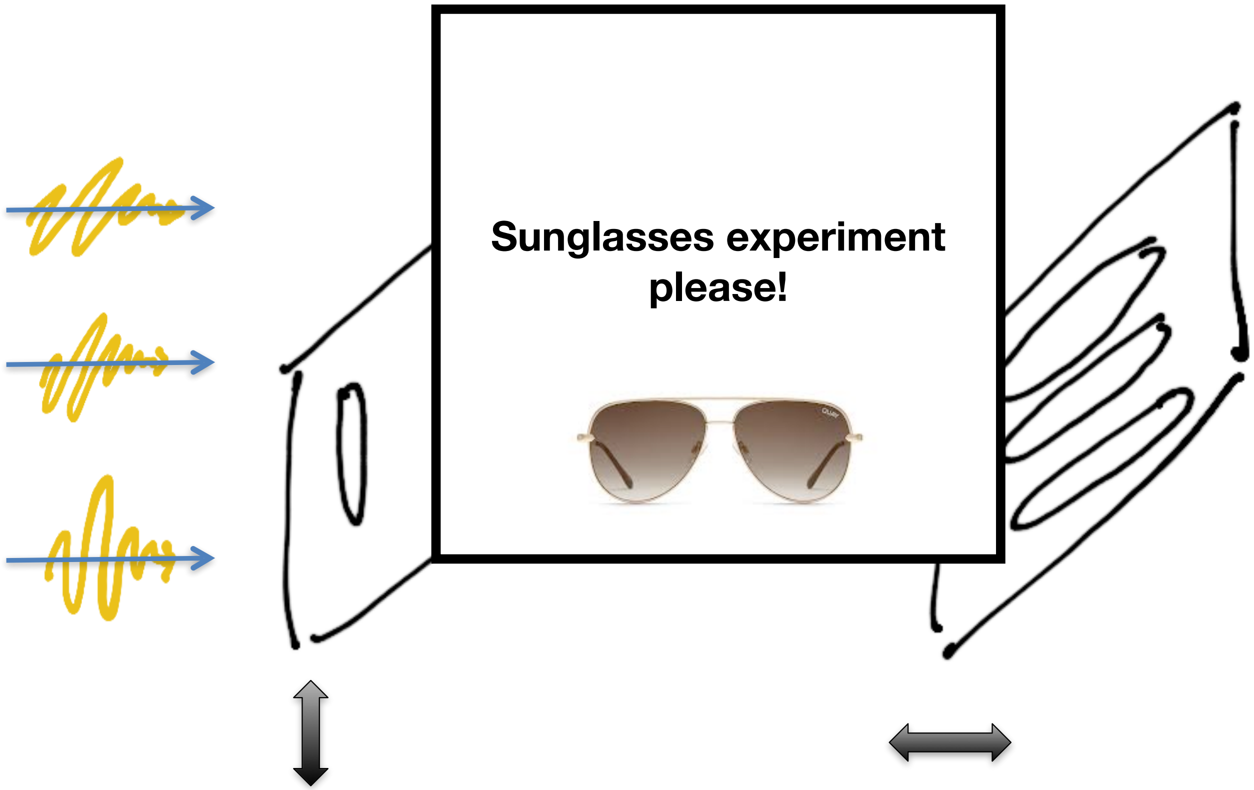
Only light polarised in fixed direction passes through

Combining filters -> less light



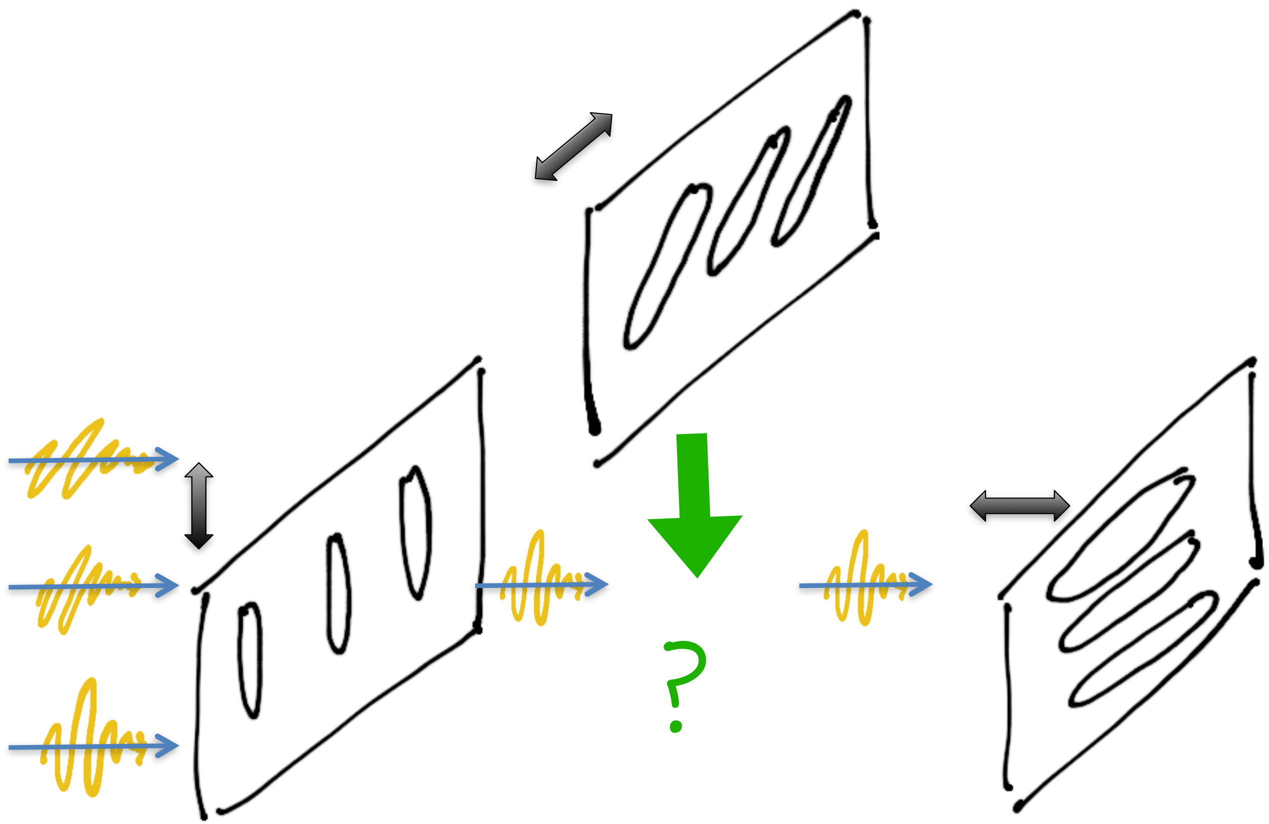
Sequence of perpendicular filters -> NO LIGHT gets ghrough

Combining filters -> less light

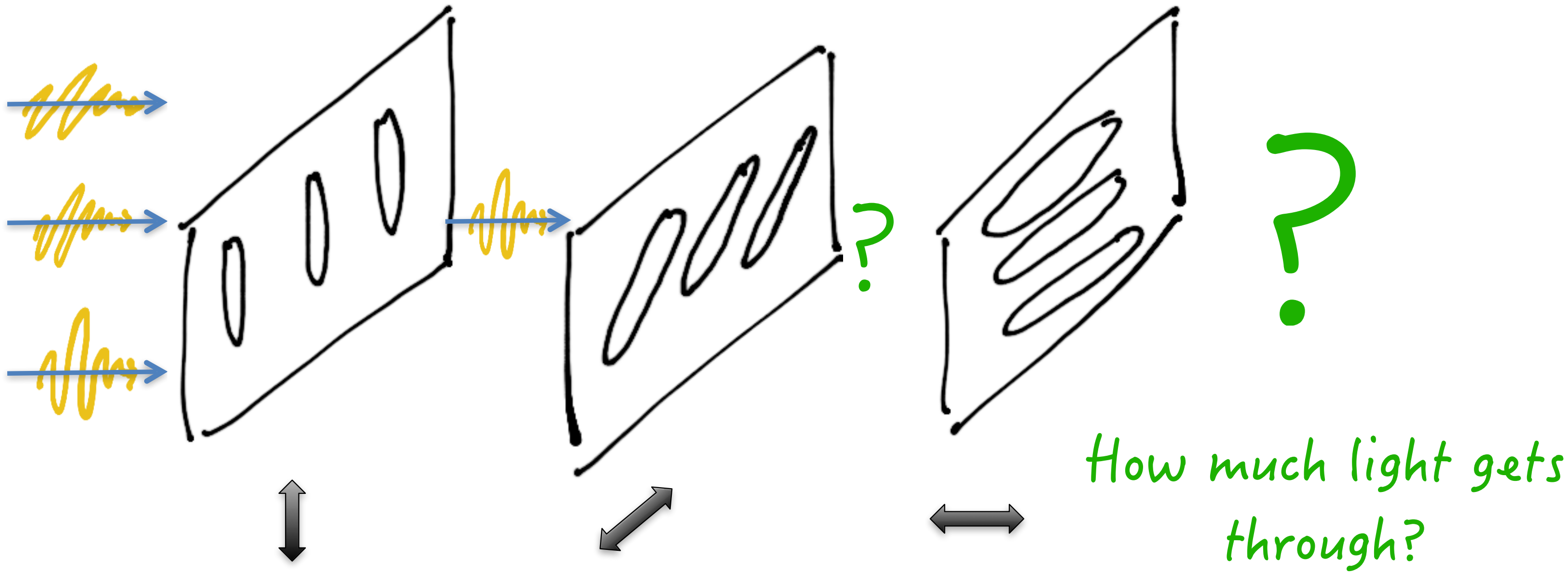


Sequence of perpendicular filters -> NO LIGHT gets ghrough

Inserting a filter…?



Inserting a filter…?



Polarisation filter measurements:

A classical model

- Light comes in single photons

Classical assumptions:

- The ‘measurement’ is deterministic (modulo our ignorance)

- Measurements do not change the system

Polarisation filter measurements:

A classical model

- Light comes in single photons

Classical assumptions

- The ‘measurement’ is deterministic

Individual photon should either go through or get absorbed determinsitically!

- Measurements do not change the system

Polarisation filter measurements:

A classical model

- Light comes in single photons

Classical assumptions

- The ‘measurement’ is deterministic

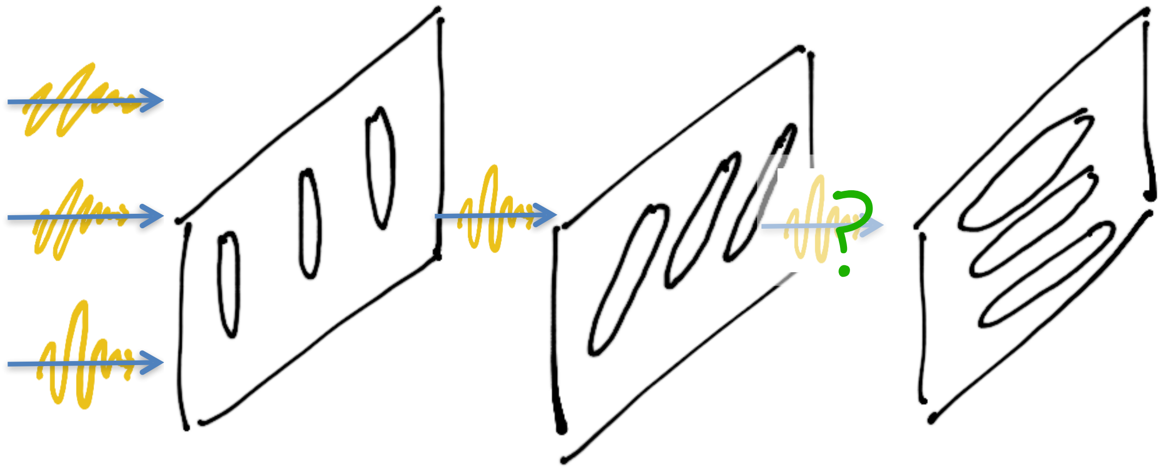
Individual photon should either go through or get absorbed **determinsitically!**

- Measurements do not change the system

Having an extra filter in between should not effect this property

Polarisation filter measurements:

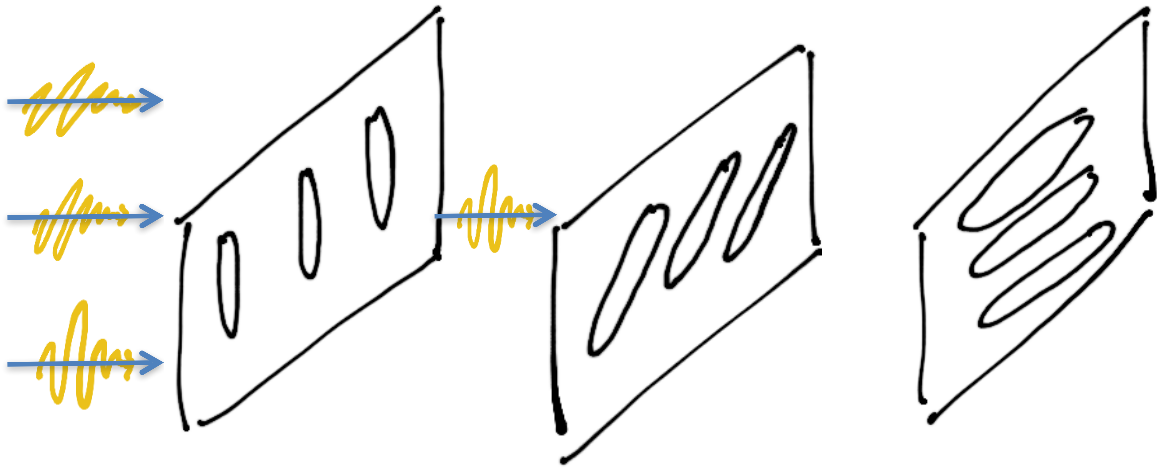
A classical model



Individual photon should either go through or get absorbed **determinsitically!**

Polarisation filter measurements:

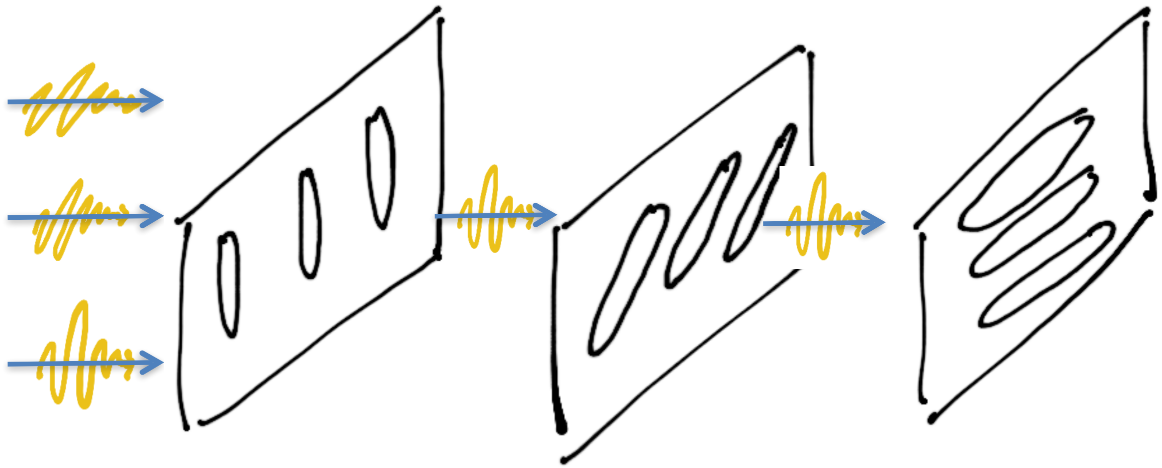
A classical model



-> if absorbed, <u>no photon out</u>

Polarisation filter measurements:

A classical model

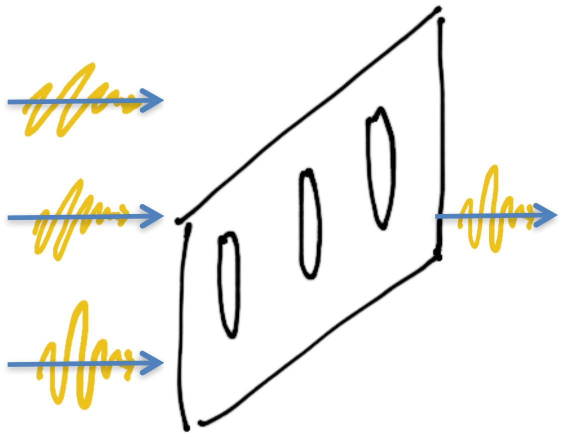


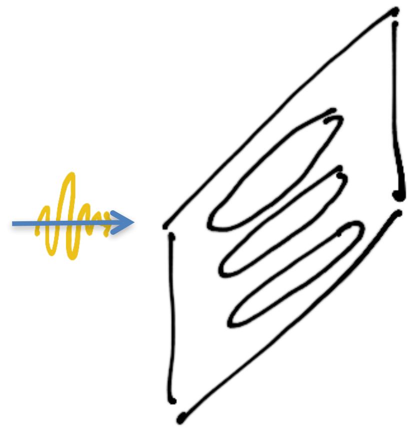
-> if not absorbed

Having an extra filter in between should not effect this property

Polarisation filter measurements:

A classical model





-> if not absorbed

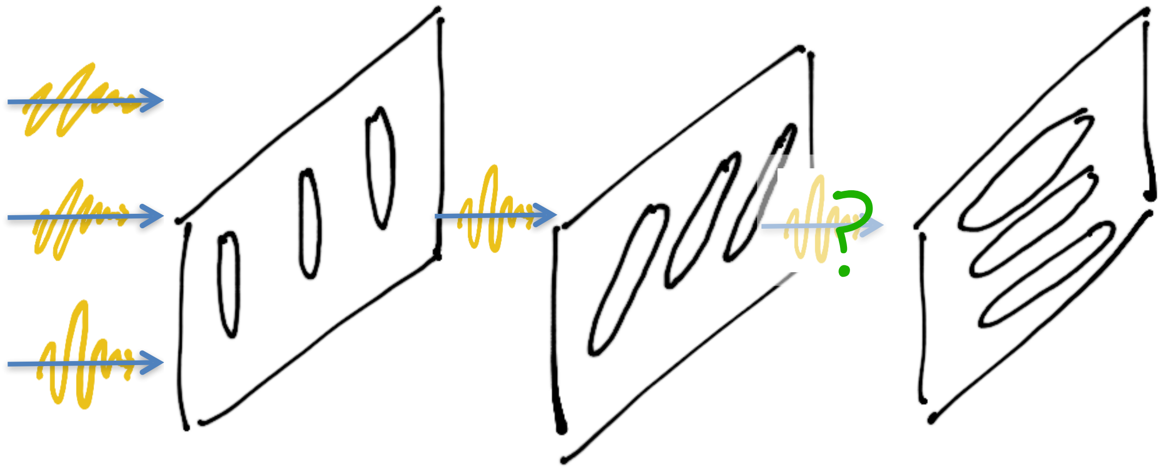
Having an extra filter in between should not effect this property

...as if no filter...

-> <u>no photon out</u>

Polarisation filter measurements:

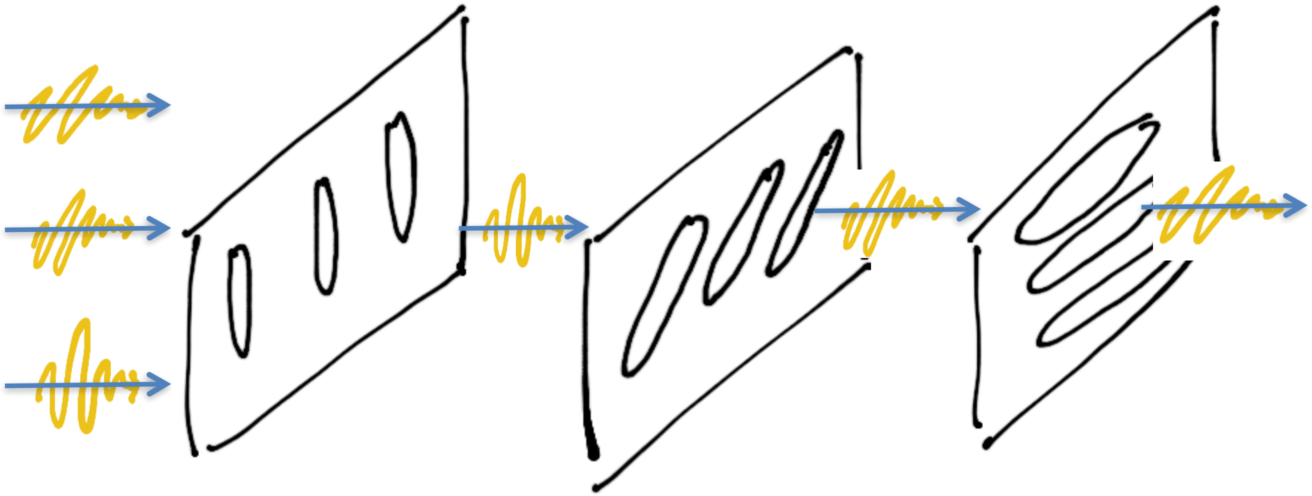
A classical model



Classically: in all cases
-> no photon out

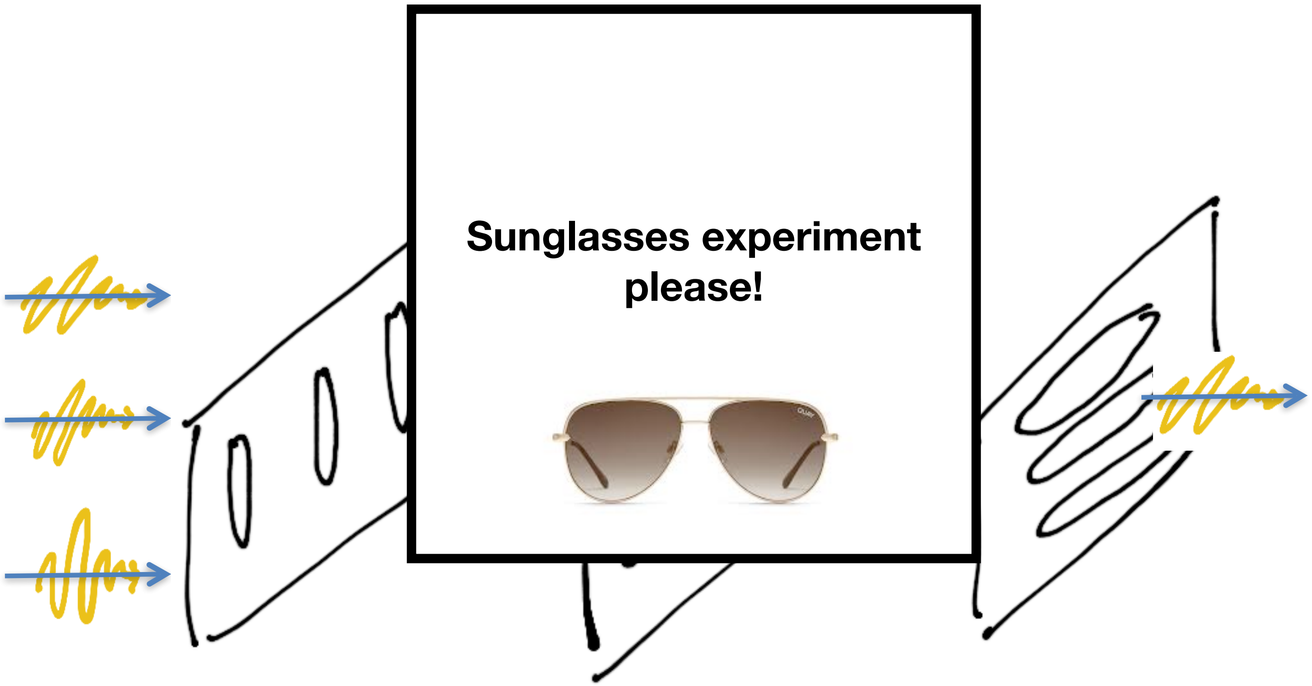
In the real ‘quantum world…

In the real ‘quantum world…



Adding a filter
-> some photons out!

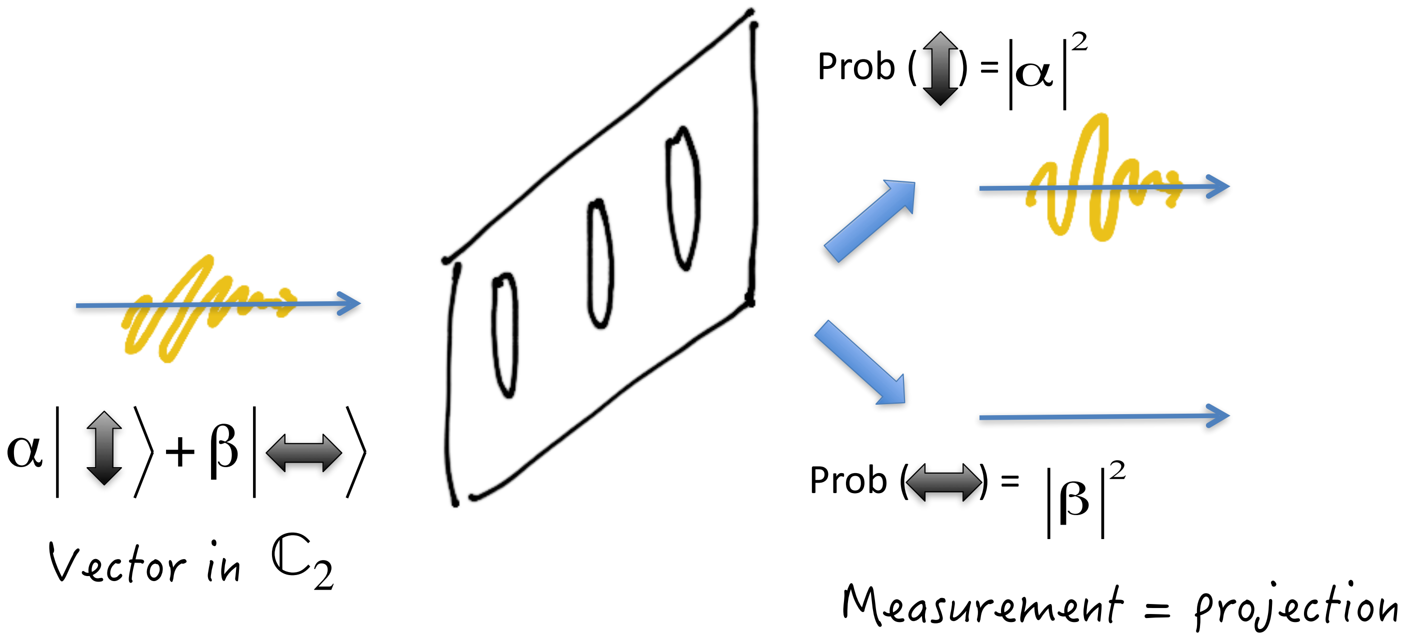
In the real 'quantum world...



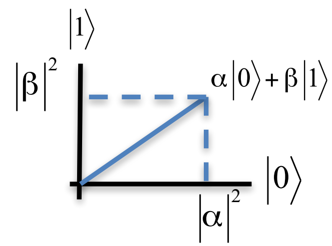
Adding a filter
-> some photons out!

Polarisation filter measurements:

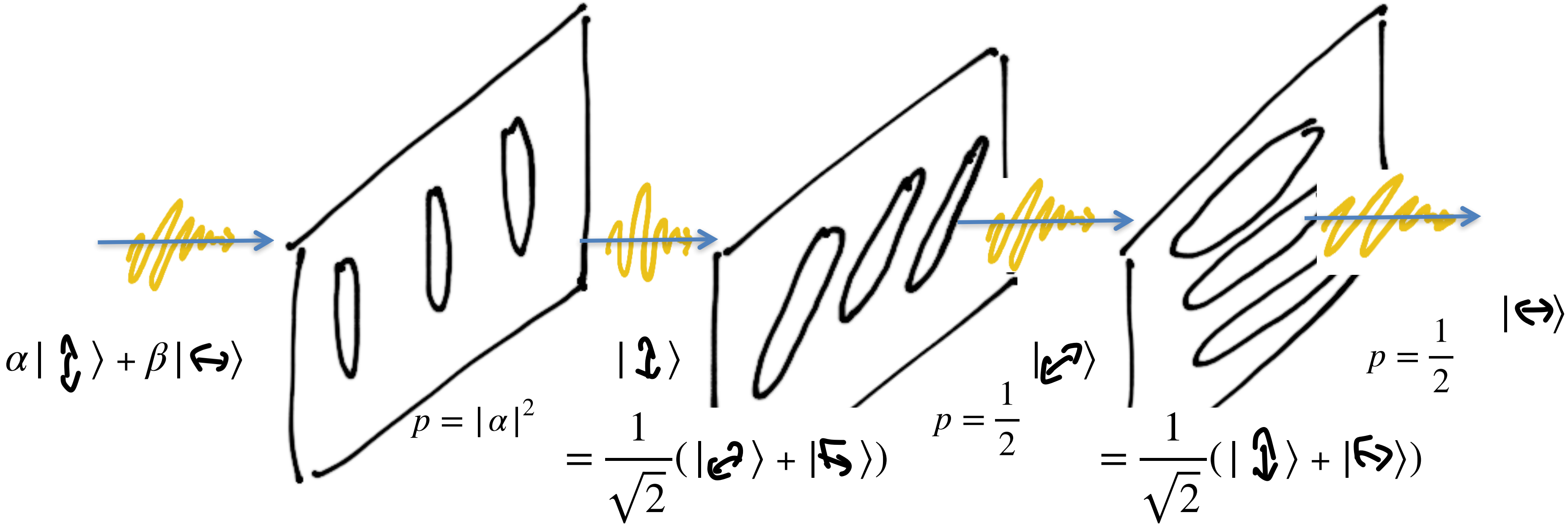
Quantum measurements



- Out come is random
- Output state depends on measurement result



QM answer: Filters as a measurement



Some easy linear algebra…

Adding a filter
-> <u>some photons out!</u>

Quantum randomness is not just ignorance!

Quantum randomness is not just ignorance!

There is no way to assign ‘value’ to the polarisation and get a deterministic outcome

Polarisation filter measurements

- Light comes in single photons

Classical assumptions

- The 'measurement' is deterministic

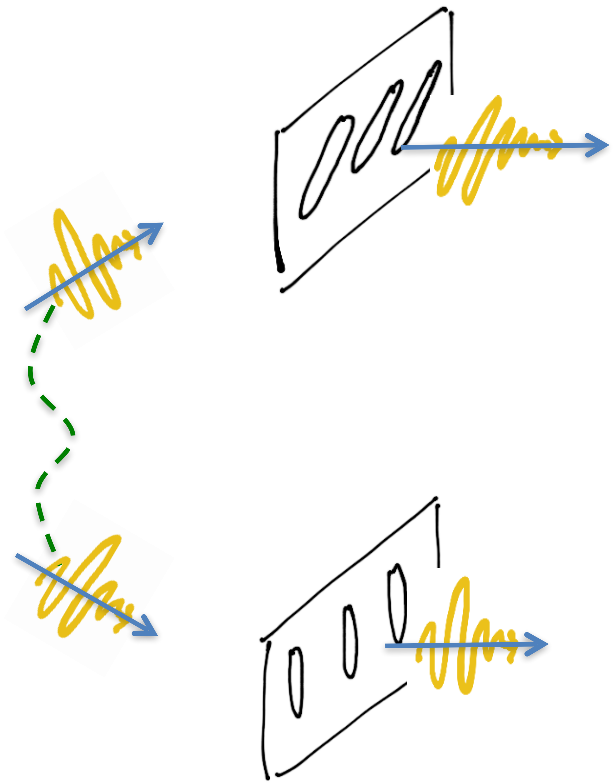
Individual photon should either go through or get absorbed **determinsitically!**

- Measurements do not change the system

~~Having an extra filter in between should not effect this property~~

I don't believe it!

Bell's theorem

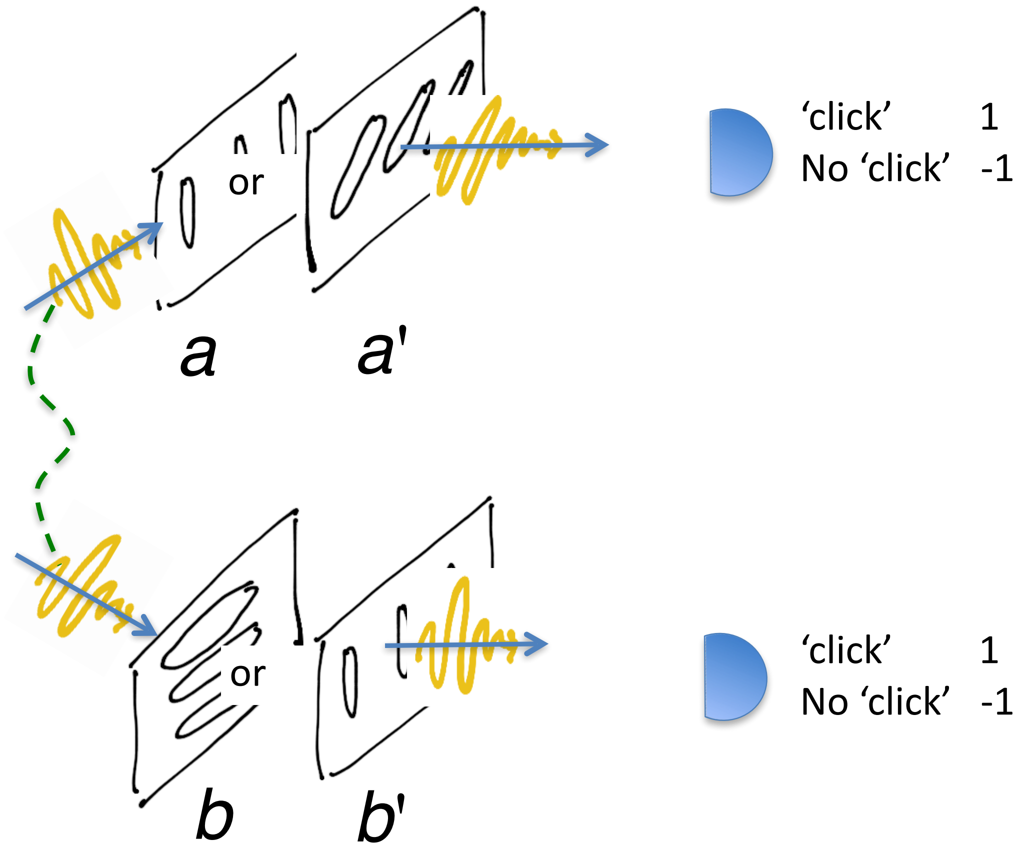


Use entangled pair to test!

Single, but distant, measurements

Locality => canNOT change state

Bell's theorem



Bell: ANY Local Hidden Variable model

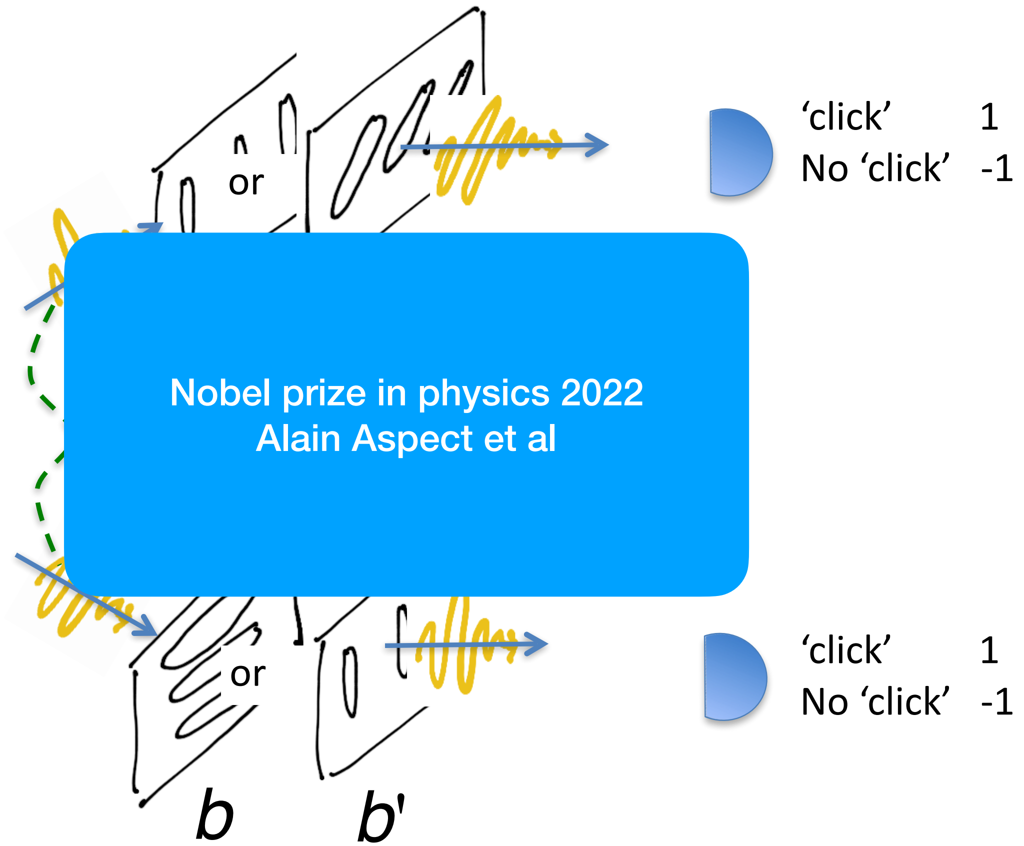
(i.e. where *some* theory knows the outcome)

$$S = \left| a.b + a.b' + a'.b - a'.b' \right| \leq 2$$

QM gives!

=2√2

Bell's theorem



Bell: ANY Local Hidden Variable model

(i.e. where *some* theory knows the outcome)

$$S = \left| a.b + a.b' + a'.b - a'.b' \right| \leq 2$$

QM gives!

=2√2

Quantum randomness is not just ignorance!

There is no way to assign ‘value’ to the polarisation and get a deterministic outcome

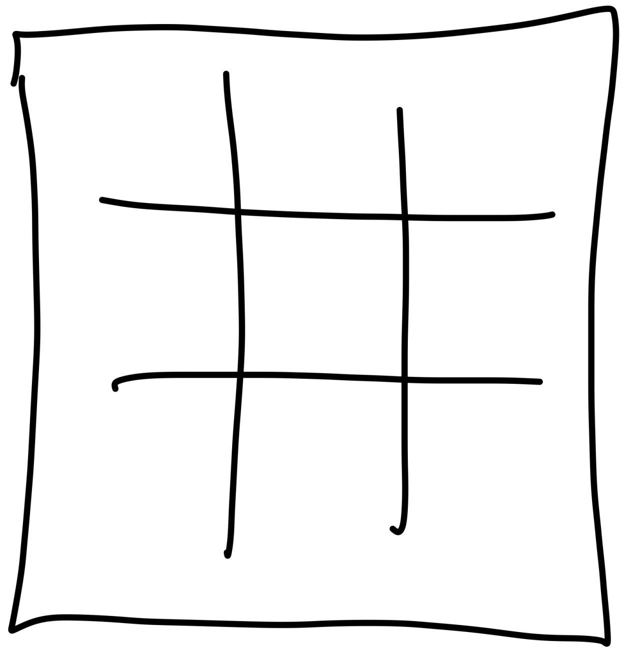
Peres-Mermin magic square game

Quantum randomness is different from classical 'randomness'

↓

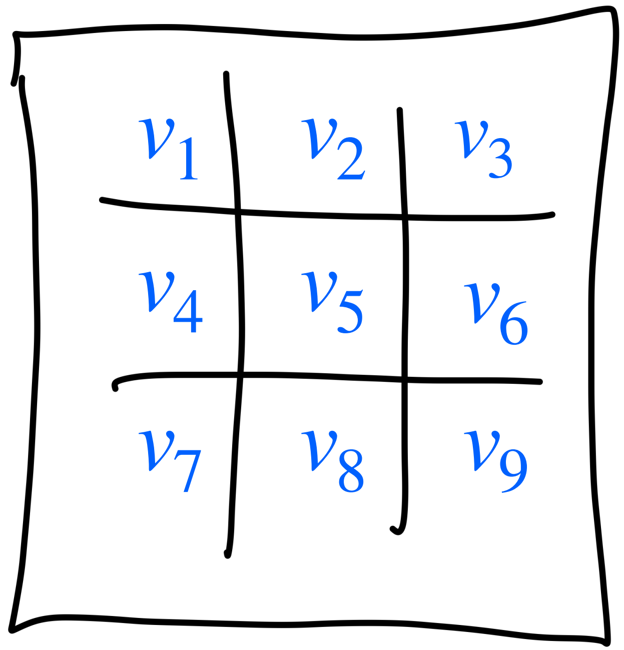
Games that 'classical' devices cannot win, but quantum can

Peres-Mermin magic square game



Peres-Mermin magic square game

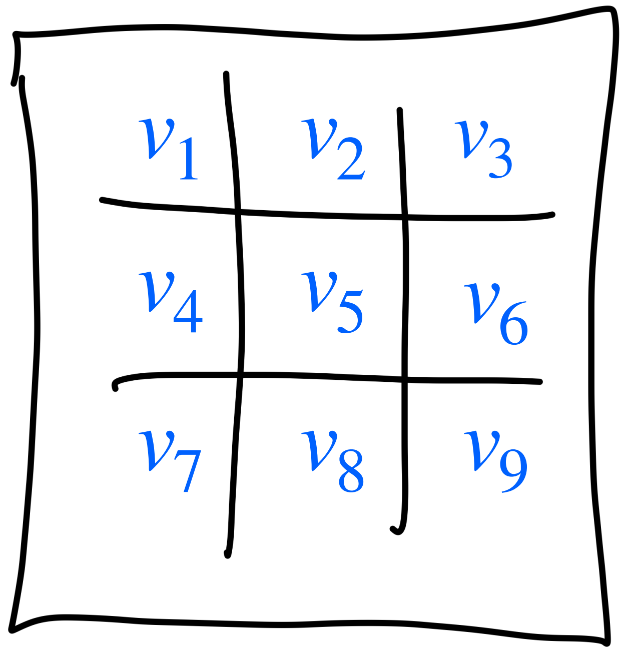
- Player assigns values to all squares in grid
  $v_i = \pm 1$



Peres-Mermin magic square game

- Player assigns values to all squares in grid
  $$v_i = \pm 1$$

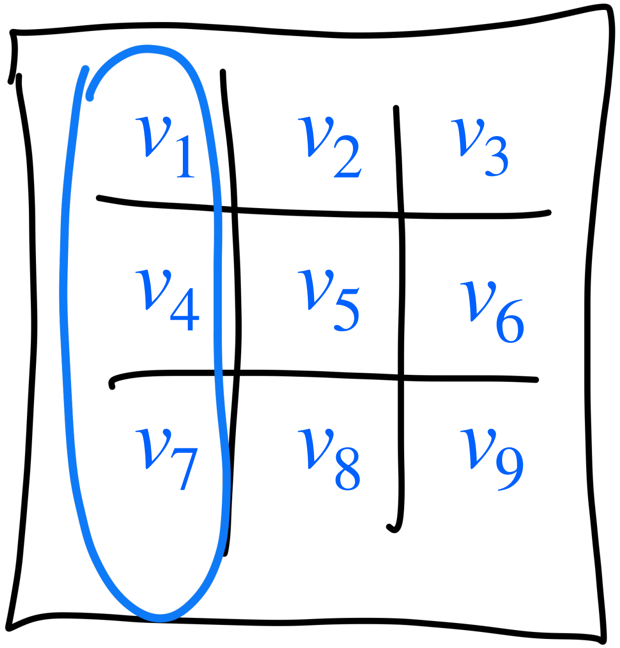
- Referee chooses a column or a row, at random, and reads the the product of the values



Peres-Mermin magic square game

- Player assigns values to all squares in grid
  $$v_i = \pm 1$$

- Referee chooses a column or a row, at random, and reads the the product of the values

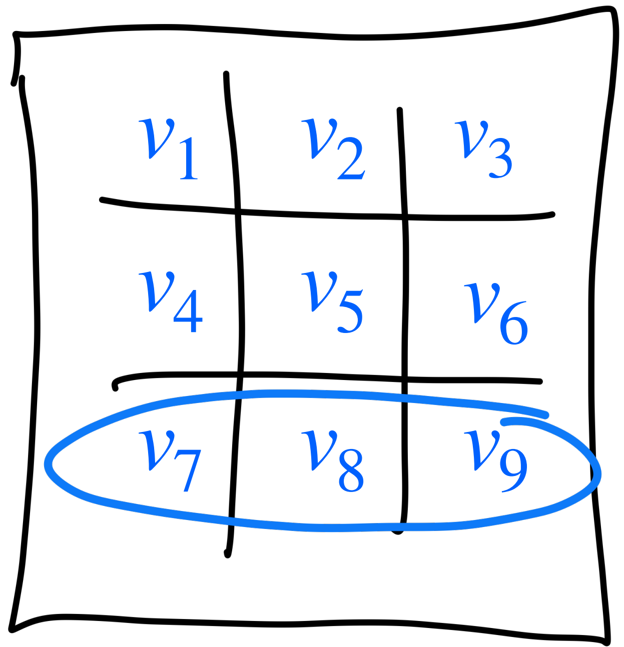


$$c_1 = v_1 \,.\, v_4 \,.\, v_7$$

Peres-Mermin magic square game

- Player assigns values to all squares in grid
  $v_i = \pm 1$

- Referee chooses a column or a row, at random, and reads the the product of the values

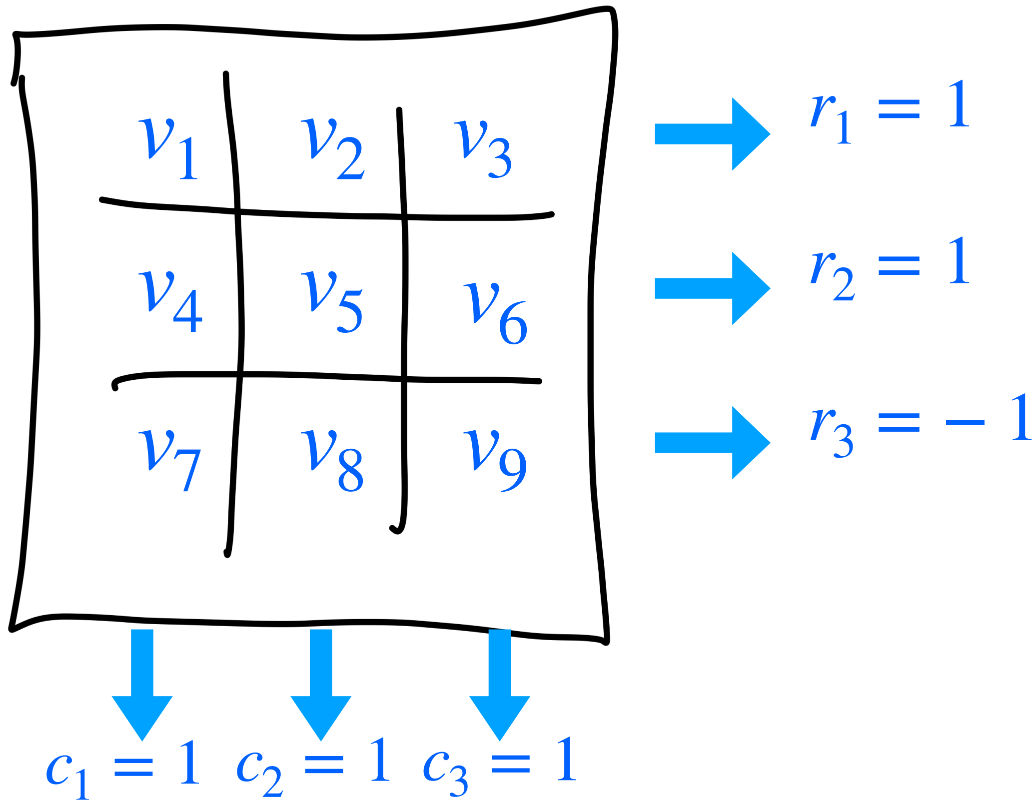


$r_3 = v_7 \, . \, v_8 \, . \, v_9$

Peres-Mermin magic square game

- Player assigns values to all squares in grid $v_i = \pm 1$
- Referee chooses a column or a row, at random, and reads the the product of the values
- Player wins if

$$c_1 = v_1 . v_4 . v_7 = 1$$
$$c_2 = v_2 . v_5 . v_8 = 1$$
$$c_3 = v_3 . v_6 . v_9 = 1$$
$$r_1 = v_1 . v_2 . v_3 = 1$$
$$r_2 = v_4 . v_5 . v_6 = 1$$
$$r_3 = v_7 . v_8 . v_9 = -1$$



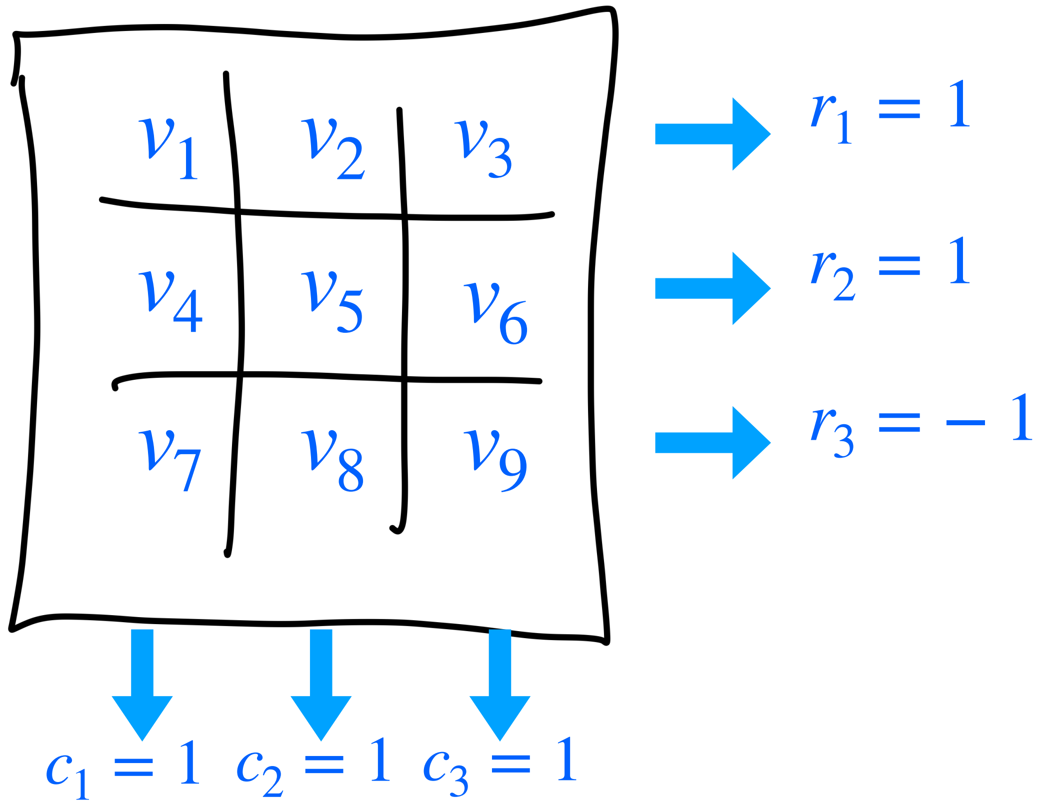
Peres-Mermin magic square game

- Player assigns values to all squares in grid
  $v_i = \pm 1$

- Referee chooses a column or a row, at random, and reads the the product of the values

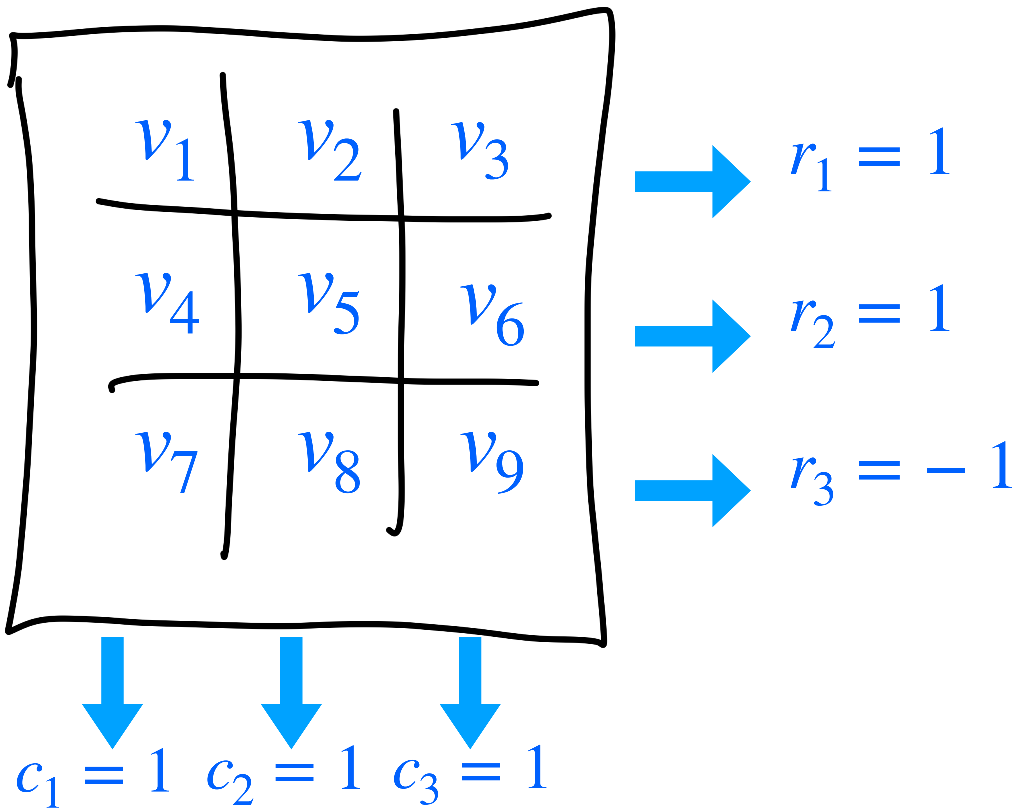
- Player wins if

$$\begin{aligned} c_1 &= v_1 \,.\, v_4 \,.\, v_7 = 1 \\ c_2 &= v_2 \,.\, v_5 \,.\, v_8 = 1 \\ c_3 &= v_3 \,.\, v_6 \,.\, v_9 = 1 \\ r_1 &= v_1 \,.\, v_2 \,.\, v_3 = 1 \\ r_2 &= v_4 \,.\, v_5 \,.\, v_6 = 1 \\ r_3 &= v_7 \,.\, v_8 \,.\, v_9 = -1 \end{aligned}$$



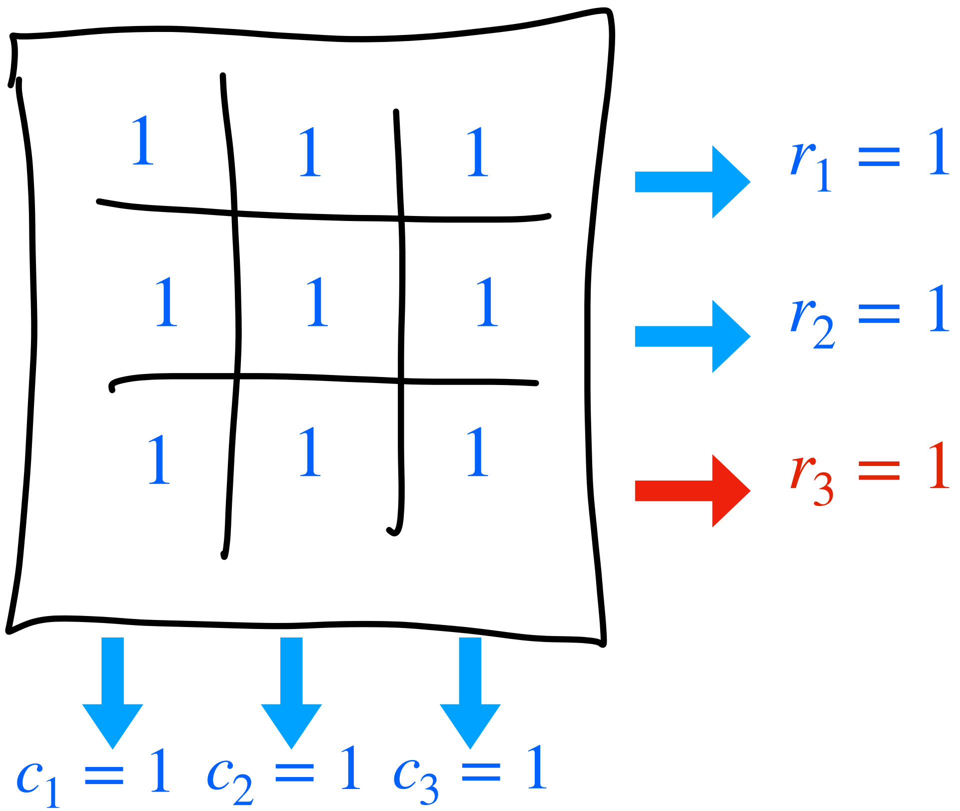
$$p(win) = \frac{1}{6}\left(p(c_1 = 1) + p(c_2 = 1) + p(c_3 = 1) + p(r_1 = 1) + p(r_2 = 1) + p(r_3 = -1)\right)$$

Best possible $p(win)$?



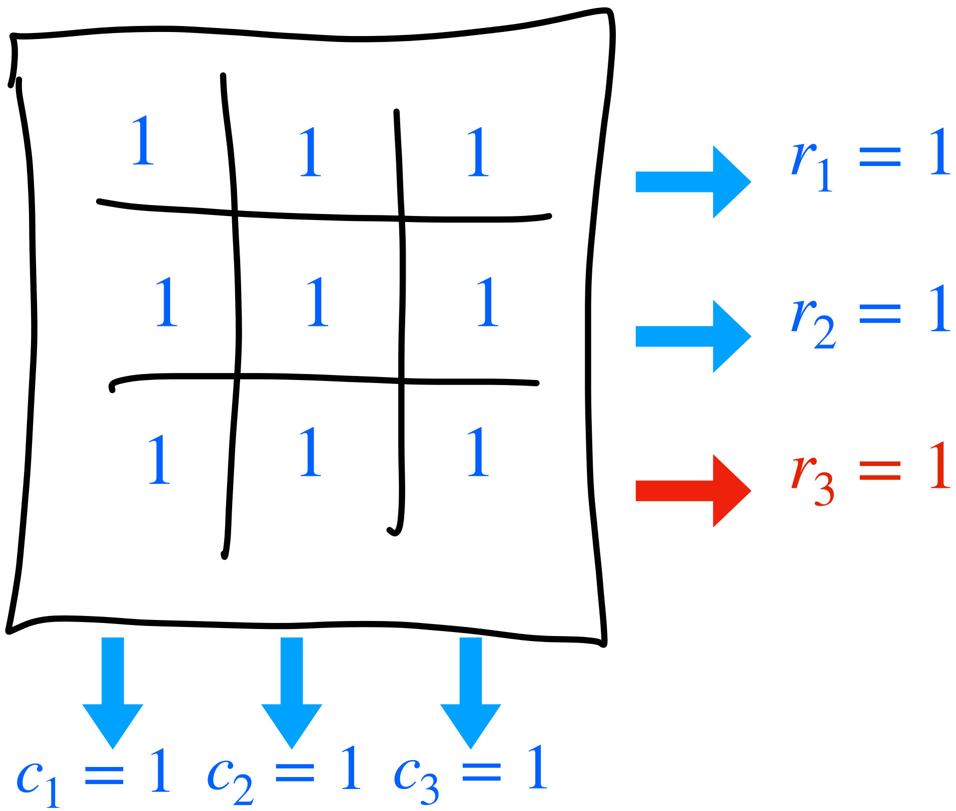
$$p(win) = \frac{1}{6}\left(p(c_1 = 1) + p(c_2 = 1) + p(c_3 = 1) + p(r_1 = 1) + p(r_2 = 1) + p(r_3 = -1)\right)$$

Best possible $p(win)$?



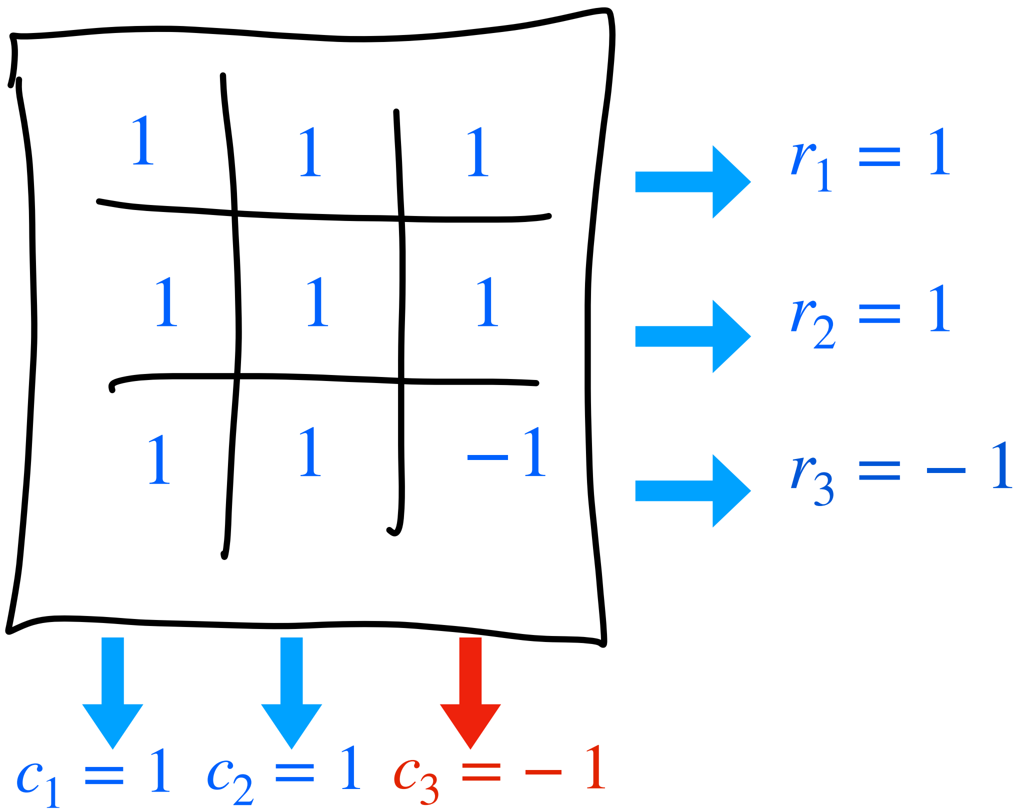
$$p(win) = \frac{1}{6}\left(p(c_1 = 1) + p(c_2 = 1) + p(c_3 = 1) + p(r_1 = 1) + p(r_2 = 1) + p(r_3 \not= -1)\right)$$

Best possible $p(win)$?



$$p(win) = \frac{5}{6}$$

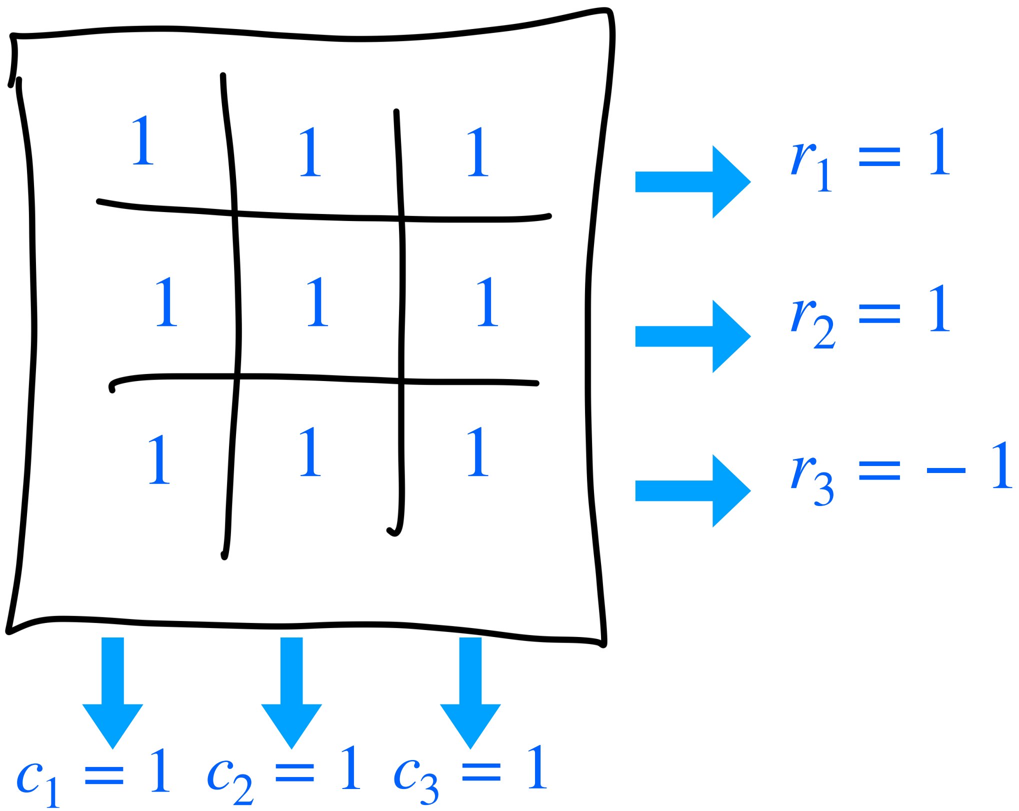
Best possible $p(win)$?



$$p(win) = \frac{5}{6}$$

Best possible $p(win)$?

- Any fixed (deterministic) assignment can only satisfy 5/6 winning conditions



Best possible $p(win)$?

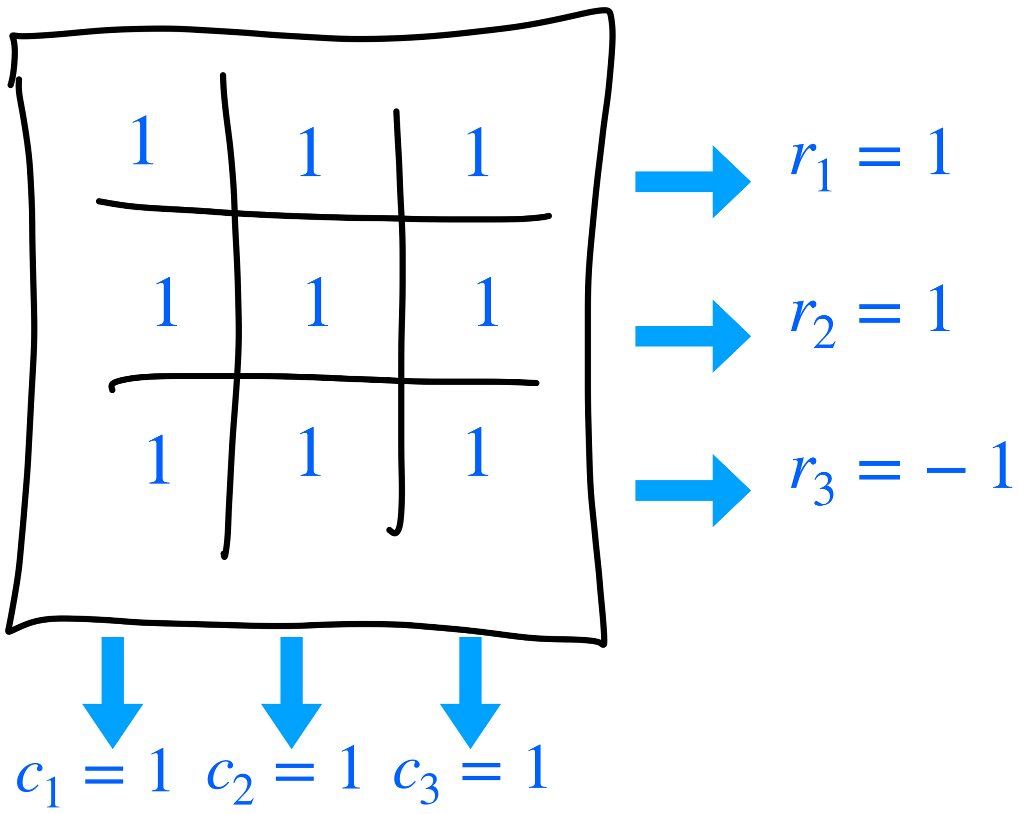
- Any fixed (deterministic) assignment can only satisfy 5/6 winning conditions

$$c_1 . c_2 . c_3 = r_1 . r_2 . r_3$$

Incompatible with

$$c_1 = c_2 = c_3 = r_1 = r_2 = 1$$
$$r_3 = -1$$

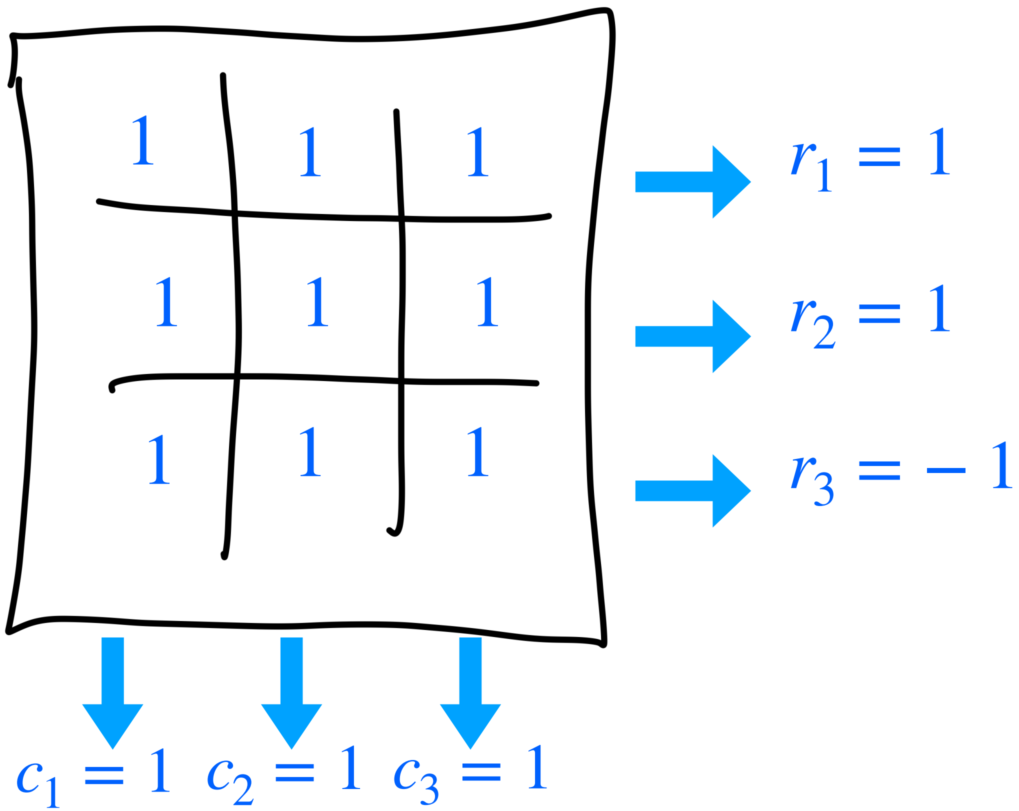
Cannot always win!



Best possible $p(win)$?

- Any fixed (deterministic) assignment can only satisfy 5/6 winning conditions

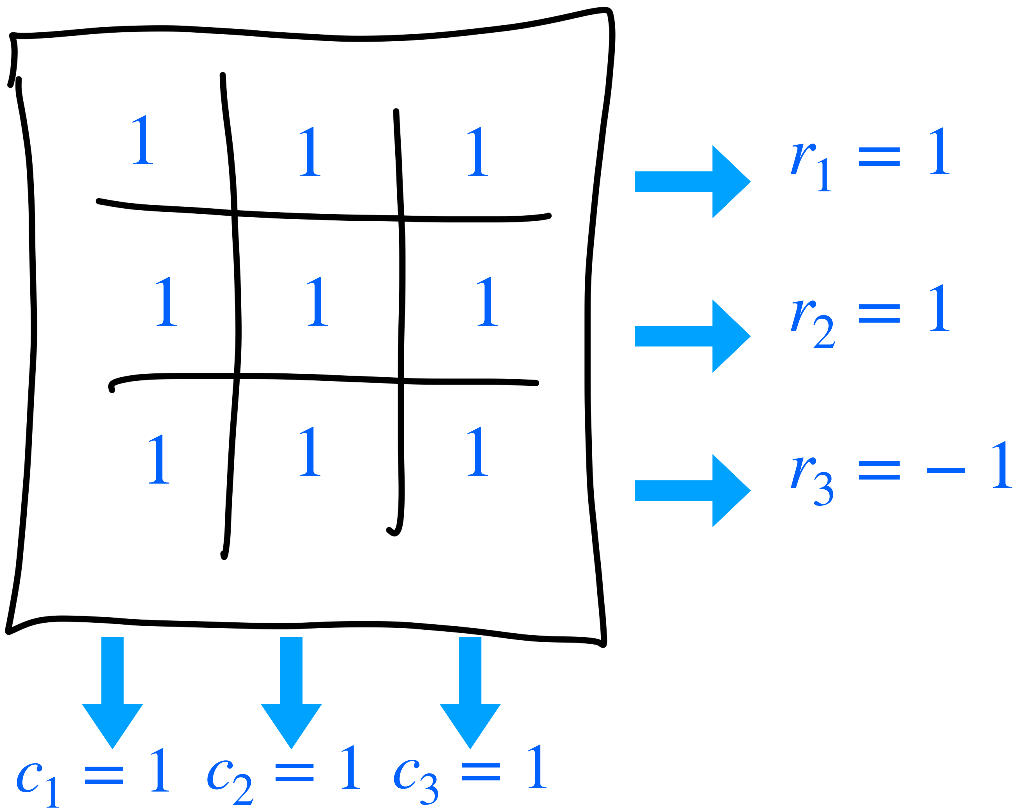
- Any randomized assignment can only do as well as the best deterministic assignment



Best possible classical $p(win)$?

- Any fixed (deterministic) assignment can only satisfy 5/6 winning conditions

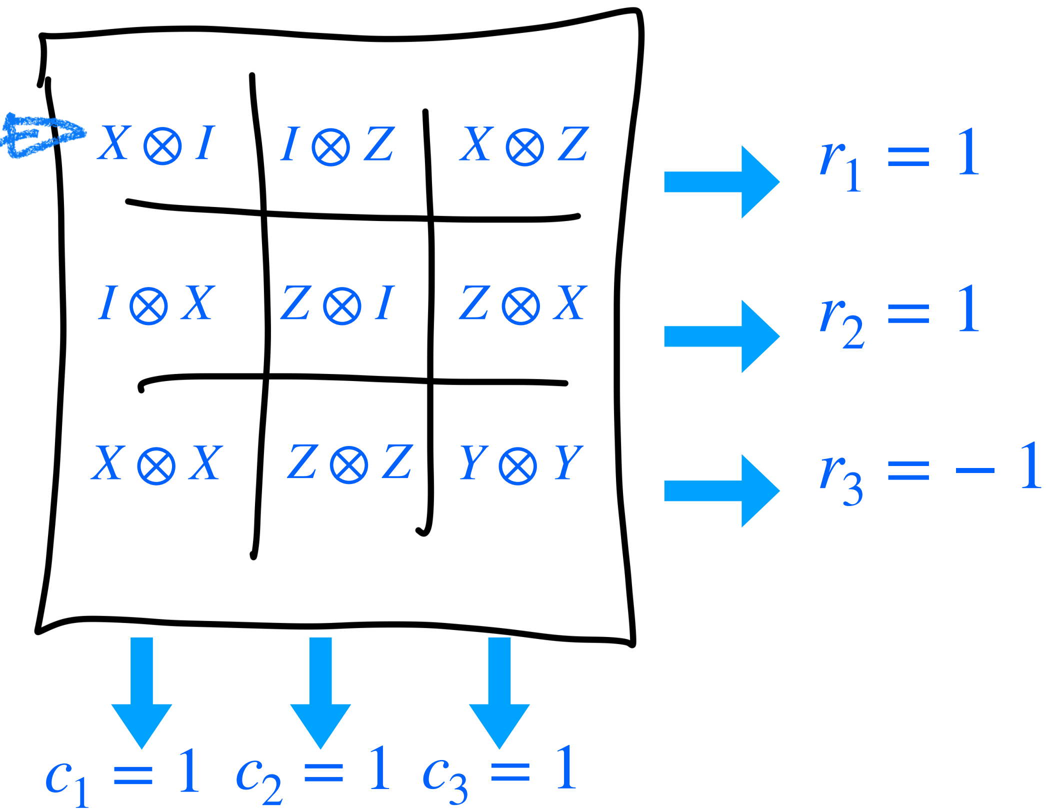
- Any randomized assignment can only do as well as the best deterministic assignment



$$p_c(win) \leq \frac{5}{6}$$

Best quantum $p(win)$?

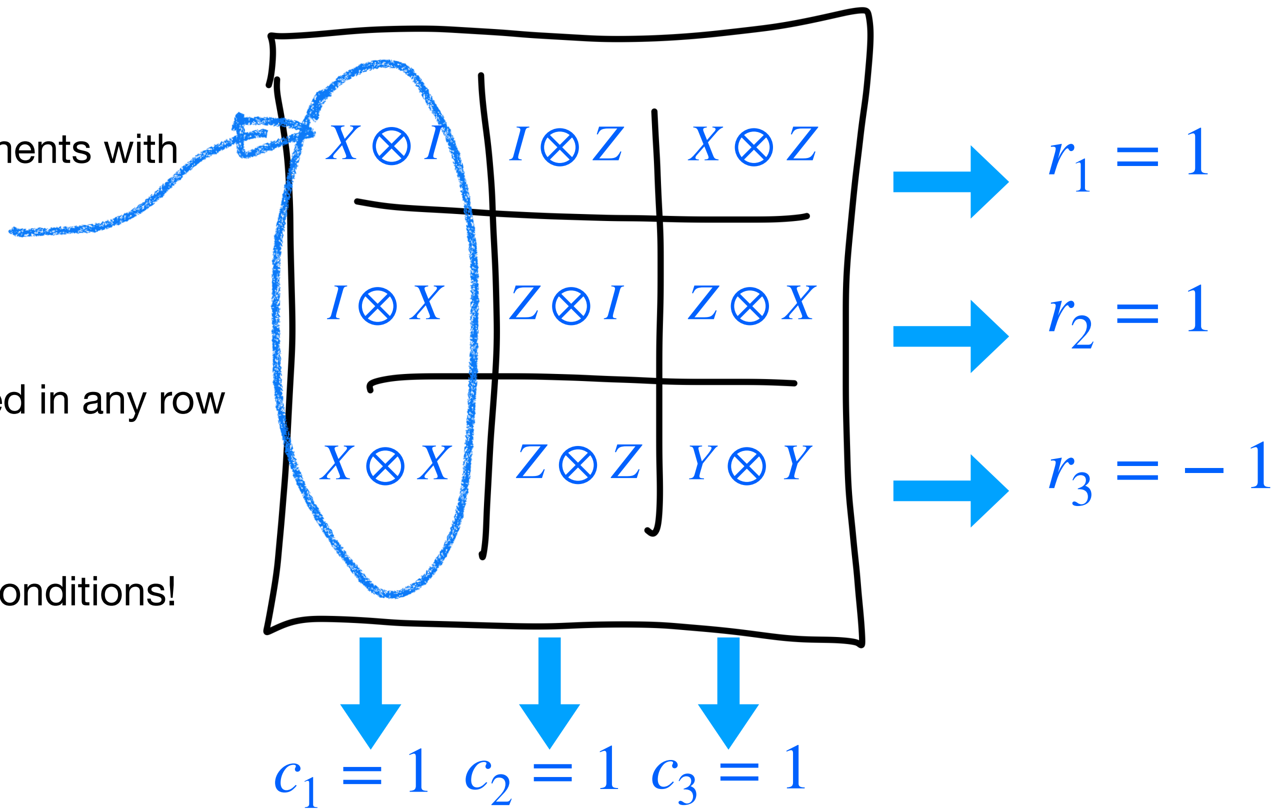
- Quantum measurements with outcomes = ± 1
- Can be co-measured in any row or column
- Satisfy all winning conditions!



$$p_Q(win) = 1$$

Best quantum $p(win)$?

- Quantum measurements with outcomes = ± 1
- Can be co-measured in any row or column
- Satisfy all winning conditions!



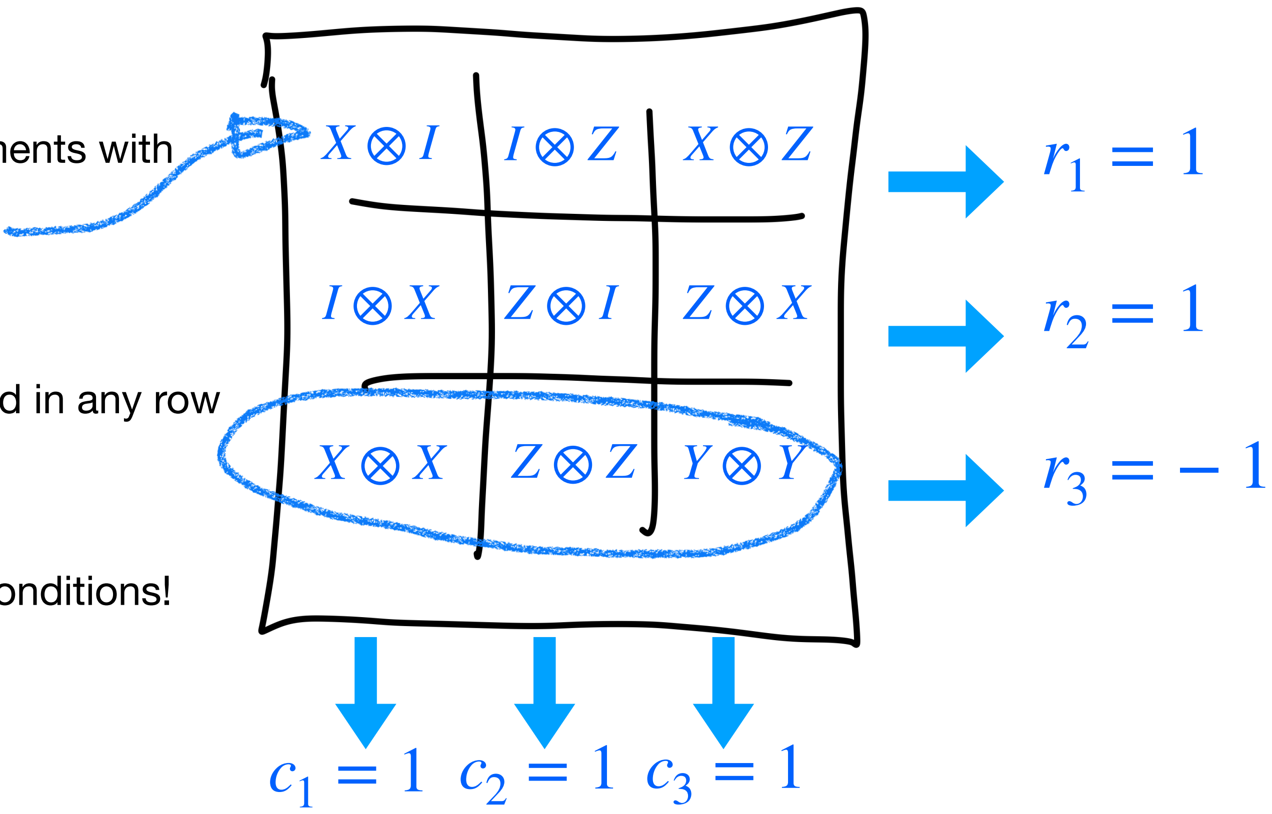
$p_Q(win) = 1$

Best quantum $p(win)$?

- Quantum measurements with outcomes = ± 1

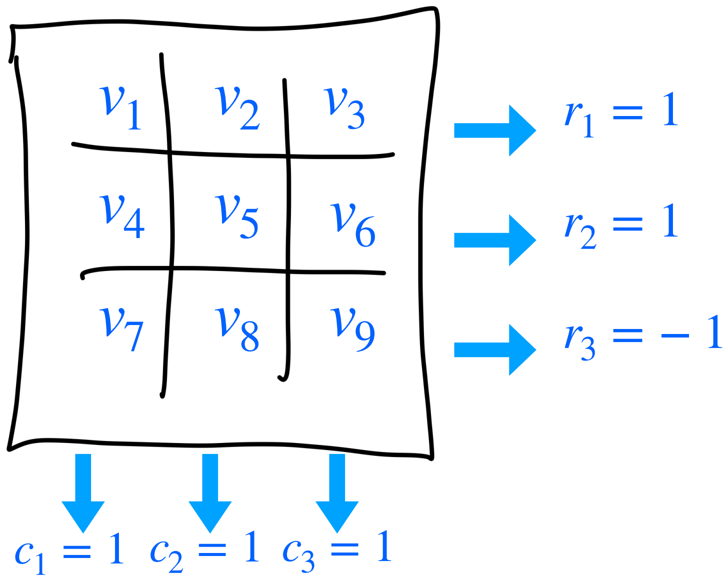
- Can be co-measured in any row or column

- Satisfy all winning conditions!



$p_Q(win) = 1$

Peres-Mermin magic square game



$$p_c(win) \leq \frac{5}{6}$$

$$p_Q(win) = 1$$

- Constraints not achievable classically, can achieve quantumly
- Directe applications to shallow circuit, provable quantum advantage [Bravyi, Gosset, Koening, Science 2017]

Behind all quantum computational advantage?

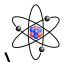
2. What is quantum computing?

2. What is quantum computing?

Bit

0 / 1

Qubit



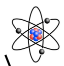
$$\alpha\left|0\right\rangle + \beta\left|1\right\rangle$$

2. What is quantum computing?

Bit

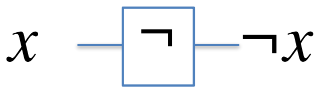
0 / 1

Qubit

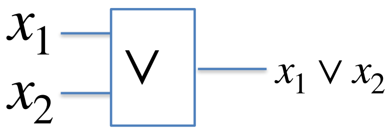


$$\alpha|0\rangle + \beta|1\rangle$$

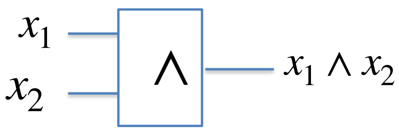
Gates



Not

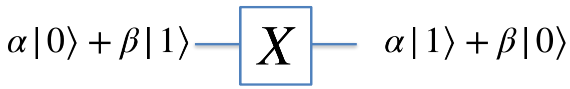


OR



AND

Unitary gates



Not

Unitary map

(Reversible)

2. What is quantum computing?

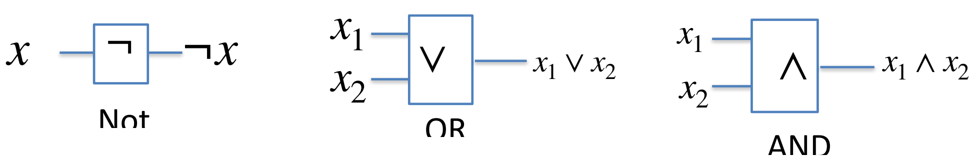
Bit

0 / 1

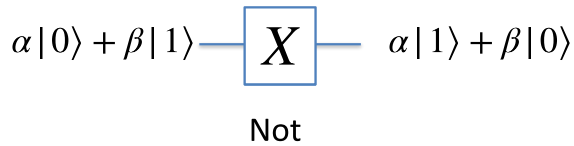
Qubit

$$\alpha|0\rangle + \beta|1\rangle$$

Gates

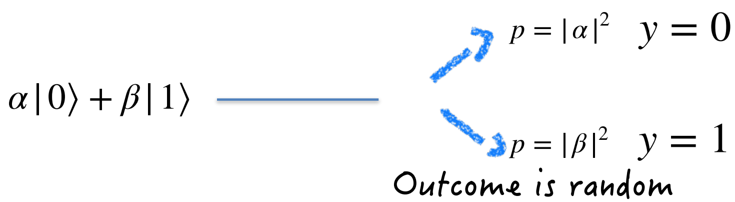


Unitary gates



Read out

Readout measurements



2. What is quantum computing?

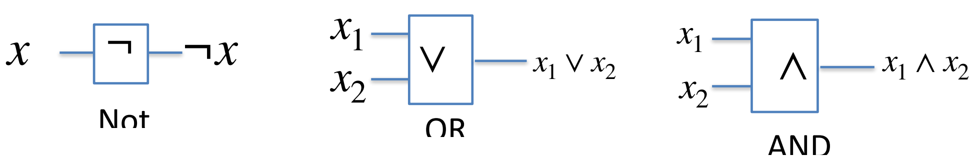
Bit

0 / 1

Qubit

$\alpha|0\rangle + \beta|$

Gates



Unitar

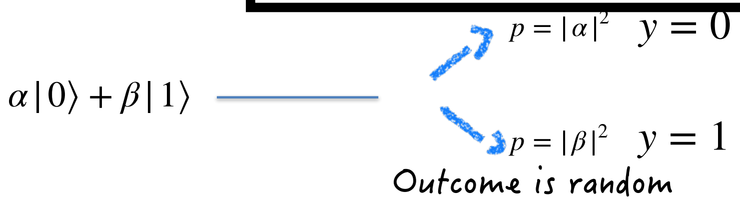
$\alpha|0\rangle + \beta|1\rangle$

Note:
Just linear algebra!

Read out

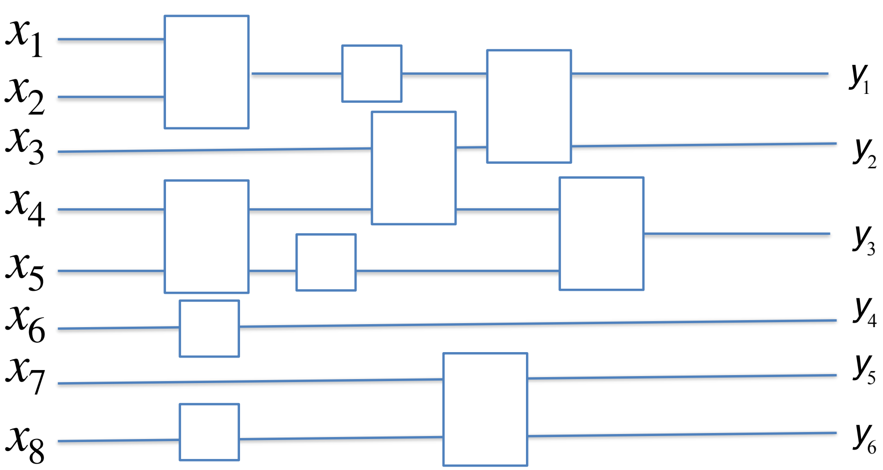
x

Reado



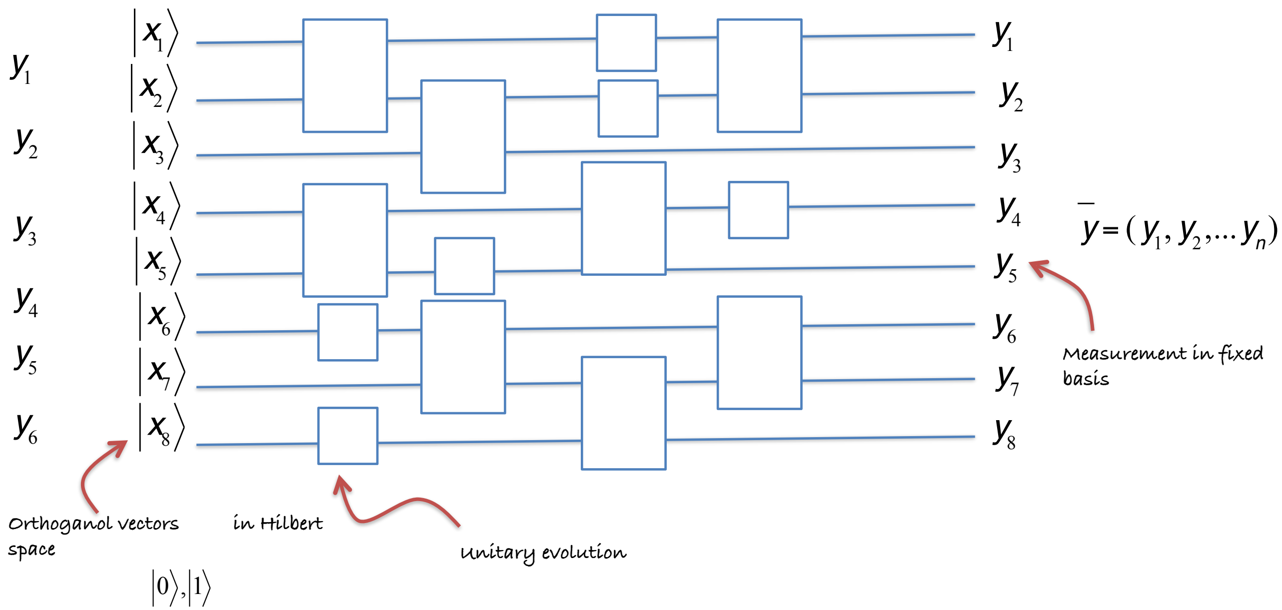
2. What is quantum computing?

Circuit model



Universal gate set: NOT, AND, OR

Quantum circuit model



Universal quantum gate set: CNOT, pi/8, H

Complexity classes for quantum computing

Decision problems:
Functions from bit strings length n to single bit

$$f : \{0,1\}^n \rightarrow \{0,1\}$$

Language L:
Set of inputs which output 1

$$x \in L \quad \text{iff} \quad f(x) = 1$$

BPP

$L \in$ BPP if $\exists$ a family of circuits $\{C_n\}$ such and a polynomial $q(n)$ such that

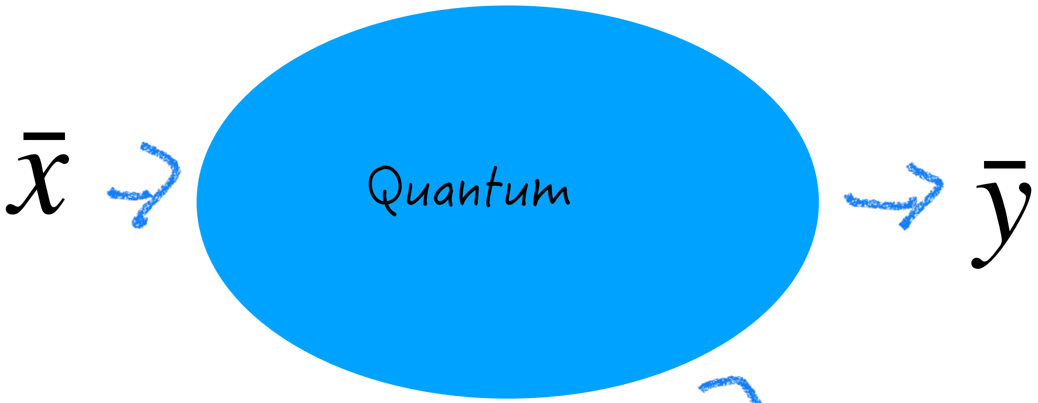
- size of circuits $|C_n| \leq q(n)$
- If $x \in L$, output 1 with probability > 2/3
- If $x \notin L$, output 1 with probability <1/3

BQP

$L \in$ BPP if $\exists$ a family of circuits $\{C_n\}$ such and a polynomial $q(n)$ such that

- size of circuits $|C_n| \leq q(n)$
- If $x \in L$, output 1 with probability > 2/3
- If $x \notin L$, output 1 with probability <1/3

Other models of quantum computation?



Measurement based quantum computation

Adiabatic quantum computation

…

Complexity-wise equivalent to circuit model

Big conjecture of quantum computing

BPP $\subset$ **BQP**

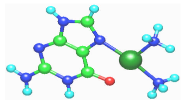
Not proven…

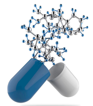
3. What can we do with quantum computers?

3. What can we do with quantum computers?

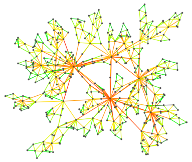

Factoring primes (cracks RSA)

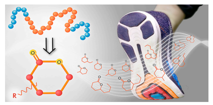
Quantum Machine Learning

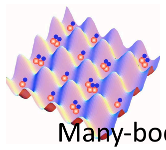

Quantum Chemisty


Drug development


Search


Quantum random walks


Material design


Many-body physics

10 or 40-70 qubits

-> 100 qubits beyond classical

3. What can we do with quantum computers?

Exponential 'improvement'

- Shor's factoring algorithm
  [Shor, FOCS 1994]
  Factors numbers into primes
  -> could 'crack' RSA

- System of linear equations
  [Harrow, Hassidim, Lloyd, PRL 2008]
  Notable application to machine learning
  -> needs 'QRAM'
  -> applications?

'Proven' quantum advantage

- Sampling problems
  [Aaronson, Arkhipov 2013]
  [Bremner, Josza, Shepherd 2011]
  Boson sampling, IQP, random shallow circuits…
  -> efficient classical simulation
  => collapse of PH
  -> applications?

- Shallow circuit advantage
  [Bravyi, Gosset, König, Science, 2018]
  Constant depth Q requires log depth C
  -> PROOF: concenquence of 'Q randomness'
  -> applications?

3. What can we do with quantum computers?

Exponential 'improvement'

- Shor's factoring algorithm
  [Shor, FOCS 1994]
  Factors numbers into primes
    -> could 'crack' RSA

- System of linear equations
  [Harrow, Hassidim, Lloyd, PRL 2008]
  Notable application to machine learning
    -> needs 'QRAM'
    -> applications?

?

'Proven' quantum advantage

- Sampling problems
  [Aaronson, Arkhipov 2013]
  [Bremner, Josza, Shepherd 2011]
  Boson sampling, IQP, random shallow circuits…
    -> efficient classical simulation
      => collapse of PH
    -> applications?

- Shallow circuit advantage
  [Bravyi, Gosset, König, Science, 2018]
  Constant depth Q requires log depth C
    -> PROOF: concenquence of 'Q randomness'
    -> applications?

3. What can we do with quantum computers?

Exponential 'improvement'

- Shor's factoring algorithm
  [Shor, FOCS 1994]
  Factors numbers into primes
  -> could 'crack' RSA

- System of linear equations
  [Harrow, Hassidim, Lloyd, PRL 2008]
  Notable application to machine learning
  -> needs 'QRAM'
  -> applications?

?

Variational, ML, ...

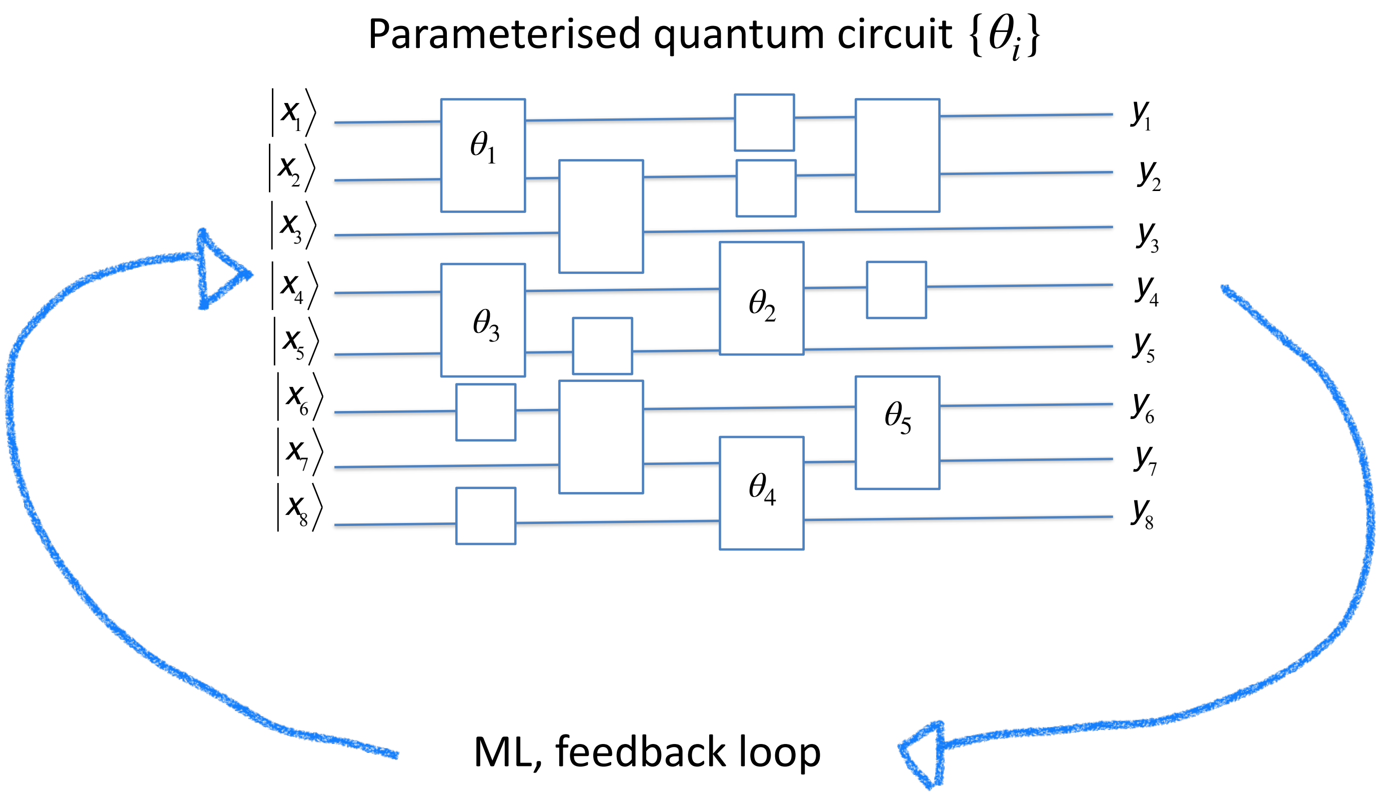
'Proven' quantum advantage

- Sampling problems
  [Aaronson, Arkhipov 2013]
  [Bremner, Josza, Shepherd 2011]
  Boson sampling, IQP, random shallow circuits...
  -> efficient classical simulation
  => collapse of PH
  -> applications?

?

- Shallow circuit advantage
  [Bravyi, Gosset, König, Science, 2018]
  Constant depth Q requires log depth C
  -> PROOF: concenquence of 'Q randomness'
  -> applications?

Variational quantum circuits, ML, ...



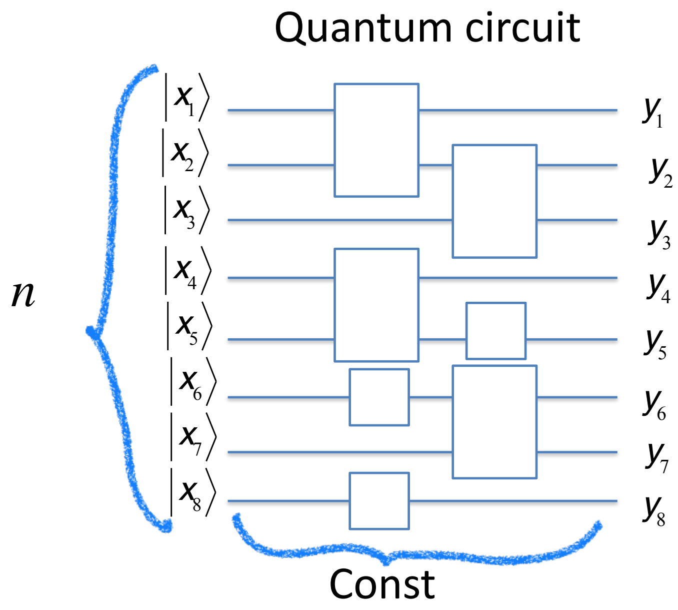
-> Quantum chemistry

-> Machine learning

-> ...

Shallow quantum circuits

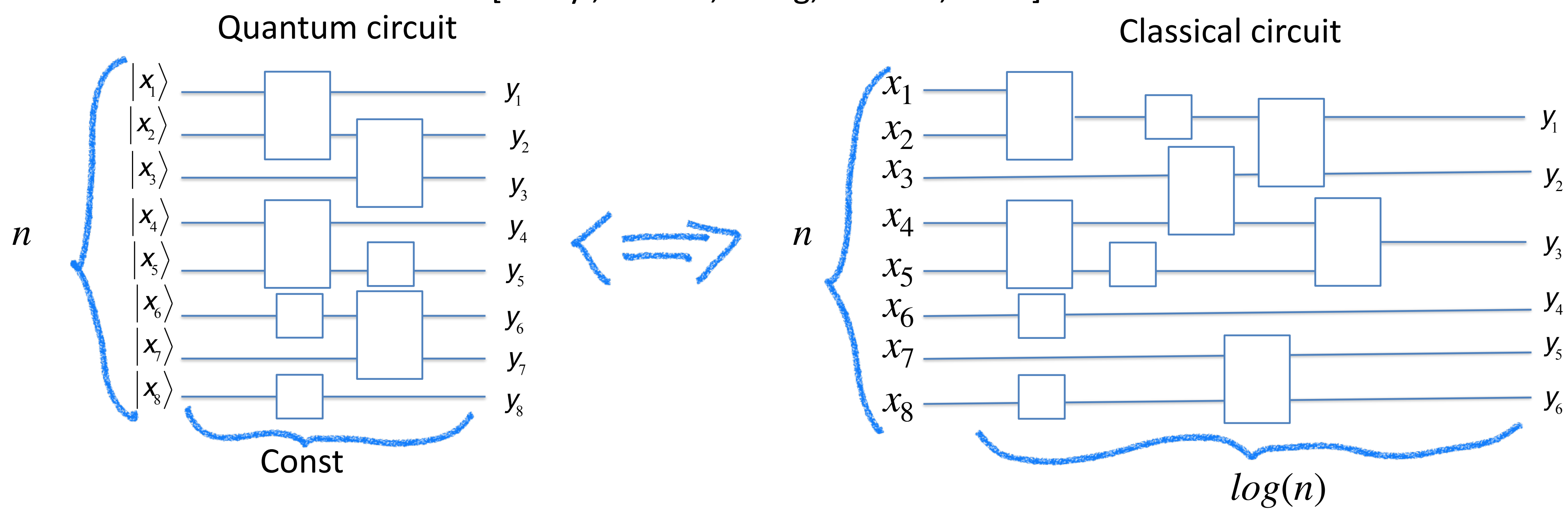
[Bravyi, Gosset, König, Science, 2018]



Relational statement $R(\bar{x}, \bar{y})$

Shallow quantum circuits

[Bravyi, Gosset, König, Science, 2018]



Relational statement $R(\bar{x}, \bar{y})$

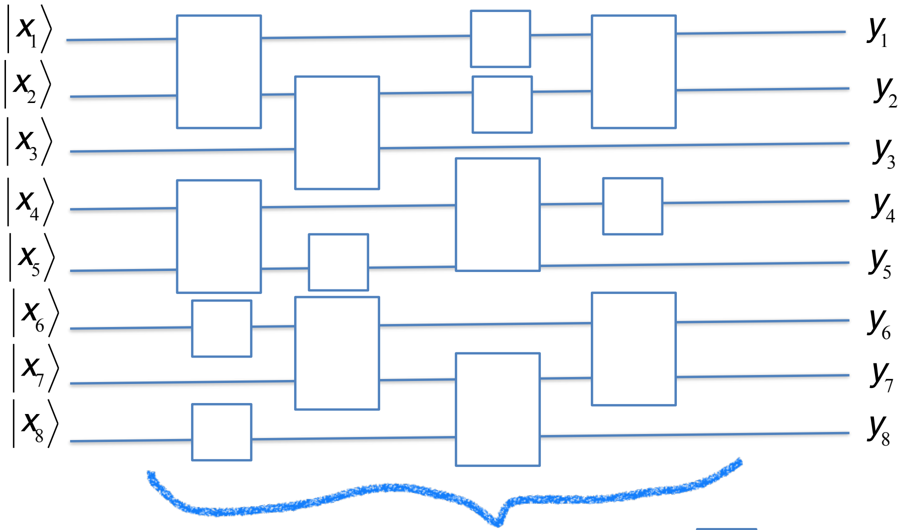
Impossible to satisfy classically in constant circuit

-> 'Circuit' magic square game…

Sampling

[Bremner, Josza, Shepherd 2011]

Subuniversal circuit families



All gates commute with X

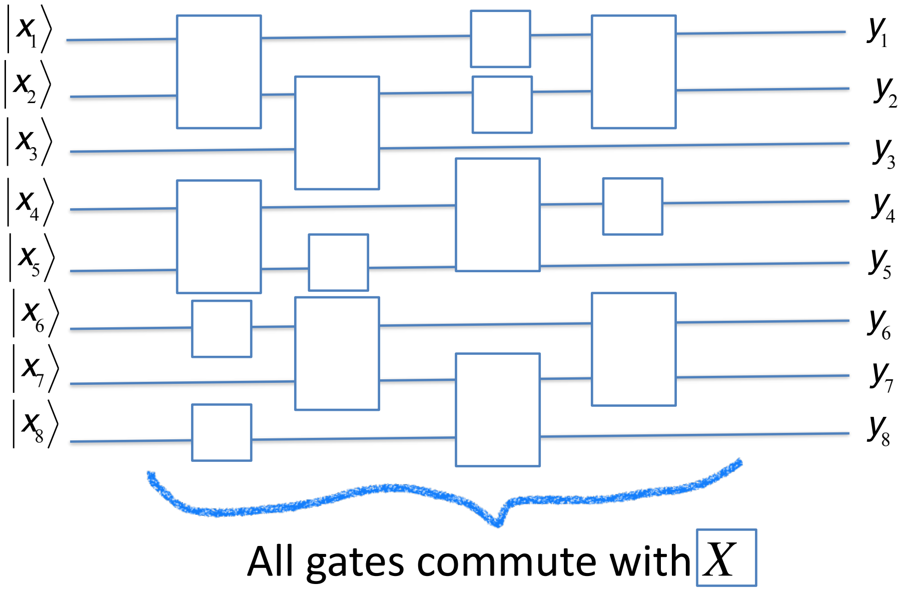
Probabilistic output:
$\bar{y}$ with prob $p(\bar{y})$

No classical poly circuit outputting $\bar{y}$ $p(\bar{y})$ else PH collapses

Sampling

[Bremner, Josza, Shepherd 2011]

Subuniversal circuit families



Probabilistic output:
$\bar{y}$ with prob $p(\bar{y})$

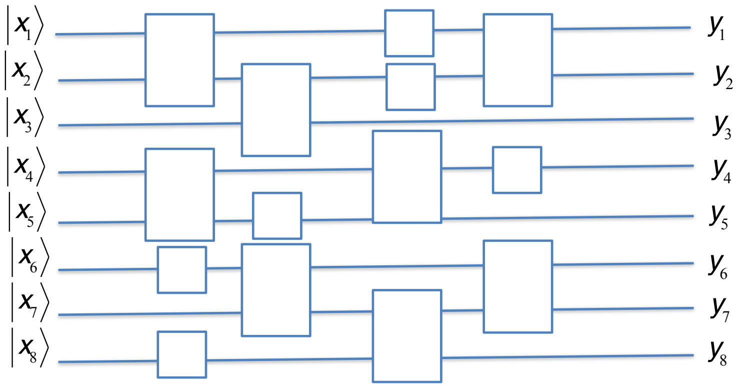
No classical poly circuit outputting $\bar{y}$ $p(\bar{y})$ else PH collapses

Quantum randomness at play here? Links to shallow circuit?

Sampling hardness implies shallow circuit

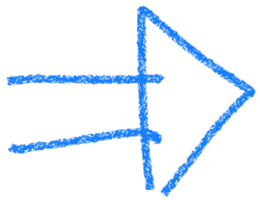
Sampling

Subuniversal circuit families

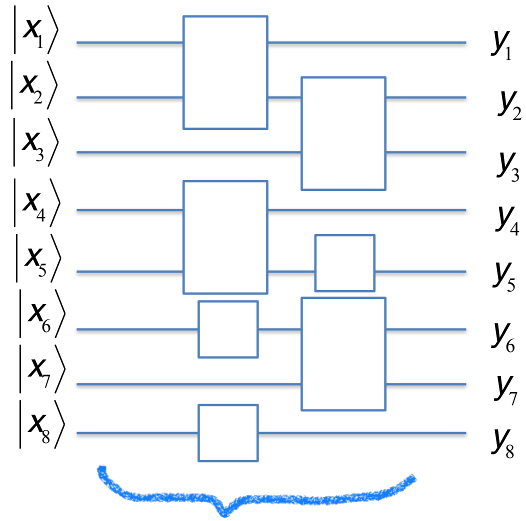


$\bar{y}$

$p(\bar{y})$



Shallow circuit advantage



Const

No classical poly circuit outputting $\bar{y}$ $p(\bar{y})$
else PH collapses

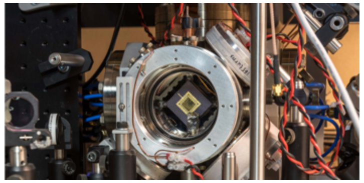
Relational statement $R(\bar{x}, \bar{y})$

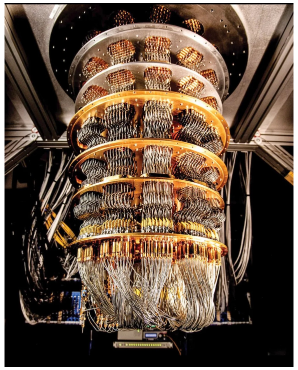
Impossible to satisfy classically in constant circuit

4. What's so hard about building a quantum computer?

Quantum coherence is fragile

- Decoherence, limits to 'classical'
- Require huge control and optimisation …

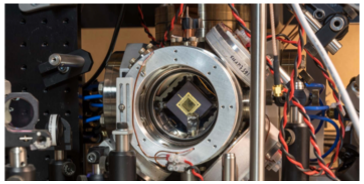


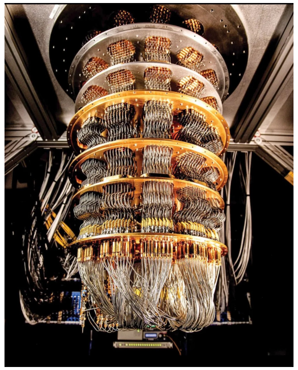


4. What's so hard about building a quantum computer?

Quantum coherence is fragile

- Decoherence, limits to 'classical'
- Require huge control and optimisation …





Quantum error correction and Fault Tolerance

- Possible!: more systems, more steps, feedback
- Huge overhead…

Quantum
the open journal for quantum science

PAPERS PERSPECTIVES

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney[1] and Martin Ekerå[2,3]

[1]Google Inc., Santa Barbara, California 93117, USA
[2]KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
[3]Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

20^6 noisy qubits to factor 2048 bits

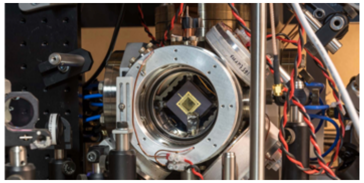
4. What's so hard about building a quantum computer?

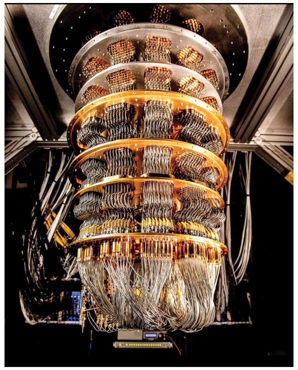
Quantum coherence is fragile

- Decoherence, limits to 'classical'
- Require huge control and optimisation …

Quantum error correction and Fault Tolerance

- Possible!: more systems, more steps, feedback
- Huge overhead…





⟨Quantum
the open journal for quantum science

PAPERS PERSPECTIVES

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney[1] and Martin Ekerå[2,3]

[1]Google Inc., Santa Barbara, California 93117, USA
[2]KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
[3]Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

20^6 noisy qubits to factor 2048 bits

Challenge: good codes/schemes, that work with real systems…

What can we do with quantum computers?

Exponential 'improvement'

- Shor's factoring algorithm [Shor, FOCS 1994]
  Factors numbers into primes
  -> could 'crack' RSA
- System of linear equations [Harrow, Hassidim, Lloyd, PRL 2008]
  Notable application to machine learning
  -> needs 'QRAM'
  -> applications?

Require FTQC

?

Variational, ML, …

'NISQ'
How much noise
FT?

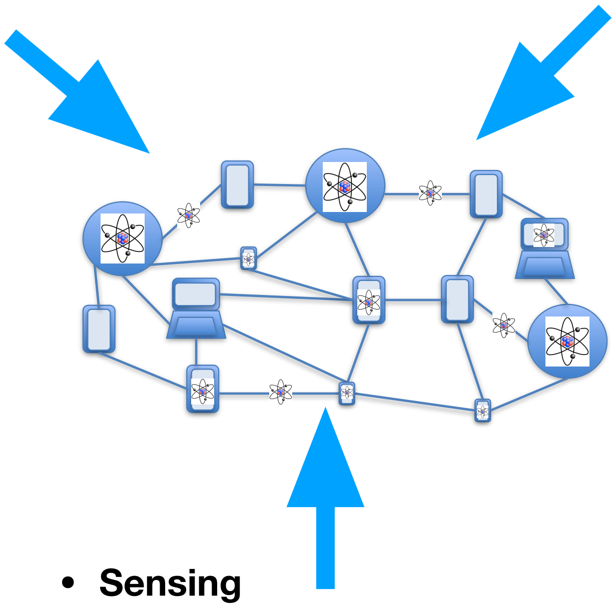
'Proven' quantum advantage

- Sampling problems
  [Aaronson, Arkhipov 2013]
  [Bremner, Josza, Shepherd 2011]
  Boson sampling, IQP, random shallow circuits…
  -> efficient classical simulation
  => collapse of PH
  -> applications?
- Shallow circuit advantage
  [Bravyi, Gosset, König, Science, 2018]
  Constant depth Q requires log depth C
  -> PROOF: concenquence of 'Q randomness'
  -> applications?

6. Quantum Networks

- **Computation**
  Exponential speed up (Shor), QML

- **Communication**
  Security (QKD), communication complexity



- **Sensing**
  Sensitivity and precision measurements impossible classically

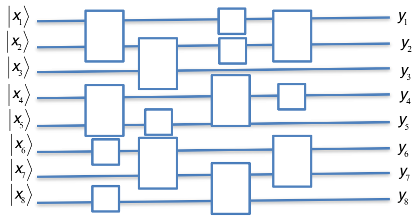
FRANCE 2030

QUANTUM FLAGSHIP

QIA QUANTUM INTERNET ALLIANCE

Conclusions

Quantum computing is not that complicated…



Just a special linear algebra processor

It's not just Shor's algorithm

Sampling

Shallow circuit

Search

…

Variational, ML, …

It's not just 'quantum computers'