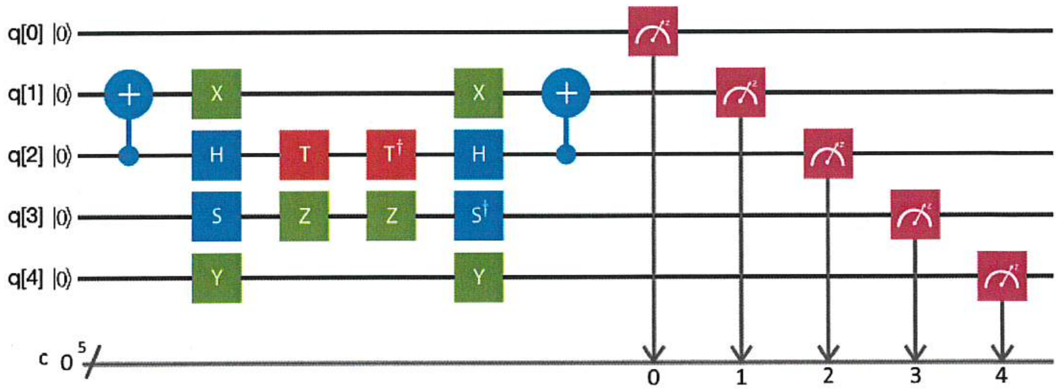
Quantum Gates

量子電腦: Quantum Circuit



Qubits **quantum gates** **measurements**

- Quantum gate $\iff$ Unitary transformation (matrix)

- $U_{n\times n} = [u_1,\dots,u_n]$ unitary $\qquad A^* = \overline{A^T}$

  $\overset{def}{\iff} U^*U = I \qquad (UU^* = I, \Rightarrow U^{-1} = U^*) \qquad \langle x, Ay\rangle = \langle A^* x, y\rangle$

  $\iff \{u_1,\dots,u_n\}$ orthonormal, $\langle u_i, u_j\rangle = u_i^* u_j = \delta_{ij}$

  $\iff \langle Ux, Uy\rangle = \langle x, y\rangle$

  $\iff \|Ux\| = \|x\|$

- 性質 (1) 下任兩個 $\Rightarrow$ 第三個 $\qquad$ in $\mathbb{R}^n$

  (a) $A^*A = I$ (unitary) $\qquad A^TA = I$ (orthogonal)

  (b) $AA = I$ (involution) $(A^{-1} = A)$

  (c) $A^* = A$ (Hermitian) $\qquad A^T = A$ (Symmetric)

  (2) A, B unitary $\Rightarrow A\otimes B$ (並聯), AB (串聯) unitary

  (3) $A: \mathcal{B}\to\mathcal{B} \qquad \mathcal{B} = \{e_1,\dots,e_n\}$ orthonormal basis of $\mathcal{H}$

  (a) A: 1-1 (onto, bijective) $\Rightarrow A$ unitary

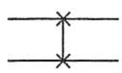
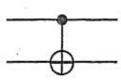
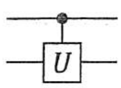
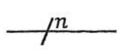
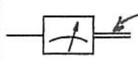
  (b) $A^2 = I \Rightarrow A$ 1-1 $\Rightarrow A$ 〃

  Pf (a) $\{a_i = Ae_i\}_{1\le i\le n} = \mathcal{B}$ (permutation)

  (b) ${}_{A}Ax = {}_{A}Ay \Rightarrow x = y$

基本 Quantum Gates

* 外, 滿足前性質(1)
· Hermitian
· $A^2 = I$

	Operator	變換 (对基底)	變換矩陣	圖示
1 qubit	Hadamard (**H**)	$H\|x\rangle = \frac{1}{\sqrt{2}}\|0\rangle + (-1)^x \frac{1}{\sqrt{2}}\|1\rangle$ $H\|0\rangle \overset{\text{def}}{=} \|+\rangle = \frac{1}{\sqrt{2}}\|0\rangle + \frac{1}{\sqrt{2}}\|1\rangle$ $H\|1\rangle \overset{\text{def}}{=} \|-\rangle = \frac{1}{\sqrt{2}}\|0\rangle - \frac{1}{\sqrt{2}}\|1\rangle$	$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$	$-\boxed{H}-$
	NOT Pauli-X (**X**)	$\mathrm{NOT}\|x\rangle = X\|x\rangle = \|1 \oplus x\rangle = \|\neg x\rangle$ $X\|0\rangle = \|1\rangle, X\|1\rangle = \|0\rangle$	$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$	$-\oplus-$ $-\boxed{X}-$
	Pauli-Y (**Y**)	$Y\|x\rangle = (-1)^x \mathrm{i}\|1 \oplus x\rangle = (-1)^x \mathrm{i}\|\neg x\rangle$ $Y\|0\rangle = \mathrm{i}\|1\rangle, Y\|1\rangle = -\mathrm{i}\|0\rangle$	$\begin{bmatrix}0 & -\mathrm{i}\\\mathrm{i} & 0\end{bmatrix}$	$-\boxed{Y}-$
	Pauli-Z (**Z**) R_π	$Z\|x\rangle = (-1)^x\|x\rangle$ $Z\|0\rangle = \|0\rangle, Z\|1\rangle = -\|1\rangle$	$\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$	$-\boxed{Z}-$
*	**Phase shift (R_ϕ)**	$R_\theta\|x\rangle = \mathrm{e}^{\mathrm{i}x\theta}\|x\rangle$ $R_\theta\|0\rangle = \|0\rangle, R_\theta\|1\rangle = \mathrm{e}^{\mathrm{i}\theta}\|1\rangle$	$\begin{bmatrix}1 & 0\\0 & \mathrm{e}^{\mathrm{i}\theta}\end{bmatrix}$	$-\boxed{R_\theta}-$
*	Phase (**S**, P) $R_{\frac{\pi}{2}}$	$S = R_{\pi/2}$ $S\|0\rangle = \|0\rangle, S\|1\rangle = \mathrm{i}\|1\rangle$	$\begin{bmatrix}1 & 0\\0 & \mathrm{i}\end{bmatrix}$	$-\boxed{S}-$
*	$\pi/8$ (**T**) $R_{\frac{\pi}{4}}$	$T = R_{\pi/4}$ $T\|0\rangle = \|0\rangle, T\|1\rangle = \mathrm{e}^{\mathrm{i}\pi/4}\|1\rangle$	$\begin{bmatrix}1 & 0\\0 & \mathrm{e}^{\mathrm{i}\pi/4}\end{bmatrix}$	$-\boxed{T}-$
2 qubit	**SWAP**	$\mathrm{SWAP}\|xy\rangle = \|yx\rangle$ $\mathrm{SWAP}\|00\rangle = \|00\rangle$ $\mathrm{SWAP}\|01\rangle = \|10\rangle$ $\mathrm{SWAP}\|10\rangle = \|01\rangle$ $\mathrm{SWAP}\|11\rangle = \|11\rangle$	$\begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}$	
	Controlled Not (**CNOT**, CX)	$\mathrm{CNOT}\|x,y\rangle = \|x, x \oplus y\rangle$ $\mathrm{CNOT}\|0,y\rangle = \|0,y\rangle$ $\mathrm{CNOT}\|1,y\rangle = \|1,1 \oplus y\rangle = \|1,\neg y\rangle$	$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix} = \begin{bmatrix}I & O\\O & X\end{bmatrix}$	
*	**Controlled U**	$C(U)\|x\rangle\|y\rangle = \|x\rangle U^x\|y\rangle$ $C(U)\|0\rangle\|y\rangle = \|0\rangle\|y\rangle$ $C(U)\|1\rangle\|y\rangle = \|1\rangle U\|y\rangle$	$\begin{bmatrix}I & O\\O & U\end{bmatrix}$	
3 qubit	Toffoli (**CCNOT**, CCX, TOFF)	$\mathrm{CCNOT}\|x,y,z\rangle = \|x,y,x \wedge y \oplus z\rangle$ $\mathrm{CCNOT}\|0,y,z\rangle = \|0,y,z\rangle$ $\mathrm{CCNOT}\|x,0,z\rangle = \|x,0,z\rangle$ $\mathrm{CCNOT}\|1,1,z\rangle = \|1,1,1 \oplus z\rangle$ $= \|1,1,\neg z\rangle$	$\begin{bmatrix}I&O&O&O\\O&I&O&O\\O&O&I&O\\O&O&O&X\end{bmatrix}$	
	n-qubit			
	measurement			

x: control bit
y: target 〃

普通 bits

1- qubit gate

- State space $\mathcal{H}_2 = \left\{ a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \;\middle|\; \begin{matrix} a \\ b \end{matrix} \in \mathbb{C} \right\}$

  basis $\mathcal{B} = \left\{ |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix},\ |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$

· Hadamard gate H

(1) $H \quad : \begin{cases} |0\rangle \longrightarrow |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle \longrightarrow |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$ $\left(\begin{matrix} |0\rangle \\ |1\rangle \end{matrix}\right.$ 等機率$\left.\right)$

$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} : \begin{matrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \longrightarrow \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} \\ \begin{bmatrix} 0 \\ 1 \end{bmatrix} \longrightarrow \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} \end{matrix}$

$\mathcal{B}' = \{ |+\rangle, |-\rangle \}$ orthonormal
Hadamard basis

(2) H : unitary, H : symmetric, $\Rightarrow H^2 = I$, $H^{-1} = H$

(3) $H^{-1} = H \quad : \begin{cases} |+\rangle \rightarrow |0\rangle \\ |-\rangle \rightarrow |1\rangle \end{cases}$

$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} : \begin{matrix} \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} \rightarrow \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{matrix}$

$$\begin{aligned} H|+\rangle &= H\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle + |0\rangle - |1\rangle) \\ &= |0\rangle \end{aligned}$$
interference (干涉)

(4) $|0\rangle -\boxed{H}- |x\rangle$
$|0\rangle -\boxed{H}- |y\rangle$

$$\begin{aligned} (H \otimes H)|00\rangle &= (H|0\rangle) \otimes (H|0\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2^2}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \end{aligned}$$

$$\begin{aligned} H^{\otimes 3}|000\rangle &= H|0\rangle \otimes H|0\rangle \otimes H|0\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2^3}}(|000\rangle + |001\rangle + \cdots + |111\rangle) \\ &= \frac{1}{\sqrt{2^3}} \sum_{y_i \in \mathbb{B}} |y_1 y_2 y_3\rangle = \frac{1}{\sqrt{8}}(|0\rangle + |1\rangle + \cdots + |7\rangle) \\ &= \frac{1}{\sqrt{2^3}} \sum_{y \in \mathbb{B}^3} |y\rangle \end{aligned}$$

2-qubit gate

- State space $\mathcal{H}_{2^2} = \left\{ a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle = \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} \;\middle|\; a,b,c,d \in \mathbb{C} \right\}$

- basis $\mathcal{B} = \left\{ |00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \right\}$

- CNOT : $|xy\rangle \longrightarrow |x, x \oplus y\rangle$, : $\begin{cases} |0y\rangle \longrightarrow |0y\rangle \\ |1y\rangle \longrightarrow |1\bar{y}\rangle \end{cases}$

: $|00\rangle \to |00\rangle$, $|01\rangle \to |01\rangle$, $|10\rangle \to |11\rangle$, $|11\rangle \to |10\rangle$

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

(1) CNOT : unitary, Hermitian, $\text{CNOT}^2 = I$.

(2) create entangled Bell states (EPR pairs) $\{|\beta_{ij}\rangle\}$ orthonormal Bell basis

CNOT $(H \otimes I)$:

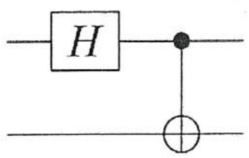
$$|00\rangle \longrightarrow |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|01\rangle \longrightarrow |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|10\rangle \longrightarrow |\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|11\rangle \longrightarrow |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

$x\rangle$
$y\rangle$



circuit

或

$$|xy\rangle \longrightarrow |\beta_{xy}\rangle = \frac{1}{\sqrt{2}}\left(|0y\rangle + (-1)^x |1\bar{y}\rangle\right)$$

pf
$$|0y\rangle \xrightarrow{H \otimes I} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|y\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}\left(|0y\rangle + |1\bar{y}\rangle\right)$$

$$|1y\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|y\rangle \longrightarrow \frac{1}{\sqrt{2}}\left(|0y\rangle - |1\bar{y}\rangle\right)$$

(3) $\longleftarrow$ (解糾纏)

3-qubit gate

(3) CCNOT : $|x, y, z\rangle \longrightarrow |x, y, x \wedge y \oplus z\rangle$

$$(|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle) \mapsto$$
$$(|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |111\rangle, |110\rangle),$$

$$\mathrm{CCNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$
$$= \begin{bmatrix} I & O & O & O \\ O & I & O & O \\ O & O & I & O \\ O & O & O & X \end{bmatrix}\text{。}$$

Boolean logic

boolean function $f: \mathbb{B}^n \longrightarrow \mathbb{B}^m$, $\mathbb{B} = \{0, 1\}$

- A set of gates Ω is universal, if all f can be built from these gates.

- 定理 1

(1) $\{\neg, \wedge, \vee\}$, $\{\neg, \wedge\}$, $\{\neg, \vee\}$ universal

(2) $\{NAND\}$ universal $\quad NAND(x,1) = \overline{x \wedge 1} = \bar{x}$

(3) $\{NOR\}$ 〃 $\quad NAND(\bar{x}, \bar{y}) = \overline{\bar{x} \wedge \bar{y}} = x \vee y$

- 定理 2 $\oplus$ 運算滿足

(1) $x \oplus y = x + y \pmod 2$

(2) $x \oplus y = y \oplus x$

$(x \oplus y) \oplus z = x \oplus (y \oplus z)$

(3) $x \wedge (y \oplus z) = (x \wedge y) \oplus (x \wedge z)$

(4) $0 \oplus x = x$

$x \oplus x = 0$

(5) $1 \oplus x = \bar{x}$

$1 \oplus x \oplus y = \bar{x} \oplus y = x \oplus \bar{y}$

(6) $x \oplus z = y \oplus z \Leftrightarrow x = y$ $\quad (\because (4))$

(7) $(-1)^{x \oplus y} = (-1)^x (-1)^y$

No.
Date: / /

Quantumn gates

- A set of quantumn gates is universal, if all unitary transformations can be built from these gates

- 定理1
  (1) {all 1-qubit gates} ∪ {CNOT} universal
  (2) {CNOT, H, T} approximately universal
  (3) {CNOT, H, S, CCNOT} 〃 〃
  (4) {H, CCNOT} 〃 〃 for orthogonal transf.

- 定理2 {CCNOT} universal for boolean f.

∵ NAND: $|x,y,1\rangle \xrightarrow{CCNOT} |x,y,x\wedge y\oplus 1\rangle = |x,y,\neg(x\wedge y)\rangle$

fan-out: $|x,1,0\rangle \xrightarrow{CCNOT} |x,1,(x\wedge 1)\oplus 0\rangle = |x,1,x\rangle$

$(|x,0\rangle \xrightarrow{CNOT} |x, x\oplus 0\rangle = |x,x\rangle)$ (cloning?)

- 定理3

(1) $HXH = Z$, $HZH = X$

$XZ = -ZX$, $\begin{cases} XZX = -Z, \\ ZXZ = -X \end{cases}$

(2) $C(e^{i\theta}I) = R_\theta \otimes I$

(3) $C(Z) = Z \otimes I$

(4) $C(Z)_{(c,t)} = C(Z)_{(t,c)}$

(5) $(X\otimes I)\, CNOT_{(c,t)}\, (X\otimes I) = CNOT_{(\neg c,t)}$

(6) $H^{\otimes 2}\, CNOT_{(c,t)}\, H^{\otimes 2} = CNOT_{(t,c)}$

証 (1) $\begin{cases} |0\rangle \xrightarrow{H} \frac{|0\rangle+|1\rangle}{\sqrt{2}} \xrightarrow{X} \frac{|1\rangle+|0\rangle}{\sqrt{2}} \xrightarrow{H} |0\rangle \\ |1\rangle \rightarrow \frac{|0\rangle-|1\rangle}{\sqrt{2}} \rightarrow \frac{|1\rangle-|0\rangle}{\sqrt{2}} \rightarrow -|1\rangle \end{cases}$

定理

(1) $|0\oplus x\rangle - |1\oplus x\rangle = \left\{\begin{matrix} |0\rangle - |1\rangle, & x=0 \\ |1\rangle - |0\rangle, & x=1 \end{matrix}\right\} = (-1)^x\left(|0\rangle - |1\rangle\right)$

(phase kick-back)

$$U_f : \begin{array}{lcl} |x\,y\rangle & \longrightarrow & |x, y\oplus f(x)\rangle \\ |x\rangle \dfrac{|0\rangle - |1\rangle}{\sqrt{2}} & \longrightarrow & |x\rangle \dfrac{|0\oplus f(x)\rangle - |1\oplus f(x)\rangle}{\sqrt{2}} = (-1)^{f(x)}|x\rangle \dfrac{|0\rangle - |1\rangle}{\sqrt{2}} \end{array}$$

(2) $H^{\otimes n}|0\cdots 0\rangle = \left(H|0\rangle\right)^{\otimes n} = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{y\in \mathbb{B}^n}|y\rangle$

(3) $\left\{\begin{matrix} x = x_1\cdots x_n \\ y = y_1\cdots y_n \end{matrix}\right. \in \mathbb{B}^n$

$$H^{\otimes n}|x\rangle = H^{\otimes n}|x_1x_2\cdots x_n\rangle = \bigotimes_{i=1}^{n} H|x_i\rangle = \frac{1}{\sqrt{2^n}}\sum_{y\in\mathbb{B}^n}(-1)^{\overset{x_1y_1+\cdots+x_ny_n}{\overset{\shortparallel}{x\cdot y}}}|y\rangle$$

Pf $\left\{\begin{matrix} H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \\ H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \end{matrix}\right. \Rightarrow H|x\rangle = \frac{1}{\sqrt{2}}\left((-1)^{x\cdot 0}|0\rangle + (-1)^{x\cdot 1}|1\rangle\right)$

$$= \frac{1}{\sqrt{2}}\sum_{y=0}^{1}(-1)^{xy}|y\rangle$$

$$\begin{aligned} H^{\otimes 3}|x_1x_2x_3\rangle &= H|x_1\rangle \otimes H|x_2\rangle \otimes H|x_3\rangle \\ &= \frac{1}{\sqrt{2}}\sum_{y_1=0}^{1}(-1)^{x_1y_1}|y_1\rangle \otimes \frac{1}{\sqrt{2}}\sum_{y_2=0}^{1}(-1)^{x_2y_2}|y_2\rangle \otimes \frac{1}{\sqrt{2}}\sum_{y_3=0}^{1}(-1)^{x_3y_3}|y_3\rangle \\ &= \frac{1}{\sqrt{2^3}}\sum_{y_1=0}^{1}\sum_{y_2=0}^{1}\sum_{y_3=0}^{1}(-1)^{x_1y_1+x_2y_2+x_3y_3}|y_1y_2y_3\rangle \\ &= \frac{1}{\sqrt{2^3}}\sum_{y\in\mathbb{B}^3}(-1)^{x\cdot y}|y\rangle \end{aligned}$$

例

$$H^{\otimes 3}|011\rangle = \frac{1}{\sqrt{2^3}}\left(|0\rangle + |1\rangle\right)\left(|0\rangle - |1\rangle\right)\left(|0\rangle - |1\rangle\right)$$

$(011)\cdot(010) = 0+1+0$

$$= \frac{1}{\sqrt{2^3}}\left(|000\rangle + |001\rangle + \cdots + (-1)^1\underline{|010\rangle} + \cdots + \underline{|111\rangle}\right)$$

$(011)\cdot(111)$
$= 0+1+1$