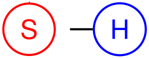
Today:Quantum.

Today:Quantum.

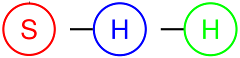
Today:Quantum.

S

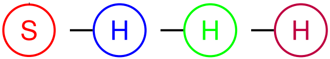
Today:Quantum.



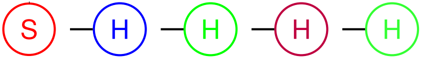
Today:Quantum.



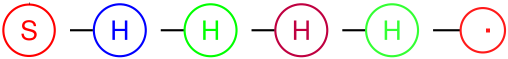
Today:Quantum.



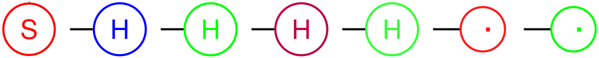
Today:Quantum.



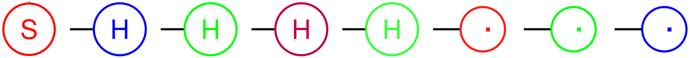
Today:Quantum.



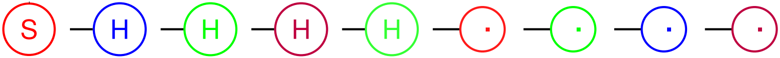
Today:Quantum.



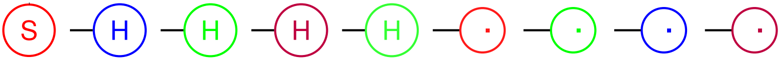
Today:Quantum.



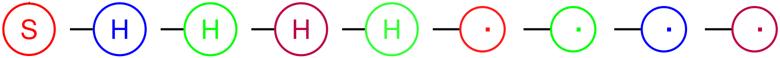
Today:Quantum.



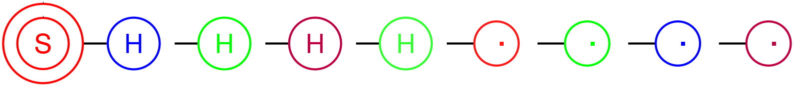
Today:Quantum.



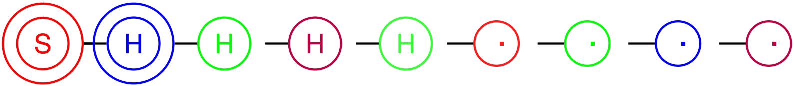
Today:Quantum.



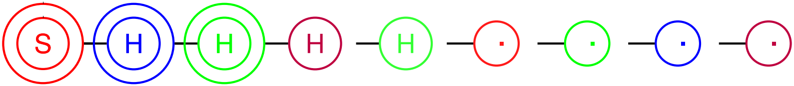
Today:Quantum.



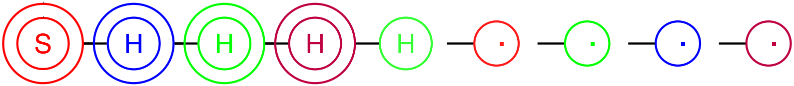
Today:Quantum.



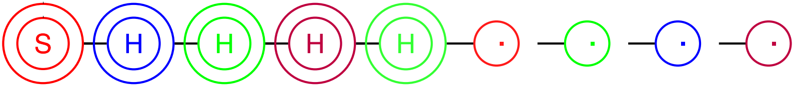
Today:Quantum.



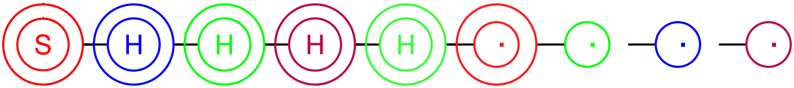
Today:Quantum.



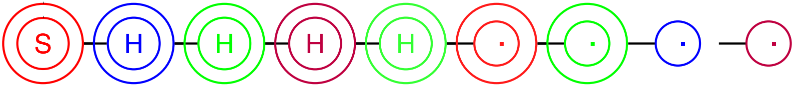
Today:Quantum.



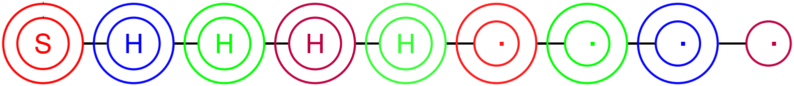
Today:Quantum.



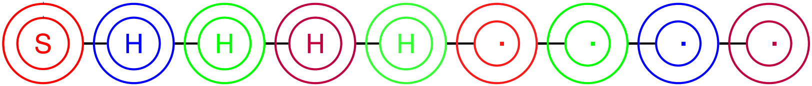
Today:Quantum.



Today:Quantum.



Today:Quantum.

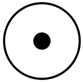


Qubit/electron.

-

Qubit/electron.

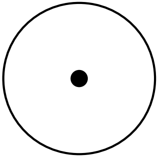
ground state



$|0\rangle$

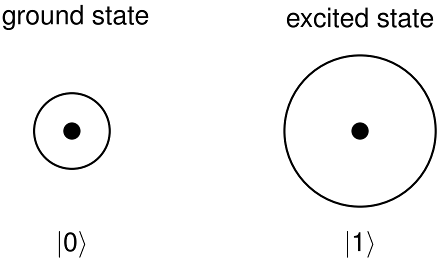
Qubit/electron.

excited state



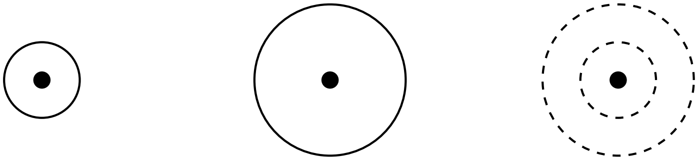
$|1\rangle$

Qubit/electron.



Qubit/electron.

ground state | excited state | Superposition

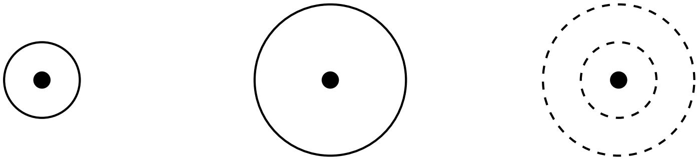


$|0\rangle$ | $|1\rangle$ | $\alpha_0 |0\rangle + \alpha_1 |1\rangle$

Complex numbers α_0 and α_1.

Qubit/electron.

ground state | excited state | Superposition

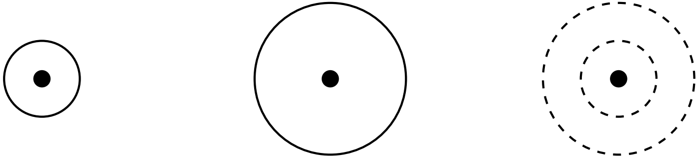


$|0\rangle$ | $|1\rangle$ | $\alpha_0 |0\rangle + \alpha_1 |1\rangle$

Complex numbers α_0 and α_1.
$|\alpha_0|^2 + |\alpha_1|^2 = 1$.

Qubit/electron.

ground state | excited state | Superposition



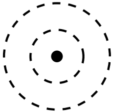
$|0\rangle$ | $|1\rangle$ | $\alpha_0 |0\rangle + \alpha_1 |1\rangle$

Complex numbers α_0 and α_1.

$|\alpha_0|^2 + |\alpha_1|^2 = 1$.

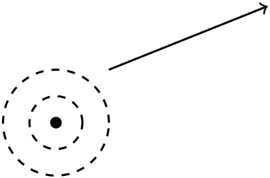
α_0, α_1 are “amplitudes.”

Measurement.



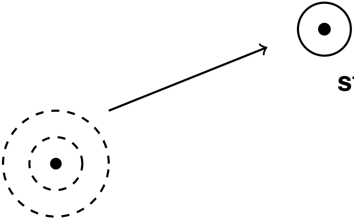
$\alpha_0 |0\rangle + \alpha_1 |1\rangle$

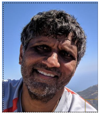
Measurement.



$\alpha_0 |0\rangle + \alpha_1 |1\rangle$

Measurement.

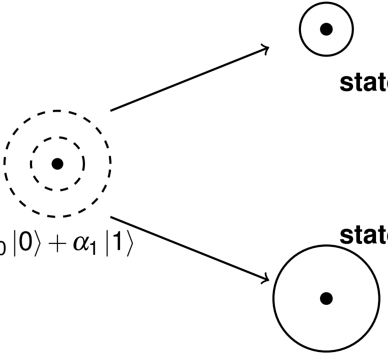


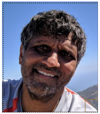


state $|0\rangle$ **with prob** $|\alpha_0|^2$

$\alpha_0 |0\rangle + \alpha_1 |1\rangle$

Measurement.



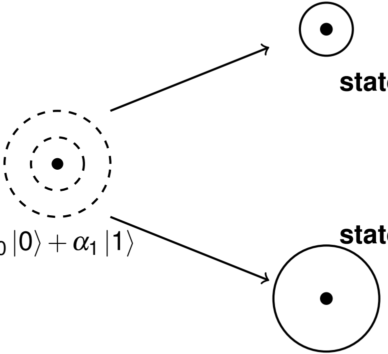


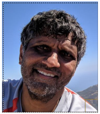
state $|0\rangle$ with prob $|\alpha_0|^2$

$\alpha_0 |0\rangle + \alpha_1 |1\rangle$

state $|1\rangle$ with prob $|\alpha_1|^2$

Measurement.





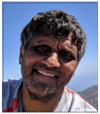
state $|0\rangle$ **with prob** $|\alpha_0|^2$

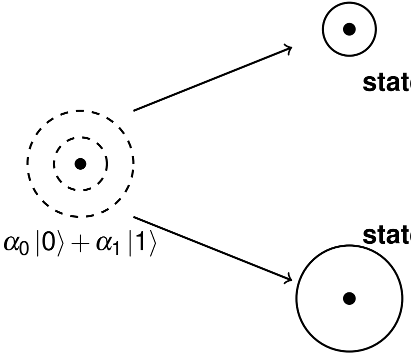
$\alpha_0 |0\rangle + \alpha_1 |1\rangle$

state $|1\rangle$ **with prob** $|\alpha_1|^2$

Remember $|\alpha_0|^2 + |\alpha_1|^2 = 1$.

Measurement.





state $|0\rangle$ **with prob** $|\alpha_0|^2$

state $|1\rangle$ **with prob** $|\alpha_1|^2$

Remember $|\alpha_0|^2 + |\alpha_1|^2 = 1$.

Amplitudes $\rightarrow$ probabilities on measurement!!!

Two qubits..a dollar.

One bit:

Two qubits..a dollar.

One bit:

Classic State: 0 or 1.

Two qubits..a dollar.

One bit:

Classic State: 0 or 1.

Quantum State:

Two qubits..a dollar.

One bit:
Classic State: 0 or 1.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.

Two qubits..a dollar.

One bit:
Classic State: 0 or 1.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.
Measure : 0 or 1.

Two qubits..a dollar.

One bit:

Classic State: 0 or 1.

Quantum State:

Internal:

$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.

Measure : 0 or 1.

Two numbers internally,

Two qubits..a dollar.

One bit:
Classic State: 0 or 1.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.
Measure : 0 or 1.
Two numbers internally, measurement yields one bit.

Two qubits..a dollar.

One bit:
Classic State: 0 or 1.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.
Measure : 0 or 1.
Two numbers internally, measurement yields one bit.

Two bits:

Two qubits..a dollar.

One bit:
Classic State: 0 or 1.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.
Measure : 0 or 1.
Two numbers internally, measurement yields one bit.

Two bits:
Classical State: 00, 01, 10, 11.

Two qubits..a dollar.

One bit:

Classic State: 0 or 1.

Quantum State:

Internal:

$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.

Measure : 0 or 1.

Two numbers internally, measurement yields one bit.

Two bits:

Classical State: 00, 01, 10, 11.

Quantum State:

Two qubits..a dollar.

One bit:

Classic State: 0 or 1.

Quantum State:

Internal:

$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.

Measure : 0 or 1.

Two numbers internally, measurement yields one bit.

Two bits:

Classical State: 00, 01, 10, 11.

Quantum State:

Internal:

Two qubits..a dollar.

One bit:
Classic State: 0 or 1.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.
Measure : 0 or 1.
Two numbers internally, measurement yields one bit.

Two bits:
Classical State: 00, 01, 10, 11.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{01} |10\rangle + \alpha_{11} |11\rangle$

Two qubits..a dollar.

One bit:
Classic State: 0 or 1.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.
Measure : 0 or 1.
Two numbers internally, measurement yields one bit.

Two bits:
Classical State: 00, 01, 10, 11.
Quantum State:
Internal:

$$|\alpha\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{01} |10\rangle + \alpha_{11} |11\rangle$$

$$|\alpha_{00}|^2 + \cdots + |\alpha_{11}|^2 = 1$$

Two qubits..a dollar.

One bit:

Classic State: 0 or 1.

Quantum State:

Internal:

$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.

Measure : 0 or 1.

Two numbers internally, measurement yields one bit.

Two bits:

Classical State: 00, 01, 10, 11.

Quantum State:

Internal:

$|\alpha\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{01} |10\rangle + \alpha_{11} |11\rangle$

$|\alpha_{00}|^2 + \cdots + |\alpha_{11}|^2 = 1$

Measure : 00, 01, 10, 11.

Two qubits..a dollar.

One bit:
Classic State: 0 or 1.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.
Measure : 0 or 1.
Two numbers internally, measurement yields one bit.

Two bits:
Classical State: 00, 01, 10, 11.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{01} |10\rangle + \alpha_{11} |11\rangle$
$|\alpha_{00}|^2 + \cdots + |\alpha_{11}|^2 = 1$
Measure : 00, 01, 10, 11.
4 internal numbers,

Two qubits..a dollar.

One bit:

Classic State: 0 or 1.

Quantum State:

Internal:

$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.

Measure : 0 or 1.

Two numbers internally, measurement yields one bit.

Two bits:

Classical State: 00, 01, 10, 11.

Quantum State:

Internal:

$|\alpha\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{01} |10\rangle + \alpha_{11} |11\rangle$

$|\alpha_{00}|^2 + \cdots + |\alpha_{11}|^2 = 1$

Measure : 00, 01, 10, 11.

4 internal numbers, measurement yields two bits.

Two qubits..a dollar.

One bit:

Classic State: 0 or 1.

Quantum State:

Internal:

$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.

Measure : 0 or 1.

Two numbers internally, measurement yields one bit.

Ooh!

Two bits:

Classical State: 00, 01, 10, 11.

Quantum State:

Internal:

$|\alpha\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{01} |10\rangle + \alpha_{11} |11\rangle$

$|\alpha_{00}|^2 + \cdots + |\alpha_{11}|^2 = 1$

Measure : 00, 01, 10, 11.

4 internal numbers, measurement yields two bits.

Two qubits..a dollar.

One bit:
Classic State: 0 or 1.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.
Measure : 0 or 1.
Two numbers internally, measurement yields one bit.

Ooh! Something new,

Two bits:
Classical State: 00, 01, 10, 11.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{01} |10\rangle + \alpha_{11} |11\rangle$
$|\alpha_{00}|^2 + \cdots + |\alpha_{11}|^2 = 1$
Measure : 00, 01, 10, 11.
4 internal numbers, measurement yields two bits.

Two qubits..a dollar.

One bit:
Classic State: 0 or 1.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.
Measure : 0 or 1.
Two numbers internally, measurement yields one bit.

Two bits:
Classical State: 00, 01, 10, 11.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{01} |10\rangle + \alpha_{11} |11\rangle$
$|\alpha_{00}|^2 + \cdots + |\alpha_{11}|^2 = 1$
Measure : 00, 01, 10, 11.
4 internal numbers, measurement yields two bits.

Ooh! Something new, with two.

Two qubits..a dollar.

One bit:

Classic State: 0 or 1.

Quantum State:

Internal:

$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.

Measure : 0 or 1.

Two numbers internally, measurement yields one bit.

Two bits:

Classical State: 00, 01, 10, 11.

Quantum State:

Internal:

$|\alpha\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{01} |10\rangle + \alpha_{11} |11\rangle$

$|\alpha_{00}|^2 + \cdots + |\alpha_{11}|^2 = 1$

Measure : 00, 01, 10, 11.

4 internal numbers, measurement yields two bits.

Ooh! Something new, with two.

Partial Measure: look at one bit.

Two qubits..a dollar.

One bit:

Classic State: 0 or 1.

Quantum State:

Internal:

$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.

Measure : 0 or 1.

Two numbers internally, measurement yields one bit.

Two bits:

Classical State: 00, 01, 10, 11.

Quantum State:

Internal:

$|\alpha\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{01} |10\rangle + \alpha_{11} |11\rangle$

$|\alpha_{00}|^2 + \cdots + |\alpha_{11}|^2 = 1$

Measure : 00, 01, 10, 11.

4 internal numbers, measurement yields two bits.

Ooh! Something new, with two.

Partial Measure: look at one bit.

Result: 0

Two qubits..a dollar.

One bit:
Classic State: 0 or 1.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.
Measure : 0 or 1.
Two numbers internally, measurement yields one bit.

Two bits:
Classical State: 00, 01, 10, 11.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{01} |10\rangle + \alpha_{11} |11\rangle$
$|\alpha_{00}|^2 + \cdots + |\alpha_{11}|^2 = 1$
Measure : 00, 01, 10, 11.
4 internal numbers, measurement yields two bits.

Ooh! Something new, with two.

Partial Measure: look at one bit.
Result: 0 (with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$.)

Two qubits..a dollar.

One bit:
Classic State: 0 or 1.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.
Measure : 0 or 1.
Two numbers internally, measurement yields one bit.

Two bits:
Classical State: 00, 01, 10, 11.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{01} |10\rangle + \alpha_{11} |11\rangle$
$|\alpha_{00}|^2 + \cdots + |\alpha_{11}|^2 = 1$
Measure : 00, 01, 10, 11.
4 internal numbers, measurement yields two bits.

Ooh! Something new, with two.

Partial Measure: look at one bit.
Result: 0 (with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$.)

What is the state of the system if result is 0?

Two qubits..a dollar.

One bit:

Classic State: 0 or 1.

Quantum State:

Internal:

$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.

Measure : 0 or 1.

Two numbers internally, measurement yields one bit.

Two bits:

Classical State: 00, 01, 10, 11.

Quantum State:

Internal:

$|\alpha\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{01} |10\rangle + \alpha_{11} |11\rangle$

$|\alpha_{00}|^2 + \cdots + |\alpha_{11}|^2 = 1$

Measure : 00, 01, 10, 11.

4 internal numbers, measurement yields two bits.

Ooh! Something new, with two.

Partial Measure: look at one bit.

Result: 0 (with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$.)

What is the state of the system if result is 0?

New Internal state: $\frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$

Two qubits..a dollar.

One bit:
Classic State: 0 or 1.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.
Measure : 0 or 1.
Two numbers internally, measurement yields one bit.

Two bits:
Classical State: 00, 01, 10, 11.
Quantum State:
Internal:
$|\alpha\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{01} |10\rangle + \alpha_{11} |11\rangle$
$|\alpha_{00}|^2 + \cdots + |\alpha_{11}|^2 = 1$
Measure : 00, 01, 10, 11.
4 internal numbers, measurement yields two bits.

Ooh! Something new, with two.

Partial Measure: look at one bit.
Result: 0 (with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$.)

What is the state of the system if result is 0?

New Internal state: $\frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$

Scaling to make probabilities add to 1.

Joint State: Entanglement

Qubit one internal state: $\alpha_0 |0\rangle + \alpha_1 |1\rangle$

Joint State: Entanglement

Qubit one internal state: $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
Qubit two internal state: $\beta_0 |0\rangle + \beta_1 |1\rangle$

Joint State: Entanglement

Qubit one internal state: $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
Qubit two internal state: $\beta_0 |0\rangle + \beta_1 |1\rangle$

Joint State: $\alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle$,

Joint State: Entanglement

Qubit one internal state: $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
Qubit two internal state: $\beta_0 |0\rangle + \beta_1 |1\rangle$

Joint State: $\alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle$,

Can all two bit states be decomposed?

Joint State: Entanglement

Qubit one internal state: $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
Qubit two internal state: $\beta_0 |0\rangle + \beta_1 |1\rangle$

Joint State: $\alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle$,

Can all two bit states be decomposed? Yes?

Joint State: Entanglement

Qubit one internal state: $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
Qubit two internal state: $\beta_0 |0\rangle + \beta_1 |1\rangle$

Joint State: $\alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle$,

Can all two bit states be decomposed? Yes? No?

Joint State: Entanglement

Qubit one internal state: $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
Qubit two internal state: $\beta_0 |0\rangle + \beta_1 |1\rangle$

Joint State: $\alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle$,

Can all two bit states be decomposed? Yes? No?

No!

Joint State: Entanglement

Qubit one internal state: $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
Qubit two internal state: $\beta_0 |0\rangle + \beta_1 |1\rangle$

Joint State: $\alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle$,

Can all two bit states be decomposed? Yes? No?

No! $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$.

Joint State: Entanglement

Qubit one internal state: $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
Qubit two internal state: $\beta_0 |0\rangle + \beta_1 |1\rangle$

Joint State: $\alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle$,

Can all two bit states be decomposed? Yes? No?

No! $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$.

Proof: Exercise 10.1

Joint State: Entanglement

Qubit one internal state: $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
Qubit two internal state: $\beta_0 |0\rangle + \beta_1 |1\rangle$

Joint State: $\alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle$,

Can all two bit states be decomposed? Yes? No?

No! $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$.

Proof: Exercise 10.1
No solution to the system of four polynomial equations.

Joint State: Entanglement

Qubit one internal state: $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
Qubit two internal state: $\beta_0 |0\rangle + \beta_1 |1\rangle$

Joint State: $\alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle$,

Can all two bit states be decomposed? Yes? No?

No! $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$.

Proof: Exercise 10.1
  No solution to the system of four polynomial equations.
  Product of $\alpha_0\beta_1 = 0$ means one must be 0

Joint State: Entanglement

Qubit one internal state: $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
Qubit two internal state: $\beta_0 |0\rangle + \beta_1 |1\rangle$

Joint State: $\alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle$,

Can all two bit states be decomposed? Yes? No?

No! $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$.

Proof: Exercise 10.1
No solution to the system of four polynomial equations.
Product of $\alpha_0\beta_1 = 0$ means one must be 0 $\ldots$

Joint State: Entanglement

Qubit one internal state: $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
Qubit two internal state: $\beta_0 |0\rangle + \beta_1 |1\rangle$

Joint State: $\alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle$,

Can all two bit states be decomposed? Yes? No?

No! $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$.

Proof: Exercise 10.1
No solution to the system of four polynomial equations.
Product of $\alpha_0\beta_1 = 0$ means one must be 0 $\ldots$

"Bell State."

Joint State: Entanglement

Qubit one internal state: $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
Qubit two internal state: $\beta_0 |0\rangle + \beta_1 |1\rangle$

Joint State: $\alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle$,

Can all two bit states be decomposed? Yes? No?

No! $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$.

Proof: Exercise 10.1
   No solution to the system of four polynomial equations.
   Product of $\alpha_0\beta_1 = 0$ means one must be 0 ...

"Bell State."

One key to the power of quantum.

Joint State: Entanglement

Qubit one internal state: $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
Qubit two internal state: $\beta_0 |0\rangle + \beta_1 |1\rangle$

Joint State: $\alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle$,

Can all two bit states be decomposed? Yes? No?

No! $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$.

Proof: Exercise 10.1
  No solution to the system of four polynomial equations.
  Product of $\alpha_0\beta_1 = 0$ means one must be 0 ...

"Bell State."

One key to the power of quantum.

Entanglement: measure the first bit as 0, the other bit is zero.

Joint State: Entanglement

Qubit one internal state: $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
Qubit two internal state: $\beta_0 |0\rangle + \beta_1 |1\rangle$

Joint State: $\alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle$,

Can all two bit states be decomposed? Yes? No?

No! $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$.

Proof: Exercise 10.1
No solution to the system of four polynomial equations.
Product of $\alpha_0\beta_1 = 0$ means one must be 0 $\ldots$

"Bell State."

One key to the power of quantum.

Entanglement: measure the first bit as 0, the other bit is zero.

More complicated actually: Bell-CHSH inequalities.

n-qubits.

Internal State: $\alpha_{0\ldots 0}\left|0\cdots 0\right\rangle + \alpha_{0\ldots 1}\left|0\cdots 1\right\rangle + \cdots + \alpha_{1\ldots 1}\left|1\cdots 1\right\rangle.$

n-qubits.

Internal State: $\alpha_{0\ldots0}\left|0\cdots0\right\rangle + \alpha_{0\ldots1}\left|0\cdots1\right\rangle + \cdots + \alpha_{1\ldots1}\left|1\cdots1\right\rangle$.

Internal state described by 2^n amplitudes:

n-qubits.

Internal State: $\alpha_{0\ldots0}\left|0\cdots0\right\rangle + \alpha_{0\ldots1}\left|0\cdots1\right\rangle + \cdots + \alpha_{1\ldots1}\left|1\cdots1\right\rangle.$

Internal state described by 2^n amplitudes: complex numbers.

n-qubits.

Internal State: $\alpha_{0\ldots0}\,|0\cdots0\rangle + \alpha_{0\ldots1}\,|0\cdots1\rangle + \cdots + \alpha_{1\ldots1}\,|1\cdots1\rangle$.

Internal state described by 2^n amplitudes: complex numbers.

Full measurement still yields “only” n bits.

n-qubits.

Internal State: $\alpha_{0\ldots 0}\left|0\cdots 0\right\rangle + \alpha_{0\ldots 1}\left|0\cdots 1\right\rangle + \cdots + \alpha_{1\ldots 1}\left|1\cdots 1\right\rangle$.

Internal state described by 2^n amplitudes: complex numbers.

Full measurement still yields "only" n bits.

Partial measurement yields k bits

n-qubits.

Internal State: $\alpha_{0\ldots0}|0\cdots0\rangle + \alpha_{0\ldots1}|0\cdots1\rangle + \cdots + \alpha_{1\ldots1}|1\cdots1\rangle$.

Internal state described by 2^n amplitudes: complex numbers.

Full measurement still yields "only" n bits.

Partial measurement yields k bits
and leaves a superposition on consistent states.

n-qubits.

Internal State: $\alpha_{0\ldots0}\,|0\cdots0\rangle + \alpha_{0\ldots1}\,|0\cdots1\rangle + \cdots + \alpha_{1\ldots1}\,|1\cdots1\rangle$.

Internal state described by 2^n amplitudes: complex numbers.

Full measurement still yields “only” n bits.

Partial measurement yields k bits
and leaves a superposition on consistent states.

Feynmann: how to simulate an n particle system.

n-qubits.

Internal State: $\alpha_{0\ldots0}\,|0\cdots0\rangle + \alpha_{0\ldots1}\,|0\cdots1\rangle + \cdots + \alpha_{1\ldots1}\,|1\cdots1\rangle$.

Internal state described by 2^n amplitudes: complex numbers.

Full measurement still yields "only" n bits.

Partial measurement yields k bits
and leaves a superposition on consistent states.

Feynmann: how to simulate an n particle system.
Need to maintain 2^n numbers.

n-qubits.

Internal State: $\alpha_{0\ldots0}\left|0\cdots0\right\rangle + \alpha_{0\ldots1}\left|0\cdots1\right\rangle + \cdots + \alpha_{1\ldots1}\left|1\cdots1\right\rangle.$

Internal state described by 2^n amplitudes: complex numbers.

Full measurement still yields "only" n bits.

Partial measurement yields k bits
and leaves a superposition on consistent states.

Feynmann: how to simulate an n particle system.
Need to maintain 2^n numbers.
Still no answer.

n-qubits.

Internal State: $\alpha_{0\ldots0}\left|0\cdots0\right\rangle+\alpha_{0\ldots1}\left|0\cdots1\right\rangle+\cdots+\alpha_{1\ldots1}\left|1\cdots1\right\rangle.$

Internal state described by 2^n amplitudes: complex numbers.

Full measurement still yields "only" n bits.

Partial measurement yields k bits
and leaves a superposition on consistent states.

Feynmann: how to simulate an n particle system.
Need to maintain 2^n numbers.
Still no answer.

Flip it around, what can an n qubit quantum computer do?

n-qubits.

Internal State: $\alpha_{0\ldots0}\left|0\cdots0\right\rangle + \alpha_{0\ldots1}\left|0\cdots1\right\rangle + \cdots + \alpha_{1\ldots1}\left|1\cdots1\right\rangle$.

Internal state described by 2^n amplitudes: complex numbers.

Full measurement still yields "only" n bits.

Partial measurement yields k bits
and leaves a superposition on consistent states.

Feynmann: how to simulate an n particle system.
Need to maintain 2^n numbers.
Still no answer.

Flip it around, what can an n qubit quantum computer do?

Notation

Vectors and Amplitudes:

Notation

Vectors and Amplitudes:
state is vector of 2^n amplitudes: one for each pattern of n bits.

Notation

Vectors and Amplitudes:

state is vector of 2^n amplitudes: one for each pattern of n bits.

Could be vector $[\alpha_{0\cdots0}, \ldots, \alpha_{1\cdots1}]$

Notation

Vectors and Amplitudes:

state is vector of 2^n amplitudes: one for each pattern of n bits.

Could be vector $[\alpha_{0\cdots 0}, \ldots, \alpha_{1\cdots 1}]$

Dirac or Bra-Ket notation:

Notation

Vectors and Amplitudes:

state is vector of 2^n amplitudes: one for each pattern of n bits.

Could be vector $[\alpha_{0\cdots 0},\ldots,\alpha_{1\cdots 1}]$

Dirac or Bra-Ket notation:

Amplitude of 0, $|0\rangle$.

Notation

Vectors and Amplitudes:

state is vector of 2^n amplitudes: one for each pattern of n bits.

Could be vector $[\alpha_{0\cdots0}, \ldots, \alpha_{1\cdots1}]$

Dirac or Bra-Ket notation:

Amplitude of 0, $|0\rangle$.

State is $\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$.

Notation

Vectors and Amplitudes:

state is vector of 2^n amplitudes: one for each pattern of n bits.

Could be vector $[\alpha_{0\cdots 0}, \ldots, \alpha_{1\cdots 1}]$

Dirac or Bra-Ket notation:

Amplitude of 0, $|0\rangle$.

State is $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$.

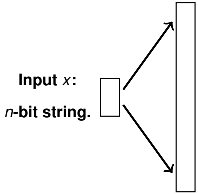
Quantum Computer

Start with n qubits,

Input x**:**

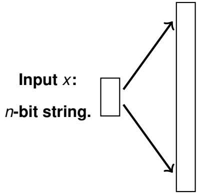
n**-bit string.**

Quantum Computer



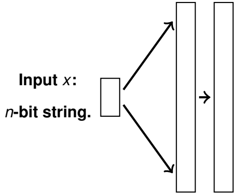
Start with n qubits, make superposition,

Quantum Computer



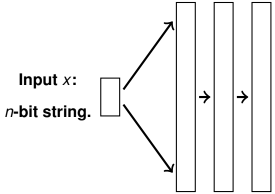
Start with n qubits,
make superposition,
do some quantum op's,

Quantum Computer



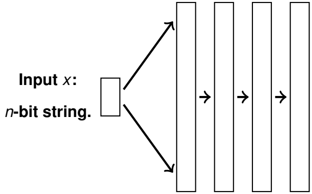
Start with n qubits,
make superposition,
do some quantum op's,

Quantum Computer



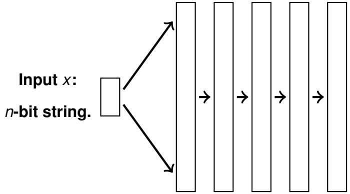
Start with n qubits,
make superposition,
do some quantum op's,

Quantum Computer



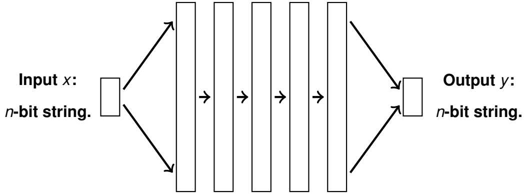
Start with *n* qubits,
make superposition,
do some quantum op's,

Quantum Computer



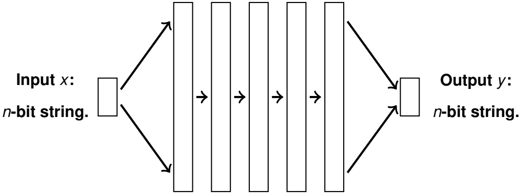
Start with n qubits,
make superposition,
do some quantum op's,

Quantum Computer



Start with n qubits,
make superposition,
do some quantum op's,
measure to get n bits.

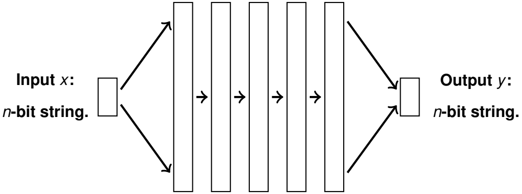
Quantum Computer



Exponential action

Start with n qubits,
make superposition,
do some quantum op's,
measure to get n bits.

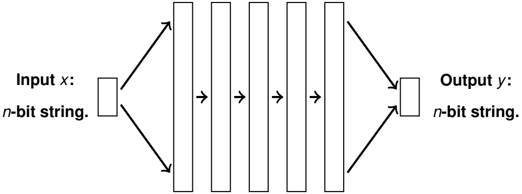
Quantum Computer



Start with n qubits,
make superposition,
do some quantum op's,
measure to get n bits.

Exponential action $\rightarrow$ Factor in polynomial time!

Quantum Computer

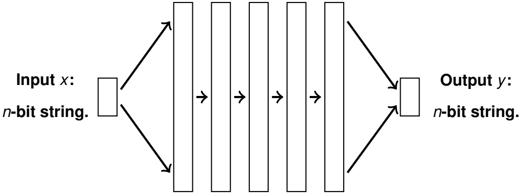


Start with n qubits,
make superposition,
do some quantum op's,
measure to get n bits.

Exponential action $\rightarrow$ Factor in polynomial time!

Can't watch where the action happens.

Quantum Computer



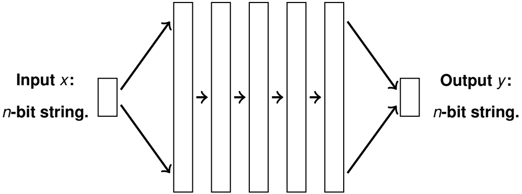
Start with n qubits,
make superposition,
do some quantum op's,
measure to get n bits.

Exponential action $\rightarrow$ Factor in polynomial time!

Can't watch where the action happens.

Measurement is random.

Quantum Computer



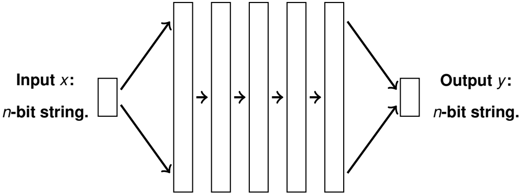
Start with n qubits,
make superposition,
do some quantum op's,
measure to get n bits.

Exponential action $\rightarrow$ Factor in polynomial time!

Can't watch where the action happens.

Measurement is random.
This is ok, as long as answer is right with decent probability.

Quantum Computer



Start with n qubits,
make superposition,
do some quantum op's,
measure to get n bits.

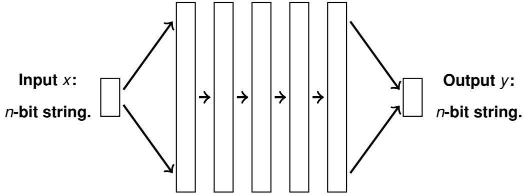
Exponential action $\rightarrow$ Factor in polynomial time!

Can't watch where the action happens.

Measurement is random.
  This is ok, as long as answer is right with decent probability.

Why different than probability?

Quantum Computer



Start with n qubits,
make superposition,
do some quantum op's,
measure to get n bits.

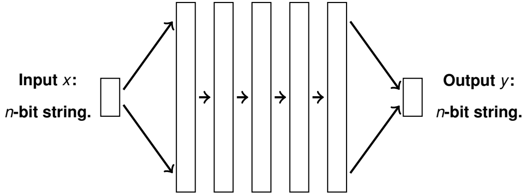
Exponential action $\rightarrow$ Factor in polynomial time!

Can't watch where the action happens.

Measurement is random.
This is ok, as long as answer is right with decent probability.

Why different than probability?
After all, can generate lots of possibilities.

Quantum Computer



Start with n qubits,
make superposition,
do some quantum op's,
measure to get n bits.

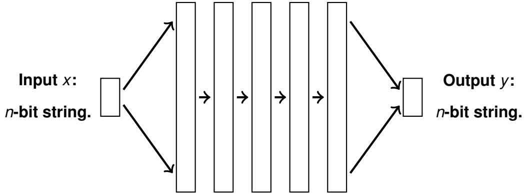
Exponential action $\rightarrow$ Factor in polynomial time!

Can't watch where the action happens.

Measurement is random.
This is ok, as long as answer is right with decent probability.

Why different than probability?
After all, can generate lots of possibilities.

Quantum Computer



Start with n qubits,
make superposition,
do some quantum op's,
measure to get n bits.

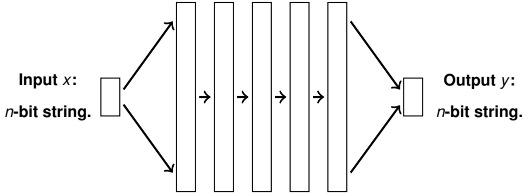
Exponential action $\rightarrow$ Factor in polynomial time!

Can't watch where the action happens.

Measurement is random.
This is ok, as long as answer is right with decent probability.

Why different than probability?
After all, can generate lots of possibilities.
Partial measure changes remaining state. State $\equiv$ amplitudes.

Quantum Computer



Start with n qubits,
make superposition,
do some quantum op's,
measure to get n bits.

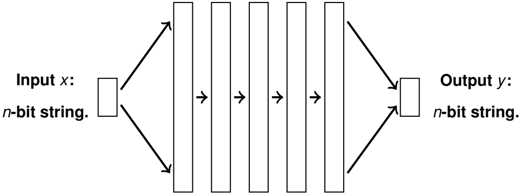
Exponential action $\rightarrow$ Factor in polynomial time!

Can't watch where the action happens.

Measurement is random.
This is ok, as long as answer is right with decent probability.

Why different than probability?
After all, can generate lots of possibilities.
Partial measure changes remaining state. State $\equiv$ amplitudes.
Conditional probability?

Quantum Computer



Start with n qubits,
make superposition,
do some quantum op's,
measure to get n bits.

Exponential action $\rightarrow$ Factor in polynomial time!

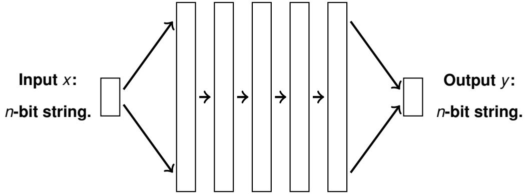
Can't watch where the action happens.

Measurement is random.
This is ok, as long as answer is right with decent probability.

Why different than probability?
After all, can generate lots of possibilities.
Partial measure changes remaining state. State $\equiv$ amplitudes.
Conditional probability?

Can add/subtract/scale amplitudes using Quantum gates.

Quantum Computer



Start with n qubits,
make superposition,
do some quantum op's,
measure to get n bits.

Exponential action $\rightarrow$ Factor in polynomial time!

Can't watch where the action happens.

Measurement is random.
This is ok, as long as answer is right with decent probability.

Why different than probability?
After all, can generate lots of possibilities.
Partial measure changes remaining state. State $\equiv$ amplitudes.
Conditional probability?

Can add/subtract/scale amplitudes using Quantum gates.
Not clear how to do it for probability.

Circuits.

Quantum Fourier Transform Circuit:

Circuits.

Quantum Fourier Transform Circuit:

Input: $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$.

Circuits.

Quantum Fourier Transform Circuit:

Input: $\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$.
Output: $\sum_{x\in\{0,1\}^n} \beta_x |x\rangle$.

Circuits.

Quantum Fourier Transform Circuit:

Input: $\sum_{x\in\{0,1\}^n} \alpha_x \left|x\right\rangle$.
Output: $\sum_{x\in\{0,1\}^n} \beta_x \left|x\right\rangle$.

Where β is Fourier Transform of α.

Circuits.

Quantum Fourier Transform Circuit:

Input: $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$.
Output: $\sum_{x \in \{0,1\}^n} \beta_x |x\rangle$.

Where β is Fourier Transform of α.
Note: n-qubit circuit, computing on 2^n amplitudes!

Circuits.

Quantum Fourier Transform Circuit:

Input: $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$.
Output: $\sum_{x \in \{0,1\}^n} \beta_x |x\rangle$.

Where β is Fourier Transform of α.
Note: n-qubit circuit, computing on 2^n amplitudes!
Randomized computations can't compute on probabilities.

Circuits.

Quantum Fourier Transform Circuit:

Input: $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$.
Output: $\sum_{x \in \{0,1\}^n} \beta_x |x\rangle$.

Where β is Fourier Transform of α.
Note: n-qubit circuit, computing on 2^n amplitudes!
Randomized computations can't compute on probabilities.

Measurement:

Circuits.

Quantum Fourier Transform Circuit:

Input: $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$.
Output: $\sum_{x \in \{0,1\}^n} \beta_x |x\rangle$.

Where β is Fourier Transform of α.
Note: n-qubit circuit, computing on 2^n amplitudes!
Randomized computations can't compute on probabilities.

Measurement: gives x with probability $|\beta_x|^2$.

Circuits.

Quantum Fourier Transform Circuit:

Input: $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$.
Output: $\sum_{x \in \{0,1\}^n} \beta_x |x\rangle$.

Where β is Fourier Transform of α.
Note: n-qubit circuit, computing on 2^n amplitudes!
Randomized computations can't compute on probabilities.

Measurement: gives x with probability $|\beta_x|^2$.
No access to β_x.

Circuits.

Quantum Fourier Transform Circuit:

Input: $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$.
Output: $\sum_{x \in \{0,1\}^n} \beta_x |x\rangle$.

Where β is Fourier Transform of α.
Note: n-qubit circuit, computing on 2^n amplitudes!
Randomized computations can't compute on probabilities.

Measurement: gives x with probability $|\beta_x|^2$.
No access to β_x.
Just get index x with probability according to Fourier coefficient β_x.

Circuits.

Quantum Fourier Transform Circuit:

Input: $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$.
Output: $\sum_{x \in \{0,1\}^n} \beta_x |x\rangle$.

Where β is Fourier Transform of α.
Note: n-qubit circuit, computing on 2^n amplitudes!
Randomized computations can't compute on probabilities.

Measurement: gives x with probability $|\beta_x|^2$.
No access to β_x.
Just get index x with probability according to Fourier coefficient β_x.
Quantum Fourier Sampling.

Circuits.

Quantum Fourier Transform Circuit:

Input: $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$.
Output: $\sum_{x \in \{0,1\}^n} \beta_x |x\rangle$.

Where β is Fourier Transform of α.
Note: n-qubit circuit, computing on 2^n amplitudes!
Randomized computations can't compute on probabilities.

Measurement: gives x with probability $|\beta_x|^2$.
No access to β_x.
Just get index x with probability according to Fourier coefficient β_x.
Quantum Fourier Sampling. Actual output is one x!

Circuits.

Quantum Fourier Transform Circuit:

Input: $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$.
Output: $\sum_{x \in \{0,1\}^n} \beta_x |x\rangle$.

Where β is Fourier Transform of α.
Note: n-qubit circuit, computing on 2^n amplitudes!
Randomized computations can't compute on probabilities.

Measurement: gives x with probability $|\beta_x|^2$.
No access to β_x.
Just get index x with probability according to Fourier coefficient β_x.
Quantum Fourier Sampling. Actual output is one x!

Classical Functions: $f(x)$

Circuits.

Quantum Fourier Transform Circuit:

Input: $\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$.
Output: $\sum_{x\in\{0,1\}^n} \beta_x |x\rangle$.

Where β is Fourier Transform of α.
Note: n-qubit circuit, computing on 2^n amplitudes!
Randomized computations can't compute on probabilities.

Measurement: gives x with probability $|\beta_x|^2$.
No access to β_x.
Just get index x with probability according to Fourier coefficient β_x.
Quantum Fourier Sampling. Actual output is one x!

Classical Functions: $f(x)$
Quantum Analog: copies input and computes $f(x)$.

Circuits.

Quantum Fourier Transform Circuit:

Input: $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$.
Output: $\sum_{x \in \{0,1\}^n} \beta_x |x\rangle$.

Where β is Fourier Transform of α.
Note: n-qubit circuit, computing on 2^n amplitudes!
Randomized computations can't compute on probabilities.

Measurement: gives x with probability $|\beta_x|^2$.
No access to β_x.
Just get index x with probability according to Fourier coefficient β_x.
Quantum Fourier Sampling. Actual output is one x!

Classical Functions: $f(x)$
Quantum Analog: copies input and computes $f(x)$.

Input: $\sum_{x \in \{0,1\}^n} \alpha_x |x, 0\rangle$.

Circuits.

Quantum Fourier Transform Circuit:

Input: $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$.
Output: $\sum_{x \in \{0,1\}^n} \beta_x |x\rangle$.

Where β is Fourier Transform of α.
Note: n-qubit circuit, computing on 2^n amplitudes!
Randomized computations can't compute on probabilities.

Measurement: gives x with probability $|\beta_x|^2$.
No access to β_x.
Just get index x with probability according to Fourier coefficient β_x.
Quantum Fourier Sampling. Actual output is one x!

Classical Functions: $f(x)$
Quantum Analog: copies input and computes $f(x)$.

Input: $\sum_{x \in \{0,1\}^n} \alpha_x |x, 0\rangle$.
Output: $\sum_{x \in \{0,1\}^n} \alpha_x |x, f(x)\rangle$.

Circuits.

Quantum Fourier Transform Circuit:

Input: $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$.
Output: $\sum_{x \in \{0,1\}^n} \beta_x |x\rangle$.

Where β is Fourier Transform of α.
Note: n-qubit circuit, computing on 2^n amplitudes!
Randomized computations can't compute on probabilities.

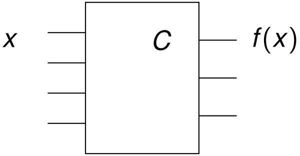
Measurement: gives x with probability $|\beta_x|^2$.
No access to β_x.
Just get index x with probability according to Fourier coefficient β_x.
Quantum Fourier Sampling. Actual output is one x!

Classical Functions: $f(x)$
Quantum Analog: copies input and computes $f(x)$.

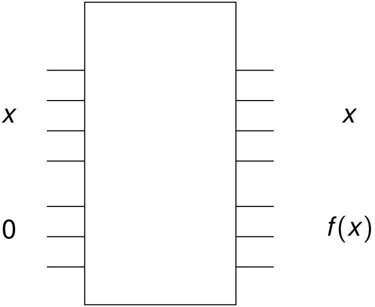
Input: $\sum_{x \in \{0,1\}^n} \alpha_x |x, 0\rangle$.
Output: $\sum_{x \in \{0,1\}^n} \alpha_x |x, f(x)\rangle$.

Random computations are fine with this; same α_x.

Classical/Quantum Circuit.



Classical



Quantum

Quantum Fourier Transform: more detail

n-qubits.

Quantum Fourier Transform: more detail

n-qubits.

2^n amplitudes: $\alpha_{0\cdots 0}, \ldots, \alpha_{1\cdots 1}$.

Quantum Fourier Transform: more detail

n-qubits.

2^n amplitudes: $\alpha_{0\cdots 0}, \ldots, \alpha_{1\cdots 1}$.

QFT:

Quantum Fourier Transform: more detail

n-qubits.

2^n amplitudes: $\alpha_{0\cdots0}, \ldots, \alpha_{1\cdots1}$.

QFT:

Fourier transform of amplitudes: $\beta_{0\cdots0}, \ldots, \beta_{1\cdots1}$.

Quantum Fourier Transform: more detail

n-qubits.

2^n amplitudes: $\alpha_{0\cdots 0}, \ldots, \alpha_{1\cdots 1}$.

QFT:

Fourier transform of amplitudes: $\beta_{0\cdots 0}, \ldots, \beta_{1\cdots 1}$.

Measure: get each n-bit string y with probability

Quantum Fourier Transform: more detail

n-qubits.

2^n amplitudes: $\alpha_{0\cdots0}, \ldots, \alpha_{1\cdots1}$.

QFT:

Fourier transform of amplitudes: $\beta_{0\cdots0}, \ldots, \beta_{1\cdots1}$.

Measure: get each n-bit string y with probability $|\beta_y|^2$.

Quantum Fourier Transform: more detail

n-qubits.

2^n amplitudes: $\alpha_{0\cdots0}, \ldots, \alpha_{1\cdots1}$.

QFT:
 Fourier transform of amplitudes: $\beta_{0\cdots0}, \ldots, \beta_{1\cdots1}$.

Measure: get each n-bit string y with probability $|\beta_y|^2$.

Fourier Transform:

Quantum Fourier Transform: more detail

n-qubits.

2^n amplitudes: $\alpha_{0\cdots 0}, \ldots, \alpha_{1\cdots 1}$.

QFT:

Fourier transform of amplitudes: $\beta_{0\cdots 0}, \ldots, \beta_{1\cdots 1}$.

Measure: get each n-bit string y with probability $|\beta_y|^2$.

Fourier Transform: multiplies by $M(\omega_{2^n})$ with $O(n^2)$ gates.

Quantum Fourier Transform: more detail

n-qubits.

2^n amplitudes: $\alpha_{0\cdots0}, \ldots, \alpha_{1\cdots1}$.

QFT:

Fourier transform of amplitudes: $\beta_{0\cdots0}, \ldots, \beta_{1\cdots1}$.

Measure: get each n-bit string y with probability $|\beta_y|^2$.

Fourier Transform: multiplies by $M(\omega_{2^n})$ with $O(n^2)$ gates.

Size of circuit is polynomial in n.

Quantum Fourier Transform: more detail

n-qubits.

2^n amplitudes: $\alpha_{0\cdots 0}, \ldots, \alpha_{1\cdots 1}$.

QFT:
Fourier transform of amplitudes: $\beta_{0\cdots 0}, \ldots, \beta_{1\cdots 1}$.

Measure: get each n-bit string y with probability $|\beta_y|^2$.

Fourier Transform: multiplies by $M(\omega_{2^n})$ with $O(n^2)$ gates.

Size of circuit is polynomial in n.
Gates act on all states in parallel.

Quantum Fourier Transform: more detail

n-qubits.

2^n amplitudes: $\alpha_{0\cdots 0}, \ldots, \alpha_{1\cdots 1}$.

QFT:
Fourier transform of amplitudes: $\beta_{0\cdots 0}, \ldots, \beta_{1\cdots 1}$.

Measure: get each n-bit string y with probability $|\beta_y|^2$.

Fourier Transform: multiplies by $M(\omega_{2^n})$ with $O(n^2)$ gates.

Size of circuit is polynomial in n.
Gates act on all states in parallel.
(like randomized computations.)

Quantum Fourier Transform: more detail

n-qubits.

2^n amplitudes: $\alpha_{0\cdots0}, \ldots, \alpha_{1\cdots1}$.

QFT:
 Fourier transform of amplitudes: $\beta_{0\cdots0}, \ldots, \beta_{1\cdots1}$.

Measure: get each n-bit string y with probability $|\beta_y|^2$.

Fourier Transform: multiplies by $M(\omega_{2^n})$ with $O(n^2)$ gates.

Size of circuit is polynomial in n.
 Gates act on all states in parallel.
 (like randomized computations.)
 Can compute (even subtract) with amplitudes!

Quantum Fourier Transform: more detail

n-qubits.

2^n amplitudes: $\alpha_{0\cdots0}, \ldots, \alpha_{1\cdots1}$.

QFT:
Fourier transform of amplitudes: $\beta_{0\cdots0}, \ldots, \beta_{1\cdots1}$.

Measure: get each n-bit string y with probability $|\beta_y|^2$.

Fourier Transform: multiplies by $M(\omega_{2^n})$ with $O(n^2)$ gates.

Size of circuit is polynomial in n.
Gates act on all states in parallel.
(like randomized computations.)
Can compute (even subtract) with amplitudes!
(which randomized computations can't do much.)

Quantum Fourier Transform: more detail

n-qubits.

2^n amplitudes: $\alpha_{0\cdots0}, \ldots, \alpha_{1\cdots1}$.

QFT:
Fourier transform of amplitudes: $\beta_{0\cdots0}, \ldots, \beta_{1\cdots1}$.

Measure: get each n-bit string y with probability $|\beta_y|^2$.

Fourier Transform: multiplies by $M(\omega_{2^n})$ with $O(n^2)$ gates.

Size of circuit is polynomial in n.
Gates act on all states in parallel.
(like randomized computations.)
Can compute (even subtract) with amplitudes!
(which randomized computations can't do much.)

FFT or multiply by $M(\omega_{2^n})$ finds "period" of periodic input.

Factoring and Roots of Unity

Factoring can be accomplished by finding non-negative square roots.

Factoring and Roots of Unity

Factoring can be accomplished by finding non-negative square roots.

Claim: If x is a non-trivial root of 1 modulo N then $gcd(x+1, N)$ is a non-trivial factor of N.

Factoring and Roots of Unity

Factoring can be accomplished by finding non-negative square roots.

Claim: If x is a non-trivial root of 1 modulo N then $gcd(x+1, N)$ is a non-trivial factor of N.

Harder claim: If N is an odd composite than for at least half of the x's, either $gcd(x, N) \neq 1$ or the *order* r of x is even and $x^{r/2}$ is a nontrivial square root of 1 mod N.

Factoring and Roots of Unity

Factoring can be accomplished by finding non-negative square roots.

Claim: If x is a non-trivial root of 1 modulo N then $gcd(x+1, N)$ is a non-trivial factor of N.

Harder claim: If N is an odd composite than for at least half of the x's, either $gcd(x, N) \neq 1$ or the *order* r of x is even and $x^{r/2}$ is a nontrivial square root of 1 mod N.

Example: 15
$4^2 = 1 \pmod{15} \implies 4-1$ or $4+1$ are non-trivial factors of fifteen.

Factoring and Roots of Unity

Factoring can be accomplished by finding non-negative square roots.

Claim: If x is a non-trivial root of 1 modulo N then $gcd(x+1, N)$ is a non-trivial factor of N.

Harder claim: If N is an odd composite than for at least half of the x's, either $gcd(x, N) \neq 1$ or the *order* r of x is even and $x^{r/2}$ is a nontrivial square root of 1 mod N.

Example: 15
$4^2 = 1 \pmod{15} \implies 4-1$ or $4+1$ are non-trivial factors of fifteen.

More generally: $x^2 = 1 \pmod{15} \implies x^2 - 1 = (x+1)(x-1) = 0 \pmod{15}$.

Roots and Unity and Fourier Transform

Initialize with state:

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}}\sum_{a=0}^{M-1}|a,0\rangle$

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, 0\rangle$

Compute:

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, 0\rangle$

Compute: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, f(a)\rangle\,, \quad f(a) = x^a$

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, 0\rangle$

Compute: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, f(a)\rangle, \quad f(a) = x^a$

Measure second register: first register now has period r!

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, 0\rangle$

Compute: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, f(a)\rangle\,, \quad f(a) = x^a$

Measure second register: first register now has period r!

Claim: Resulting α has nonzero amplitudes with period r.

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, 0\rangle$

Compute: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, f(a)\rangle$, $\quad f(a) = x^a$

Measure second register: first register now has period r!

Claim: Resulting α has nonzero amplitudes with period r.
$x^a = z$ for $a = j, j+r, j+2(r), \ldots$

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, 0\rangle$

Compute: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, f(a)\rangle, \quad f(a) = x^a$

Measure second register: first register now has period r!

Claim: Resulting α has nonzero amplitudes with period r.
$x^a = z$ for $a = j, j+r, j+2(r), \ldots$ since $x^r = 1$.

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, 0\rangle$

Compute: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, f(a)\rangle, \quad f(a) = x^a$

Measure second register: first register now has period r!

Claim: Resulting α has nonzero amplitudes with period r.
$x^a = z$ for $a = j, j + r, j + 2(r), \ldots$ since $x^r = 1$.

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}}\sum_{a=0}^{M-1}|a,0\rangle$

Compute: $\frac{1}{\sqrt{M}}\sum_{a=0}^{M-1}|a,f(a)\rangle, \quad f(a)=x^a$

Measure second register: first register now has period r!

Claim: Resulting α has nonzero amplitudes with period r.
$x^a = z$ for $a = j, j+r, j+2(r), \ldots$ since $x^r = 1$.

Claim: QFT of period k signal $\implies$ periodic signal of M/k

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, 0\rangle$

Compute: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, f(a)\rangle, \quad f(a) = x^a$

Measure second register: first register now has period r!

Claim: Resulting α has nonzero amplitudes with period r.
$x^a = z$ for $a = j, j + r, j + 2(r), \ldots$ since $x^r = 1$.

Claim: QFT of period k signal $\implies$ periodic signal of M/k with 0 shift!

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}}\sum_{a=0}^{M-1}|a,0\rangle$

Compute: $\frac{1}{\sqrt{M}}\sum_{a=0}^{M-1}|a,f(a)\rangle\,, \quad f(a)=x^a$

Measure second register: first register now has period r!

Claim: Resulting α has nonzero amplitudes with period r.
$x^a = z$ for $a = j, j+r, j+2(r), \ldots$ since $x^r = 1$.

Claim: QFT of period k signal $\implies$ periodic signal of M/k with 0 shift!

Do several times:

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, 0\rangle$

Compute: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, f(a)\rangle, \quad f(a) = x^a$

Measure second register: first register now has period r!

Claim: Resulting α has nonzero amplitudes with period r.
$x^a = z$ for $a = j, j+r, j+2(r), \ldots$ since $x^r = 1$.

Claim: QFT of period k signal $\implies$ periodic signal of M/k with 0 shift!

Do several times:
Run and measure QFT output,

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, 0\rangle$

Compute: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, f(a)\rangle\,, \quad f(a) = x^a$

Measure second register: first register now has period r!

Claim: Resulting α has nonzero amplitudes with period r.
$x^a = z$ for $a = j, j + r, j + 2(r), \ldots$ since $x^r = 1$.

Claim: QFT of period k signal $\implies$ periodic signal of M/k with 0 shift!

Do several times:
Run and measure QFT output,
Result is multiple of $M/(r)$.

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}}\sum_{a=0}^{M-1}|a,0\rangle$

Compute: $\frac{1}{\sqrt{M}}\sum_{a=0}^{M-1}|a,f(a)\rangle, \quad f(a)=x^a$

Measure second register: first register now has period r!

Claim: Resulting α has nonzero amplitudes with period r.
$x^a = z$ for $a = j, j+r, j+2(r), \ldots$ since $x^r = 1$.

Claim: QFT of period k signal $\implies$ periodic signal of M/k with 0 shift!

Do several times:
Run and measure QFT output,
Result is multiple of $M/(r)$.

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, 0\rangle$

Compute: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, f(a)\rangle, \quad f(a) = x^a$

Measure second register: first register now has period r!

Claim: Resulting α has nonzero amplitudes with period r.
$x^a = z$ for $a = j, j+r, j+2(r), \ldots$ since $x^r = 1$.

Claim: QFT of period k signal $\Longrightarrow$ periodic signal of M/k with 0 shift!

Do several times:
Run and measure QFT output,
Result is multiple of $M/(r)$.

Compute GCD of results:

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}}\sum_{a=0}^{M-1}|a,0\rangle$

Compute: $\frac{1}{\sqrt{M}}\sum_{a=0}^{M-1}|a,f(a)\rangle\,, \quad f(a)=x^a$

Measure second register: first register now has period r!

Claim: Resulting α has nonzero amplitudes with period r.
$x^a = z$ for $a = j, j+r, j+2(r), \ldots$ since $x^r = 1$.

Claim: QFT of period k signal $\implies$ periodic signal of M/k with 0 shift!

Do several times:
Run and measure QFT output,
Result is multiple of $M/(r)$.

Compute GCD of results: will likely be $M/(r)$.

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, 0\rangle$

Compute: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, f(a)\rangle, \quad f(a) = x^a$

Measure second register: first register now has period r!

Claim: Resulting α has nonzero amplitudes with period r.
$x^a = z$ for $a = j, j+r, j+2(r), \ldots$ since $x^r = 1$.

Claim: QFT of period k signal $\implies$ periodic signal of M/k with 0 shift!

Do several times:
Run and measure QFT output,
Result is multiple of $M/(r)$.

Compute GCD of results: will likely be $M/(r)$.
Order of x is r.

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}}\sum_{a=0}^{M-1}|a,0\rangle$

Compute: $\frac{1}{\sqrt{M}}\sum_{a=0}^{M-1}|a,f(a)\rangle, \quad f(a)=x^a$

Measure second register: first register now has period r!

Claim: Resulting α has nonzero amplitudes with period r.
$x^a = z$ for $a = j, j+r, j+2(r), \ldots$ since $x^r = 1$.

Claim: QFT of period k signal $\implies$ periodic signal of M/k with 0 shift!

Do several times:
Run and measure QFT output,
Result is multiple of $M/(r)$.

Compute GCD of results: will likely be $M/(r)$.
Order of x is r. Check GCD$(N, x^{r/2}+1)$.

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, 0\rangle$

Compute: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, f(a)\rangle, \quad f(a) = x^a$

Measure second register: first register now has period r!

Claim: Resulting α has nonzero amplitudes with period r.
$x^a = z$ for $a = j, j + r, j + 2(r), \ldots$ since $x^r = 1$.

Claim: QFT of period k signal $\Longrightarrow$ periodic signal of M/k with 0 shift!

Do several times:
Run and measure QFT output,
Result is multiple of $M/(r)$.

Compute GCD of results: will likely be $M/(r)$.
Order of x is r. Check $\text{GCD}(N, x^{r/2} + 1)$.

Details: need period r to divide M.

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, 0\rangle$

Compute: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, f(a)\rangle$, $\quad f(a) = x^a$

Measure second register: first register now has period r!

Claim: Resulting α has nonzero amplitudes with period r.
$x^a = z$ for $a = j, j+r, j+2(r), \ldots$ since $x^r = 1$.

Claim: QFT of period k signal $\implies$ periodic signal of M/k with 0 shift!

Do several times:
Run and measure QFT output,
Result is multiple of $M/(r)$.

Compute GCD of results: will likely be $M/(r)$.
Order of x is r. Check GCD$(N, x^{r/2}+1)$.

Details: need period r to divide M. What is M?

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}}\sum_{a=0}^{M-1}|a,0\rangle$

Compute: $\frac{1}{\sqrt{M}}\sum_{a=0}^{M-1}|a,f(a)\rangle, \quad f(a)=x^a$

Measure second register: first register now has period r!

Claim: Resulting α has nonzero amplitudes with period r.
$x^a = z$ for $a = j, j+r, j+2(r), \ldots$ since $x^r = 1$.

Claim: QFT of period k signal $\implies$ periodic signal of M/k with 0 shift!

Do several times:
Run and measure QFT output,
Result is multiple of $M/(r)$.

Compute GCD of results: will likely be $M/(r)$.
Order of x is r. Check GCD$(N, x^{r/2}+1)$.

Details: need period r to divide M. What is M? 2^n.

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, 0\rangle$

Compute: $\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, f(a)\rangle, \quad f(a) = x^a$

Measure second register: first register now has period r!

Claim: Resulting α has nonzero amplitudes with period r.
$x^a = z$ for $a = j, j+r, j+2(r), \ldots$ since $x^r = 1$.

Claim: QFT of period k signal $\implies$ periodic signal of M/k with 0 shift!

Do several times:
Run and measure QFT output,
Result is multiple of $M/(r)$.

Compute GCD of results: will likely be $M/(r)$.
Order of x is r. Check GCD$(N, x^{r/2} + 1)$.

Details: need period r to divide M. What is M? 2^n.
Need more sophisticated analysis...

Roots and Unity and Fourier Transform

Initialize with state: $\frac{1}{\sqrt{M}}\sum_{a=0}^{M-1}|a,0\rangle$

Compute: $\frac{1}{\sqrt{M}}\sum_{a=0}^{M-1}|a,f(a)\rangle, \quad f(a)=x^a$

Measure second register: first register now has period r!

Claim: Resulting α has nonzero amplitudes with period r.
$x^a = z$ for $a = j, j+r, j+2(r), \ldots$ since $x^r = 1$.

Claim: QFT of period k signal $\implies$ periodic signal of M/k with 0 shift!

Do several times:
Run and measure QFT output,
Result is multiple of $M/(r)$.

Compute GCD of results: will likely be $M/(r)$.
Order of x is r. Check GCD$(N, x^{r/2}+1)$.

Details: need period r to divide M. What is M? 2^n.
Need more sophisticated analysis...but same ideas.

Mini-Conclusion.

Quantum Fourier Transform $\Longrightarrow$ Factoring!

What's a gate look like?

Hadamard Gate.

$$|0\rangle \;\text{—}\boxed{H}\text{—}\!\!\longrightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad |1\rangle \;\text{—}\boxed{H}\text{—}\!\!\longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

What's a gate look like?

Hadamard Gate.

$$|0\rangle \;\text{—}\boxed{\text{H}}\text{—}\!\!\longrightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad |1\rangle \;\text{—}\boxed{\text{H}}\text{—}\!\!\longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Two bits.

What's a gate look like?

Hadamard Gate.

$|0\rangle \;\text{—}\boxed{H}\longrightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad |1\rangle \;\text{—}\boxed{H}\longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

Two bits.

$H(\alpha_0|0\rangle + \alpha_1|1\rangle)$

What's a gate look like?

Hadamard Gate.

$$|0\rangle \;-\!\boxed{H}\!\longrightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad |1\rangle \;-\!\boxed{H}\!\longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Two bits.

$$H(\alpha_0|0\rangle + \alpha_1|1\rangle) = \frac{\alpha_0+\alpha_1}{\sqrt{2}}|0\rangle + \frac{\alpha_0-\alpha_1}{\sqrt{2}}|1\rangle.$$

What's a gate look like?

Hadamard Gate.

$$|0\rangle \;\text{—}\boxed{\text{H}}\!\longrightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad |1\rangle \;\text{—}\boxed{\text{H}}\!\longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Two bits.

$H(\alpha_0|0\rangle + \alpha_1|1\rangle) = \frac{\alpha_0+\alpha_1}{\sqrt{2}}|0\rangle + \frac{\alpha_0-\alpha_1}{\sqrt{2}}|1\rangle$.

Notice: added amplitudes

What's a gate look like?

Hadamard Gate.

$$|0\rangle \; \text{—}\boxed{\text{H}}\longrightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad |1\rangle \; \text{—}\boxed{\text{H}}\longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Two bits.

$H(\alpha_0|0\rangle + \alpha_1|1\rangle) = \frac{\alpha_0+\alpha_1}{\sqrt{2}}|0\rangle + \frac{\alpha_0-\alpha_1}{\sqrt{2}}|1\rangle$.

Notice: added amplitudes and even subtracted amplitudes!

What's a gate look like?

Hadamard Gate.

$$|0\rangle \longrightarrow \boxed{H} \longrightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad |1\rangle \longrightarrow \boxed{H} \longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Two bits.

$H(\alpha_0|0\rangle + \alpha_1|1\rangle) = \frac{\alpha_0+\alpha_1}{\sqrt{2}}|0\rangle + \frac{\alpha_0-\alpha_1}{\sqrt{2}}|1\rangle$.

Notice: added amplitudes and even subtracted amplitudes!

Not so easy or even possible with probability.

What's a gate look like?

Hadamard Gate.

$$|0\rangle \;\text{—}\boxed{\text{H}}\longrightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad |1\rangle \;\text{—}\boxed{\text{H}}\longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Two bits.

$H(\alpha_0|0\rangle + \alpha_1|1\rangle) = \frac{\alpha_0+\alpha_1}{\sqrt{2}}|0\rangle + \frac{\alpha_0-\alpha_1}{\sqrt{2}}|1\rangle$.

Notice: added amplitudes and even subtracted amplitudes!

Not so easy or even possible with probability.

Hadamard: Reflection over line at angle $\pi/8$ on the (x,y)- plane.

What's a gate look like?

Hadamard Gate.

$$|0\rangle \;\text{—}\boxed{\text{H}}\longrightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad |1\rangle \;\text{—}\boxed{\text{H}}\longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Two bits.

$H(\alpha_0|0\rangle + \alpha_1|1\rangle) = \frac{\alpha_0+\alpha_1}{\sqrt{2}}|0\rangle + \frac{\alpha_0-\alpha_1}{\sqrt{2}}|1\rangle$.

Notice: added amplitudes and even subtracted amplitudes!

Not so easy or even possible with probability.

Hadamard: Reflection over line at angle $\pi/8$ on the (x, y)- plane.
$x = \alpha_0, y = \alpha_1$.

What's a gate look like?

Hadamard Gate.

$|0\rangle \;\text{—}\boxed{H}\text{—}\!\!\longrightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad |1\rangle \;\text{—}\boxed{H}\text{—}\!\!\longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

Two bits.

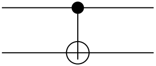
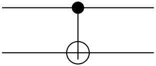
$H(\alpha_0|0\rangle + \alpha_1|1\rangle) = \frac{\alpha_0+\alpha_1}{\sqrt{2}}|0\rangle + \frac{\alpha_0-\alpha_1}{\sqrt{2}}|1\rangle$.

Notice: added amplitudes and even subtracted amplitudes!

Not so easy or even possible with probability.

Hadamard: Reflection over line at angle $\pi/8$ on the (x,y)- plane.
$x = \alpha_0, y = \alpha_1$.

Controlled Not Gate.

$|00\rangle$  $|00\rangle$ $|10\rangle$  $|11\rangle$

Note:
Operating on $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$.

What's a gate look like?

Hadamard Gate.

$|0\rangle \longrightarrow \boxed{H} \longrightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad |1\rangle \longrightarrow \boxed{H} \longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

Two bits.

$H(\alpha_0|0\rangle + \alpha_1|1\rangle) = \frac{\alpha_0+\alpha_1}{\sqrt{2}}|0\rangle + \frac{\alpha_0-\alpha_1}{\sqrt{2}}|1\rangle.$

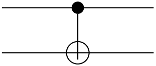
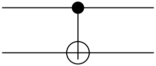
Notice: added amplitudes and even subtracted amplitudes!

Not so easy or even possible with probability.

Hadamard: Reflection over line at angle $\pi/8$ on the (x,y)- plane.

$x = \alpha_0, y = \alpha_1.$

Controlled Not Gate.

$|00\rangle$  $|00\rangle$ $\qquad$ $|10\rangle$  $|11\rangle$

Note:

Operating on $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$.

One gets $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{11}|10\rangle + \alpha_{10}|11\rangle$.

Quantum Fourier Transform.

Fourier Transform:

Quantum Fourier Transform.

Fourier Transform:

Split into odd and even inputs.

Quantum Fourier Transform.

Fourier Transform:

Split into odd and even inputs.

Recurse: 2 subcircuits

Quantum Fourier Transform.

Fourier Transform:
Split into odd and even inputs.
Recurse: 2 subcircuits
Combine Input $x0$ and $x1$ from subcircuits.

Quantum Fourier Transform.

Fourier Transform:

Split into odd and even inputs.

Recurse: 2 subcircuits

Combine Input $x0$ and $x1$ from subcircuits.

Recursively compute A_e and A_o on $\frac{n}{2}$ roots of unity:

Quantum Fourier Transform.

Fourier Transform:
  Split into odd and even inputs.
  Recurse: 2 subcircuits
  Combine Input $x0$ and $x1$ from subcircuits.

Recursively compute A_e and A_o on $\frac{n}{2}$ roots of unity:
$\omega^2, \omega^4, \omega^6, \ldots, \omega^n$.

Quantum Fourier Transform.

Fourier Transform:
  Split into odd and even inputs.
  Recurse: 2 subcircuits
  Combine Input $x0$ and $x1$ from subcircuits.

Recursively compute A_e and A_o on $\frac{n}{2}$ roots of unity:
$\omega^2, \omega^4, \omega^6, \ldots, \omega^n$.

For each $i \leq n/2$.

Quantum Fourier Transform.

Fourier Transform:
  Split into odd and even inputs.
  Recurse: 2 subcircuits
  Combine Input $x0$ and $x1$ from subcircuits.

Recursively compute A_e and A_o on $\frac{n}{2}$ roots of unity: $\omega^2, \omega^4, \omega^6, \ldots, \omega^n$.

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

Quantum Fourier Transform.

Fourier Transform:

Split into odd and even inputs.

Recurse: 2 subcircuits

Combine Input $x0$ and $x1$ from subcircuits.

Recursively compute A_e and A_o on $\frac{n}{2}$ roots of unity: $\omega^2, \omega^4, \omega^6, \ldots, \omega^n$.

For each $i \le n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

$$A(\omega^{i+n/2}) = A_e(\omega^{2i}) - \omega^i A_o(\omega^{2i})$$

Quantum Fourier Transform.

Fourier Transform:
Split into odd and even inputs.
Recurse: 2 subcircuits
Combine Input $x0$ and $x1$ from subcircuits.

Recursively compute A_e and A_o on $\frac{n}{2}$ roots of unity: $\omega^2, \omega^4, \omega^6, \ldots, \omega^n$.

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

$$A(\omega^{i+n/2}) = A_e(\omega^{2i}) - \omega^i A_o(\omega^{2i})$$

Runtime Recurrence:

Quantum Fourier Transform.

Fourier Transform:
Split into odd and even inputs.
Recurse: 2 subcircuits
Combine Input $x0$ and $x1$ from subcircuits.

Recursively compute A_e and A_o on $\frac{n}{2}$ roots of unity:
$\omega^2, \omega^4, \omega^6, \ldots, \omega^n$.

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

$$A(\omega^{i+n/2}) = A_e(\omega^{2i}) - \omega^i A_o(\omega^{2i})$$

Runtime Recurrence:
$T(n) = 2T(n/2) + O(n)$

Quantum Fourier Transform.

Fourier Transform:
Split into odd and even inputs.
Recurse: 2 subcircuits
Combine Input $x0$ and $x1$ from subcircuits.

Recursively compute A_e and A_o on $\frac{n}{2}$ roots of unity:
$\omega^2, \omega^4, \omega^6, \ldots, \omega^n$.

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

$$A(\omega^{i+n/2}) = A_e(\omega^{2i}) - \omega^i A_o(\omega^{2i})$$

Runtime Recurrence:
$T(n) = 2T(n/2) + O(n) = O(n \log n)$!

Quantum Fourier Tansform.

FFT:

Quantum Fourier Tansform.

FFT:

For each $i \leq n/2$.

Quantum Fourier Tansform.

FFT:

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

Quantum Fourier Tansform.

FFT:

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

$$A(\omega^{i+n/2}) = A_e(\omega^{2i}) - \omega^i A_o(\omega^{2i})$$

Quantum Fourier Tansform.

FFT:

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

$$A(\omega^{i+n/2}) = A_e(\omega^{2i}) - \omega^i A_o(\omega^{2i})$$

Split: ignore low order bit.

Quantum Fourier Tansform.

FFT:

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

$$A(\omega^{i+n/2}) = A_e(\omega^{2i}) - \omega^i A_o(\omega^{2i})$$

Split: ignore low order bit.

The amplitudes of both will be processed in parallel.

Quantum Fourier Tansform.

FFT:

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

$$A(\omega^{i+n/2}) = A_e(\omega^{2i}) - \omega^i A_o(\omega^{2i})$$

Split: ignore low order bit.

The amplitudes of both will be processed in parallel.

Recurse: build one QFT circuit on $n-1$ bits.

Quantum Fourier Tansform.

FFT:

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

$$A(\omega^{i+n/2}) = A_e(\omega^{2i}) - \omega^i A_o(\omega^{2i})$$

Split: ignore low order bit.

The amplitudes of both will be processed in parallel.

Recurse: build one QFT circuit on $n-1$ bits.

The circuit will work on amplitudes of strings for both $x0$ and $x1$.

Quantum Fourier Tansform.

FFT:

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

$$A(\omega^{i+n/2}) = A_e(\omega^{2i}) - \omega^i A_o(\omega^{2i})$$

Split: ignore low order bit.

The amplitudes of both will be processed in parallel.

Recurse: build one QFT circuit on $n-1$ bits.

The circuit will work on amplitudes of strings for both $x0$ and $x1$.

Combine: Add Hadamard Gate on nth bit.

Quantum Fourier Tansform.

FFT:

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

$$A(\omega^{i+n/2}) = A_e(\omega^{2i}) - \omega^i A_o(\omega^{2i})$$

Split: ignore low order bit.

The amplitudes of both will be processed in parallel.

Recurse: build one QFT circuit on $n-1$ bits.

The circuit will work on amplitudes of strings for both $x0$ and $x1$.

Combine: Add Hadamard Gate on nth bit.

Combines amplitudes of $x0$ and $x1$

Quantum Fourier Tansform.

FFT:

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

$$A(\omega^{i+n/2}) = A_e(\omega^{2i}) - \omega^i A_o(\omega^{2i})$$

Split: ignore low order bit.
The amplitudes of both will be processed in parallel.
Recurse: build one QFT circuit on $n-1$ bits.
The circuit will work on amplitudes of strings for both $x0$ and $x1$.
Combine: Add Hadamard Gate on nth bit.
Combines amplitudes of $x0$ and $x1$ in fancy way.

Quantum Fourier Tansform.

FFT:

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

$$A(\omega^{i+n/2}) = A_e(\omega^{2i}) - \omega^i A_o(\omega^{2i})$$

Split: ignore low order bit.
  The amplitudes of both will be processed in parallel.

Recurse: build one QFT circuit on $n-1$ bits.
  The circuit will work on amplitudes of strings for both $x0$ and $x1$.

Combine: Add Hadamard Gate on nth bit.
  Combines amplitudes of $x0$ and $x1$ in fancy way.
    E.g. $\alpha_{0x} \pm \alpha_{1x}$ plus scaling.

Quantum Fourier Tansform.

FFT:

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

$$A(\omega^{i+n/2}) = A_e(\omega^{2i}) - \omega^i A_o(\omega^{2i})$$

Split: ignore low order bit.

The amplitudes of both will be processed in parallel.

Recurse: build one QFT circuit on $n-1$ bits.

The circuit will work on amplitudes of strings for both $x0$ and $x1$.

Combine: Add Hadamard Gate on nth bit.

Combines amplitudes of $x0$ and $x1$ in fancy way.

E.g. $\alpha_{0x} \pm \alpha_{1x}$ plus scaling.

Quantum Fourier Tansform.

FFT:

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

$$A(\omega^{i+n/2}) = A_e(\omega^{2i}) - \omega^i A_o(\omega^{2i})$$

Split: ignore low order bit.
The amplitudes of both will be processed in parallel.
Recurse: build one QFT circuit on $n-1$ bits.
The circuit will work on amplitudes of strings for both $x0$ and $x1$.
Combine: Add Hadamard Gate on nth bit.
Combines amplitudes of $x0$ and $x1$ in fancy way.
E.g. $\alpha_{0x} \pm \alpha_{1x}$ plus scaling.

Note: need to do more than combine, need to multiply some by ω^j.
(Phase.)

Quantum Fourier Tansform.

FFT:

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

$$A(\omega^{i+n/2}) = A_e(\omega^{2i}) - \omega^i A_o(\omega^{2i})$$

Split: ignore low order bit.
The amplitudes of both will be processed in parallel.
Recurse: build one QFT circuit on $n-1$ bits.
The circuit will work on amplitudes of strings for both $x0$ and $x1$.
Combine: Add Hadamard Gate on nth bit.
Combines amplitudes of $x0$ and $x1$ in fancy way.
E.g. $\alpha_{0x} \pm \alpha_{1x}$ plus scaling.

Note: need to do more than combine, need to multiply some by ω^j. (Phase.)

See Book for details

Quantum Fourier Tansform.

FFT:

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

$$A(\omega^{i+n/2}) = A_e(\omega^{2i}) - \omega^i A_o(\omega^{2i})$$

Split: ignore low order bit.

The amplitudes of both will be processed in parallel.

Recurse: build one QFT circuit on $n-1$ bits.

The circuit will work on amplitudes of strings for both $x0$ and $x1$.

Combine: Add Hadamard Gate on nth bit.

Combines amplitudes of $x0$ and $x1$ in fancy way.

E.g. $\alpha_{0x} \pm \alpha_{1x}$ plus scaling.

Note: need to do more than combine, need to multiply some by ω^j. (Phase.)

See Book for details

$O(n)$ gates for phase multiplication.

Quantum Fourier Tansform.

FFT:

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

$$A(\omega^{i+n/2}) = A_e(\omega^{2i}) - \omega^i A_o(\omega^{2i})$$

Split: ignore low order bit.
  The amplitudes of both will be processed in parallel.
Recurse: build one QFT circuit on $n-1$ bits.
  The circuit will work on amplitudes of strings for both $x0$ and $x1$.
Combine: Add Hadamard Gate on nth bit.
  Combines amplitudes of $x0$ and $x1$ in fancy way.
    E.g. $\alpha_{0x} \pm \alpha_{1x}$ plus scaling.

Note: need to do more than combine, need to multiply some by ω^j. (Phase.)

See Book for details

$O(n)$ gates for phase multiplication.
  Use conditional phase gates in construction.

Quantum Fourier Tansform.

FFT:

For each $i \leq n/2$.

$$A(\omega^i) = A_e(\omega^{2i}) + \omega^i A_o(\omega^{2i})$$

$$A(\omega^{i+n/2}) = A_e(\omega^{2i}) - \omega^i A_o(\omega^{2i})$$

Split: ignore low order bit.
The amplitudes of both will be processed in parallel.
Recurse: build one QFT circuit on $n-1$ bits.
The circuit will work on amplitudes of strings for both $x0$ and $x1$.
Combine: Add Hadamard Gate on nth bit.
Combines amplitudes of $x0$ and $x1$ in fancy way.
E.g. $\alpha_{0x} \pm \alpha_{1x}$ plus scaling.

Note: need to do more than combine, need to multiply some by ω^j. (Phase.)

See Book for details

$O(n)$ gates for phase multiplication.
Use conditional phase gates in construction.

Size: $S(n) = S(n-1) + O(n) = O(n^2)$.

Quantum Supremacy

Random Circuit Sampling.

Quantum Supremacy

Random Circuit Sampling.
    Random Quantum circuit generates distribution.

Quantum Supremacy

Random Circuit Sampling.
  Random Quantum circuit generates distribution.

Classically "can't" generate that distribution.

Quantum Supremacy

Random Circuit Sampling.
  Random Quantum circuit generates distribution.

Classically “can’t” generate that distribution.
  (Bouland, Fefferman, Nirkhe, Vazirani)

Quantum Supremacy

Random Circuit Sampling.
  Random Quantum circuit generates distribution.

Classically “can’t” generate that distribution.
  (Bouland, Fefferman, Nirkhe, Vazirani)

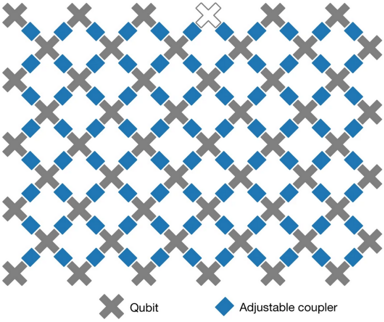
Google: Nature Paper.

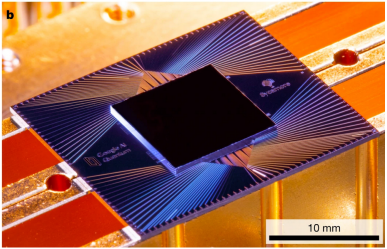
Quantum Supremacy

Random Circuit Sampling.
  Random Quantum circuit generates distribution.

Classically “can’t” generate that distribution.
  (Bouland, Fefferman, Nirkhe, Vazirani)

Google: Nature Paper.





And that was quantum..

And that was quantum..

And the semester.

And that was quantum..

And the semester.

It is a total privilege teaching you!!!

And that was quantum..

And the semester.

It is a total privilege teaching you!!!

From me, Professor Raghavendra and the whole staff.

And that was quantum..

And the semester.

It is a total privilege teaching you!!!

From me, Professor Raghavendra and the whole staff.

Good luck (skill) on Final...

And that was quantum..

And the semester.

It is a total privilege teaching you!!!

From me, Professor Raghavendra and the whole staff.

Good luck (skill) on Final...