Mathematical Symmetries in Quantum Information Science

David W. Lyons

Professor of Mathematical Sciences, Lebanon Valley College

Perry Lectures, Eastern Illinois University
1 November 2019

Outline

Outline

n bits versus n quantum bits

String of n bits:

n bits versus n quantum bits

String of n bits: A string of 0's and 1's of length n

n bits versus n quantum bits

String of n bits: A string of 0's and 1's of length n

Example with $n = 8$: The ascii code for the letter 'G'

$$○●○○○●●● = 01000111$$

n bits versus n quantum bits

String of n bits: A string of 0's and 1's of length n

Example with $n = 8$: The ascii code for the letter 'G'

$$\bigcirc\bullet\bigcirc\bigcirc\bigcirc\bullet\bullet\bullet = 01000111$$

n-qubit state:

n bits versus n quantum bits

String of n bits: A string of 0's and 1's of length n

Example with $n = 8$: The ascii code for the letter 'G'

○●○○○●●● $= 01000111$

n-qubit state: A superposition of n-bit strings

n bits versus n quantum bits

String of n bits: A string of 0's and 1's of length n

Example with $n = 8$: The ascii code for the letter 'G'

$$○●○○○●●● = 01000111$$

n-qubit state: A superposition of n-bit strings

Example with $n = 3$:

$$2○○● \;-\; i○●○ \;+\; (3+i)○●●$$

n bits versus n quantum bits

String of n bits: A string of 0's and 1's of length n

Example with $n = 8$: The ascii code for the letter 'G'

○●○○○●●● $= 01000111$

n-qubit state: A superposition of n-bit strings

Example with $n = 3$:

2○○● $-$ i○●○ $+$ $(3+i)$○●●

$$2\,|001\rangle - i\,|010\rangle + (3+i)\,|011\rangle$$

n bits versus n quantum bits

String of n bits: A string of 0's and 1's of length n

Example with $n = 8$: The ascii code for the letter 'G'

$$○●○○○●●● = 01000111$$

n-qubit state: A superposition of n-bit strings

Example with $n = 3$:

$$2\,○○● \;-\; i\,○●○ \;+\; (3+i)\,○●●$$

$$2\,|001\rangle - i\,|010\rangle + (3+i)\,|011\rangle$$

n-qubit state space

- "superposition" means "linear combination"
- the set of n-qubit states is a complex vector space of dimension

n bits versus n quantum bits

String of n bits: A string of 0's and 1's of length n

Example with $n = 8$: The ascii code for the letter 'G'

$$\bigcirc\!\bullet\!\bigcirc\!\bigcirc\!\bigcirc\!\bullet\!\bullet\!\bullet = 01000111$$

n-qubit state: A superposition of n-bit strings

Example with $n = 3$:

$$2\bigcirc\bigcirc\bullet \;-\; i\bigcirc\bullet\bigcirc \;+\; (3+i)\bigcirc\bullet\bullet$$

$$2\,|001\rangle - i\,|010\rangle + (3+i)\,|011\rangle$$

n-qubit state space

- "superposition" means "linear combination"
- the set of n-qubit states is a complex vector space of dimension 2^n

Systems of many quantum bits

Combining two qubits

$$\text{state of qubit } A = a\bigcirc + b\CIRCLE$$
$$\text{state of qubit } B = c\bigcirc + d\CIRCLE$$

Systems of many quantum bits

Combining two qubits

$$\text{state of qubit } A = a\bigcirc + b\bullet$$
$$\text{state of qubit } B = c\bigcirc + d\bullet$$
$$\text{composite state of qubits } AB = (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Systems of many quantum bits

Combining two qubits

$$\begin{aligned} \text{state of qubit } A &= a\bigcirc + b\bullet \\ \text{state of qubit } B &= c\bigcirc + d\bullet \\ \text{composite state of qubits } AB &= (a\bigcirc + b\bullet)(c\bigcirc + d\bullet) \\ &= ac\bigcirc\bigcirc + ad\bigcirc\bullet + bc\bullet\bigcirc + bd\bullet\bullet \end{aligned}$$

Entangled qubits

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bigcirc\bullet + \bullet\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Entangled qubits

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bigcirc\bullet + \bullet\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: $a = b = c = 1$

Entangled qubits

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bigcirc\bullet + \bullet\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: $a = b = c = 1$

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Entangled qubits

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bigcirc\bullet + \bullet\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: $a = b = c = 1$

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: This is not possible.

Entangled qubits

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bigcirc\bullet + \bullet\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: $a = b = c = 1$

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: This is not possible. Why?

Entangled qubits

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bigcirc\bullet + \bullet\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: $a = b = c = 1$

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: This is not possible. Why? Suppose factorization is possible.

Entangled qubits

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bigcirc\newmoon + \newmoon\bigcirc + \newmoon\newmoon \stackrel{?}{=} (a\bigcirc + b\newmoon)(c\bigcirc + d\newmoon)$$

Answer: $a = b = c = 1$

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \newmoon\newmoon \stackrel{?}{=} (a\bigcirc + b\newmoon)(c\bigcirc + d\newmoon)$$

Answer: This is not possible. Why? Suppose factorization is possible. Then we must have $ac = bd = 1$,

Entangled qubits

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bigcirc\bullet + \bullet\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: $a = b = c = 1$

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: This is not possible. Why? Suppose factorization is possible. Then we must have $ac = bd = 1$, so a, b, c, d are all nonzero.

Entangled qubits

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bigcirc\bullet + \bullet\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: $a = b = c = 1$

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: This is not possible. Why? Suppose factorization is possible. Then we must have $ac = bd = 1$, so a, b, c, d are all nonzero. But we must also have $ad = 0$,

Entangled qubits

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bigcirc\bullet + \bullet\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: $a = b = c = 1$

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: This is not possible. Why? Suppose factorization is possible. Then we must have $ac = bd = 1$, so a, b, c, d are all nonzero. But we must also have $ad = 0$, so one or both of a, d must be zero.

Entangled qubits

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bigcirc\bullet + \bullet\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: $a = b = c = 1$

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: This is not possible. Why? Suppose factorization is possible. Then we must have $ac = bd = 1$, so a, b, c, d are all nonzero. But we must also have $ad = 0$, so one or both of a, d must be zero. This is a contradiction.

Entangled qubits

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bigcirc\bullet + \bullet\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: $a = b = c = 1$

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: This is not possible. Why? Suppose factorization is possible. Then we must have $ac = bd = 1$, so a, b, c, d are all nonzero. But we must also have $ad = 0$, so one or both of a, d must be zero. This is a contradiction. Therefore factorization must not be possible.

Entangled qubits

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bigcirc\bullet + \bullet\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: $a = b = c = 1$

Puzzle: factor this 2-qubit state

$$\bigcirc\bigcirc + \bullet\bullet \stackrel{?}{=} (a\bigcirc + b\bullet)(c\bigcirc + d\bullet)$$

Answer: This is not possible. Why? Suppose factorization is possible. Then we must have $ac = bd = 1$, so a, b, c, d are all nonzero. But we must also have $ad = 0$, so one or both of a, d must be zero. This is a contradiction. Therefore factorization must not be possible.

Product states versus Entangled states

A state that factors is called a *product* state. A state that does not factor is called *entangled*.

Outline

Some quantum gates

$$\rightarrow \boxed{\quad X \quad} \rightarrow$$

Some quantum gates

$$\bigcirc \rightarrow \boxed{\quad X \quad} \rightarrow$$

Some quantum gates

$$\bigcirc \rightarrow \boxed{\quad X \quad} \rightarrow \bullet$$

Some quantum gates

$$\rightarrow \boxed{\quad X \quad} \rightarrow$$

Some quantum gates

$$\bullet \to \boxed{X} \to$$

Some quantum gates

$$\bullet \to \boxed{\quad X \quad} \to \circ$$

Some quantum gates

$$\rightarrow \boxed{X} \rightarrow$$

Some quantum gates

$$a\bigcirc + b\newmoon \quad \rightarrow \boxed{\quad X \quad} \rightarrow$$

Some quantum gates

$$a\bigcirc + b\CIRCLE \quad \rightarrow \boxed{\quad X \quad} \rightarrow \quad a\CIRCLE + b\bigcirc$$

Some quantum gates

$$a\bigcirc + b\bullet \quad \to \boxed{\quad X \quad} \to \quad a\bullet + b\bigcirc$$

$$\to \boxed{\quad Z \quad} \to$$

$$\to \boxed{\quad R_\phi \quad} \to$$

Some quantum gates

$$a\bigcirc + b\newmoon \quad \to \boxed{\quad X \quad} \to \quad a\newmoon + b\bigcirc$$

$$\bigcirc \to \boxed{\quad Z \quad} \to$$

$$\bigcirc \to \boxed{\quad R_\phi \quad} \to$$

Some quantum gates

$$a\bigcirc + b\bullet \;\to\; \boxed{X} \;\to\; a\bullet + b\bigcirc$$

$$\bigcirc \;\to\; \boxed{Z} \;\to\; \bigcirc$$

$$\bigcirc \;\to\; \boxed{R_\phi} \;\to\; \bigcirc$$

Some quantum gates

$$a\bigcirc + b\bullet \quad \to \boxed{\quad X \quad} \to \quad a\bullet + b\bigcirc$$

$$\to \boxed{\quad Z \quad} \to$$

$$\to \boxed{\quad R_\phi \quad} \to$$

Some quantum gates

$$a\bigcirc + b\bullet \quad \to \boxed{\quad X \quad} \to \quad a\bullet + b\bigcirc$$

$$\bullet \to \boxed{\quad Z \quad} \to$$

$$\bullet \to \boxed{\quad R_\phi \quad} \to$$

Some quantum gates

$$a\bigcirc + b\CIRCLE \;\to\; \boxed{X} \;\to\; a\CIRCLE + b\bigcirc$$

$$\CIRCLE \to \boxed{Z} \to -\CIRCLE$$

$$\CIRCLE \to \boxed{R_\phi} \to e^{i\phi}\,\CIRCLE$$

Some quantum gates

$$a\bigcirc + b\bullet \quad \rightarrow \boxed{\quad X \quad} \rightarrow \quad a\bullet + b\bigcirc$$

$$\rightarrow \boxed{\quad Z \quad} \rightarrow$$

$$\rightarrow \boxed{\quad R_\phi \quad} \rightarrow$$

Some quantum gates

$$a\bigcirc + b\bullet \quad \rightarrow \quad \boxed{\quad X \quad} \quad \rightarrow \quad a\bullet + b\bigcirc$$

$$a\bigcirc + b\bullet \quad \rightarrow \quad \boxed{\quad Z \quad} \quad \rightarrow$$

$$a\bigcirc + b\bullet \quad \rightarrow \quad \boxed{\quad R_\phi \quad} \quad \rightarrow$$

Some quantum gates

$$a\bigcirc + b\bullet \;\to\; \boxed{\;X\;} \;\to\; a\bullet + b\bigcirc$$

$$a\bigcirc + b\bullet \;\to\; \boxed{\;Z\;} \;\to\; a\bigcirc - b\bullet$$

$$a\bigcirc + b\bullet \;\to\; \boxed{\;R_\phi\;} \;\to\; a\bigcirc + be^{i\phi}\bullet$$

Some quantum gates

$$a\bigcirc + b\bullet \;\rightarrow\; \boxed{\;X\;} \;\rightarrow\; a\bullet + b\bigcirc$$

$$a\bigcirc + b\bullet \;\rightarrow\; \boxed{\;Z\;} \;\rightarrow\; a\bigcirc - b\bullet$$

$$a\bigcirc + b\bullet \;\rightarrow\; \boxed{\;R_\phi\;} \;\rightarrow\; a\bigcirc + be^{i\phi}\bullet$$

$$\rightarrow\; \boxed{\;H\;} \;\rightarrow$$

Some quantum gates

$$a\bigcirc + b\bullet \rightarrow \boxed{X} \rightarrow a\bullet + b\bigcirc$$

$$a\bigcirc + b\bullet \rightarrow \boxed{Z} \rightarrow a\bigcirc - b\bullet$$

$$a\bigcirc + b\bullet \rightarrow \boxed{R_\phi} \rightarrow a\bigcirc + be^{i\phi}\bullet$$

$$\bigcirc \rightarrow \boxed{H} \rightarrow$$

Some quantum gates

$$a\bigcirc + b\bullet \rightarrow \boxed{X} \rightarrow a\bullet + b\bigcirc$$

$$a\bigcirc + b\bullet \rightarrow \boxed{Z} \rightarrow a\bigcirc - b\bullet$$

$$a\bigcirc + b\bullet \rightarrow \boxed{R_\phi} \rightarrow a\bigcirc + be^{i\phi}\bullet$$

$$\bigcirc \rightarrow \boxed{H} \rightarrow \frac{1}{\sqrt{2}}(\bigcirc + \bullet) = {\color{red}\bullet}$$

Some quantum gates

$$a\bigcirc + b\bullet \rightarrow \boxed{X} \rightarrow a\bullet + b\bigcirc$$

$$a\bigcirc + b\bullet \rightarrow \boxed{Z} \rightarrow a\bigcirc - b\bullet$$

$$a\bigcirc + b\bullet \rightarrow \boxed{R_\phi} \rightarrow a\bigcirc + be^{i\phi}\bullet$$

$$\rightarrow \boxed{H} \rightarrow$$

Some quantum gates

$$a\bigcirc + b\bullet \;\to\; \boxed{X} \;\to\; a\bullet + b\bigcirc$$

$$a\bigcirc + b\bullet \;\to\; \boxed{Z} \;\to\; a\bigcirc - b\bullet$$

$$a\bigcirc + b\bullet \;\to\; \boxed{R_\phi} \;\to\; a\bigcirc + be^{i\phi}\bullet$$

$$\bullet \;\to\; \boxed{H} \;\to$$

Some quantum gates

$$a\bigcirc + b\bullet \rightarrow \boxed{X} \rightarrow a\bullet + b\bigcirc$$

$$a\bigcirc + b\bullet \rightarrow \boxed{Z} \rightarrow a\bigcirc - b\bullet$$

$$a\bigcirc + b\bullet \rightarrow \boxed{R_\phi} \rightarrow a\bigcirc + be^{i\phi}\bullet$$

$$\bullet \rightarrow \boxed{H} \rightarrow \frac{1}{\sqrt{2}}(\bigcirc - \bullet) = {\color{green}\bullet}$$

Some quantum gates

$$a\bigcirc + b\bullet \;\to\; \boxed{X} \;\to\; a\bullet + b\bigcirc$$

$$a\bigcirc + b\bullet \;\to\; \boxed{Z} \;\to\; a\bigcirc - b\bullet$$

$$a\bigcirc + b\bullet \;\to\; \boxed{R_\phi} \;\to\; a\bigcirc + be^{i\phi}\bullet$$

$$\to\; \boxed{H} \;\to$$

Some quantum gates

$$a\bigcirc + b\bullet \;\to\; \boxed{X} \;\to\; a\bullet + b\bigcirc$$

$$a\bigcirc + b\bullet \;\to\; \boxed{Z} \;\to\; a\bigcirc - b\bullet$$

$$a\bigcirc + b\bullet \;\to\; \boxed{R_\phi} \;\to\; a\bigcirc + be^{i\phi}\bullet$$

$$a\bigcirc + b\bullet \;\to\; \boxed{H} \;\to$$

Some quantum gates

$$a\bigcirc + b\bullet \rightarrow \boxed{X} \rightarrow a\bullet + b\bigcirc$$

$$a\bigcirc + b\bullet \rightarrow \boxed{Z} \rightarrow a\bigcirc - b\bullet$$

$$a\bigcirc + b\bullet \rightarrow \boxed{R_\phi} \rightarrow a\bigcirc + be^{i\phi}\bullet$$

$$a\bigcirc + b\bullet \rightarrow \boxed{H} \rightarrow a\textcolor{red}{\bullet} + b\textcolor{green}{\bullet}$$

Some quantum gates

$$a\bigcirc + b\bullet \to \boxed{X} \to a\bullet + b\bigcirc$$

$$a\bigcirc + b\bullet \to \boxed{Z} \to a\bigcirc - b\bullet$$

$$a\bigcirc + b\bullet \to \boxed{R_\phi} \to a\bigcirc + be^{i\phi}\bullet$$

$$a\bigcirc + b\bullet \to \boxed{H} \to a{\color{red}\bullet} + b{\color{green}\bullet}$$

$$\to \boxed{CZ} \to$$

Some quantum gates

$$a\bigcirc + b\bullet \rightarrow \boxed{X} \rightarrow a\bullet + b\bigcirc$$

$$a\bigcirc + b\bullet \rightarrow \boxed{Z} \rightarrow a\bigcirc - b\bullet$$

$$a\bigcirc + b\bullet \rightarrow \boxed{R_\phi} \rightarrow a\bigcirc + be^{i\phi}\bullet$$

$$a\bigcirc + b\bullet \rightarrow \boxed{H} \rightarrow a\bullet + b\bullet$$

$$a\bigcirc\bigcirc + b\bigcirc\bullet + c\bullet\bigcirc + d\bullet\bullet \rightarrow \boxed{CZ} \rightarrow$$

Some quantum gates

$$a\bigcirc + b\bullet \to \boxed{X} \to a\bullet + b\bigcirc$$

$$a\bigcirc + b\bullet \to \boxed{Z} \to a\bigcirc - b\bullet$$

$$a\bigcirc + b\bullet \to \boxed{R_\phi} \to a\bigcirc + be^{i\phi}\bullet$$

$$a\bigcirc + b\bullet \to \boxed{H} \to a{\color{red}\bullet} + b{\color{green}\bullet}$$

$$\begin{matrix} a\bigcirc\bigcirc + b\bigcirc\bullet \\ + c\bullet\bigcirc + d\bullet\bullet \end{matrix} \to \boxed{CZ} \to \begin{matrix} a\bigcirc\bigcirc + b\bigcirc\bullet \\ + c\bullet\bigcirc - d\bullet\bullet \end{matrix}$$

Some quantum gates

$$a\bigcirc + b\newcommand{\fb}{\large\bullet}\fb \;\rightarrow\; \boxed{X} \;\rightarrow\; a\fb + b\bigcirc$$

$$a\bigcirc + b\fb \;\rightarrow\; \boxed{Z} \;\rightarrow\; a\bigcirc - b\fb$$

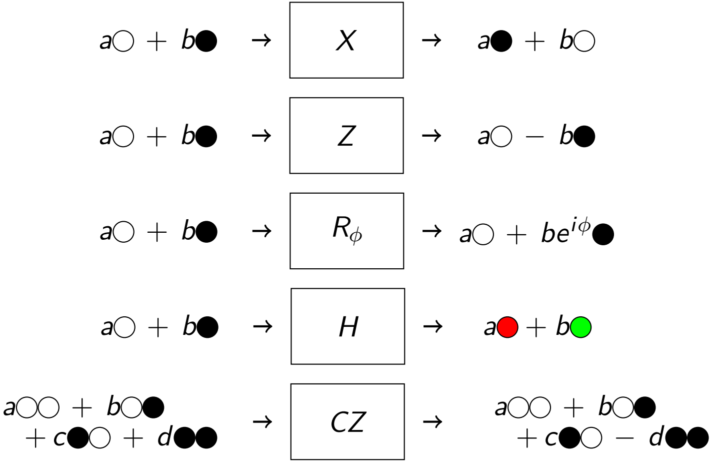
$$a\bigcirc + b\fb \;\rightarrow\; \boxed{R_\phi} \;\rightarrow\; a\bigcirc + be^{i\phi}\fb$$

$$a\bigcirc + b\fb \;\rightarrow\; \boxed{H} \;\rightarrow\; a{\color{red}\fb} + b{\color{green}\fb}$$

$$\begin{array}{l} a\bigcirc\bigcirc + b\bigcirc\fb \\ \quad + c\fb\bigcirc + d\fb\fb \end{array} \;\rightarrow\; \boxed{CZ} \;\rightarrow\; \begin{array}{l} a\bigcirc\bigcirc + b\bigcirc\fb \\ \quad + c\fb\bigcirc - d\fb\fb \end{array}$$

Pop quiz! $Z = R_\phi$ for what value of ϕ?

Some quantum gates



Pop quiz! $Z = R_\phi$ for what value of ϕ? Answer: $\phi = \pi$

Some quantum gates, cont'd

$$\bigcirc = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad \bullet = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Some quantum gates, cont'd

$$\bigcirc = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad \bullet = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \qquad {\color{red}\bullet} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \qquad {\color{green}\bullet} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

Some quantum gates, cont'd

$$\bigcirc = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad \bullet = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \qquad {\color{red}\bullet} = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \qquad {\color{green}\bullet} = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Z = R_\pi = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$R_\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

Some quantum gates: Quiz!

$$X\bigcirc =$$

Some quantum gates: Quiz!

$$X\bigcirc = \bullet$$

Some quantum gates: Quiz!

$$X\bigcirc = \CIRCLE$$
$$H\bigcirc =$$

Some quantum gates: Quiz!

$$X\bigcirc = \bullet$$

$$H\bigcirc = {\color{red}\bullet}$$

Some quantum gates: Quiz!

$$X\bigcirc = \bullet$$
$$H\bigcirc = {\color{red}\bullet}$$
$$(H \otimes H)\bigcirc\bullet =$$

Some quantum gates: Quiz!

$$X\bigcirc = \bullet$$

$$H\bigcirc = {\color{red}\bullet}$$

$$(H \otimes H)\bigcirc\bullet = {\color{red}\bullet}{\color{green}\bullet}$$

Some quantum gates: Quiz!

$$X\bigcirc = \bullet$$

$$H\bigcirc = \textcolor{red}{\bullet}$$

$$(H \otimes H)\bigcirc\bullet = \textcolor{red}{\bullet}\textcolor{green}{\bullet}$$

$$CZ(\bigcirc\bigcirc + \bullet\bullet) =$$

Some quantum gates: Quiz!

$$X\bigcirc = \bullet$$

$$H\bigcirc = {\color{red}\bullet}$$

$$(H \otimes H)\bigcirc\bullet = {\color{red}\bullet}{\color{green}\bullet}$$

$$CZ(\bigcirc\bigcirc + \bullet\bullet) = \bigcirc\bigcirc - \bullet\bullet$$

Some quantum gates: Quiz!

$$X\bigcirc = \bullet$$

$$H\bigcirc = {\color{red}\bullet}$$

$$(H \otimes H)\bigcirc\bullet = {\color{red}\bullet}{\color{green}\bullet}$$

$$CZ(\bigcirc\bigcirc + \bullet\bullet) = \bigcirc\bigcirc - \bullet\bullet$$

$$(R_a \otimes R_b \otimes R_{-(a+b)})(\bigcirc\bigcirc\bigcirc + \bullet\bullet\bullet) =$$

Some quantum gates: Quiz!

$$
\begin{aligned}
X\bigcirc &= \bullet \\
H\bigcirc &= \color{red}{\bullet} \\
(H \otimes H)\bigcirc\bullet &= \color{red}{\bullet}\color{green}{\bullet} \\
CZ(\bigcirc\bigcirc + \bullet\bullet) &= \bigcirc\bigcirc - \bullet\bullet \\
(R_a \otimes R_b \otimes R_{-(a+b)})(\bigcirc\bigcirc\bigcirc + \bullet\bullet\bullet) &= \bigcirc\bigcirc\bigcirc + \bullet\bullet\bullet
\end{aligned}
$$

Outline

Measure a qubit

Measurement of $a\bigcirc + b\bullet$ results in ...

Measure a qubit

Measurement of $a\bigcirc + b\CIRCLE$ results in ...

outcome (post-measurement state)	with probability
$\bigcirc$	$\lvert a\rvert^2$
$\CIRCLE$	$\lvert b\rvert^2$

Measure a qubit

Measurement of $a\bigcirc + b\CIRCLE$ results in ...

outcome (post-measurement state)	with probability
$\bigcirc$	$\lvert a\rvert^2$
$\CIRCLE$	$\lvert b\rvert^2$

Example: Measuring $\textcolor{red}{\CIRCLE} = \frac{1}{\sqrt{2}}(\bigcirc + \CIRCLE)$ results in outcome $\bigcirc$, $\CIRCLE$ with equal probability

Measure a qubit

Measurement of $a\bigcirc + b\bullet$ results in ...

outcome (post-measurement state)	with probability
$\bigcirc$	$\lvert a\rvert^2$
$\bullet$	$\lvert b\rvert^2$

Example: Measuring $\textcolor{red}{\bullet} = \frac{1}{\sqrt{2}}(\bigcirc + \bullet)$ results in outcome $\bigcirc$, $\bullet$ with equal probability

Example: Measuring $\frac{3}{5}\bigcirc + \frac{4}{5}\bullet$ results in outcome $\bigcirc$ with probability

Measure a qubit

Measurement of $a\bigcirc + b\bullet$ results in ...

outcome (post-measurement state)	with probability
$\bigcirc$	$\lvert a \rvert^2$
$\bullet$	$\lvert b \rvert^2$

Example: Measuring $\textcolor{red}{\bullet} = \frac{1}{\sqrt{2}}(\bigcirc + \bullet)$ results in outcome $\bigcirc$, $\bullet$ with equal probability

Example: Measuring $\frac{3}{5}\bigcirc + \frac{4}{5}\bullet$ results in outcome $\bigcirc$ with probability $9/25$

Summary: Quantum Mechanics* in a Nutshell

quantum states:	linear combinations of bit strings
evolution of states:	unitary transformations of state space
measurement:	finite set of outcome states with probability distribution
quantum computer:	put the above ingredients together

* (some details and complications are omitted)

Example: a circuit for making the EPR state

$$\downarrow$$
$$\boxed{H \otimes H}$$
$$\downarrow$$

$$\downarrow$$
$$\boxed{CZ}$$
$$\downarrow$$

$$\downarrow$$
$$\boxed{I \otimes H}$$
$$\downarrow$$

Example: a circuit for making the EPR state

$$\bigcirc\!\bigcirc$$

$$\downarrow$$

$$\boxed{H \otimes H}$$

$$\downarrow$$

$$\downarrow$$

$$\boxed{CZ}$$

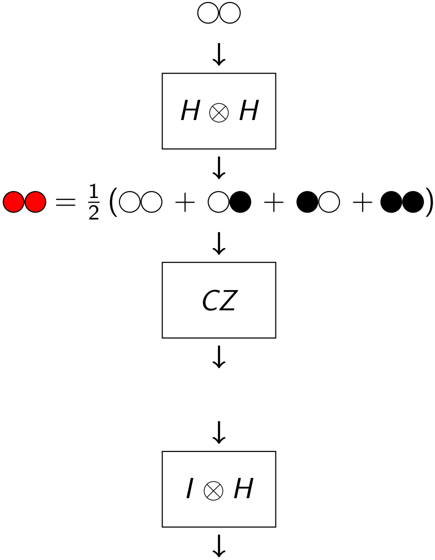
$$\downarrow$$

$$\downarrow$$

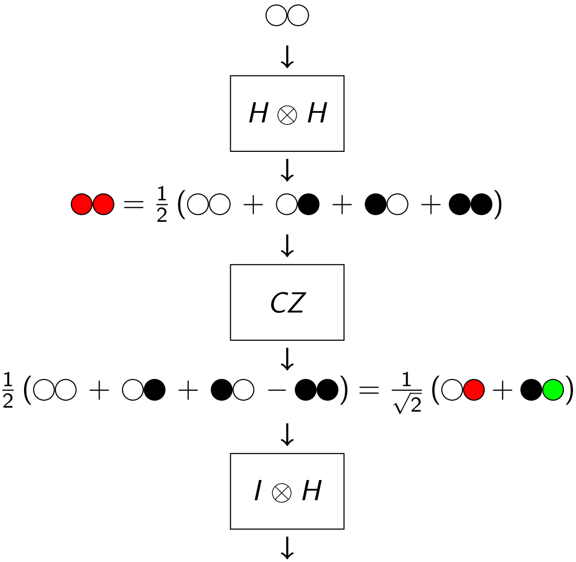
$$\boxed{I \otimes H}$$

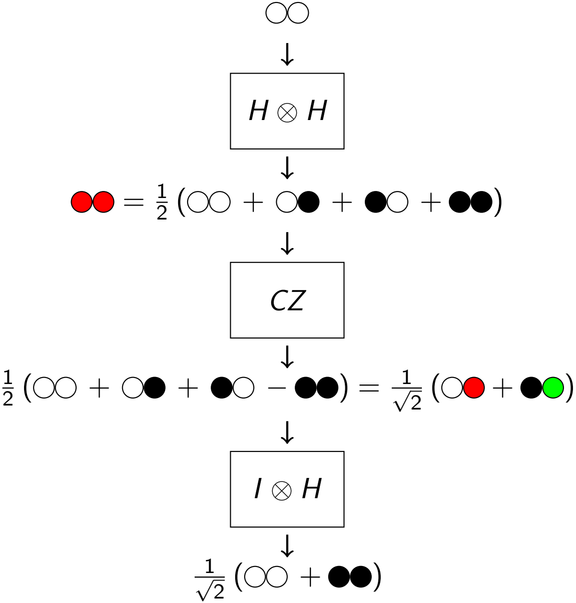
$$\downarrow$$

Example: a circuit for making the EPR state



Example: a circuit for making the EPR state




$H \otimes H$
$\frac{1}{2}$
CZ
$\frac{1}{2}$
$\frac{1}{\sqrt{2}}$
$I \otimes H$
$\frac{1}{\sqrt{2}}$

Brief survey: some things quantum computers will do

- Shor's factoring algorithm
- Grover's search algorithm
- A zoo of linear algebra algorithms
- Monte Carlo simulation

Outline

1. Introduction
   - Quantum states
   - Evolution of quantum states
   - Measurement of quantum states
2. Werner Symmetry
   - Stabilizer groups
   - Werner operators and Werner states
   - Werner states
3. Function-encoding States
   - Boolean functions
   - Pascal's triangle and the parity party trick

Stabilizer groups

Examples of local unitary operators that do not affect a state

$$(X \otimes X)(\bigcirc\bigcirc + \bullet\bullet) = \bullet\bullet + \bigcirc\bigcirc$$
$$(I \otimes Z \otimes Z)(\bigcirc\bigcirc\bigcirc + \bullet\bullet\bullet) = \bigcirc\bigcirc\bigcirc + \bullet\bullet\bullet$$

Stabilizer groups

Examples of local unitary operators that do not affect a state

$$(X \otimes X)(\bigcirc\bigcirc + \bullet\bullet) = \bullet\bullet + \bigcirc\bigcirc$$
$$(I \otimes Z \otimes Z)(\bigcirc\bigcirc\bigcirc + \bullet\bullet\bullet) = \bigcirc\bigcirc\bigcirc + \bullet\bullet\bullet$$

Definition: a linear operator A stabilizes a state vector ψ

Stabilizer groups

Examples of local unitary operators that do not affect a state

$$(X \otimes X)(\bigcirc\bigcirc + \bullet\bullet) = \bullet\bullet + \bigcirc\bigcirc$$
$$(I \otimes Z \otimes Z)(\bigcirc\bigcirc\bigcirc + \bullet\bullet\bullet) = \bigcirc\bigcirc\bigcirc + \bullet\bullet\bullet$$

Definition: a linear operator A stabilizes a state vector ψ

$$A\psi = \psi$$

Stabilizer groups

Examples of local unitary operators that do not affect a state

$$(X \otimes X)(\bigcirc\bigcirc + \bullet\bullet) = \bullet\bullet + \bigcirc\bigcirc$$
$$(I \otimes Z \otimes Z)(\bigcirc\bigcirc\bigcirc + \bullet\bullet\bullet) = \bigcirc\bigcirc\bigcirc + \bullet\bullet\bullet$$

Definition: a linear operator A stabilizes a state vector ψ

$$A\psi = (\text{some constant times})\ \psi$$

Outline

Werner stabilizer type

The Werner stabilizer group

Consider the group of operators of the form

$$U^{\otimes n} = U \otimes U \otimes \cdots \otimes U$$

where U is an arbitrary 1-qubit unitary operator

Werner stabilizer type

The Werner stabilizer group

Consider the group of operators of the form

$$U^{\otimes n} = U \otimes U \otimes \cdots \otimes U$$

where U is an arbitrary 1-qubit unitary operator

Motivation: These states are resources quantum codes, communication protocols, nonlocality study, more...

Werner stabilizer type

The Werner stabilizer group

Consider the group of operators of the form

$$U^{\otimes n} = U \otimes U \otimes \cdots \otimes U$$

where U is an arbitrary 1-qubit unitary operator

Motivation: These states are resources quantum codes, communication protocols, nonlocality study, more...
This motivates the following...

Werner stabilizer type

The Werner stabilizer group

Consider the group of operators of the form

$$U^{\otimes n} = U \otimes U \otimes \cdots \otimes U$$

where U is an arbitrary 1-qubit unitary operator

Motivation: These states are resources quantum codes, communication protocols, nonlocality study, more...
This motivates the following...

Problem: Classify the Werner states

(i) Describe all states that are stabilized by the Werner group.

Werner stabilizer type

The Werner stabilizer group

Consider the group of operators of the form

$$U^{\otimes n} = U \otimes U \otimes \cdots \otimes U$$

where U is an arbitrary 1-qubit unitary operator

Motivation: These states are resources quantum codes, communication protocols, nonlocality study, more...
This motivates the following...

Problem: Classify the Werner states

(i) Describe all states that are stabilized by the Werner group.
(ii) Eliminate redundancies from the answer to (i).

Outline

Werner-stabilized states

Example: A state whose stabilizer is the Werner group

The "singlet" state $\bigcirc\!\bullet - \bullet\!\bigcirc$

Werner-stabilized states

Example: A state whose stabilizer is the Werner group

The "singlet" state $\bigcirc\!\bullet - \bullet\!\bigcirc$

For example:

$$
\begin{aligned}
(H \otimes H)(\bigcirc\!\bullet - \bullet\!\bigcirc) &= {\color{red}\bullet}{\color{green}\bullet} - {\color{green}\bullet}{\color{red}\bullet} \\
&= \frac{1}{2}\left((\bigcirc + \bullet)(\bigcirc - \bullet) - (\bigcirc - \bullet)(\bigcirc + \bullet)\right) \\
&= -(\bigcirc\!\bullet - \bullet\!\bigcirc)
\end{aligned}
$$

Werner-stabilized states

Example: A state whose stabilizer is the Werner group

The "singlet" state $\bigcirc\!\!\bullet - \bullet\!\!\bigcirc$

For example:

$$
\begin{aligned}
(H \otimes H)(\bigcirc\bullet - \bullet\bigcirc) &= {\color{red}\bullet}{\color{green}\bullet} - {\color{green}\bullet}{\color{red}\bullet} \\
&= \frac{1}{2}\left((\bigcirc + \bullet)(\bigcirc - \bullet) - (\bigcirc - \bullet)(\bigcirc + \bullet)\right) \\
&= -(\bigcirc\bullet - \bullet\bigcirc)
\end{aligned}
$$

Singlets as building blocks for Werner-stabilized states

- Products of singlets, for example $(\bigcirc\bullet - \bullet\bigcirc)(\bigcirc\bullet - \bullet\bigcirc)$
- Superpositions of products of singlets

Werner-stabilized states, cont'd

Fact: Any Werner-stabilized state is a superposition of products of singlets

Werner-stabilized states, cont'd

Fact: Any Werner-stabilized state is a superposition of products of singlets

Problem: Classify the Werner states.

(i) Describe all states whose stabilizer is the Werner group.
Answer: Any such state is a superposition of products of singlets.

(ii) Eliminate redundancies from the answer to (i).

Werner-stabilized states, cont'd

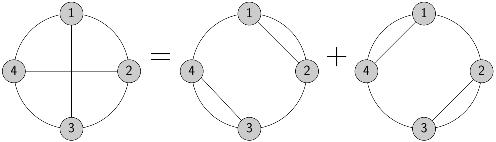
Fact: Any Werner-stabilized state is a superposition of products of singlets

Problem: Classify the Werner states.

(i) Describe all states whose stabilizer is the Werner group.
Answer: Any such state is a superposition of products of singlets.

(ii) Eliminate redundancies from the answer to (i).

Redundancy!



$$\begin{pmatrix} ○○●● - ○●●○ \\ -●○○● + ●●○○ \end{pmatrix} = \begin{pmatrix} ○●○● - ○●●○ \\ -●○○● + ●○●○ \end{pmatrix} + \begin{pmatrix} ○○●● - ○●○● \\ -●○●○ + ●●○○ \end{pmatrix}$$

Noncrossing chord diagrams

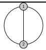
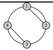
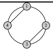
Puzzle

Given $n = 2m$ people seated at a round table, how many different noncrossing handshake configurations are there?

Noncrossing chord diagrams

Puzzle

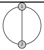
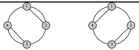
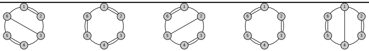
Given $n = 2m$ people seated at a round table, how many different noncrossing handshake configurations are there?

m	Noncrossing chord diagrams
2	
2	 
3	

Noncrossing chord diagrams

Puzzle

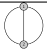
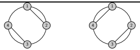
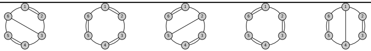
Given $n = 2m$ people seated at a round table, how many different noncrossing handshake configurations are there?

m	Noncrossing chord diagrams
2	
2	
3	
4	

Noncrossing chord diagrams

Puzzle

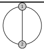
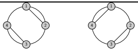
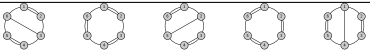
Given $n = 2m$ people seated at a round table, how many different noncrossing handshake configurations are there?

m	Noncrossing chord diagrams
2	
2	
3	
4	(42 in all)

Noncrossing chord diagrams

Puzzle

Given $n = 2m$ people seated at a round table, how many different noncrossing handshake configurations are there?

m	Noncrossing chord diagrams
2	
2	
3	
4	(42 in all)

Catalan numbers (sequence A000108 in the OEIS)

$$1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, 208012, 742900, \ldots$$

Werner-stabilized states, summary

Problem: Classify the Werner states

(i) Describe all states that are stabilized by the Werner group.
Solution: Any such state is a superposition of products of singlets. In fact, any such state is a unique superposition of singlets in a noncrossing chord diagram.

Werner-stabilized states, summary

Problem: Classify the Werner states

(i) Describe all states that are stabilized by the Werner group.
Solution: Any such state is a superposition of products of singlets. In fact, any such state is a unique superposition of singlets in a noncrossing chord diagram.

(ii) Eliminate redundancies from the answer to (i).
Solution: You get a complete, non-redundant list of Werner states using superpositions of noncrossing chord diagrams.

Werner-stabilized states, summary

Problem: Classify the Werner states

(i) Describe all states that are stabilized by the Werner group.
Solution: Any such state is a superposition of products of singlets. In fact, any such state is a unique superposition of singlets in a noncrossing chord diagram.

(ii) Eliminate redundancies from the answer to (i).
Solution: You get a complete, non-redundant list of Werner states using superpositions of noncrossing chord diagrams.

SOLVED!!!

Outline

1. Introduction
   - Quantum states
   - Evolution of quantum states
   - Measurement of quantum states
2. Werner Symmetry
   - Stabilizer groups
   - Werner operators and Werner states
   - Werner states
3. Function-encoding States
   - Boolean functions
   - Pascal's triangle and the parity party trick

Boolean functions and function-encoding states

Boolean function

bit strings$\longrightarrow$bits

Boolean functions and function-encoding states

Boolean function

bit strings ⟶ bits

Example: XOR

input	○○	○●	●○	●●
output	○	●	●	○

Boolean functions and function-encoding states

Boolean function

bit strings$\longrightarrow$bits

Example: XOR

input	○○	○●	●○	●●
output	○	●	●	○

How many Boolean functions for *n*-bit inputs?

Question: How many inputs?

Boolean functions and function-encoding states

Boolean function

bit strings$\longrightarrow$bits

Example: XOR

input	○○	○●	●○	●●
output	○	●	●	○

How many Boolean functions for n-bit inputs?

Question: How many inputs? Answer: 2^n

Boolean functions and function-encoding states

Boolean function

bit strings $\longrightarrow$ bits

Example: XOR

input	○○	○●	●○	●●
output	○	●	●	○

How many Boolean functions for n-bit inputs?

Question: How many inputs? Answer: 2^n

Question: How many functions?

Boolean functions and function-encoding states

Boolean function

bit strings $\longrightarrow$ bits

Example: XOR

input	○○	○●	●○	●●
output	○	●	●	○

How many Boolean functions for *n*-bit inputs?

Question: How many inputs? Answer: 2^n

Question: How many functions? Answer: $2^{(2^n)}$

Function-encoding states

$$[f(\text{string}) = \bigcirc] \to +\text{string}$$
$$[f(\text{string}) = \bullet] \to -\text{string}$$

Function-encoding states

$$[f(\text{string}) = \bigcirc] \to +\text{string}$$
$$[f(\text{string}) = \bullet] \to -\text{string}$$

Example: XOR as a quantum state

input	○○	○●	●○	●●
output	○	●	●	○
output $\to \pm 1$	$+1$	-1	-1	$+1$

Function-encoding states

$$[f(\text{string}) = \bigcirc] \to +\text{string}$$
$$[f(\text{string}) = \bullet] \to -\text{string}$$

Example: XOR as a quantum state

input	$\bigcirc\bigcirc$	$\bigcirc\bullet$	$\bullet\bigcirc$	$\bullet\bullet$
output	$\bigcirc$	$\bullet$	$\bullet$	$\bigcirc$
output $\to \pm 1$	$+1$	-1	-1	$+1$

$$\text{XOR state} = \bigcirc\bigcirc - \bigcirc\bullet - \bullet\bigcirc + \bullet\bullet$$

Boolean functions as polynomials

Example: $xy + xz$

input x, y, z	000	001	010	011	100	101	110	111
output $xy + xz$	0	0	0	0	0	1	1	0
output $(-1)^{xy+xz}$	$+1$	$+1$	$+1$	$+1$	$+1$	-1	-1	$+1$

$$xy + xz \text{ state} = 000 + 001 + 010 + 011 + 100 - 101 - 110 + 111$$

Boolean functions as polynomials

Example: $xy + xz$

input x, y, z	000	001	010	011	100	101	110	111
output $xy + xz$	0	0	0	0	0	1	1	0
output $(-1)^{xy+xz}$	$+1$	$+1$	$+1$	$+1$	$+1$	-1	-1	$+1$

$$xy + xz \text{ state} = 000 + 001 + 010 + 011 + 100 - 101 - 110 + 111$$

Fact

Every Boolean function is represented by a polynomial.

Boolean functions as polynomials

Example: $xy + xz$

input x, y, z	000	001	010	011	100	101	110	111
output $xy + xz$	0	0	0	0	0	1	1	0
output $(-1)^{xy+xz}$	$+1$	$+1$	$+1$	$+1$	$+1$	-1	-1	$+1$

$$xy + xz \text{ state} = 000 + 001 + 010 + 011 + 100 - 101 - 110 + 111$$

Fact

Every Boolean function is represented by a polynomial.

Quiz!

What is the polynomial for the function encoded in this state?

$$000 + 001 + 010 + 011 - 100 - 101 + 110 - 111$$

Boolean functions as polynomials

Example: $xy + xz$

input x, y, z	000	001	010	011	100	101	110	111
output $xy + xz$	0	0	0	0	0	1	1	0
output $(-1)^{xy+xz}$	$+1$	$+1$	$+1$	$+1$	$+1$	-1	-1	$+1$

$$xy + xz \text{ state} = 000 + 001 + 010 + 011 + 100 - 101 - 110 + 111$$

Fact

Every Boolean function is represented by a polynomial.

Quiz!

What is the polynomial for the function encoded in this state?

$$000 + 001 + 010 + 011 - 100 - 101 + 110 - 111$$

Answer: $x + xy + xyz$

Converting table of values to monomial coefficients, and vice-versa

Why do we care?

Monomials are blueprints for quantum gates to construct function-encoding states.

Converting table of values to monomial coefficients, and vice-versa

Why do we care?

Monomials are blueprints for quantum gates to construct function-encoding states.

Example: $x_2 x_3 x_5$ gate implementation

$C_{2,3,5}$ gate acts on qubits $2, 3, 5$, sends ●●● $\rightarrow$ $-$●●●, leaves all other strings unchanged.

Conversion example: $000 + 001 + 010 + 011 - 100 - 101 + 110 - 111$ to $x + xy + xyz$

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

Conversion example:
$000 + 001 + 010 + 011 - 100 - 101 + 110 - 111$ to $x + xy + xyz$

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} \quad \begin{array}{c} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{array}$$

Conversion example: $000 + 001 + 010 + 011 - 100 - 101 + 110 - 111$ to $x + xy + xyz$

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} \quad \begin{matrix} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{matrix} \quad \rightarrow \quad \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

Conversion example: $000 + 001 + 010 + 011 - 100 - 101 + 110 - 111$ to $x + xy + xyz$

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} \begin{matrix} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{matrix} \quad \rightarrow \quad \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} \begin{matrix} x^0y^0z^0 \\ x^0y^0z^1 \\ x^0y^1z^0 \\ x^0y^1z^1 \\ x^1y^0z^0 \\ x^1y^0z^1 \\ x^1y^1z^0 \\ x^1y^1z^1 \end{matrix}$$

Conversion example: $000 + 001 + 010 + 011 - 100 - 101 + 110 - 111$ to $x + xy + xyz$

$$
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}
\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}
\begin{array}{c} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{array}
=
\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}
\begin{array}{c} x^0y^0z^0 \\ x^0y^0z^1 \\ x^0y^1z^0 \\ x^0y^1z^1 \\ x^1y^0z^0 \\ x^1y^0z^1 \\ x^1y^1z^0 \\ x^1y^1z^1 \end{array}
$$

Conversion example, continued: $000 + 001 + 010 + 011 - 100 - 101 + 110 - 111$ to $x + xy + xyz$

$$
\begin{bmatrix}
\binom{0}{0} & \binom{0}{1} & \binom{0}{2} & \binom{0}{3} & \binom{0}{4} & \binom{0}{5} & \binom{0}{6} & \binom{0}{7} \\
\binom{1}{0} & \binom{1}{1} & \binom{1}{2} & \binom{1}{3} & \binom{1}{4} & \binom{1}{5} & \binom{1}{6} & \binom{1}{7} \\
\binom{2}{0} & \binom{2}{1} & \binom{2}{2} & \binom{2}{3} & \binom{2}{4} & \binom{2}{5} & \binom{2}{6} & \binom{2}{7} \\
\binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} & \binom{3}{4} & \binom{3}{5} & \binom{3}{6} & \binom{3}{7} \\
\binom{4}{0} & \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \binom{4}{4} & \binom{4}{5} & \binom{4}{6} & \binom{4}{7} \\
\binom{5}{0} & \binom{5}{1} & \binom{5}{2} & \binom{5}{3} & \binom{5}{4} & \binom{5}{5} & \binom{5}{6} & \binom{5}{7} \\
\binom{6}{0} & \binom{6}{1} & \binom{6}{2} & \binom{6}{3} & \binom{6}{4} & \binom{6}{5} & \binom{6}{6} & \binom{6}{7} \\
\binom{7}{0} & \binom{7}{1} & \binom{7}{2} & \binom{7}{3} & \binom{7}{4} & \binom{7}{5} & \binom{7}{6} & \binom{7}{7}
\end{bmatrix}
\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}
\begin{array}{c} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{array}
=
\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}
\begin{array}{c} x^0y^0z^0 \\ x^0y^0z^1 \\ x^0y^1z^0 \\ x^0y^1z^1 \\ x^1y^0z^0 \\ x^1y^0z^1 \\ x^1y^1z^0 \\ x^1y^1z^1 \end{array}
$$

Conversion example, continued: $000 + 001 + 010 + 011 - 100 - 101 + 110 - 111$ to $x + xy + xyz$

$$\begin{bmatrix}
\binom{0}{0} & \binom{0}{1} & \binom{0}{2} & \binom{0}{3} & \binom{0}{4} & \binom{0}{5} & \binom{0}{6} & \binom{0}{7} \\
\binom{1}{0} & \binom{1}{1} & \binom{1}{2} & \binom{1}{3} & \binom{1}{4} & \binom{1}{5} & \binom{1}{6} & \binom{1}{7} \\
\binom{2}{0} & \binom{2}{1} & \binom{2}{2} & \binom{2}{3} & \binom{2}{4} & \binom{2}{5} & \binom{2}{6} & \binom{2}{7} \\
\binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} & \binom{3}{4} & \binom{3}{5} & \binom{3}{6} & \binom{3}{7} \\
\binom{4}{0} & \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \binom{4}{4} & \binom{4}{5} & \binom{4}{6} & \binom{4}{7} \\
\binom{5}{0} & \binom{5}{1} & \binom{5}{2} & \binom{5}{3} & \binom{5}{4} & \binom{5}{5} & \binom{5}{6} & \binom{5}{7} \\
\binom{6}{0} & \binom{6}{1} & \binom{6}{2} & \binom{6}{3} & \binom{6}{4} & \binom{6}{5} & \binom{6}{6} & \binom{6}{7} \\
\binom{7}{0} & \binom{7}{1} & \binom{7}{2} & \binom{7}{3} & \binom{7}{4} & \binom{7}{5} & \binom{7}{6} & \binom{7}{7}
\end{bmatrix}
\begin{array}{c}
\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}
\end{array}
\begin{array}{c} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{array}
=
\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}
\begin{array}{c} x^0y^0z^0 \\ x^0y^0z^1 \\ x^0y^1z^0 \\ x^0y^1z^1 \\ x^1y^0z^0 \\ x^1y^0z^1 \\ x^1y^1z^0 \\ x^1y^1z^1 \end{array}$$

- Pascal's triangle mod 2 converts Boolean function tables to polynomials

Conversion example, continued: $000 + 001 + 010 + 011 - 100 - 101 + 110 - 111$ to $x + xy + xyz$

$$\begin{bmatrix}
\binom{0}{0} & \binom{0}{1} & \binom{0}{2} & \binom{0}{3} & \binom{0}{4} & \binom{0}{5} & \binom{0}{6} & \binom{0}{7} \\
\binom{1}{0} & \binom{1}{1} & \binom{1}{2} & \binom{1}{3} & \binom{1}{4} & \binom{1}{5} & \binom{1}{6} & \binom{1}{7} \\
\binom{2}{0} & \binom{2}{1} & \binom{2}{2} & \binom{2}{3} & \binom{2}{4} & \binom{2}{5} & \binom{2}{6} & \binom{2}{7} \\
\binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} & \binom{3}{4} & \binom{3}{5} & \binom{3}{6} & \binom{3}{7} \\
\binom{4}{0} & \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \binom{4}{4} & \binom{4}{5} & \binom{4}{6} & \binom{4}{7} \\
\binom{5}{0} & \binom{5}{1} & \binom{5}{2} & \binom{5}{3} & \binom{5}{4} & \binom{5}{5} & \binom{5}{6} & \binom{5}{7} \\
\binom{6}{0} & \binom{6}{1} & \binom{6}{2} & \binom{6}{3} & \binom{6}{4} & \binom{6}{5} & \binom{6}{6} & \binom{6}{7} \\
\binom{7}{0} & \binom{7}{1} & \binom{7}{2} & \binom{7}{3} & \binom{7}{4} & \binom{7}{5} & \binom{7}{6} & \binom{7}{7}
\end{bmatrix}
\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}
\begin{array}{c} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{array}
=
\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}
\begin{array}{c} x^0y^0z^0 \\ x^0y^0z^1 \\ x^0y^1z^0 \\ x^0y^1z^1 \\ x^1y^0z^0 \\ x^1y^0z^1 \\ x^1y^1z^0 \\ x^1y^1z^1 \end{array}$$

- Pascal's triangle mod 2 converts Boolean function tables to polynomials
- Pascal's triangle mod 2 is self inverse!

Conversion example, continued: $000 + 001 + 010 + 011 - 100 - 101 + 110 - 111$ to $x + xy + xyz$

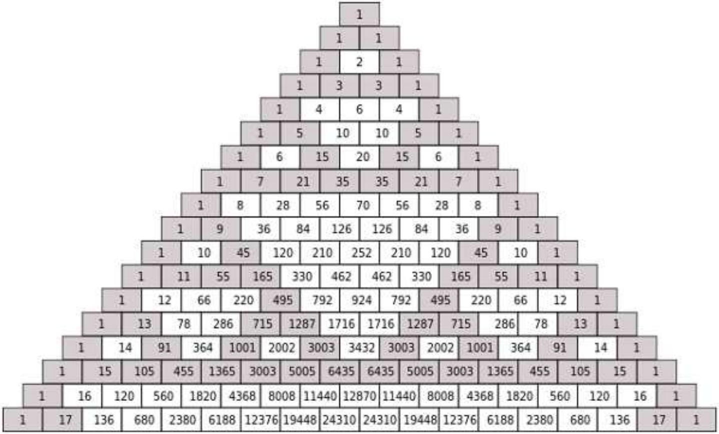
$$\begin{bmatrix}
\binom{0}{0} & \binom{0}{1} & \binom{0}{2} & \binom{0}{3} & \binom{0}{4} & \binom{0}{5} & \binom{0}{6} & \binom{0}{7} \\
\binom{1}{0} & \binom{1}{1} & \binom{1}{2} & \binom{1}{3} & \binom{1}{4} & \binom{1}{5} & \binom{1}{6} & \binom{1}{7} \\
\binom{2}{0} & \binom{2}{1} & \binom{2}{2} & \binom{2}{3} & \binom{2}{4} & \binom{2}{5} & \binom{2}{6} & \binom{2}{7} \\
\binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} & \binom{3}{4} & \binom{3}{5} & \binom{3}{6} & \binom{3}{7} \\
\binom{4}{0} & \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \binom{4}{4} & \binom{4}{5} & \binom{4}{6} & \binom{4}{7} \\
\binom{5}{0} & \binom{5}{1} & \binom{5}{2} & \binom{5}{3} & \binom{5}{4} & \binom{5}{5} & \binom{5}{6} & \binom{5}{7} \\
\binom{6}{0} & \binom{6}{1} & \binom{6}{2} & \binom{6}{3} & \binom{6}{4} & \binom{6}{5} & \binom{6}{6} & \binom{6}{7} \\
\binom{7}{0} & \binom{7}{1} & \binom{7}{2} & \binom{7}{3} & \binom{7}{4} & \binom{7}{5} & \binom{7}{6} & \binom{7}{7}
\end{bmatrix}
\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}
\begin{array}{c} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{array}
=
\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}
\begin{array}{c} x^0y^0z^0 \\ x^0y^0z^1 \\ x^0y^1z^0 \\ x^0y^1z^1 \\ x^1y^0z^0 \\ x^1y^0z^1 \\ x^1y^1z^0 \\ x^1y^1z^1 \end{array}$$

- Pascal's triangle mod 2 converts Boolean function tables to polynomials
- Pascal's triangle mod 2 is self inverse!
- Pascal's triangle mod 2 converts polynomials to Boolean function tables

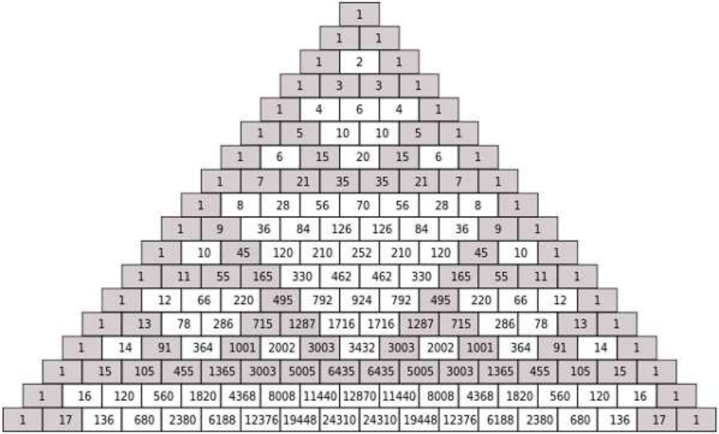
Outline

1. Introduction
   - Quantum states
   - Evolution of quantum states
   - Measurement of quantum states
2. Werner Symmetry
   - Stabilizer groups
   - Werner operators and Werner states
   - Werner states
3. Function-encoding States
   - Boolean functions
   - Pascal's triangle and the parity party trick

Pascal's triangle mod 2



Pascal's triangle mod 2



Question

Given n, k, what is the parity of $\binom{n}{k}$?

Parity party trick

$\binom{n}{k}$	

Parity party trick

$\binom{n}{k}$	
even or odd?	

Parity party trick

$\binom{n}{k}$	$\binom{5}{2}$
even or odd?	

Parity party trick

$\binom{n}{k}$	$\binom{5}{2}$
even or odd?	$\boxed{10}$

Parity party trick

$\binom{n}{k}$	$\binom{5}{2}$	$\binom{6}{4}$
even or odd?	$\boxed{10}$	

Parity party trick

$\binom{n}{k}$	$\binom{5}{2}$	$\binom{6}{4}$
even or odd?	$\boxed{10}$	$\boxed{15}$

Parity party trick

$\binom{n}{k}$	$\binom{5}{2}$	$\binom{6}{4}$	$\binom{11}{5}$
even or odd?	$\boxed{10}$	$\boxed{15}$	

Parity party trick

$\binom{n}{k}$	$\binom{5}{2}$	$\binom{6}{4}$	$\binom{11}{5}$
even or odd?	$\boxed{10}$	$\boxed{15}$	$\boxed{462}$

Parity party trick

$\binom{n}{k}$	$\binom{5}{2}$	$\binom{6}{4}$	$\binom{11}{5}$	$\binom{14}{6}$
even or odd?	$\boxed{10}$	$\boxed{15}$	$\boxed{462}$	

Parity party trick

$\binom{n}{k}$	$\binom{5}{2}$	$\binom{6}{4}$	$\binom{11}{5}$	$\binom{14}{6}$
even or odd?	$\boxed{10}$	$\boxed{15}$	$\boxed{462}$	$\boxed{3003}$

Parity party trick

$\binom{n}{k}$	$\binom{5}{2}$	$\binom{6}{4}$	$\binom{11}{5}$	$\binom{14}{6}$	$\binom{17}{9}$
even or odd?	$\boxed{10}$	$\boxed{15}$	$\boxed{462}$	$\boxed{3003}$	

Parity party trick

$\binom{n}{k}$	$\binom{5}{2}$	$\binom{6}{4}$	$\binom{11}{5}$	$\binom{14}{6}$	$\binom{17}{9}$
even or odd?	$\boxed{10}$	$\boxed{15}$	$\boxed{462}$	$\boxed{3003}$	$\boxed{24310}$

Parity party trick

$\binom{n}{k}$	$\binom{5}{2}$	$\binom{6}{4}$	$\binom{11}{5}$	$\binom{14}{6}$	$\binom{17}{9}$
even or odd?	$\boxed{10}$	$\boxed{15}$	$\boxed{462}$	$\boxed{3003}$	$\boxed{24310}$
base 2	$\binom{101}{10}$	$\binom{110}{100}$	$\binom{1011}{101}$	$\binom{1110}{110}$	$\binom{10001}{1001}$

Parity party trick

$\binom{n}{k}$	$\binom{5}{2}$	$\binom{6}{4}$	$\binom{11}{5}$	$\binom{14}{6}$	$\binom{17}{9}$
even or odd?	$\boxed{10}$	$\boxed{15}$	$\boxed{462}$	$\boxed{3003}$	$\boxed{24310}$
base 2	$\binom{101}{10}$	$\binom{110}{100}$	$\binom{1011}{101}$	$\binom{1110}{110}$	$\binom{10001}{1001}$

$\binom{n}{k}$	$\binom{13}{5}$	$\binom{13}{6}$

Parity party trick

$\binom{n}{k}$	$\binom{5}{2}$	$\binom{6}{4}$	$\binom{11}{5}$	$\binom{14}{6}$	$\binom{17}{9}$
even or odd?	$\boxed{10}$	$\boxed{15}$	$\boxed{462}$	$\boxed{3003}$	$\boxed{24310}$
base 2	$\begin{pmatrix} 101 \\ 10 \end{pmatrix}$	$\begin{pmatrix} 110 \\ 100 \end{pmatrix}$	$\begin{pmatrix} 1011 \\ 101 \end{pmatrix}$	$\begin{pmatrix} 1110 \\ 110 \end{pmatrix}$	$\begin{pmatrix} 10001 \\ 1001 \end{pmatrix}$

$\binom{n}{k}$	$\binom{13}{5}$	$\binom{13}{6}$
even or odd?		

Parity party trick

$\binom{n}{k}$	$\binom{5}{2}$	$\binom{6}{4}$	$\binom{11}{5}$	$\binom{14}{6}$	$\binom{17}{9}$
even or odd?	$\boxed{10}$	$\boxed{15}$	$\boxed{462}$	$\boxed{3003}$	$\boxed{24310}$
base 2	$\begin{pmatrix} 101 \\ 10 \end{pmatrix}$	$\begin{pmatrix} 110 \\ 100 \end{pmatrix}$	$\begin{pmatrix} 1011 \\ 101 \end{pmatrix}$	$\begin{pmatrix} 1110 \\ 110 \end{pmatrix}$	$\begin{pmatrix} 10001 \\ 1001 \end{pmatrix}$

$\binom{n}{k}$	$\binom{13}{5}$	$\binom{13}{6}$
even or odd?	odd	even

Parity party trick

$\binom{n}{k}$	$\binom{5}{2}$	$\binom{6}{4}$	$\binom{11}{5}$	$\binom{14}{6}$	$\binom{17}{9}$
even or odd?	$\boxed{10}$	$\boxed{15}$	$\boxed{462}$	$\boxed{3003}$	$\boxed{24310}$
base 2	$\begin{pmatrix} 101 \\ 10 \end{pmatrix}$	$\begin{pmatrix} 110 \\ 100 \end{pmatrix}$	$\begin{pmatrix} 1011 \\ 101 \end{pmatrix}$	$\begin{pmatrix} 1110 \\ 110 \end{pmatrix}$	$\begin{pmatrix} 10001 \\ 1001 \end{pmatrix}$

$\binom{n}{k}$	$\binom{13}{5}$	$\binom{13}{6}$
even or odd?	$\boxed{\text{odd}}$	$\boxed{\text{even}}$
base 2	$\begin{pmatrix} 1101 \\ 101 \end{pmatrix}$	$\begin{pmatrix} 1101 \\ 110 \end{pmatrix}$

Parity party trick

$\binom{n}{k}$	$\binom{5}{2}$	$\binom{6}{4}$	$\binom{11}{5}$	$\binom{14}{6}$	$\binom{17}{9}$
even or odd?	$\boxed{10}$	$\boxed{15}$	$\boxed{462}$	$\boxed{3003}$	$\boxed{24310}$
base 2	$\begin{pmatrix} 101 \\ 10 \end{pmatrix}$	$\begin{pmatrix} 110 \\ 100 \end{pmatrix}$	$\begin{pmatrix} 1011 \\ 101 \end{pmatrix}$	$\begin{pmatrix} 1110 \\ 110 \end{pmatrix}$	$\begin{pmatrix} 10001 \\ 1001 \end{pmatrix}$

$\binom{n}{k}$	$\binom{13}{5}$	$\binom{13}{6}$
even or odd?	$\boxed{\text{odd}}$	$\boxed{\text{even}}$
base 2	$\begin{pmatrix} 1101 \\ 101 \end{pmatrix}$	$\begin{pmatrix} 1101 \\ 110 \end{pmatrix}$

(A consequence of) Lucas' Theorem (1878)

$\binom{n}{k}$ is even if and only if there is a position in which the base 2 expansion for k has a 1 and the base 2 expansion for n has a zero.

Summary and Outlook

Summary and Outlook

- Quantum mechanics *blah blah blah* . . .

Summary and Outlook

- Quantum mechanics *blah blah blah* . . .
- Quantum computers *blah blah blah* . . .

Summary and Outlook

- Quantum mechanics *blah blah blah* . . .
- Quantum computers *blah blah blah* . . .
- Expect surprises and adventure!

Summary and Outlook

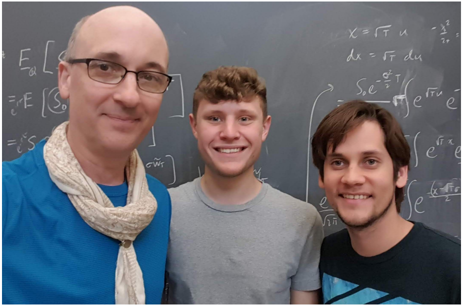
- Quantum mechanics *blah blah blah* ...
- Quantum computers *blah blah blah* ...
- Expect surprises and adventure!
- Be prepared to learn more combinatorics!

Summary and Outlook

- Quantum mechanics *blah blah blah* ...
- Quantum computers *blah blah blah* ...
- Expect surprises and adventure!
- Be prepared to learn more combinatorics!
- Have fun!

Thank you!

LVC Mathematical Physics Research Group



David Lyons　　Isaac Lehman　　David Campbell

http://quantum.lvc.edu/mathphys