ATIL SAMANCIOGLU

QUANTUM COMPUTING

Bit vs Qubit

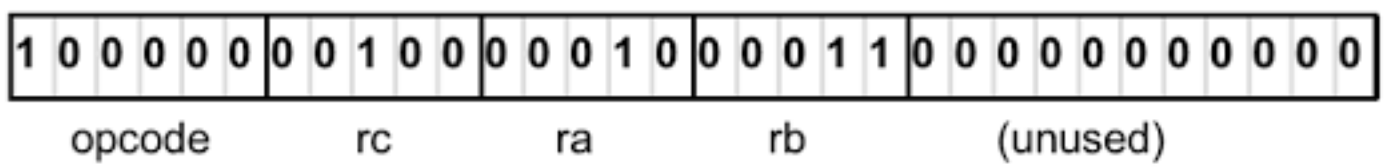
COMPUTER SCIENCE

MACHINE LANGUAGE

ASSEMBLY

HIGH LEVEL LANGUAGE

COMPUTER SCIENCE



ADD (R2, R3, R4)

A = B + C;

DECIMAL

215 = 5 * 10 ^ 0 + 1 * 10 ^ 1 + 2 * 10 ^ 2

514

5 * 10 ^ 2

4 * 10 ^ 0

1 * 10 ^ 1

BINARY

1 1 0 1 1 0 1

1 * 2 ^ 6 + 1 * 2 ^ 5 + 0 * 2 ^ 4 + 1 * 2^ 3 +

1 * 2 ^ 2 + 0 * 2 ^ 1 + 1 * 2 ^ 0

64 + 32 + 0 + 8 + 4 + 0 + 1

109

HEXADECIMAL

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
										10	11	12	13	14	15

HEXADECIMAL

A 4 F 6

10 * 16 ^ 3 + 4 * 16 ^ 2 + 15 * 16 ^ 1 + 6 * 16 ^ 0

40960 + 1024 + 240 + 6

42230

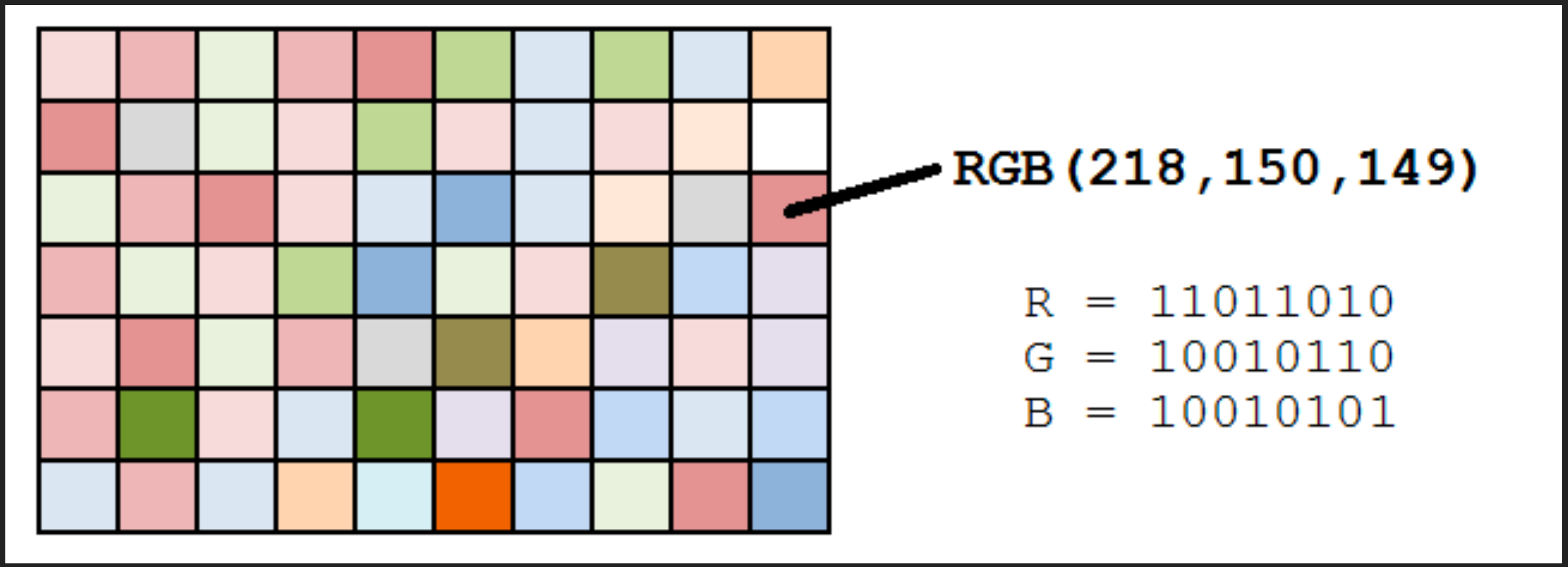
ASCII

Decimal - Binary - Octal - Hex – ASCII Conversion Chart

Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII
0	00000000	000	00	NUL	32	00100000	040	20	SP	64	01000000	100	40	@	96	01100000	140	60	`
1	00000001	001	01	SOH	33	00100001	041	21	!	65	01000001	101	41	A	97	01100001	141	61	a
2	00000010	002	02	STX	34	00100010	042	22	“	66	01000010	102	42	B	98	01100010	142	62	b
3	00000011	003	03	ETX	35	00100011	043	23	#	67	01000011	103	43	C	99	01100011	143	63	c
4	00000100	004	04	EOT	36	00100100	044	24	$	68	01000100	104	44	D	100	01100100	144	64	d
5	00000101	005	05	ENQ	37	00100101	045	25	%	69	01000101	105	45	E	101	01100101	145	65	e
6	00000110	006	06	ACK	38	00100110	046	26	&	70	01000110	106	46	F	102	01100110	146	66	f
7	00000111	007	07	BEL	39	00100111	047	27	‘	71	01000111	107	47	G	103	01100111	147	67	g
8	00001000	010	08	BS	40	00101000	050	28	(	72	01001000	110	48	H	104	01101000	150	68	h
9	00001001	011	09	HT	41	00101001	051	29	)	73	01001001	111	49	I	105	01101001	151	69	i
10	00001010	012	0A	LF	42	00101010	052	2A	*	74	01001010	112	4A	J	106	01101010	152	6A	j
11	00001011	013	0B	VT	43	00101011	053	2B	+	75	01001011	113	4B	K	107	01101011	153	6B	k
12	00001100	014	0C	FF	44	00101100	054	2C	,	76	01001100	114	4C	L	108	01101100	154	6C	l
13	00001101	015	0D	CR	45	00101101	055	2D	-	77	01001101	115	4D	M	109	01101101	155	6D	m
14	00001110	016	0E	SO	46	00101110	056	2E	.	78	01001110	116	4E	N	110	01101110	156	6E	n
15	00001111	017	0F	SI	47	00101111	057	2F	/	79	01001111	117	4F	O	111	01101111	157	6F	o
16	00010000	020	10	DLE	48	00110000	060	30	0	80	01010000	120	50	P	112	01110000	160	70	p
17	00010001	021	11	DC1	49	00110001	061	31	1	81	01010001	121	51	Q	113	01110001	161	71	q
18	00010010	022	12	DC2	50	00110010	062	32	2	82	01010010	122	52	R	114	01110010	162	72	r
19	00010011	023	13	DC3	51	00110011	063	33	3	83	01010011	123	53	S	115	01110011	163	73	s
20	00010100	024	14	DC4	52	00110100	064	34	4	84	01010100	124	54	T	116	01110100	164	74	t
21	00010101	025	15	NAK	53	00110101	065	35	5	85	01010101	125	55	U	117	01110101	165	75	u
22	00010110	026	16	SYN	54	00110110	066	36	6	86	01010110	126	56	V	118	01110110	166	76	v
23	00010111	027	17	ETB	55	00110111	067	37	7	87	01010111	127	57	W	119	01110111	167	77	w
24	00011000	030	18	CAN	56	00111000	070	38	8	88	01011000	130	58	X	120	01111000	170	78	x
25	00011001	031	19	EM	57	00111001	071	39	9	89	01011001	131	59	Y	121	01111001	171	79	y
26	00011010	032	1A	SUB	58	00111010	072	3A	:	90	01011010	132	5A	Z	122	01111010	172	7A	z
27	00011011	033	1B	ESC	59	00111011	073	3B	;	91	01011011	133	5B	[	123	01111011	173	7B	{
28	00011100	034	1C	FS	60	00111100	074	3C	<	92	01011100	134	5C	\	124	01111100	174	7C	|
29	00011101	035	1D	GS	61	00111101	075	3D	=	93	01011101	135	5D	]	125	01111101	175	7D	}
30	00011110	036	1E	RS	62	00111110	076	3E	>	94	01011110	136	5E	^	126	01111110	176	7E	~
31	00011111	037	1F	US	63	00111111	077	3F	?	95	01011111	137	5F	_	127	01111111	177	7F	DEL

Source: https://bournetocode.com/projects/GCSE_Computing_Fundamentals/pages/3-3-5-ascii.html

PIXEL



Source: https://towardsdatascience.com/steganography-hiding-an-image-inside-another-77ca66b2acb1?gi=6ec8b36cd70

BIT VS QUBIT

0 0 0 0 0 0 0 0

1 1 1 1 1 1 1 1

PREREQUISITES

|0>

$v = d / t$

python

P(A)

P(A AND B)

P((A AND B) OR C)

$$P(A \text{ AND } B) = 0$$

Mutually Exclusive

$$P(A \text{ AND } B) = P(A) \times P(B)$$

Independent

$$P(A \text{ OR } B) = P(A) + P(B)$$

Mutually Exclusive

$$P(A \text{ OR } B) = P(A) + P(B) - P(A \text{ AND } B)$$

Independent

PROBABILITY & BINARY

$$P(A) = 30\%$$

$$P(B) = 40\%$$

$$P(A \text{ OR } B) = P(A) + P(B) - P(\text{ A AND B})$$

$$= 0.3 + 0.4 - (0.3 * 0.4)$$

$$= 0.58$$

STATISTICS

15, 22, 33, 40, 55, 61, 79

Mean -> 43.57~

Median -> 40

Min -> 15

Max -> 79

15, 22, 33, 40, 55, 61, 79

$(15 - 43{,}57)^2$

$(22 - 43{,}57)^2$

$(33 - 43{,}57)^2$

$(40 - 43{,}57)^2$

$(55 - 43{,}57)^2$

$(61 - 43{,}57)^2$

$(79 - 43{,}57)^2$

$$\sqrt{515.95} = 22.71$$

Variance

Standard Deviation

COMPLEX NUMBERS

$i \rightarrow \sqrt{-1}$ (Imaginary number)

$a + bi$ (Complex number)

$$\sqrt{-9} = \sqrt{9} * \sqrt{-1}$$

$$= 3i$$

COMPLEX NUMBERS

$$\sqrt{i} = \frac{(1+i)}{\sqrt{2}}$$

COMPLEX NUMBERS

$$(3+2i) + (5+4i) = (8+6i)$$

$$(3-2i) + (-5+4i) = (-2+2i)$$

$$(3+2i) - (5+4i) = (-2-2i)$$

$$5 * (3+2i) = (15+10i)$$

$$(3+2i) / 3 = (1 + \frac{2i}{3})$$

COMPLEX NUMBERS

$$i \quad * \quad (3+2i) \quad = \quad (3i+i^2) \quad = \quad (-1+3i)$$

$$(5 + 3i) \quad * \quad (3+2i)$$

COMPLEX NUMBERS

$(3+2i) \quad -> \quad (3-2i)$

Complex Conjugate

$(5-4i) \quad -> \quad (5+4i)$

$|3+2i|^2 \quad -> \quad 3^2 + 2^2$

Squared Magnitude

Complex No * Complex Conjugate = Squared Magnitude

(3+2i) * (3-2i)

COMPLEX NUMBERS

$$\frac{(6+4i)}{(3+2i)} = \frac{(6+4i)}{(3+2i)} * \frac{(3-2i)}{(3-2i)}$$

$$= \frac{(6+4i) \;*\; (3-2i)}{(3^2+2^2)}$$

$$= \frac{(18 - 12i + 12i - 8i^2)}{13}$$

$$= 2$$

MATRIX

$$\begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 2 & 3 \\ 3 & 1 & 4 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 2 & 3 \\ 3 & 1 & 4 \\ 9 & 8 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 + 3i \\ 3 - 4i & 2 \end{bmatrix}$$

MATRIX

$$\underset{2*2}{\begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix}} + \underset{2*2}{\begin{bmatrix} 2 & 4 \\ 5 & 3 \end{bmatrix}} = \underset{2*2}{\begin{bmatrix} 2 & 6 \\ 8 & 4 \end{bmatrix}}$$

$$\begin{bmatrix} 1+2i & 2 \\ 3 & 2-5i \end{bmatrix} + \begin{bmatrix} 2 & 4 \\ 5 & 3 \end{bmatrix} = \begin{bmatrix} 3+2i & 6 \\ 8 & 5-5i \end{bmatrix}$$

MATRIX

$$\underset{2*2}{\begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix}} - \underset{2*2}{\begin{bmatrix} 2 & 4 \\ 5 & 3 \end{bmatrix}} = \underset{2*2}{\begin{bmatrix} -2 & -2 \\ -2 & -2 \end{bmatrix}}$$

$$\begin{bmatrix} 1+2i & 2 \\ 3 & 2-5i \end{bmatrix} - \begin{bmatrix} 2 & 4 \\ 5 & 3 \end{bmatrix} = \begin{bmatrix} -1+2i & -2 \\ -2 & -1-5i \end{bmatrix}$$

MATRIX

$$\begin{array}{cccc} & \text{2 * 2} & & \text{2 * 2} \\ 4 \; * & \begin{bmatrix} 2 & 4 \\ 5 & 3 \end{bmatrix} & = & \begin{bmatrix} 8 & 16 \\ 20 & 12 \end{bmatrix} \end{array}$$

$$\begin{array}{cccc} & \text{2 * 1} & & \text{2 * 1} \\ (1+2i) \; * & \begin{bmatrix} 2 \\ 5 \end{bmatrix} & = & \begin{bmatrix} 2 + 4i \\ 5 + 10i \end{bmatrix} \end{array}$$

MATRIX

$$\underset{2*2}{\begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix}} * \underset{2*2}{\begin{bmatrix} 2 & 4 \\ 5 & 3 \end{bmatrix}} = \underset{2*2}{\begin{bmatrix} 10 & 6 \\ 11 & 15 \end{bmatrix}}$$

$$0 * 2 + 2 * 5 = 10$$

$$0 * 4 + 2 * 3 = 6$$

$$3 * 2 + 1 * 5 = 11$$

$$3 * 4 + 1 * 3 = 15$$

MATRIX

$$\begin{bmatrix} 0 & 2 & 3 \\ 3 & 1 & 4 \\ 9 & 8 & 0 \end{bmatrix} * \begin{bmatrix} 1 & -3 & 4 \\ 0 & -1 & 2 \\ 3 & 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 9 & 1 & 4 \\ 15 & -6 & 14 \\ 9 & -35 & 52 \end{bmatrix}$$

MATRIX

$$\overset{3 * 2}{\begin{bmatrix} 0 & 2 \\ 3 & 1 \\ 9 & 8 \end{bmatrix}} * \overset{2 * 2}{\begin{bmatrix} 2 & 4 \\ 5 & 3 \end{bmatrix}} = \overset{3 * 2}{\begin{bmatrix} 10 & 6 \\ 11 & 15 \\ 58 & 60 \end{bmatrix}}$$

MATRIX

$$\underset{3 * 2}{\begin{bmatrix} 0 & 2 \\ 3 & 1 \\ 9 & 8 \end{bmatrix}} * \underset{2 * 1}{\begin{bmatrix} 2 \\ 5 \end{bmatrix}} = \underset{3 * 1}{\begin{bmatrix} 10 \\ 11 \\ 58 \end{bmatrix}}$$

MATRIX

$$\underset{3 * 2}{\begin{bmatrix} 0 & 2 \\ 3 & 1 \\ 9 & 8 \end{bmatrix}} \qquad \underset{2 * 1}{\begin{bmatrix} 2 \\ 5 \end{bmatrix}}$$

$$X * Y \;!=\; Y * X$$

$$(X+Y) * (Q+Z) = XQ + XZ + YQ + YZ$$

MATRIX

$$\begin{bmatrix} x \\ y \end{bmatrix} \otimes \begin{bmatrix} z \\ q \end{bmatrix} = \begin{bmatrix} xz \\ xq \\ yz \\ yq \end{bmatrix}$$

Tensor Product

$$\begin{bmatrix} 1 \\ 3 \end{bmatrix} \otimes \begin{bmatrix} 2 \\ 5 \\ 7 \end{bmatrix} = \begin{bmatrix} 2 \\ 5 \\ 7 \\ 6 \\ 15 \\ 21 \end{bmatrix}$$

MATRIX

$$\begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix} * \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix}$$

Identity Matrix (I)

$$XI = X$$

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

MATRIX

Inverse (Real Number)

$$A^{-1} = \frac{1}{A} \qquad 5^{-1} = \frac{1}{5} \qquad 10^{-1} = \frac{1}{10}$$

Inverse (Matrix)

$$AA^{-1} = I$$

$$A^{-1}A = I$$

MATRIX

$$\underset{X}{\begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix}} * \underset{X^{-1}}{\begin{bmatrix} -1/6 & 1/3 \\ 1/2 & 0 \end{bmatrix}} = \underset{I}{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}$$

Matrix Inverse

MATRIX

$$\begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix}^T = \begin{bmatrix} 0 & 3 \\ 2 & 1 \end{bmatrix}$$

Transpose

$$\begin{bmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \\ 6 & 7 & 8 \end{bmatrix}^T = \begin{bmatrix} 0 & 3 & 6 \\ 1 & 4 & 7 \\ 2 & 5 & 8 \end{bmatrix}$$

MATRIX

$$(XY)^T = Y^T X^T$$

$$\begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix} * \begin{bmatrix} 2 & 4 \\ 5 & 3 \end{bmatrix} = \begin{bmatrix} 10 & 6 \\ 11 & 15 \end{bmatrix}$$

MATRIX

$$\begin{bmatrix} 2+5i & i \\ 3 & 3-4i \end{bmatrix}^* = \begin{bmatrix} 2-5i & -i \\ 3 & 3+4i \end{bmatrix}$$

Complex Conjugate

$$\begin{bmatrix} 2+5i & i \\ 3 & 3-4i \end{bmatrix}^+ = \begin{bmatrix} 2-5i & 3 \\ -i & 3+4i \end{bmatrix}$$

Adjoint (Transpose - Complex Conjugate)

$$X^+ = (X^*)^T = (X^T)^*$$

MATRIX

if

$$X^{+} = X^{-1}$$

Unitary Matrix

$$XX^{+} = XX^{-1} = I$$

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} * \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Reversible Operation

if

$$X^{+} = X$$

Hermitian Matrix

$$\begin{bmatrix} 3 & 2+i \\ 2-i & 5 \end{bmatrix}^{+} = \begin{bmatrix} 3 & 2+i \\ 2-i & 5 \end{bmatrix}$$

Irreversible Operation

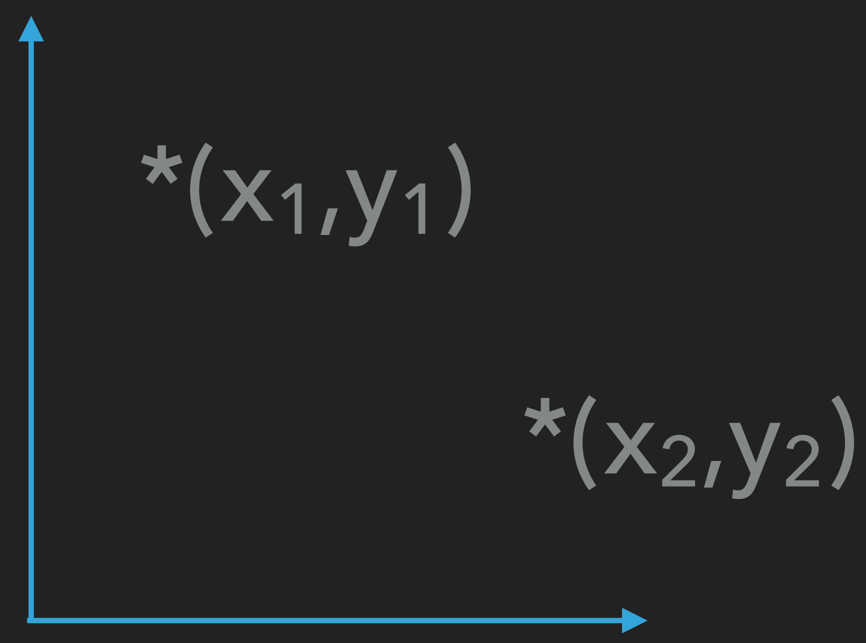
MATRIX

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

$$\begin{bmatrix} -4 \\ 3+i \\ -5i \end{bmatrix} \qquad \begin{bmatrix} 0 \\ 3 \\ 6 \end{bmatrix}$$

Vector = Column Matrix (Quantum Computing)

MATRIX

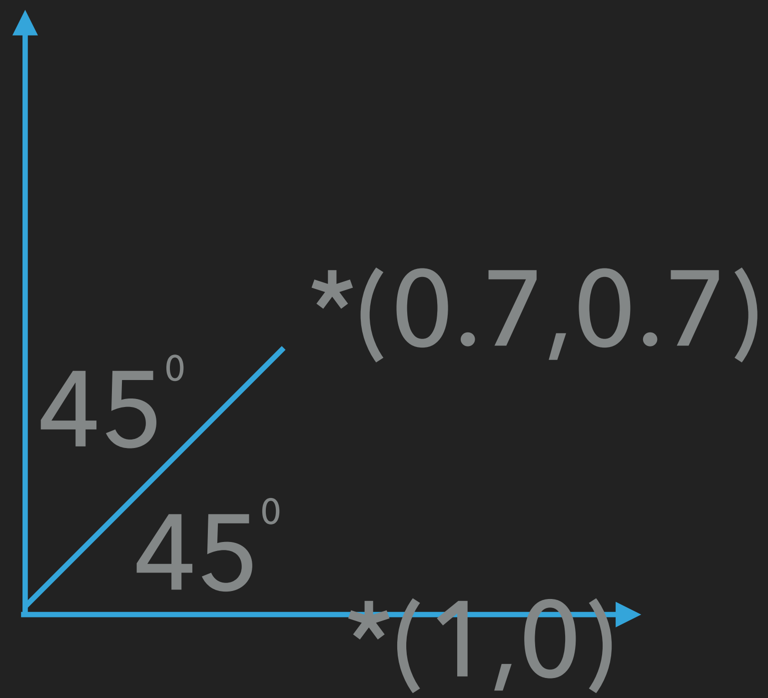


$$x_2 = Ax_1+By_1$$
$$y_2 = Cx_1+Dy_1$$

$$\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} A & B \\ C & D \end{bmatrix} * \begin{bmatrix} x_1 \\ y_1 \end{bmatrix}$$

Linear Transformation

MATRIX

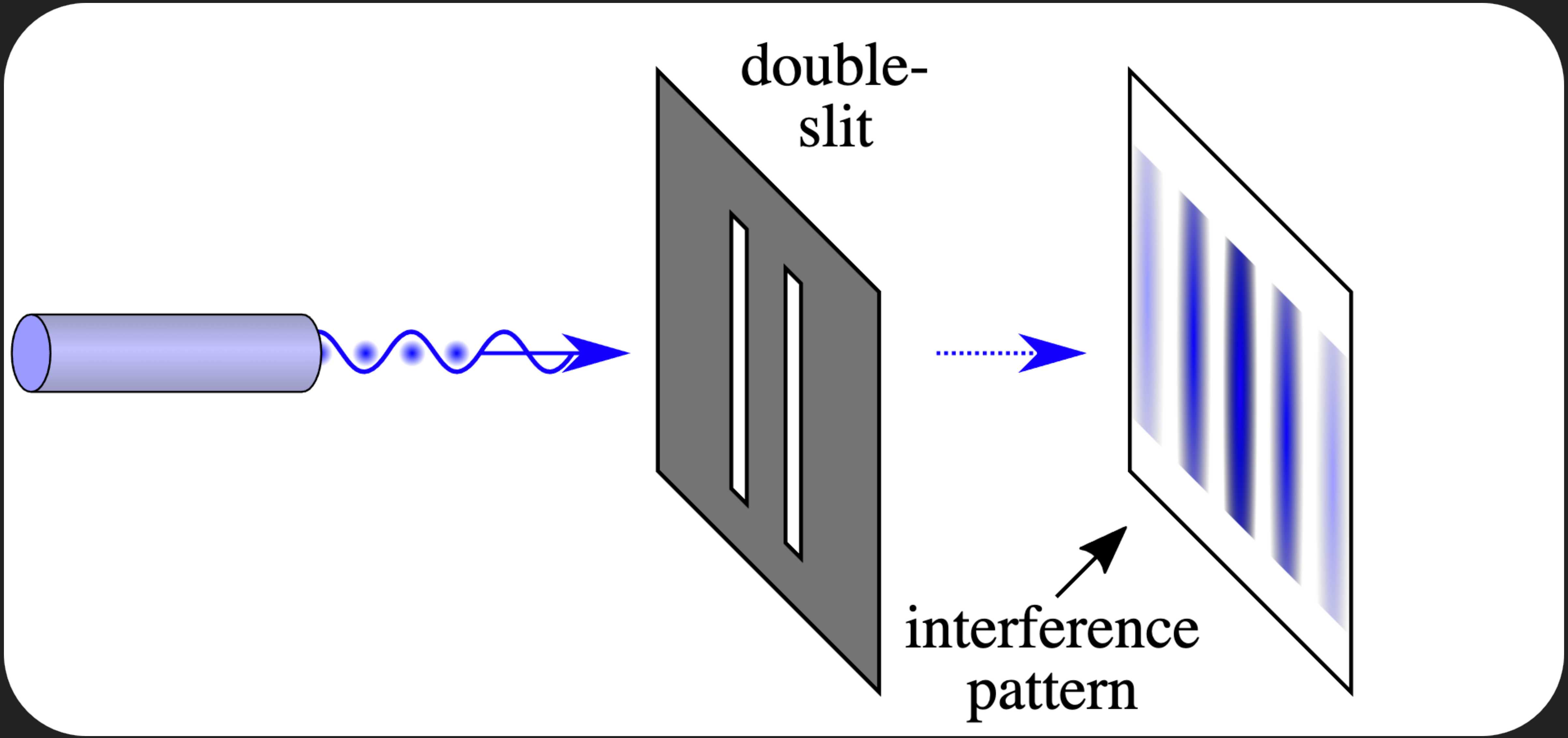


$$x_2 = Ax_1 + By_1$$
$$y_2 = Cx_1 + Dy_1$$

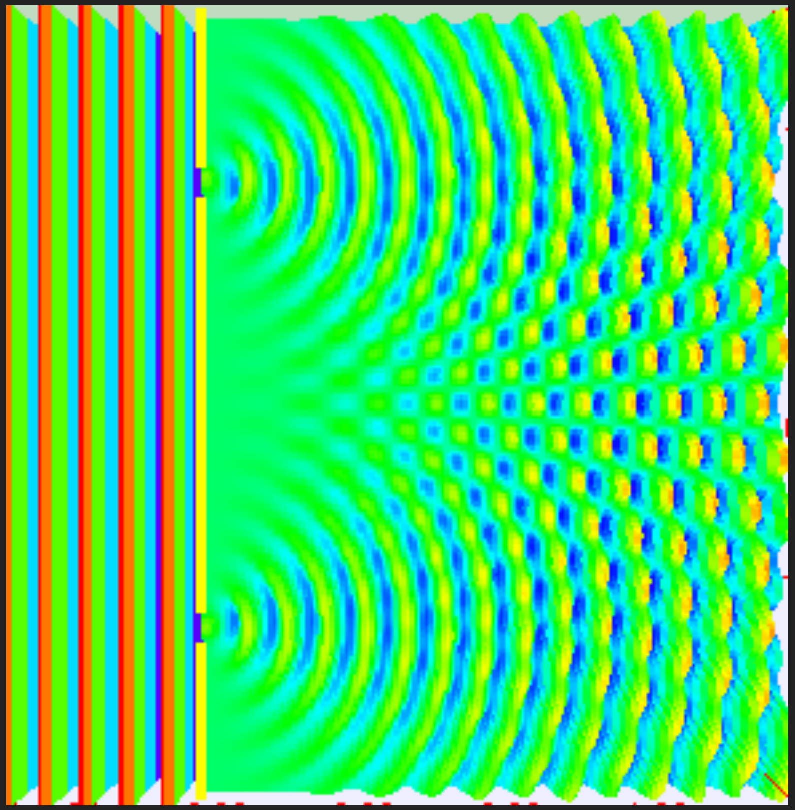
$$\begin{bmatrix} 0.7 \\ 0.7 \end{bmatrix} = \begin{bmatrix} \cos(45) & -\sin(45) \\ +\sin(45) & \cos(45) \end{bmatrix} * \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

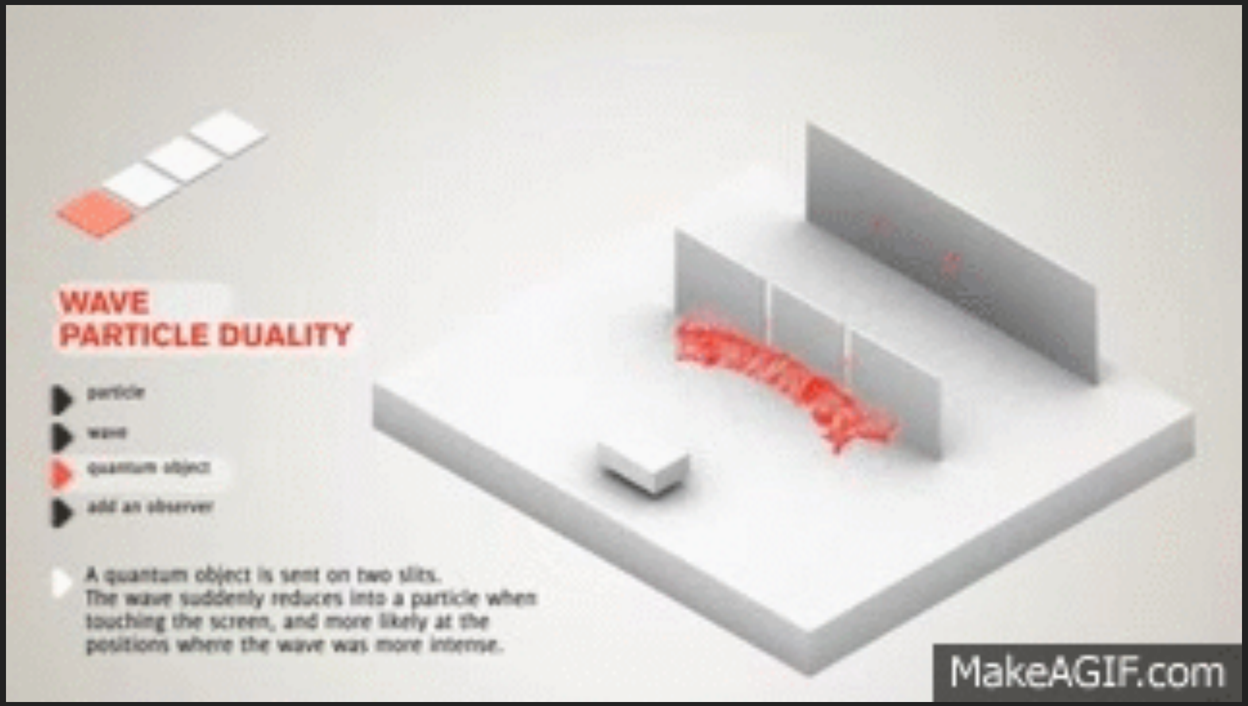
Rotation

DOUBLE SLIT / YOUNG



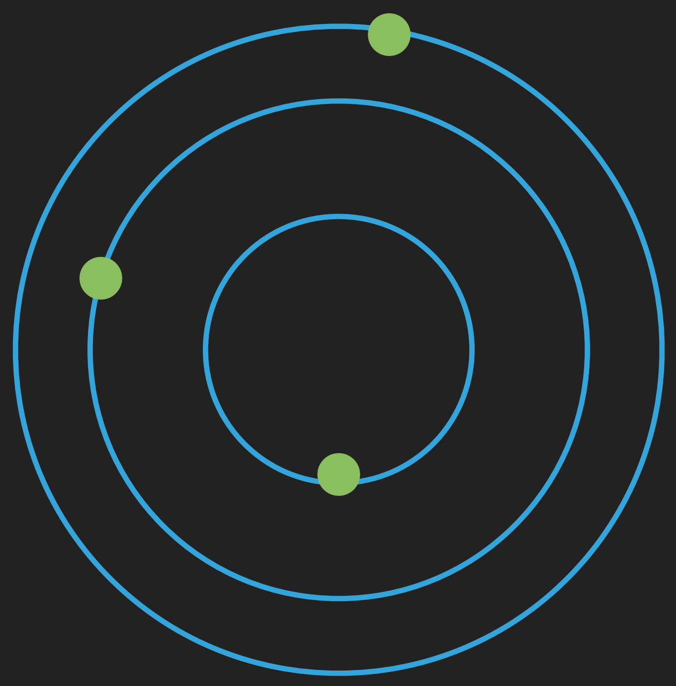
DOUBLE SLIT / YOUNG

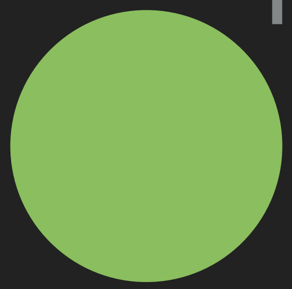




Collapse of the Wave Function

ENTANGLEMENT





n, l, m_l, m_s

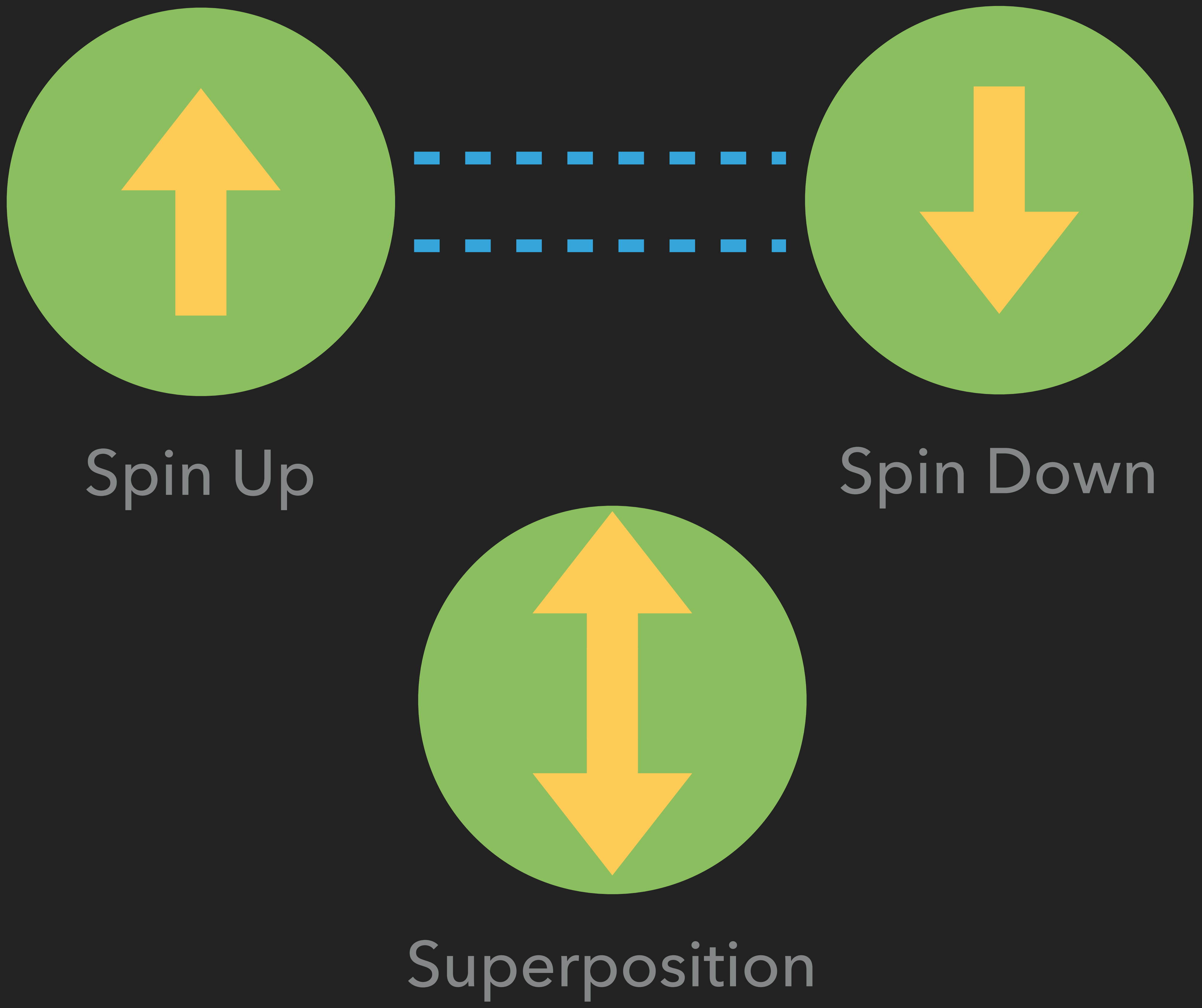
Principal

Orbital Angular Momentum

Magnetic

Electron Spin

ENTANGLEMENT



QUBIT

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

Spin Down

Qubit Down State

Classical Bit 0

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

Spin Up

Qubit Up State

Classical Bit 1

QUBIT

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

P(Spin Down) = 1

P(Spin Up) = 0

$$\begin{bmatrix} p \\ q \end{bmatrix}$$

$$p = a + bi$$

$$|p|^2 = a^2 + b^2$$

$$|p|^2 + |q|^2 = 1$$

SPIN

$$\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

Vector in

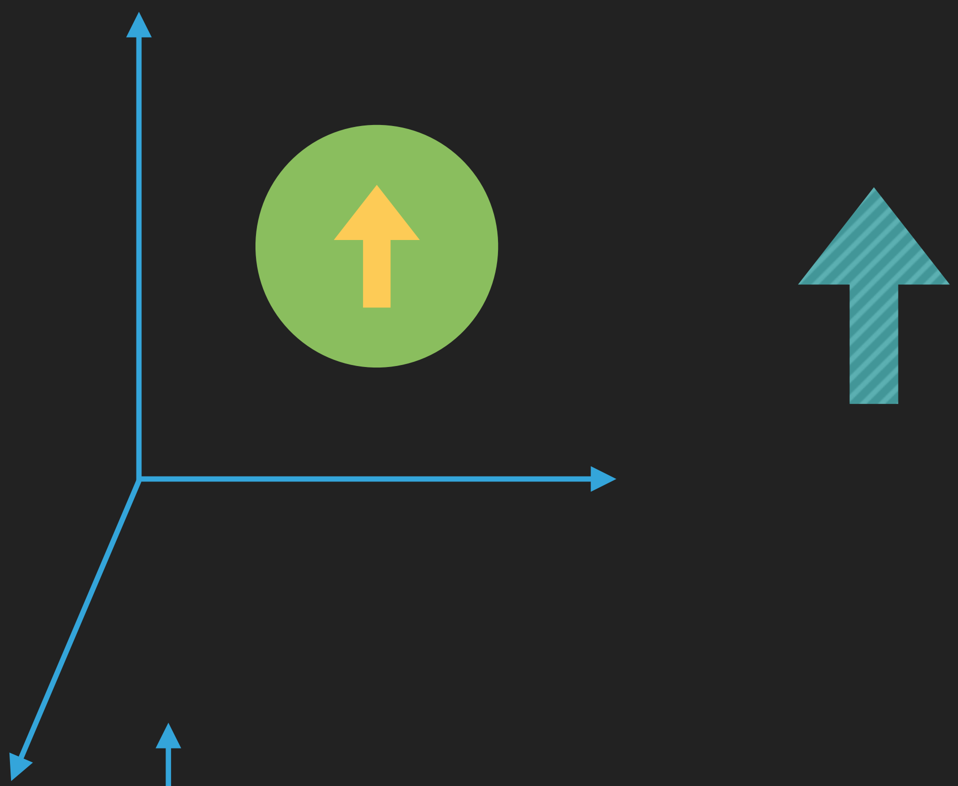
Superposition

$$P(\text{Spin Down}) = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$$

$$P(\text{Spin Up}) = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$$

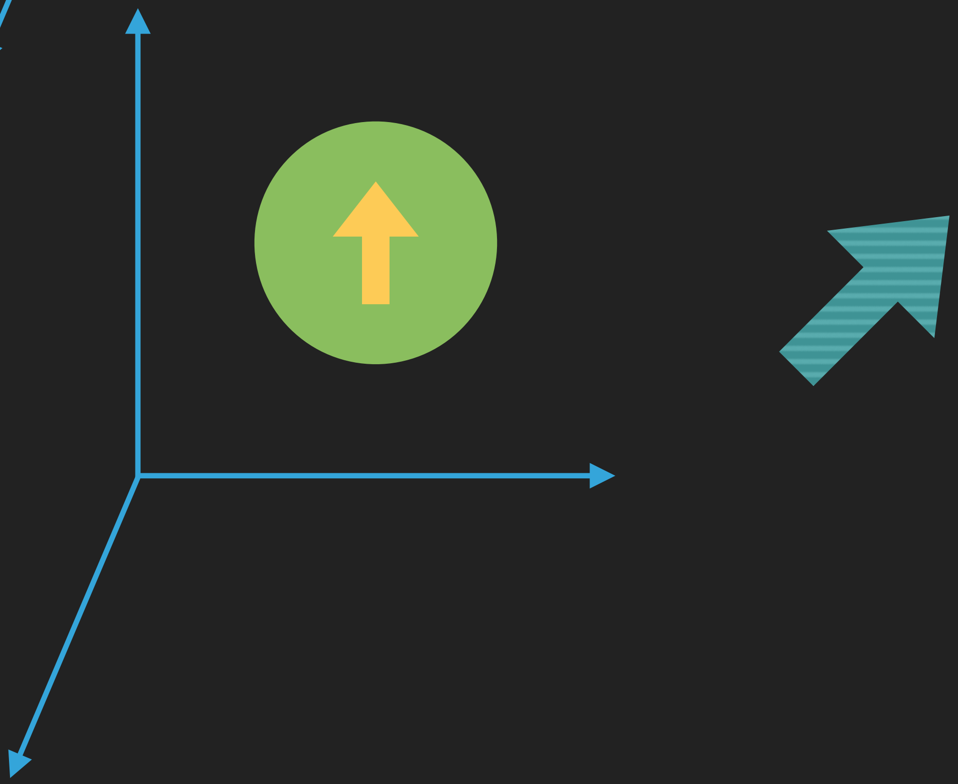
1

SPIN



P(Spin Down) = 0

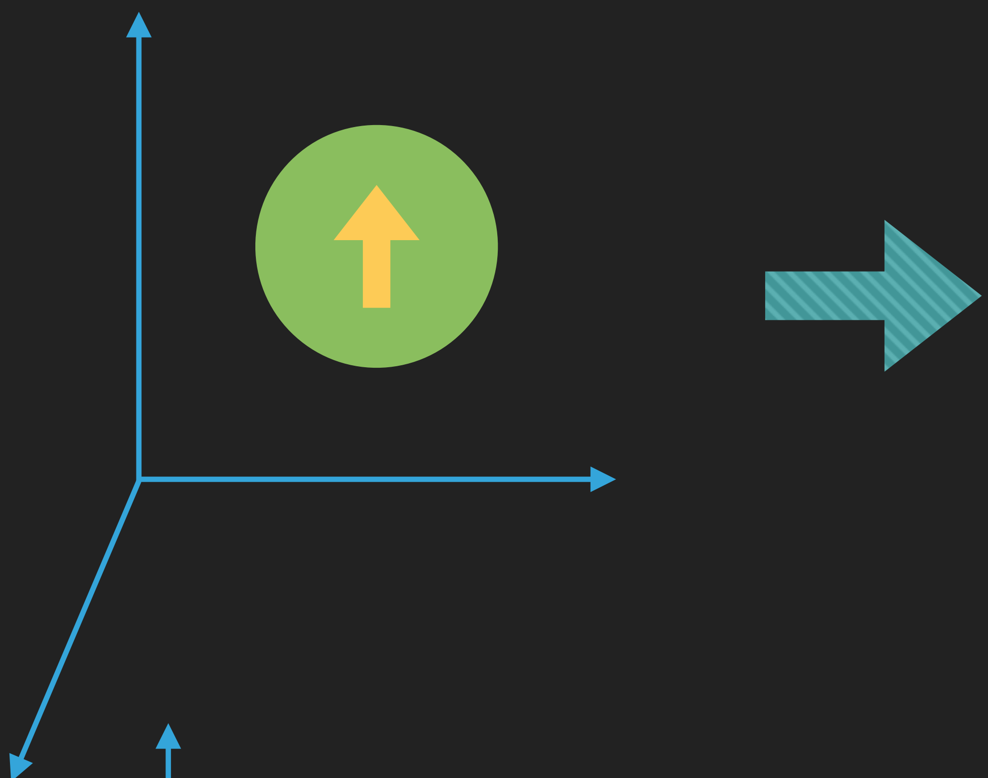
P(Spin Up) = 1



P(Spin Down) = 0.2

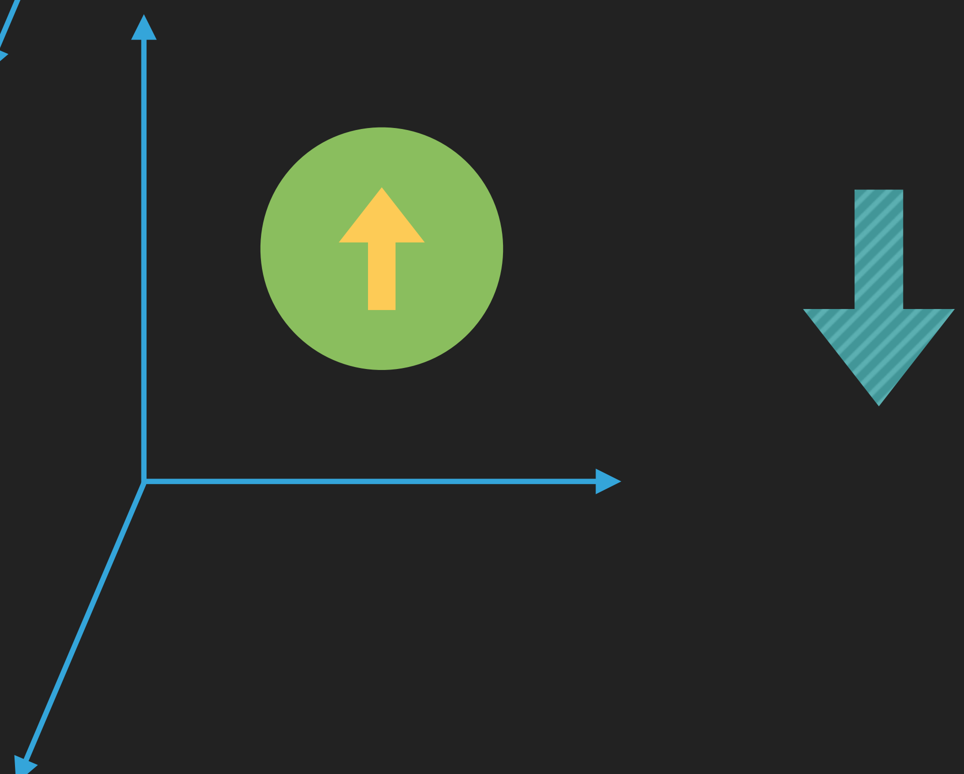
P(Spin Up) = 0.8

SPIN



P(Spin Down) = 0.5

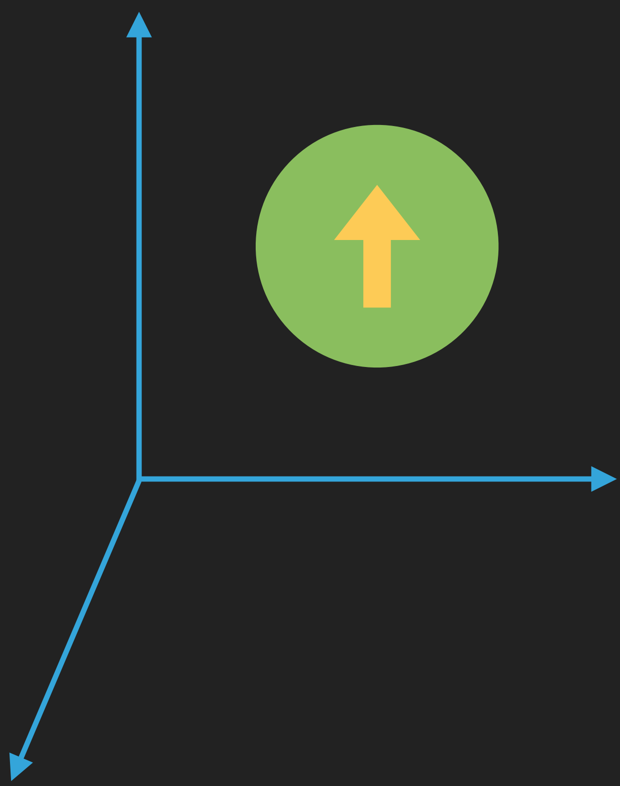
P(Spin Up) = 0.5



P(Spin Down) = 0

P(Spin Up) = 1

SPIN



P(Spin Down) = 0

P(Spin Up) = 1

$$A = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad E = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Inner Product

$$A^{+} * E$$

SPIN

$$A = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad E = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$A^{+} * E$$

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

$$1^2 = 1$$

BRA-KET

$$A = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad E = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$< A \mid E >$ $<A| * |E>$

Bra   Ket A^+ E

$$|1> \quad \begin{bmatrix} 0 \\ 1 \end{bmatrix} \qquad |0> \quad \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

BRA-KET

$$\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$= \frac{1}{\sqrt{2}} \left(|0> + |1> \right)$$

MULTI QUBIT

$$\begin{array}{c c c c c}
0\,0 & \begin{bmatrix}1\\0\\0\\0\end{bmatrix} & \begin{bmatrix}0\\1\\0\\0\end{bmatrix} & \begin{bmatrix}0\\0\\1\\0\end{bmatrix} & \begin{bmatrix}0\\0\\0\\1\end{bmatrix} \\
0\,1 & & & & \\
1\,0 & & & & \\
1\,1 & & & &
\end{array}$$

$$|00> \qquad |01> \qquad |10> \qquad |11>$$

$$|0> \otimes |0> \qquad |0> \otimes |1> \qquad |1> \otimes |0> \qquad |1> \otimes |1>$$

MULTI QUBIT

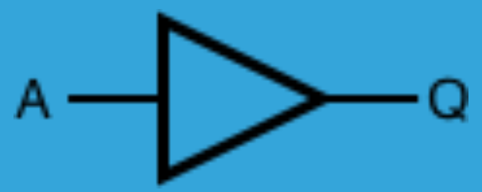
$$\begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

$$\frac{1}{\sqrt{2}} (|00> + |11>)$$

Superposition + Entanglement

CLASSICAL GATES

Buffer



A	Q
0	0
1	1

NOT

A	Q
0	1
1	0

By Inductiveload - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=5729014
By Inductiveload - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=5729018

CLASSICAL GATES

AND

A	B	Q
0	0	0
0	1	0
1	0	0
1	1	1

CLASSICAL GATES

OR

A	B	Q
0	0	0
0	1	1
1	0	1
1	1	1

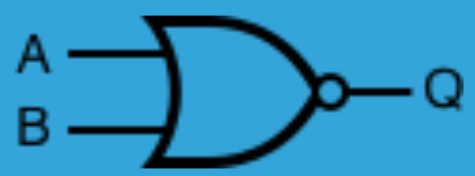
CLASSICAL GATES

NAND

A	B	Q
0	0	1
0	1	1
1	0	1
1	1	0

CLASSICAL GATES

NOR



A	B	Q
0	0	1
0	1	0
1	0	0
1	1	0

By Inductiveload - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=5729017

CLASSICAL GATES

XOR

A	B	Q
0	0	0
0	1	1
1	0	1
1	1	0

CLASSICAL GATES

XNOR

A	B	Q
0	0	1
0	1	0
1	0	0
1	1	1

By Inductiveload - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=5729020

QUANTUM GATES

$$X\ (\mathrm{NOT}) \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

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

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

QUANTUM GATES

Y (Pauli Y) $\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

Z (Pauli Z) $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

QUANTUM GATES

H (Hadamard) $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

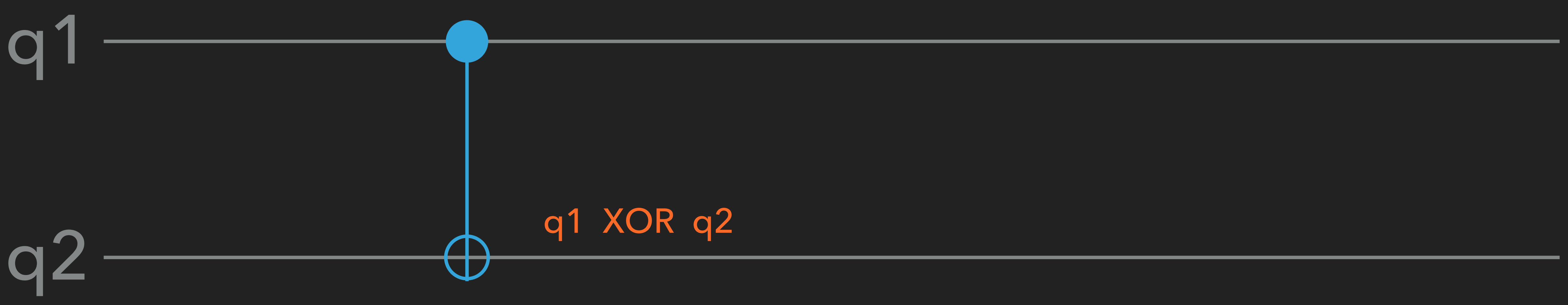
H | 0> $\frac{1}{\sqrt{2}}(|0> + |1>)$

H | 1> $\frac{1}{\sqrt{2}}(|0> - |1>)$

QUANTUM GATES

CNOT

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

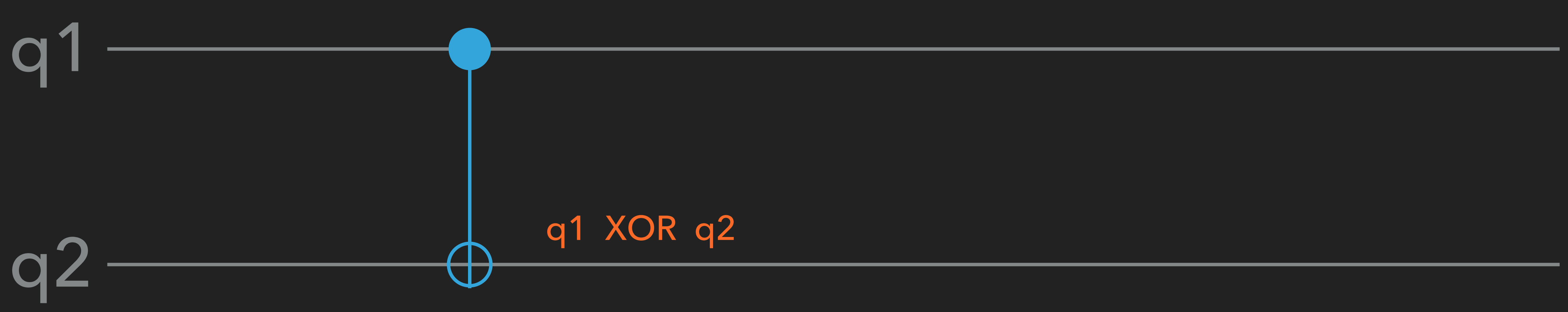


QUANTUM GATES

CNOT

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

Alternative



QUANTUM GATES

CNOT | 00> = |00>

CNOT | 01> = |11>

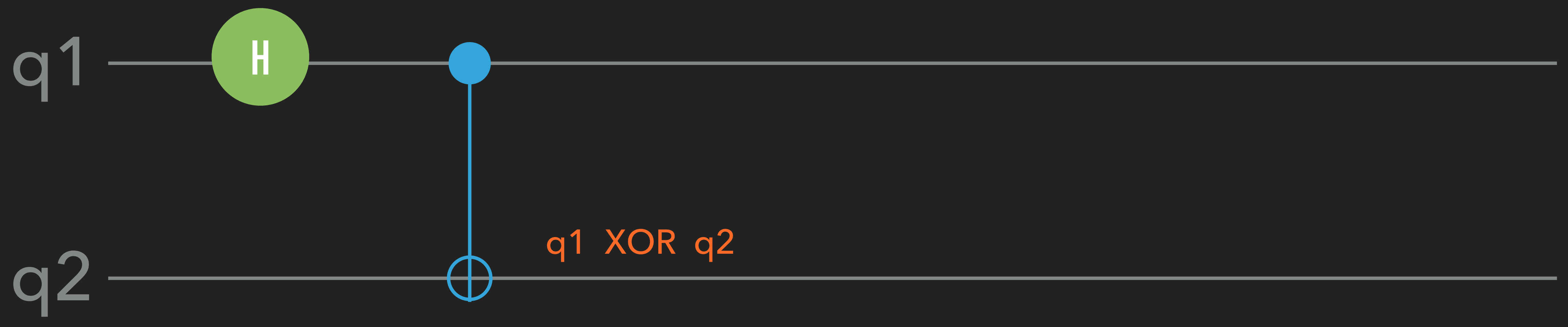
CNOT | 10> = |10>

CNOT | 11> = |01>

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

QUANTUM GATES

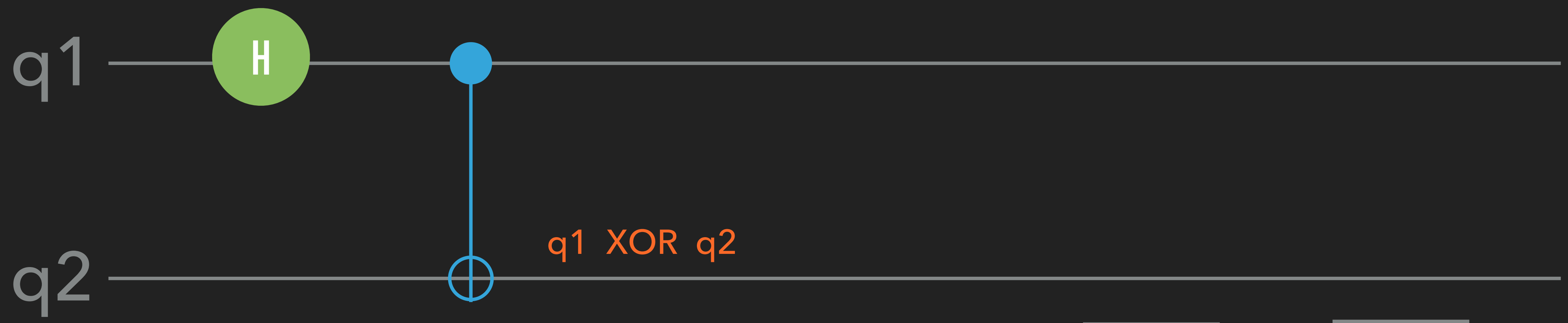
Hadamard & CNOT



$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} * \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

QUANTUM GATES

Hadamard & CNOT

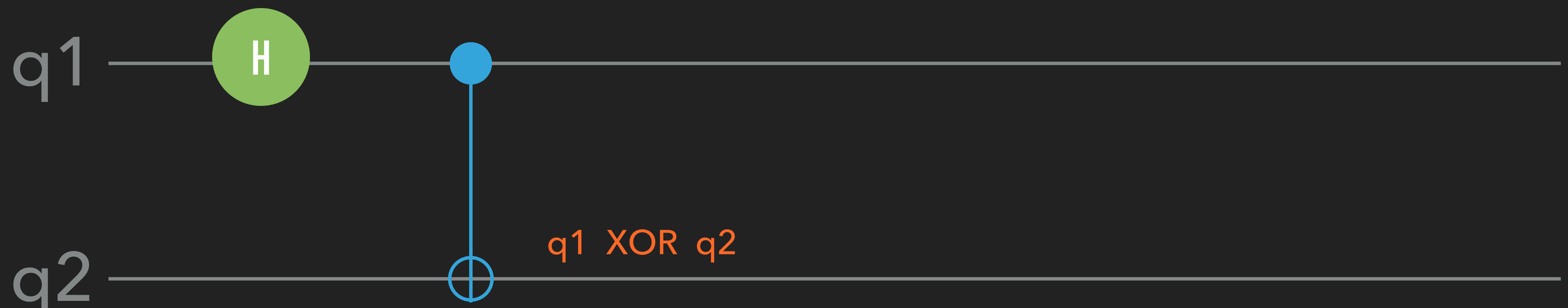


$$\begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{bmatrix} = \begin{bmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\\0\\0\end{bmatrix}$$

$$|0\rangle \otimes |+\rangle = |0+\rangle$$

QUANTUM GATES

Hadamard & CNOT



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

Z GATE

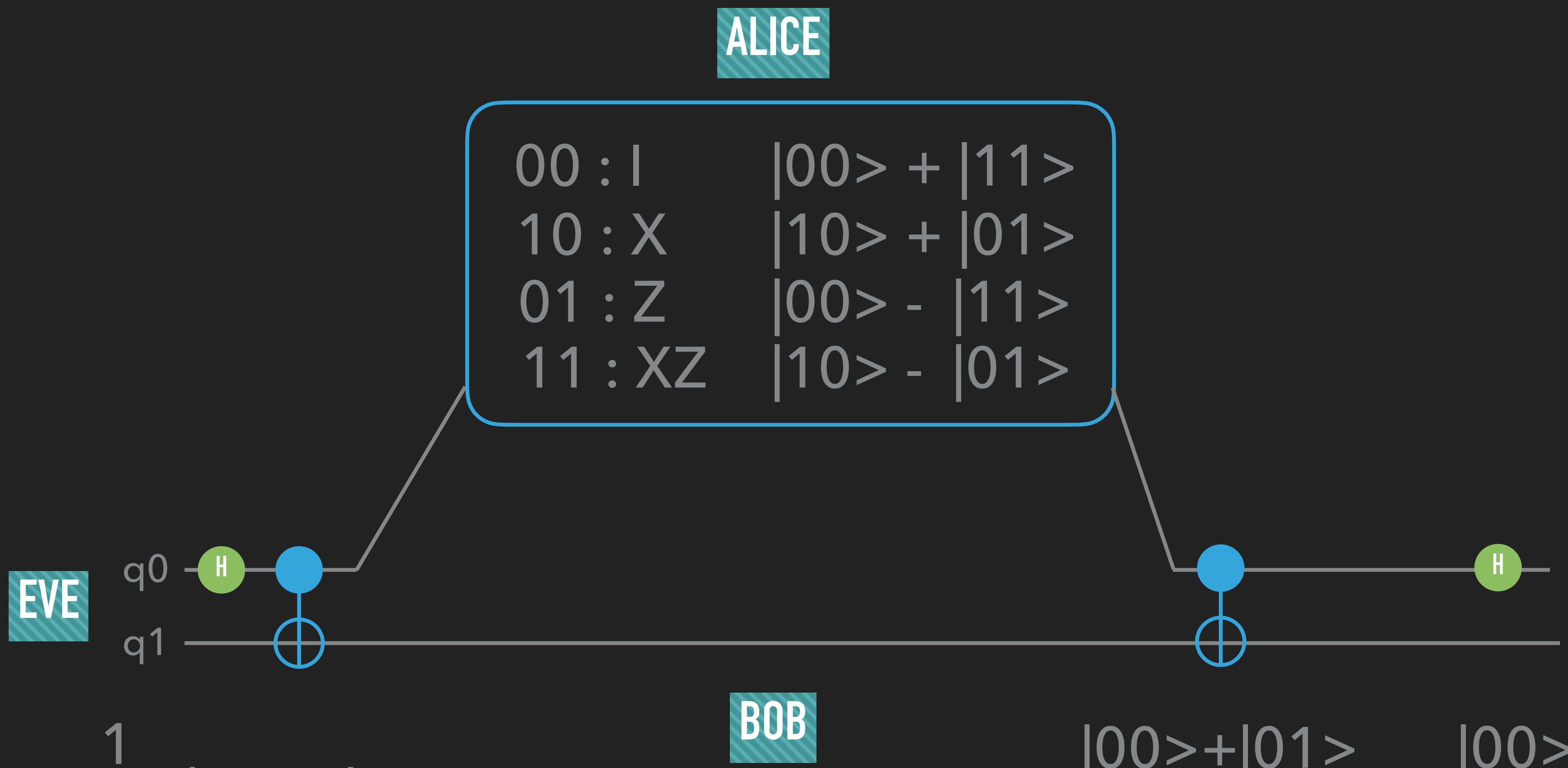
$Z|0\rangle = |0\rangle$

$Z|1\rangle = -|1\rangle$

$$Z\left(\frac{1}{\sqrt{2}}|00\rangle+|11\rangle\right) = \frac{1}{\sqrt{2}}|00\rangle-|11\rangle$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} * \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ -\frac{1}{\sqrt{2}} \end{bmatrix}$$

SUPERDENSE CODING



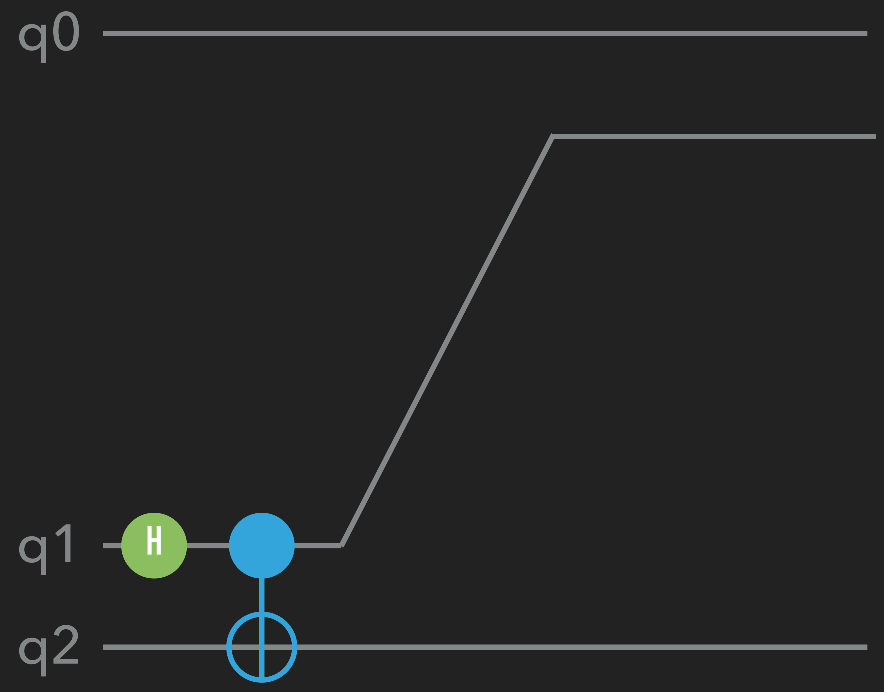
$$\frac{1}{\sqrt{2}} |00\rangle+|11\rangle$$

$\|00\rangle+\|01\rangle$	$\|00\rangle$
$\|10\rangle+\|11\rangle$	$\|10\rangle$
$\|00\rangle-\|01\rangle$	$\|01\rangle$
$\|10\rangle-\|11\rangle$	$\|11\rangle$

QUANTUM TELEPORTATION

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

ALICE



$\frac{1}{\sqrt{2}} |00\rangle + |11\rangle$

BOB

TOTAL QUANTUM STATE

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \otimes \frac{1}{\sqrt{2}} |00\rangle + |11\rangle$$

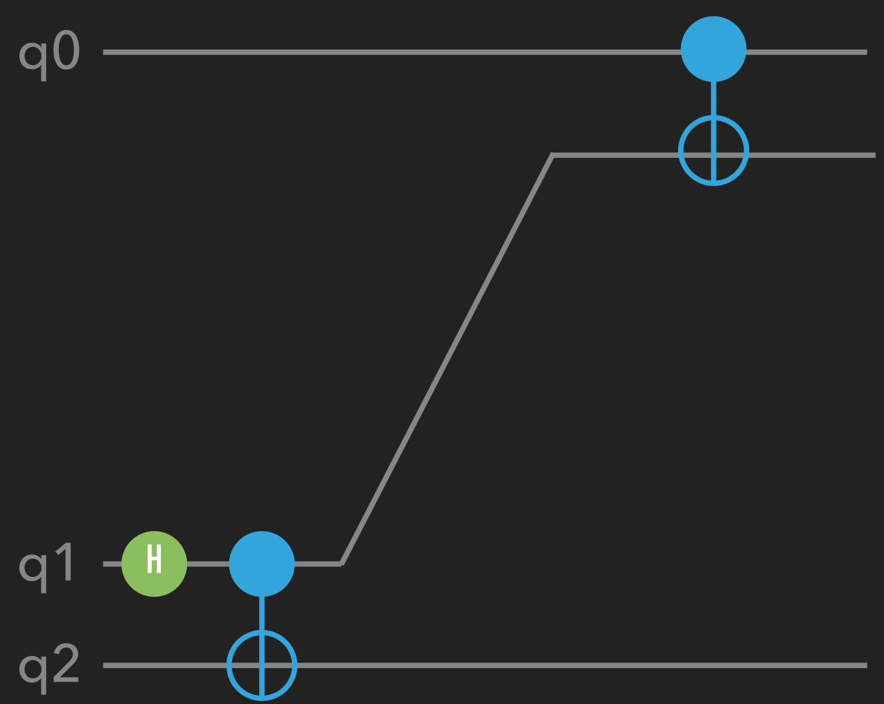
$$=$$

$$\frac{1}{\sqrt{2}} [\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle]$$

QUANTUM TELEPORTATION

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

ALICE



$$\frac{1}{\sqrt{2}} |00\rangle + |11\rangle$$

BOB

TOTAL QUANTUM STATE

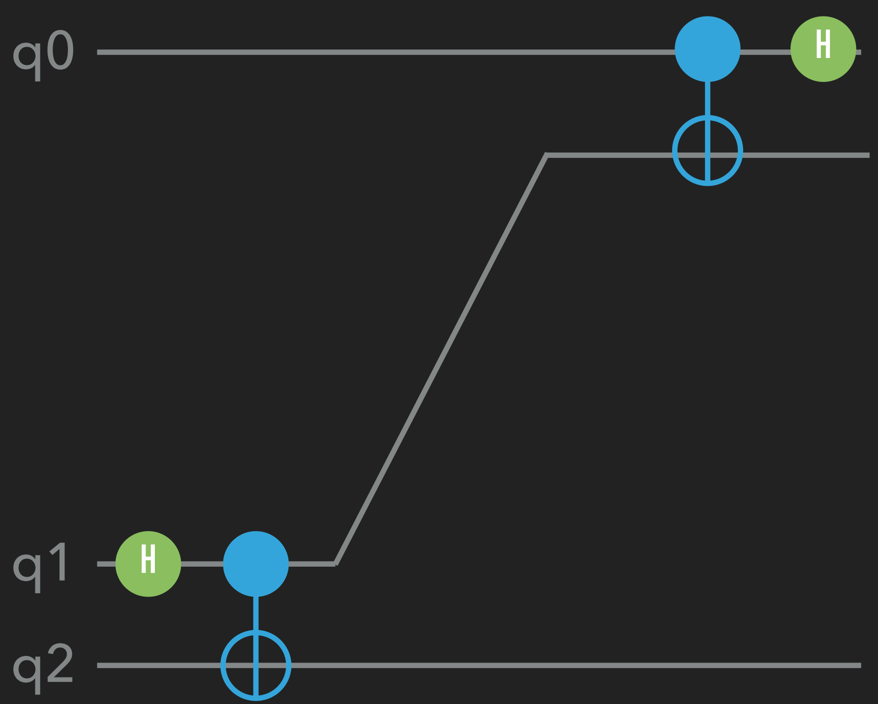
$$\frac{1}{\sqrt{2}} [\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle]$$

$$\frac{1}{\sqrt{2}} [\alpha|000\rangle + \alpha|011\rangle + \beta|101\rangle + \beta|110\rangle]$$

QUANTUM TELEPORTATION

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

ALICE



$\frac{1}{\sqrt{2}} |00\rangle + |11\rangle$

BOB

TOTAL QUANTUM STATE

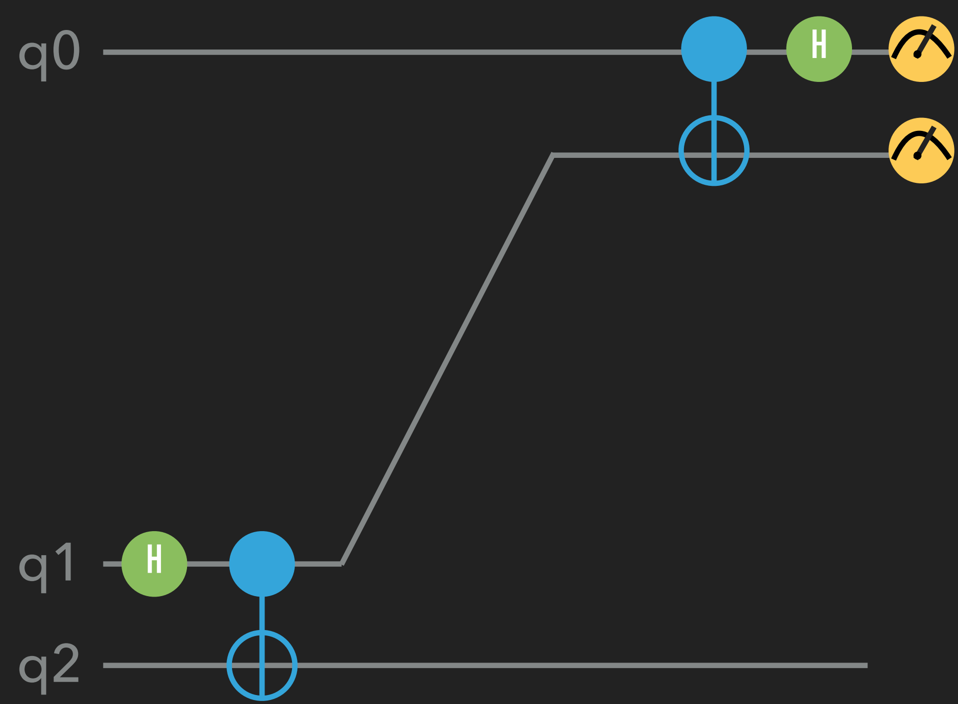
$$\frac{1}{\sqrt{2}} [\alpha|000\rangle + \alpha|011\rangle + \beta|101\rangle + \beta|110\rangle]$$

$$\frac{1}{\sqrt{2}} [\alpha|000\rangle + \alpha|011\rangle + \alpha|100\rangle + \alpha|111\rangle + \beta|001\rangle + \beta|010\rangle - \beta|101\rangle - \beta|110\rangle]$$

QUANTUM TELEPORTATION

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

ALICE



$$\frac{1}{\sqrt{2}}\,|00\rangle + |11\rangle$$

BOB

MEASUREMENT

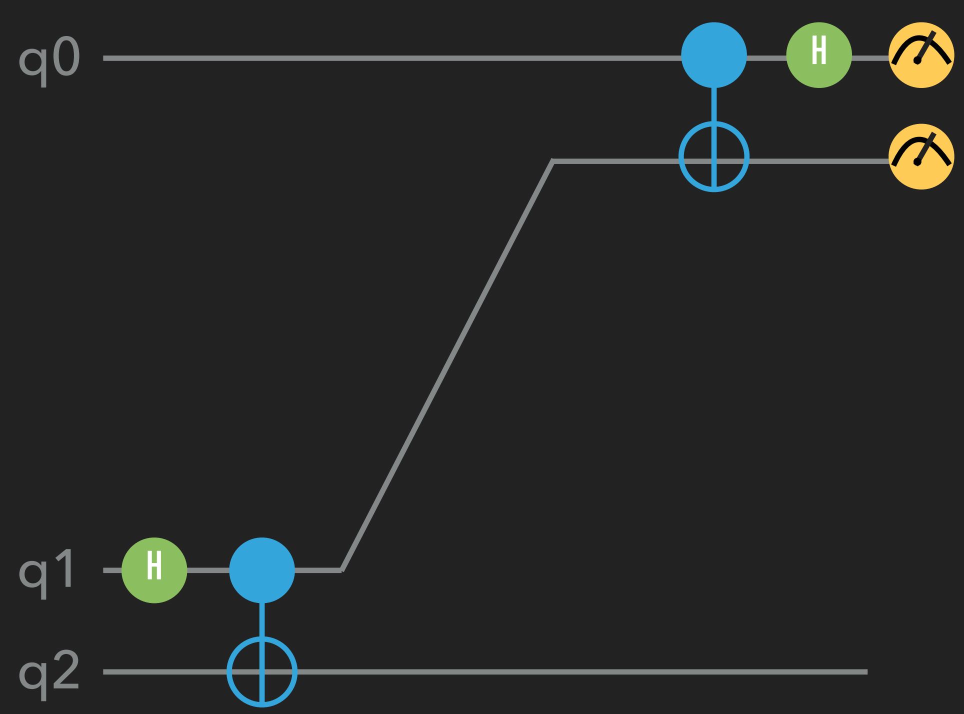
$$\frac{1}{\sqrt{2}}\big[\alpha|000\rangle + \alpha|011\rangle + \alpha|100\rangle + \alpha|111\rangle + \beta|001\rangle + \beta|010\rangle - \beta|101\rangle - \beta|110\rangle\big]$$

Q0,Q1	00	01	10	11
Q2	$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|1\rangle + \beta\|0\rangle$	$\alpha\|0\rangle - \beta\|1\rangle$	$\alpha\|1\rangle - \beta\|0\rangle$

QUANTUM TELEPORTATION

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

ALICE



$$\frac{1}{\sqrt{2}} |00\rangle + |11\rangle$$

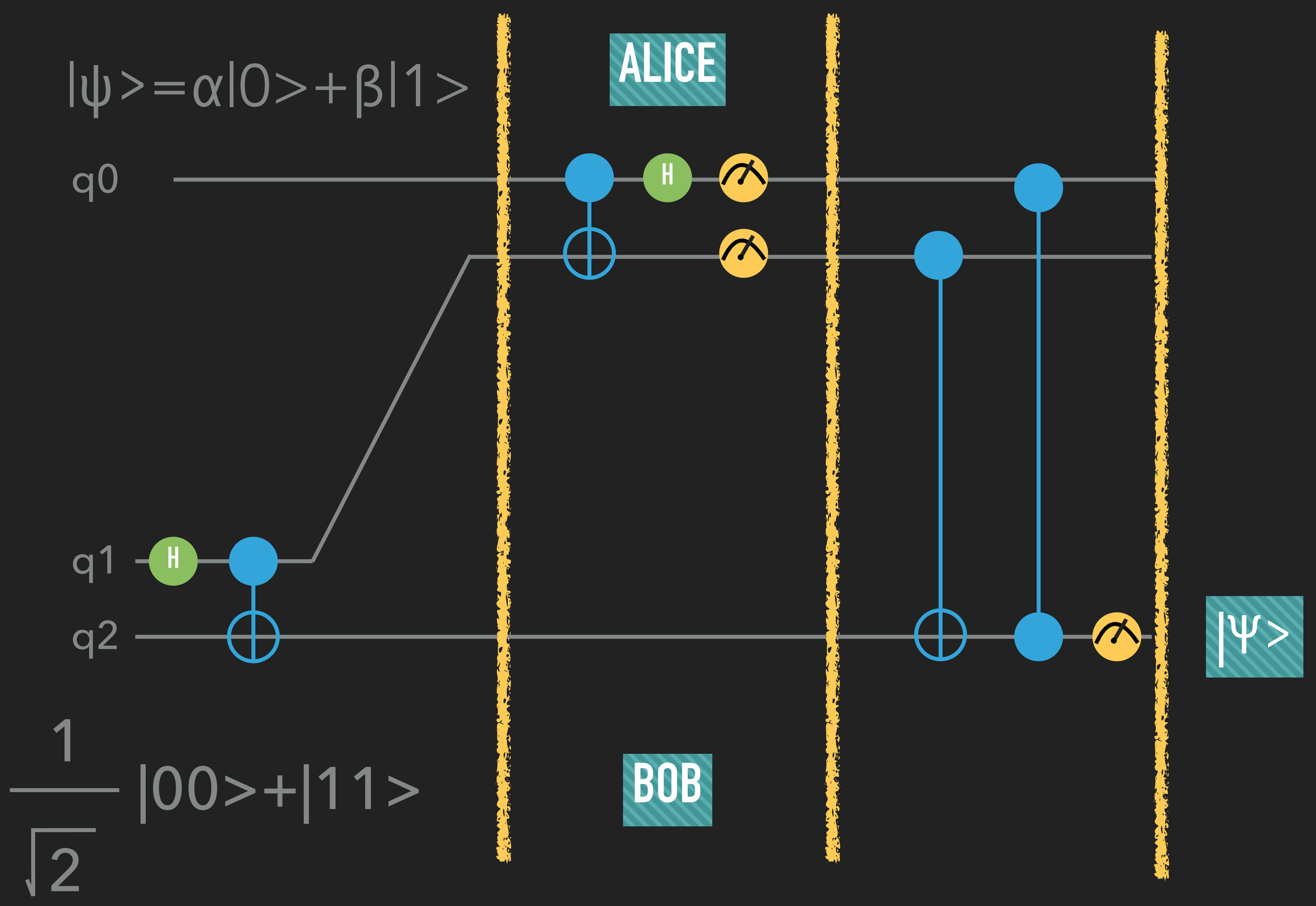
BOB

MEASUREMENT

$$\frac{1}{\sqrt{2}} [\alpha|000\rangle + \alpha|011\rangle + \alpha|100\rangle + \alpha|111\rangle + \beta|001\rangle + \beta|010\rangle - \beta|101\rangle - \beta|110\rangle]$$

Q0,Q1	00	01	10	11
Q2	$\alpha|0\rangle+\beta|1\rangle$	$\alpha|1\rangle+\beta|0\rangle$	$\alpha|0\rangle-\beta|1\rangle$	$\alpha|1\rangle-\beta|0\rangle$
	I	X	Z	XZ

QUANTUM TELEPORTATION



BERNSTEIN - VAZIRANI ALGORITHM

1011001

AND

0000001

1

1011001

AND

0000010

0

N BITS

DEUTSCH ALGORITHM

	f(0)	f(1)	
1	0	0	Constant
2	0	1	Balanced
3	1	0	Balanced
4	1	1	Constant

f : {0,1} -> {0,1}

f(0) = f(1) Constant

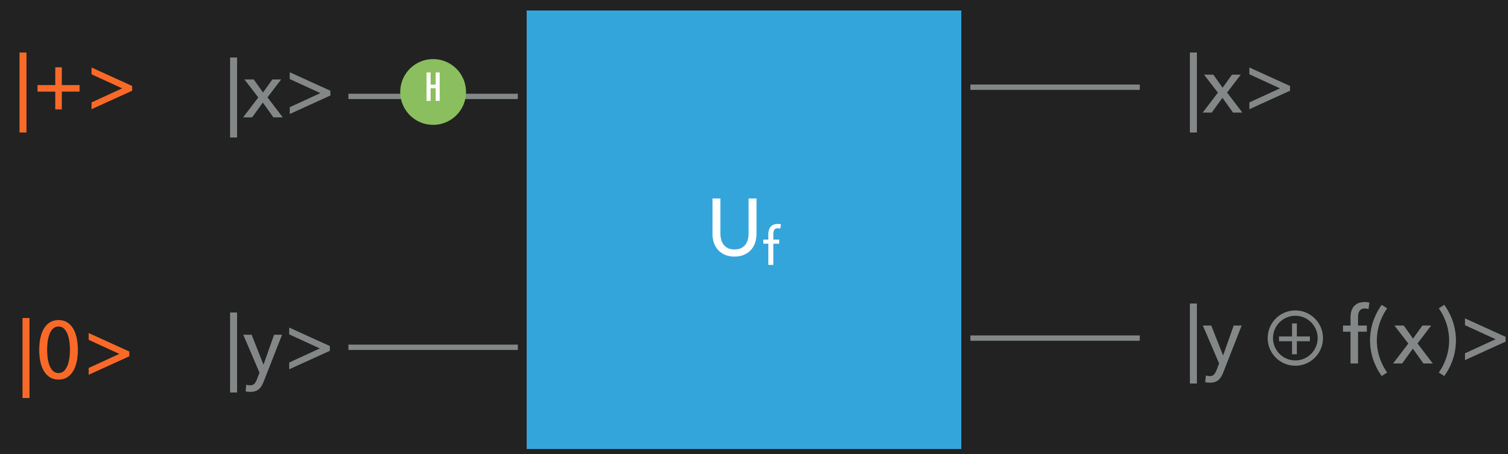
DEUTSCH ALGORITHM

$$|x> |y> \xrightarrow{U_f} |x> |y \oplus f(x)> \xrightarrow{U_f} |x> |y \oplus f(x)> \oplus f(x)>$$

$$|x> |y \oplus 0>$$

$$|x> |y>$$

DEUTSCH ALGORITHM



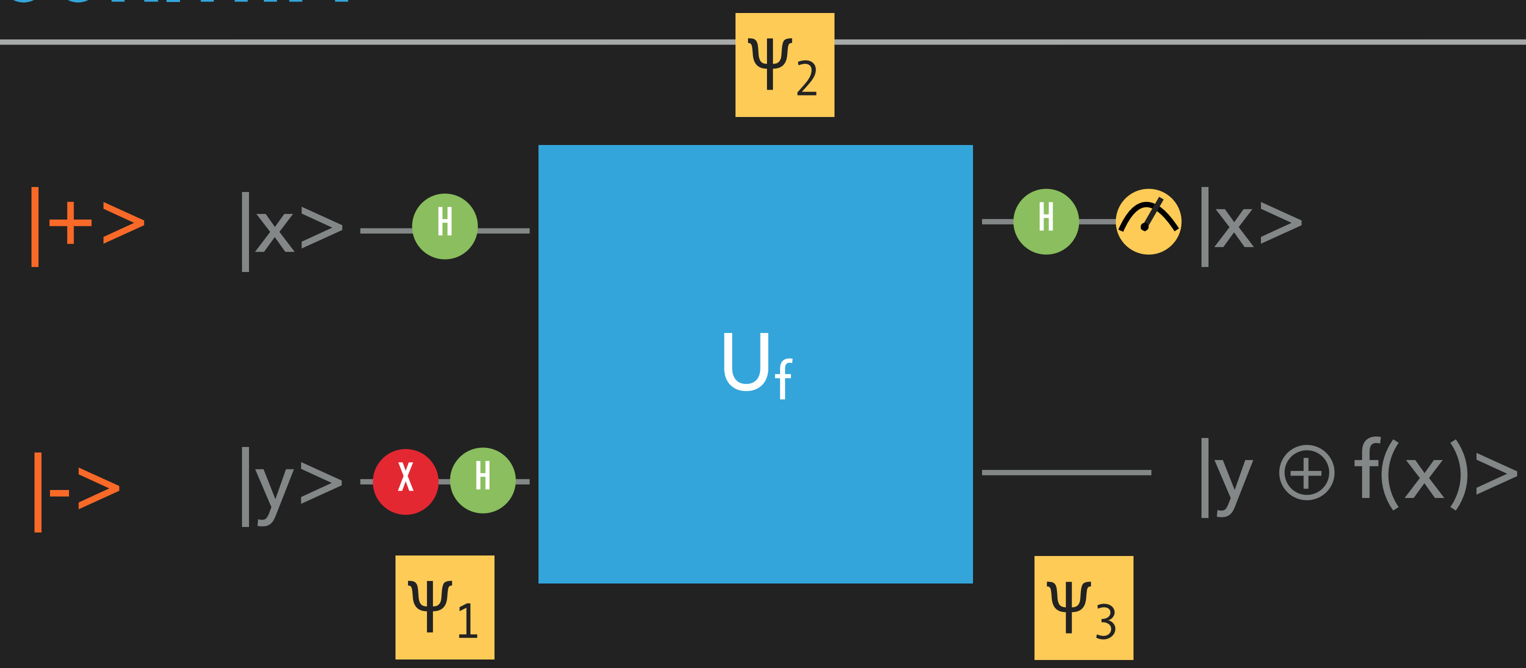
$$U_f(|+>\otimes|0>) \longrightarrow U_f\left(\frac{1}{\sqrt{2}}(|0>+|1>)\otimes|0>\right)$$

$$= \frac{1}{\sqrt{2}} U_f\,|0>\otimes|0>) + \frac{1}{\sqrt{2}} U_f\,|1>\otimes|0>)$$

$$= \frac{1}{\sqrt{2}} |0>\,f(0)\oplus|0> + \frac{1}{\sqrt{2}} |1>\,f(1)\oplus|0>$$

$|0>\,f(0)$ $|1>\,f(1)$

DEUTSCH ALGORITHM



|+> |->

$$= \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle)$$

Ψ_1

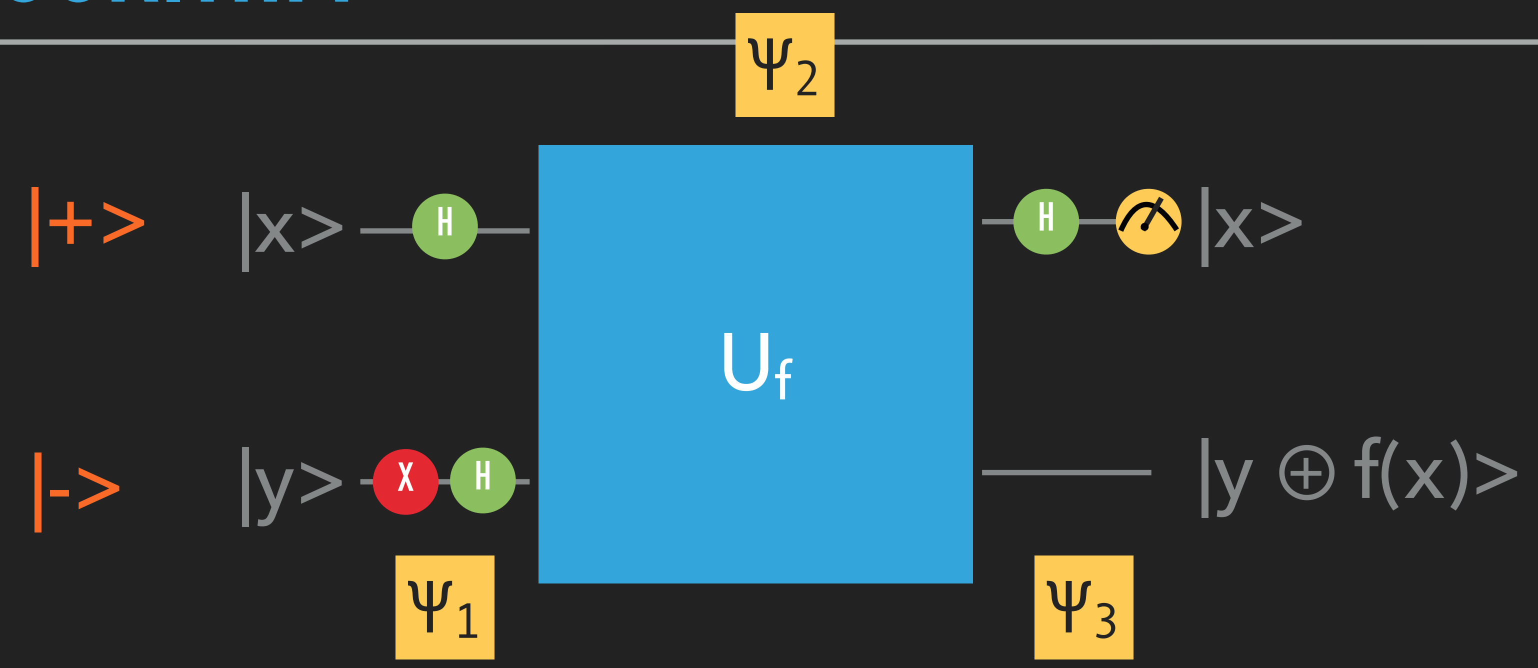
$$= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

$$\rightarrow \frac{1}{2}(|0\rangle |0 \oplus f(0)\rangle - |0 |1 \oplus f(0)\rangle + |1\rangle |0 \oplus f(1)\rangle - |1\rangle |1 \oplus f(1)\rangle)$$

Ψ_2

$$= \frac{1}{2}(|0\rangle |f(0)\rangle - |0 |1 \oplus f(0)\rangle + |1\rangle | f(1)\rangle - |1\rangle |1 \oplus f(1)\rangle)$$

DEUTSCH ALGORITHM



$$\Psi_2 = \frac{1}{2}(|0\rangle|f(0)\rangle - |0|1 \oplus f(0)\rangle + |1\rangle|f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle)$$

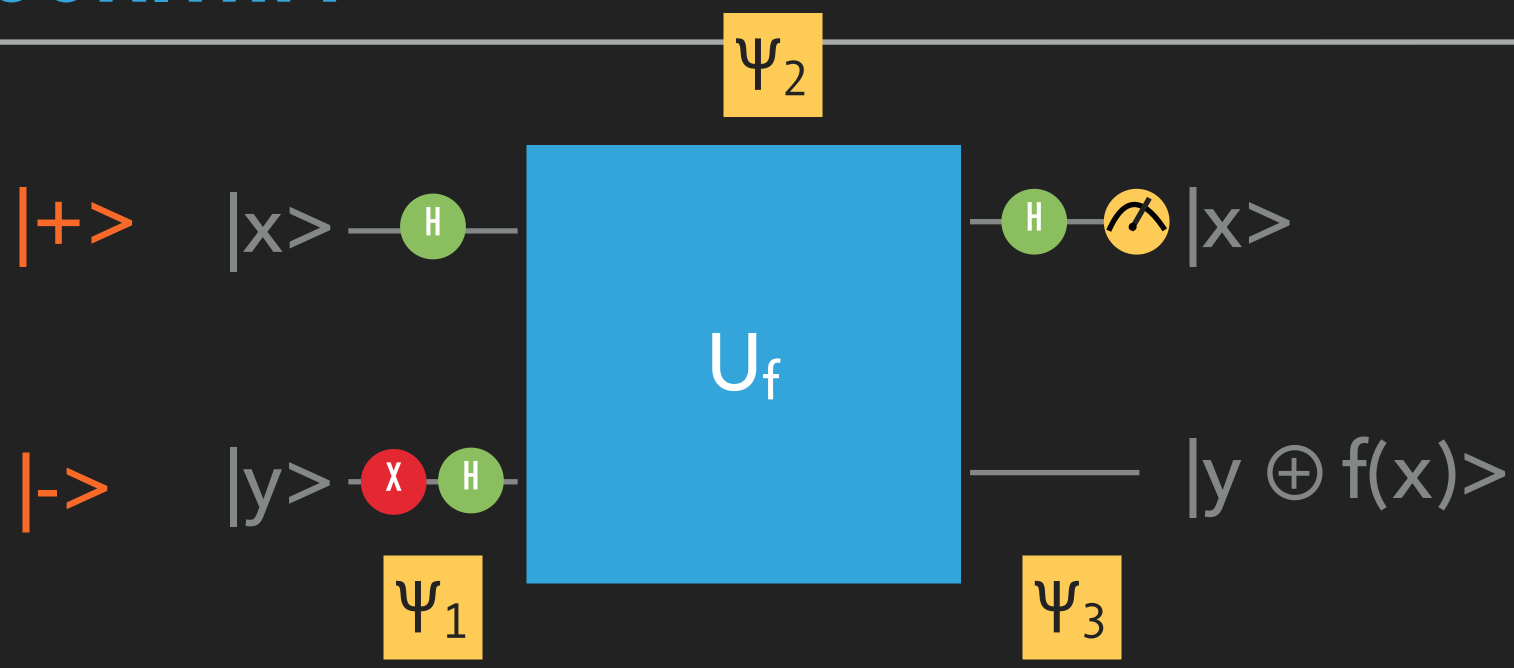
-> **IF F(0) = F(1) (CONSTANT)**

$$= \frac{1}{2}(|0\rangle|f(0)\rangle - |0|1 \oplus f(0)\rangle + |1\rangle|f(0)\rangle - |1\rangle|1 \oplus f(0)\rangle)$$

$$= \frac{1}{2}((|0\rangle+|1\rangle)|f(0)\rangle) + (-|0\rangle-|1\rangle)|1 \oplus f(0)\rangle$$

$$= \frac{1}{2}(|0\rangle+|1\rangle)(|f(0)\rangle- |1 \oplus f(0)\rangle$$

DEUTSCH ALGORITHM

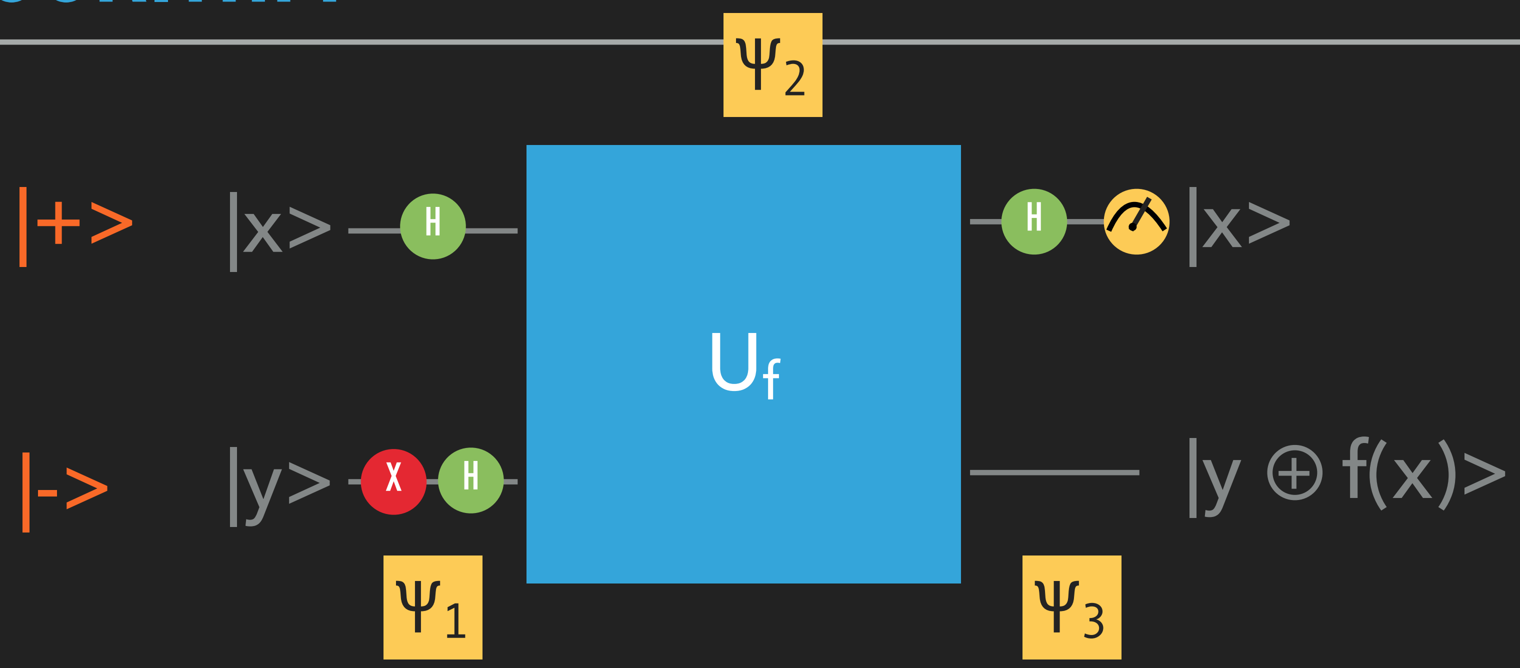


$$\Psi_2 = \frac{1}{2} (|0\rangle + |1\rangle)\ (|f(0)\rangle - |1 \oplus f(0)\rangle$$

$$= \frac{1}{\sqrt{2}} (|+\rangle)\ (|f(0)\rangle - |1 \oplus f(0)\rangle$$

$$\Psi_3 \quad H(|+\rangle) = |0\rangle$$

DEUTSCH ALGORITHM



$$\Psi_2 = \frac{1}{2}\left(|0\rangle\,|f(0)\rangle - |0\;|1 \oplus f(0)\rangle + |1\rangle\,|f(1)\rangle - |1\rangle\,|1 \oplus f(1)\rangle\right)$$

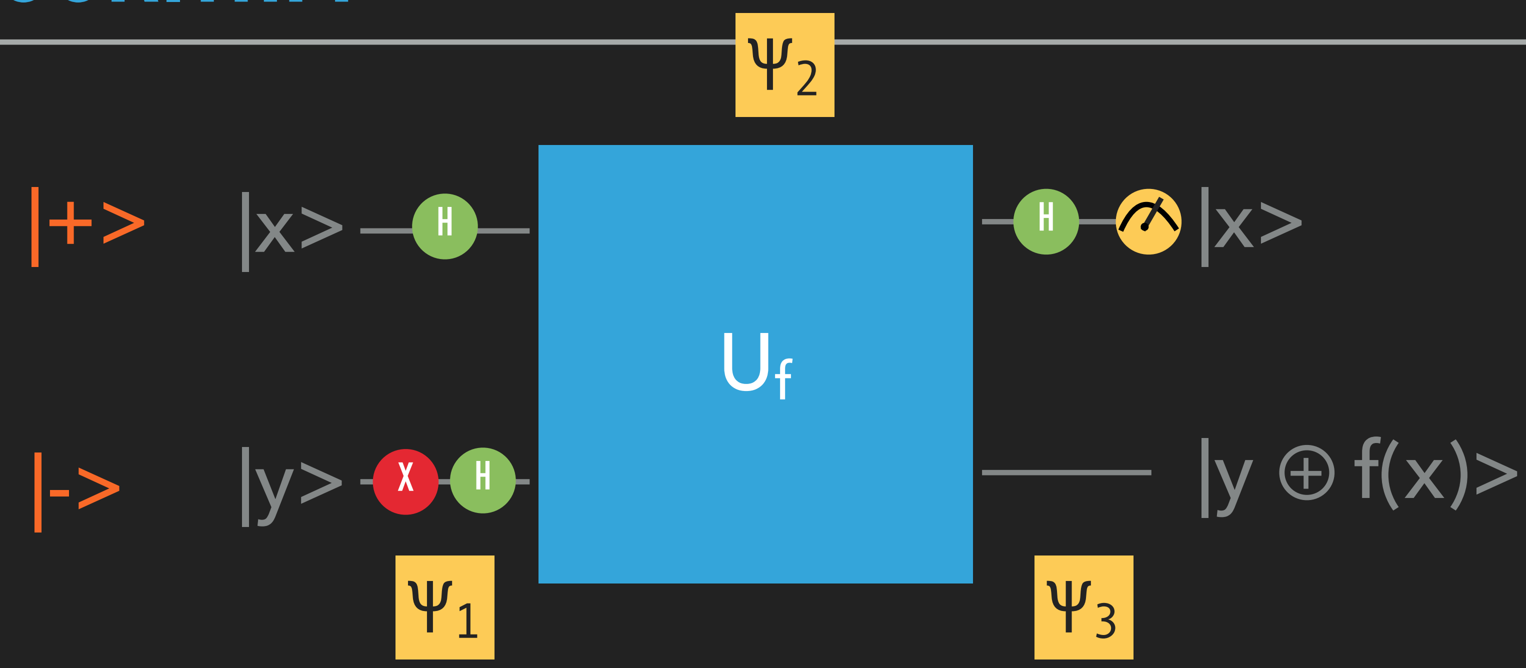
-> **IF F(0) != F(1) (BALANCED)** **F(0) = F(1) XOR 1**

$$= \frac{1}{2}\left(|0\rangle\,|f(0)\rangle - |0\rangle\,|f(1)\rangle + |1\rangle\,|f(1)\rangle - |1\rangle\,|f(0)\rangle\right)$$

$$= \frac{1}{2}\left(|0\rangle \otimes (|f(0)\rangle - |f(1)\rangle) - |1\rangle \otimes (|f(0)\rangle - |f(1)\rangle)\right)$$

$$= \frac{1}{2}\left(|0\rangle - |1\rangle\right) \otimes \left(|f(0)\rangle - |f(1)\rangle\right)$$

DEUTSCH ALGORITHM



$$\Psi_2 = \frac{1}{2}(|0\rangle - |1\rangle) \otimes (|f(0)\rangle - |f(1)\rangle)$$

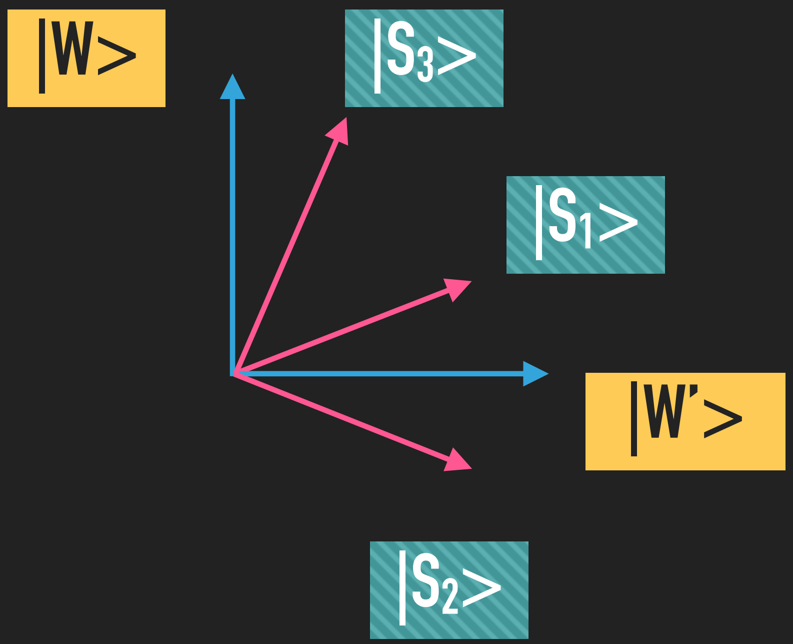
$$= \frac{1}{\sqrt{2}}(|-\rangle) \otimes (|f(0)\rangle - |f(1)\rangle)$$

$$\Psi_3 \quad H(|-\rangle) = |1\rangle$$

GROVERS ALGORITHM

$$|W\rangle \quad \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \qquad |W'\rangle \quad \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

$$|S_1\rangle \quad \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \qquad |S_2\rangle \quad \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix}$$



DINNER PARTY

JAMES AND LARS

OR

KIRK AND ROB

AND NOT

LARS AND ROB

DINNER PARTY

SHOR'S ALGORITHM

PRIME FACTORS

$N = 60 = 2^2 * 3 * 5$

$n = \text{len}(N)$

$N = P * Q$

$O(2^n)$

MODULAR ARITHMETIC

$3 = 26 \pmod{23}$

$20 = 43 \pmod{23}$

$1 = 24 \pmod{23}$

$22 = -1 \pmod{23}$

$46 + 18 \pmod{23}$

$= 0 + 18 \pmod{23}$

$46 * 18 \pmod{23}$

$= 0 * 18 \pmod{23}$

SHOR'S ALGORITHM

GCD

$$\gcd(15,21) = 3$$

$$3 * 5 \qquad 3 * 7$$

FIND PRIME FACTORS OF 21

$$N = 21$$

$$x^2 = 1 \pmod{21}$$

$$x ?\ 1, -1, 8, -8, 13, 20, -20$$

$$8^2 - 1^2 = 0 \pmod{21}$$

$$(8 - 1) * (8 + 1)$$

SHOR'S ALGORITHM

$$(8 - 1) * (8 + 1)$$

$$\gcd(21, 8+1) = 3$$

$$\gcd(21, 8-1) = 7$$

GENERAL RULE

$$x \neq \pm 1 \pmod{N}$$

$$x^2 = 1 \pmod{N}$$

$$\gcd(N, x+1)$$

SHOR'S ALGORITHM

$N = 21$

$x = 2$ (random #)

$x^6 = (x^3)^2 = 1 \pmod{21}$

50% PROBABILITY

$2^1 = 2 \pmod{21}$

$2^2 = 4 \pmod{21}$

$2^3 = 8 \pmod{21}$

$2^4 = 16 \pmod{21}$

$2^5 = 11 \pmod{21}$

$2^6 = 1 \pmod{21}$

$2^7 = 2 \pmod{21}$

$2^8 = 4 \pmod{21}$

SHOR'S ALGORITHM

Quantum Fourier Transform (QFT)

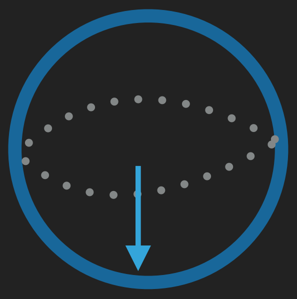
Modular Exponentiation - Quantum Phase Estimation

QUANTUM FOURIER TRANSFORM: Computational Basis -> Fourier Basis

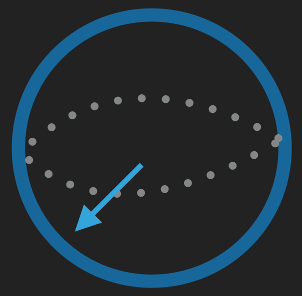
1 QUBIT {|0>, |1>} {|+>, |->}

|0>

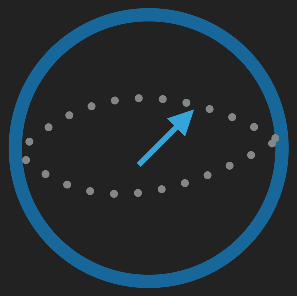
|1>



|+>



|->



SHOR'S ALGORITHM

QUANTUM FOURIER TRANSFORM: Computational Basis -> Fourier Basis

2 QUBIT {|00>, |10>, |01>, |11>}

$$QFT\,|x\rangle = |\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2*pi*i*x*y}{N}} |y\rangle$$

Note: $e^{pi*i} = -1$

$N = 2^n$

n = # Qubits

https://www.youtube.com/watch?v=v0YEaeIClKY

SHOR'S ALGORITHM

$$\text{QFT } |x\rangle = |\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2*pi*i*x*y}{N}} |y\rangle$$

QUANTUM FOURIER TRANSFORM:

1 QUBIT

$$N = 2^1$$

$$= \frac{1}{\sqrt{2}} \sum_{y=0}^{2-1} e^{\frac{2*pi*i*x*y}{2}} |y\rangle$$

$$= \frac{1}{\sqrt{2}} e^{\frac{2*pi*i*x*0}{2}} |0\rangle + \frac{1}{\sqrt{2}} e^{\frac{2*pi*i*x*1}{2}} |1\rangle$$

SHOR'S ALGORITHM

$$= \frac{1}{\sqrt{2}} e^{\frac{2*pi*i*x*0}{2}} |0> + \frac{1}{\sqrt{2}} e^{\frac{2*pi*i*x*1}{2}} |1>$$

$$= \frac{1}{\sqrt{2}} |0> + \frac{1}{\sqrt{2}} e^{pi*i*x} |1>$$

if (x = 0):

$$\frac{1}{\sqrt{2}} |0> + |1>$$

|+>

if (x = 1):

$$\frac{1}{\sqrt{2}} |0> - |1>$$

|->

SHOR'S ALGORITHM

$$QFT|x\rangle = |\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2*pi*i*x*y}{N}} |y\rangle \qquad N = 2^n$$

$$y = [y_1, y_2, y_3, \ldots, y_n]$$

$$|0\rangle, |1\rangle, |2\rangle, |3\rangle\ ?$$

$$|2\rangle = |10\rangle$$

$$= 2^{n-1} * y_1 + 2^{n-2} * y_2 + \ldots. + 2^0 * y_n$$

$$y = \sum_{k=0}^{n} y_k\, 2^{n-k}$$

SHOR'S ALGORITHM

$$\text{QFT}\,|x\rangle = |\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2*pi*i*x*y}{N}} |y\rangle \qquad N = 2^n$$

$$y = \sum_{k=0}^{n} y_k\, 2^{n-k}$$

$$\text{QFT}\,|x\rangle = |\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2*pi*i*x*\sum_{k=0}^{n} \frac{y_k}{2^k}} |y_1, y_2, y_3, \ldots, y_n\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \prod_{k=1}^{n} e^{\frac{2*pi*i*x*y_k}{2^k}} |y_1, y_2, y_3, \ldots, y_n\rangle$$

SHOR'S ALGORITHM

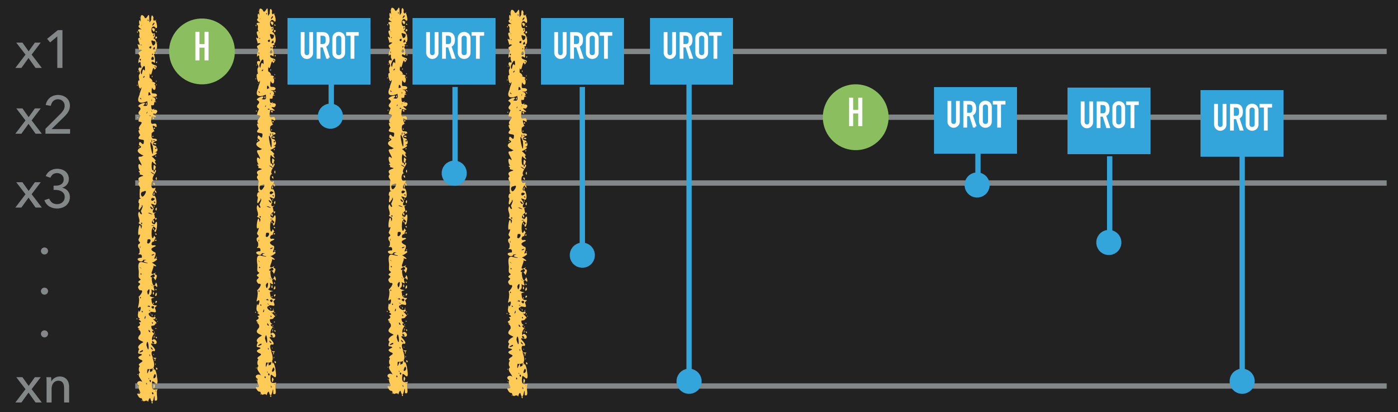
$$= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \prod_{k=1}^{n} e^{\frac{2*pi*i*x*y_k}{2^k}} |y_1, y_2, y_3, \ldots, y_n>$$

$$= \frac{1}{\sqrt{N}} (|0> + e^{\frac{2*pi*i*x}{2^1}} |1>) \otimes (|0> + e^{\frac{2*pi*i*x}{2^2}} |1>) \otimes$$

$$(|0> + e^{\frac{2*pi*i*x}{2^3}} |1>) \otimes \cdots\cdots\cdots \otimes (|0> + e^{\frac{2*pi*i*x}{2^n}} |1>)$$

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2*pi*i}{2^k}} \end{bmatrix}$$

SHOR'S ALGORITHM



$$= \; |x_1x_2x_3x_4x_5x_6....x_n>$$

$$= \; (\,|0>+ \; e^{\frac{2*pi*i*x_1}{2}}\,|1>) \otimes |x_2x_3x_4x_5x_6....x_n>$$

$$= \; (\,|0>+ \; e^{\frac{2*pi*i*x_2}{2^2}}\; e^{\frac{2*pi*i*x_1}{2^1}}\,|1>) \otimes |x_2x_3x_4x_5x_6....x_n>$$

$$= \; (\,|0>+ \; e^{\frac{2*pi*i*x_3}{2^3}}\; e^{\frac{2*pi*i*x_2}{2^2}}\; e^{\frac{2*pi*i*x_1}{2^1}}\,|1>) \otimes |x_2x_3x_4x_5x_6....x_n>$$

Reverse Order

SHOR'S ALGORITHM

QUANTUM PHASE ESTIMATION:

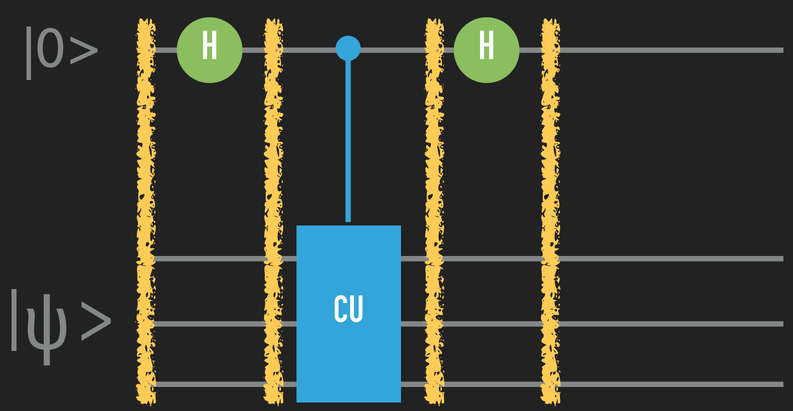
$$U\,|\psi> \;=\; e^{i\Theta}|\psi>$$

$$\frac{1}{\sqrt{2}}(|0>+|1>) \;\Rightarrow\; \begin{array}{l} P(1) = 50\% \\ P(0) = 50\% \end{array}$$

$$e^{\frac{i\,*\,pi}{2}}\,\frac{1}{\sqrt{2}}(|0>+|1>) \;\Rightarrow\; \begin{array}{l} P(1) = \left| e^{\frac{i\,*\,pi}{2}} * \frac{1}{\sqrt{2}} \right|^{2} = 50\% \\ P(0) = 50\% \end{array}$$

SHOR'S ALGORITHM

QUANTUM PHASE ESTIMATION:



$$|0\rangle\,|\psi\rangle$$

$$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\,|\psi\rangle = \frac{1}{\sqrt{2}}\,(|0\rangle\,|\psi\rangle) + (|1\rangle\,|\psi\rangle)$$

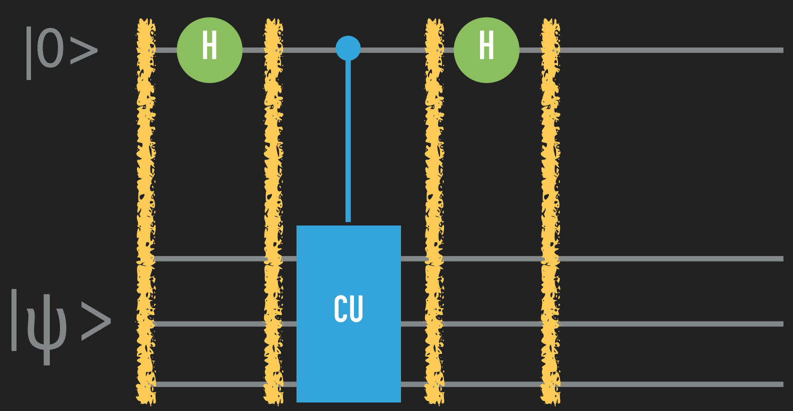
$$\frac{1}{\sqrt{2}}\,(|0\rangle\,|\psi\rangle) + (|1\rangle\,e^{i\theta}\,|\psi\rangle)$$

$$\frac{1}{\sqrt{2}}\,\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}\,|\psi\rangle\,) + e^{i\theta}\,\frac{(|0\rangle - |1\rangle)}{\sqrt{2}}\,|\psi\rangle\,)$$

$$= \frac{1}{2}\,[\,|0\rangle(\,1+e^{i\theta}\,) + |1\rangle(\,1-e^{i\theta}\,)\,]\,|\psi\rangle$$

SHOR'S ALGORITHM

QUANTUM PHASE ESTIMATION:



$$\frac{1}{2}\left[|0\rangle\left(1+e^{i\theta}\right) + |1\rangle\left(1-e^{i\theta}\right)\right]|\psi\rangle$$

$$P(1) = \left|1-e^{i\theta} * \frac{1}{2}\right|^2$$

$$P(0) = \left|1+e^{i\theta} * \frac{1}{2}\right|^2$$

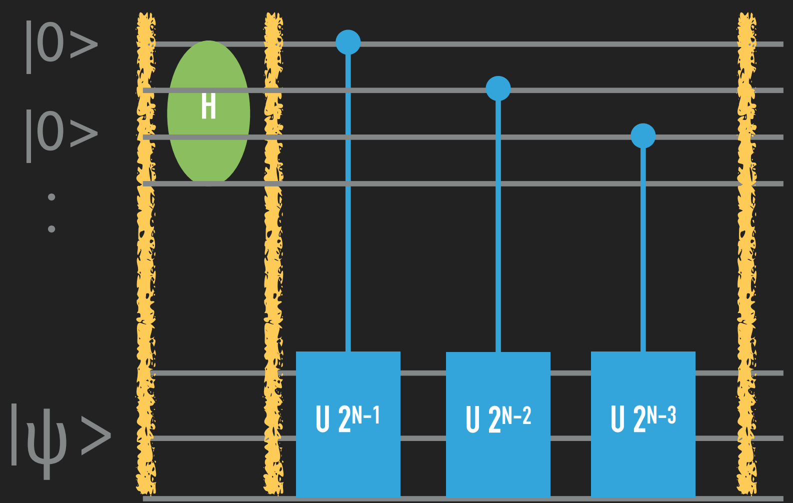
$\theta = 1$ $P(0) = 0.9999..$

$\theta = 10$ $P(0) = 0.9924..$

SHOR'S ALGORITHM

QUANTUM PHASE ESTIMATION:

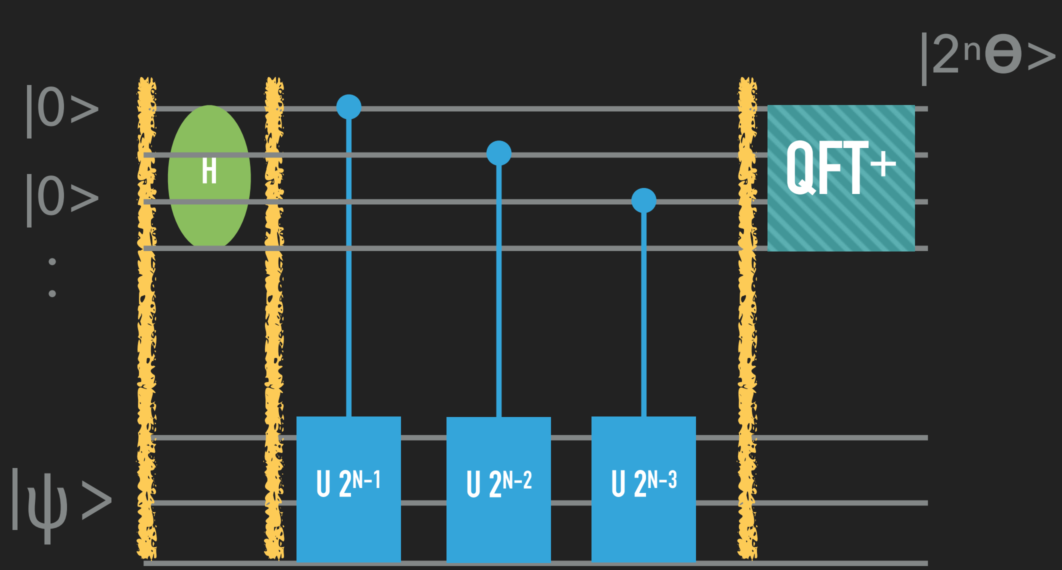
$$|0>^{*n} \; |\psi>$$



$$\frac{1}{\sqrt{2}}^{n} (|0> +|1>)^{*n} \; |\psi>$$

$$\frac{1}{\sqrt{2}}^{n} (|0> + e^{i\theta 2^{n-1}} |1>) \otimes (|0> + e^{i\theta 2^{n-2}} |1>)$$

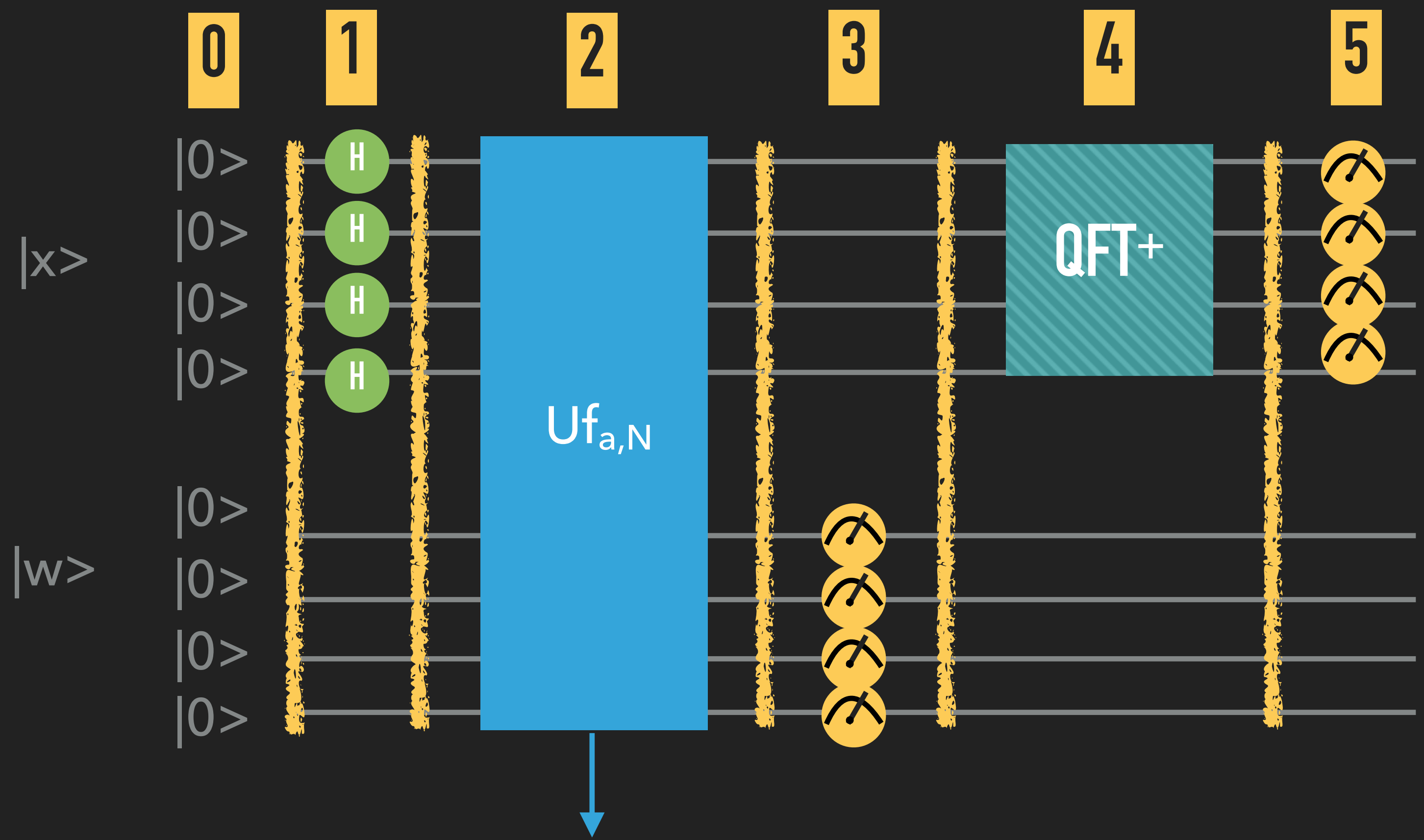
$$\otimes \cdots\cdots\cdots \otimes (|0> + e^{i\theta 2^{0}} |1>)$$



QFT VS QPE:

$$\frac{\theta * 2pi}{2^{n}}$$

SHOR'S ALGORITHM



N = pq

N = 15

15 = [1111]

$f_{a,N}(x) = a^x \bmod(N)$

$|x\rangle\,|w\rangle \rightarrow |x\rangle\,|w \oplus f_{a,N}(x)\rangle$

0 $\quad |0\rangle^{*4}\ |0\rangle^{*4}$

1 $\quad \frac{1}{4}\left[\,|0000\rangle + |0001\rangle + \ldots\ldots + |1111\rangle\right]\ |0\rangle^{*4}$

2 $\quad \frac{1}{4}\left[\,|0000\rangle\,|0 \oplus (13^{0} \bmod 15)\rangle + |0001\rangle\,|0 \oplus (13^{1} \bmod 15)\rangle + \ldots\right.$

$\left.\ldots\ldots\right]$

SHOR'S ALGORITHM

2

$$\frac{1}{4}\left[\,|0000\rangle\,|0 \oplus (13^{0} \mathrm{mod} 15)\rangle + |0001\rangle\,|0 \oplus (13^{1} \mathrm{mod} 15)\rangle + \ldots \ldots\ldots \right]$$

$$\frac{1}{4}\left[\,|0000\rangle\,|(13^{0} \mathrm{mod} 15)\rangle + |0001\rangle\,|(13^{1} \mathrm{mod} 15)\rangle + \ldots \right]$$

$|x\rangle\ |w\rangle$

$$\frac{1}{4}\left[\begin{array}{c} |0\rangle\,|1\rangle + |1\rangle\,|13\rangle + |2\rangle|4\rangle + |3\rangle|7\rangle + \\ |4\rangle\,|1\rangle + |5\rangle\,|13\rangle + |6\rangle|4\rangle + |7\rangle|7\rangle + \\ |8\rangle\,|1\rangle + |9\rangle\,|13\rangle + |10\rangle|4\rangle + |11\rangle|7\rangle + \\ |12\rangle\,|1\rangle + |13\rangle\,|13\rangle + |14\rangle|4\rangle + |15\rangle|7\rangle \end{array}\right]$$

if measure ($|w\rangle$) = 7:

3

$$x = \frac{1}{4}\left[|3\rangle + |7\rangle + |11\rangle + |15\rangle\right]$$

SHOR'S ALGORITHM

3

$$|x\rangle\,|w\rangle = \frac{1}{2}\,[|3\rangle + |7\rangle + |11\rangle + |15\rangle] \otimes |7\rangle$$

4

$$QFT\,|x\rangle = |\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2*pi*i*x*y}{N}} |y\rangle$$

$$QFT^{+}\,|\tilde{x}\rangle = |x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{-2*pi*i*x*y}{N}} |y\rangle$$

$$QFT\,|3\rangle = \frac{1}{\sqrt{16}} \sum_{y=0}^{15} e^{\frac{-2*pi*i*3*y}{16}} |y\rangle$$

SHOR'S ALGORITHM

4 $$QFT^{+}|x\rangle = \frac{1}{8}\sum_{y=0}^{15}\left[e^{-3*pi/8*y} + e^{-7*pi/8*y} + e^{-11*pi/8*y} + e^{-15*pi/8*y}\right]|y\rangle$$

$$= \frac{1}{8}\left[4\,|0000\rangle + 4i\,|0100\rangle - 4\,|1000\rangle - 4i\,|1100\rangle\right]$$

$|0\rangle$ $|4\rangle$ $|8\rangle$ $|12\rangle$

5 Measure: 0, 4 , 8 , 12

$$x^{r/2} = 13^{4/2} = 4 \pmod{15}$$

x+1, x-1 gcd (x+1, N) = gcd (5,15) = 5

5 3 gcd (x-1, N) = gcd (3,15) = 3

SHOR'S ALGORITHM

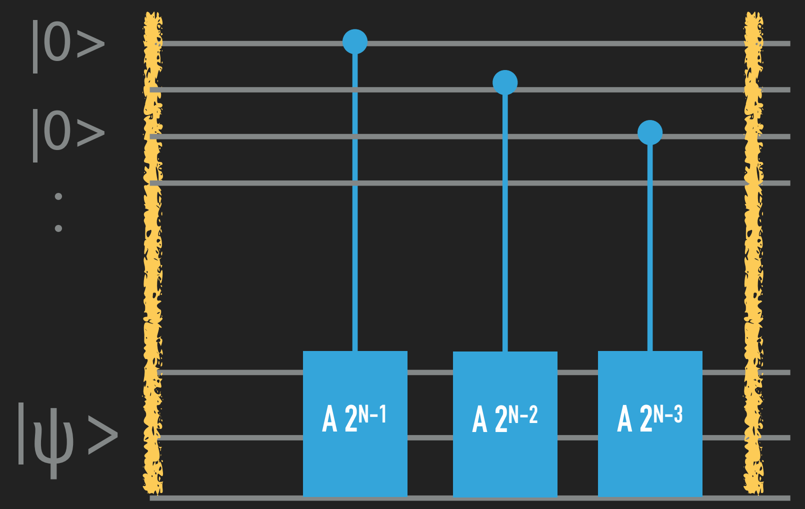
$$f_{a,N}(x) = a^x \bmod(N)$$

$$x = [x1, x2, x3 \ldots\ldots xn] = 2^{n-1}x_1 + 2^{n-2}x_2 + \ldots\ldots + 2^0\, x_n$$

$$f_{a,N}(x) = a^x \bmod(N)$$

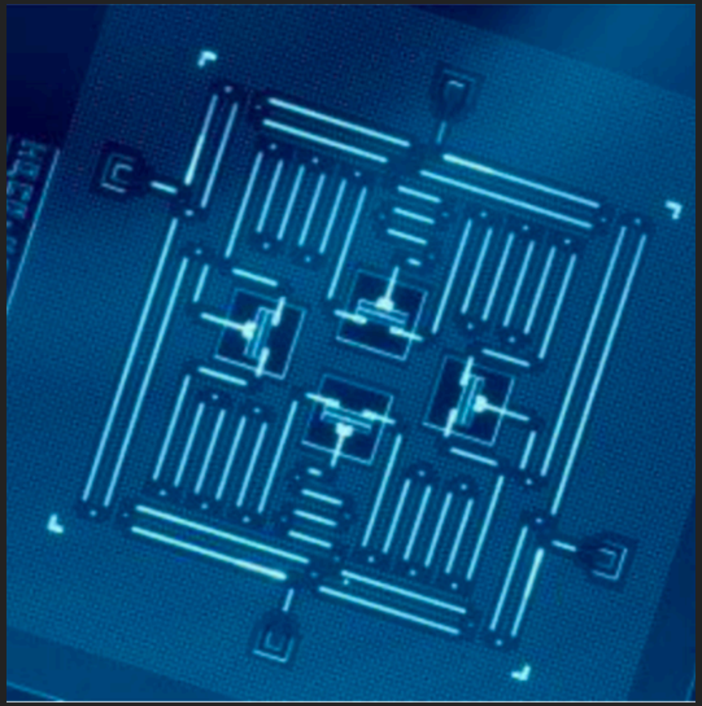
$$= a^{2^{n-1}x_1 + 2^{n-2}x_2 + \ldots\ldots + 2^0\, x_n} \bmod(N)$$

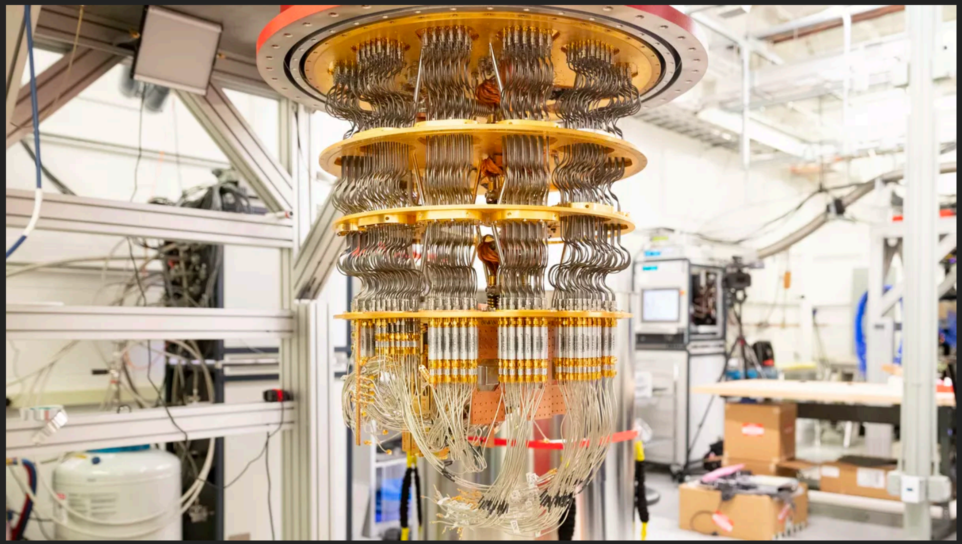
$$= a^{2^{n-1}x_1}\, a^{2^{n-2}x_2} \ldots\ldots a^{2^{n0}x_n}$$



QUANTUM HARDWARE

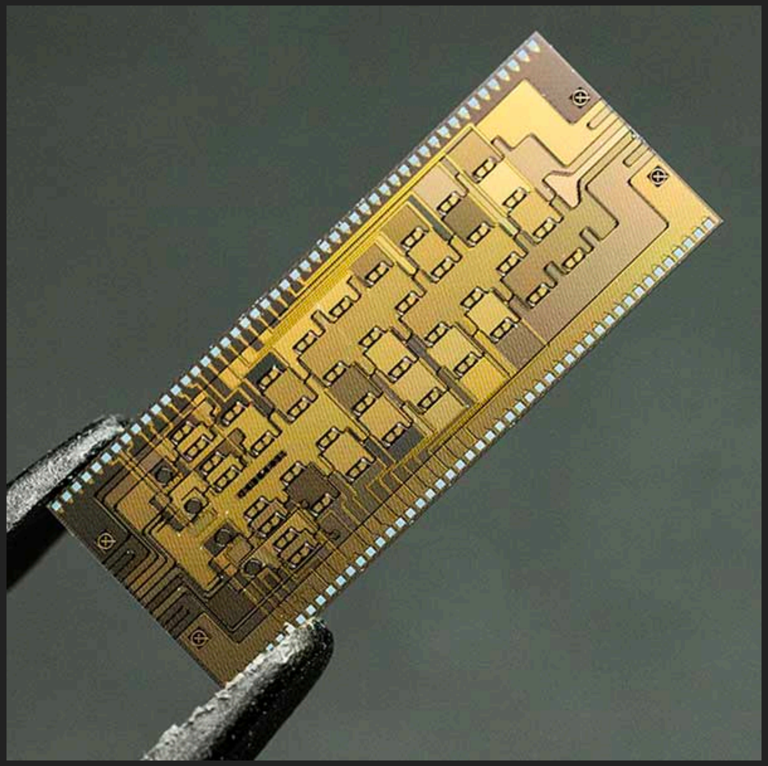
SUPERCONDUCTING QUBITS





QUANTUM HARDWARE

PHOTONIC QUANTUM COMPUTER



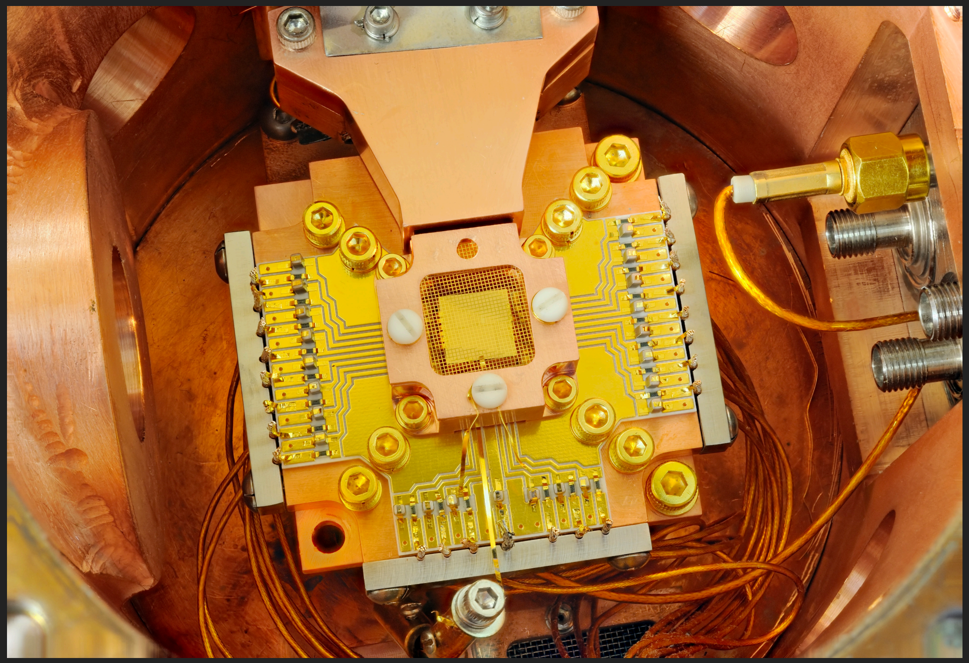
XANADU

PsiQuantum

https://engineersforum.com.ng/2021/03/08/in-the-quest-to-hundreds-of-qubits-photons-may-have-quantum-advantage/

QUANTUM HARDWARE

ION TRAPS



Honeywell

IONQ

By National Institute of Standards and Technology - Quantum Computing; Ion Trapping, Public Domain, https://commons.wikimedia.org/w/index.php?curid=51195437

QUANTUM HARDWARE

DWAVE

D:wave
The Quantum Computing Company™

https://www.datacenterdynamics.com/en/news/d-wave-announces-2000-qubit-quantum-computer-sells-first-unit/