Kvantni algebrajski učinki

Luna Strah

9. 9. 2022

mentor: doc. dr. Matija Pretnar

Motivacija

Motivacija

Kvantno programiranje

- Enakost programov

Motivacija

Kvantno programiranje

- Enakost programov
- Novi problemi za teorijo programskih jezikov

Pregled

1. Kvantno računalništvo
2. Interpretacije operacij
3. Polnost

Kvantni vektorji

Definicija (Binarni vektorji)

Binarni vektorji so elementi množice $\mathbf{B}_n := \{0,1\}^n$ *in jih pišemo kot nize.*

Primer: $\mathbf{B}_2 = \{\mathbf{00}, \mathbf{01}, \mathbf{10}, \mathbf{11}\}$.

Kvantni vektorji

Definicija (Binarni vektorji)

Binarni vektorji so elementi množice $\mathbf{B}_n := \{0,1\}^n$ *in jih pišemo kot nize.*

Primer: $\mathbf{B}_2 = \{\mathbf{00}, \mathbf{01}, \mathbf{10}, \mathbf{11}\}$.

Definicija (Kvantni prostor)

Kvantni vektorji (nadaljnje vektorji) so elementi prostora $\mathbf{H}_n := \mathbb{C}^{2^n}$. *Kubiti so elementi* $\mathbf{H} := \mathbf{H}_1$.
Če je $\{e_j\}$ *standardna baza* $\mathbf{H}_n$ *pišemo* $|j\rangle := e_j$.

Očitno je $\mathbf{H}_n = \mathcal{L}_{\mathbb{C}}(\{|j\rangle \mid j \in \mathbf{B}_n\})$.

Primeri

Primer ($n = 1$)

$$a = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = a_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + a_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} = a_0 \left|\mathbf{0}\right\rangle + a_1 \left|\mathbf{1}\right\rangle .$$

Primeri

Primer ($n = 1$)

$$a = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = a_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + a_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} = a_0 \left|\mathbf{0}\right\rangle + a_1 \left|\mathbf{1}\right\rangle .$$

Primer ($n = 2$)

$$a = \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} a_{\mathbf{00}} \\ a_{\mathbf{01}} \\ a_{\mathbf{10}} \\ a_{\mathbf{11}} \end{bmatrix} = a_{00} \left|\mathbf{00}\right\rangle + a_{01} \left|\mathbf{01}\right\rangle + a_{10} \left|\mathbf{10}\right\rangle + a_{11} \left|\mathbf{11}\right\rangle .$$

Primeri

Primer ($n = 1$)

$$a = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = a_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + a_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} = a_0 \left|\mathbf{0}\right\rangle + a_1 \left|\mathbf{1}\right\rangle .$$

Primer ($n = 2$)

$$a = \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} a_{\mathbf{00}} \\ a_{\mathbf{01}} \\ a_{\mathbf{10}} \\ a_{\mathbf{11}} \end{bmatrix} = a_{00} \left|\mathbf{00}\right\rangle + a_{01} \left|\mathbf{01}\right\rangle + a_{10} \left|\mathbf{10}\right\rangle + a_{11} \left|\mathbf{11}\right\rangle .$$

Primer

$$\mathbf{h} := \rho \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \rho \left(\left|\mathbf{0}\right\rangle + \left|\mathbf{1}\right\rangle\right), \quad \mathbf{h}_n := \rho^n \sum_{j \in \mathbf{B}_n} \left|j\right\rangle , \quad \rho := \frac{1}{\sqrt{2}}.$$

Tenzorski produkt

Definicija (Tenzorski produkt)

Tenzorski produkt prostorov $\mathbf{H}_m$ *in* $\mathbf{H}_n$ *je enak* $\mathbf{H}_{m+n}$.
Če sta $a \in \mathbf{H}_m$ *in* $b \in \mathbf{H}_n$ *je* $a \otimes b \in \mathbf{H}_m \otimes \mathbf{H}_n = \mathbf{H}_{m+n}$.

Tenzorski produkt

Definicija (Tenzorski produkt)

Tenzorski produkt prostorov $\mathbf{H}_m$ *in* $\mathbf{H}_n$ *je enak* $\mathbf{H}_{m+n}$.
Če sta $a \in \mathbf{H}_m$ *in* $b \in \mathbf{H}_n$ *je* $a \otimes b \in \mathbf{H}_m \otimes \mathbf{H}_n = \mathbf{H}_{m+n}$.

Primer ($n = m = 1$)

$$\begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \otimes \begin{bmatrix} b_0 \\ b_1 \end{bmatrix} = \begin{bmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 b_0 \\ a_1 b_1 \end{bmatrix}$$

Posledica

$$|j\rangle \otimes |k\rangle = |j\rangle\,|k\rangle = |jk\rangle\,, \quad a \otimes b = \sum_{\substack{j \in \mathbf{B}_n, \\ k \in \mathbf{B}_m}} a_j b_k\,|jk\rangle$$

Unitarna vrata

Definicija (Unitarna vrata)

Unitarna vrata reda n so unitarne matrike dimenzije 2^n.

Unitarna vrata

Definicija (Unitarna vrata)

Unitarna vrata reda n so unitarne matrike dimenzije 2^n. Tenzorski produkt $U \otimes V = [u_{jk}V]_{j,k}$ uporabljen na $a \otimes b$ je enak $Ua \otimes Vb$.

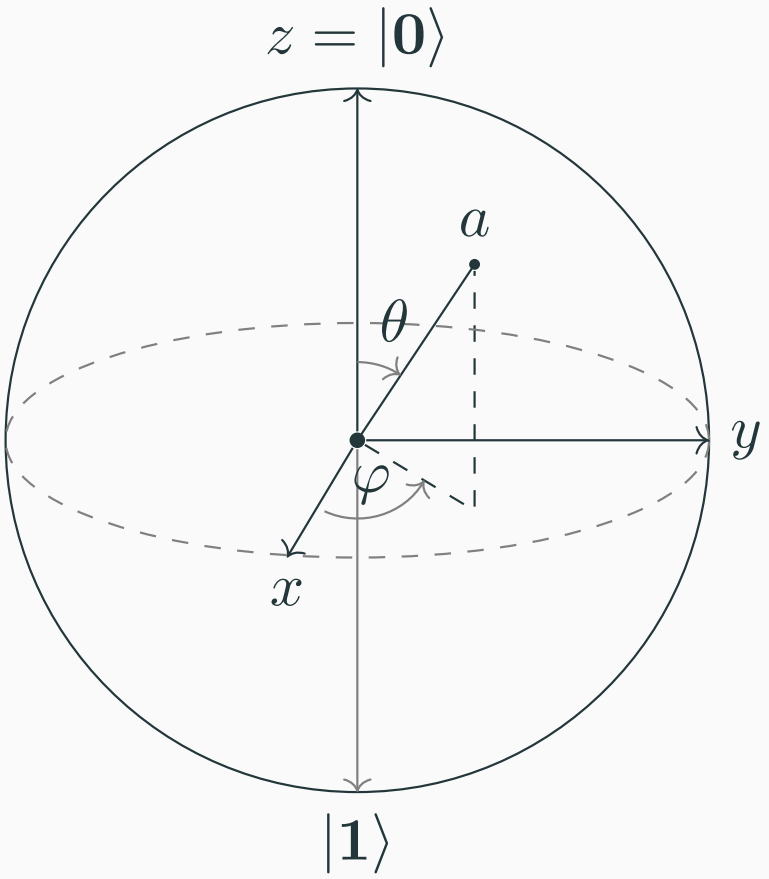
Primer (Tenzorski produkt unitarnih vrat)

$$\begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} \otimes B = \begin{bmatrix} a_{00}B & a_{01}B \\ a_{10}B & a_{11}B \end{bmatrix}.$$

Blochova sfera

Kubit a predstavimo kot točko v $\mathbb{S}^2$ z identifikacijo:

$$a = \cos\frac{\theta}{2}\,|\mathbf{0}\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|\mathbf{1}\rangle$$



Primeri

Primer (Paulijeve matrike)

To so matrike rotacije okrog osi na Blochovi sferi:

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Velja $X^2 = Y^2 = Z^2 = I_2$.

Primeri

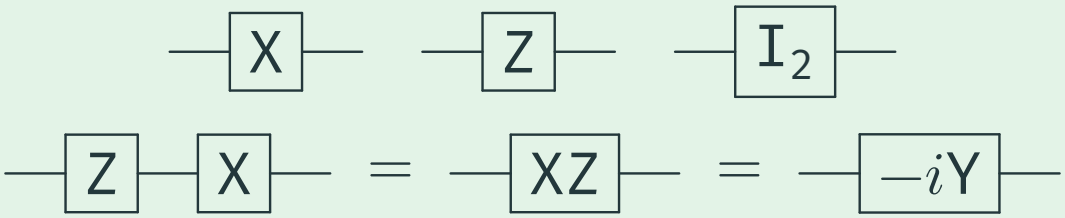
Primer (Paulijeve matrike)

To so matrike rotacije okrog osi na Blochovi sferi:

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Velja $X^2 = Y^2 = Z^2 = I_2$.

Primer (Paulijeve matrike)



Kvantna meritev

Definicija (Kvantna meritev)

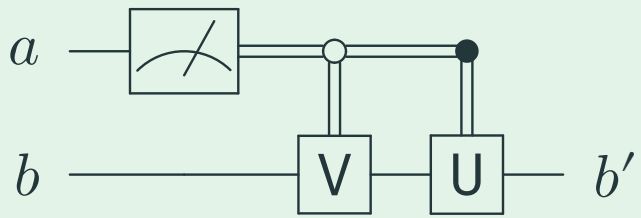
Meritev kubita $a = a_0 |\mathbf{0}\rangle + a_1 |\mathbf{1}\rangle$ *označimo* $M(a)$ *in je* 0 *z verjetnostjo* $|a_0|^2$ *in* 1 *z verjetnostjo* $|a_1|^2$*. To „uniči“ kubit* a*.*

Kvantna meritev

Definicija (Kvantna meritev)

Meritev kubita $a = a_0 |\mathbf{0}\rangle + a_1 |\mathbf{1}\rangle$ *označimo* $M(a)$ *in je* 0 *z verjetnostjo* $|a_0|^2$ *in* 1 *z verjetnostjo* $|a_1|^2$*. To „uniči“ kubit* a*.*

Primer (Pogojna uporaba vrat)



if $\underline{\text{measure}}(a) = 0$ **then** Ub **else** Vb

Kvantna kontrola

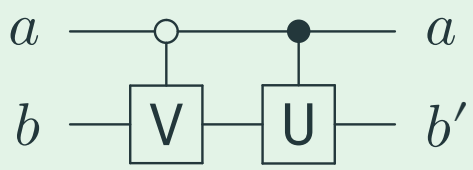
Definicija

Kontrola „na ena“.

$$C_{r,s}(U)\,|j\rangle = \begin{cases} |j\rangle & ; \quad j_r = 0 \\ |j_1 \ldots\rangle\,|Uj_s\rangle\,|\ldots j_n\rangle & ; \quad j_r = 1 \end{cases}$$

Posebej za $U \in \mathrm{U}_2$ označimo $\mathtt{c}U := C_{1,2}(U) = D(\mathtt{I}_2, \mathtt{U})$.

Primer (Pogojna uporaba vrat)



if $\underline{\text{measure}}(a) = 0$ **then** (a, Ub) **else** (a, Vb)

Opazljivke

Definicija

Opazljivka je sebi-adjungiran operator na prostoru $\mathbf{H}_n$ oziroma $2^n \times 2^n$ hermitska matrika.

Opazljivke

Definicija

Opazljivka je sebi-adjungiran operator na prostoru $\mathbf{H}_n$ oziroma $2^n \times 2^n$ hermitska matrika.

Definicija

Rezultati meritve opazljivke v stanju u je ena od lastnih vrednosti λ_j z verjetnostjo $|P_{\lambda_j} u|^2$, stanje u se pa po meritvi spremeni v izmerjeno stanje, torej $P_{\lambda_j} u$.

Jezik

Definicija

Členost je oblike $(p \mid m_1, ..., m_k)$*, kjer so* $p, m_i \in \mathbb{N}$*.*

Neformalno členost pove, da operacija O *sprejme* p *parametrov in* k *računskih spremenljivk, kjer* i*-ta sprejme* m_i *parametrov. Pišemo* $\mathsf{O} : (p \mid m_1, ..., m_k)$*.*

Jezik

Definicija

Členost je oblike $(p \mid m_1, ..., m_k)$*, kjer so* $p, m_i \in \mathbb{N}$*.*

Neformalno členost pove, da operacija $\mathsf{0}$ *sprejme* p *parametrov in* k *računskih spremenljivk, kjer* i*-ta sprejme* m_i *parametrov. Pišemo* $\mathsf{0} : (p \mid m_1, ..., m_k)$*.*

Definicija

Interpretacija operacije s členostjo $(p \mid m_1, ..., m_k)$ *je preslikava oblike* $\mathbf{M}_{2^{m_1}} \oplus \cdots \oplus \mathbf{M}_{2^{m_k}} \to \mathbf{M}_{2^p}$*.*

C^*-algebre

Definicija

Množica A je C^*-algebra, če:

(a) *je Banachova $\mathbb{C}$-algebra z enoto,*

(b) *ima involucijo $(-)^*$,*

(c) *za vsak $a \in A$ velja $\|a\|^2 = \|a^*a\|$.*

Primer

Množice $\mathbf{M}_n := M_n(\mathbb{C})$ so C^*-algebre.

Definicija

Preslikava $f : A \to B$ je $*$-homomorfizem, če je linearna in ohranja množenje, enoto, ter involucijo.

Osnovne operacije

Definicija

Meritev in uporabo vrat interpretiramo z $*$-homomorfizmoma $\mathsf{measure} : \mathbf{M}_1 \oplus \mathbf{M}_1 \to \mathbf{M}_2$ *in* $\mathsf{apply}_\mathsf{U} : \mathbf{M}_{2^p} \to \mathbf{M}_{2^p}$, *s predpisoma*

$$\mathsf{measure}(\alpha, \beta) = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \qquad \mathsf{apply}_\mathsf{U}(A) = U^* A U.$$

Polnost

Izrek (Polnost v posebnem)

1. *Za vsak $*$-homomorfizem $f : \mathbf{M}_{2^{m_1}} \oplus \cdots \oplus \mathbf{M}_{2^{m_k}} \to \mathbf{M}_{2^p}$ obstaja izraz v algebrajski teoriji, ki ne vsebuje operacije* new, *tako da je $x_1 : m_1, ..., x_k : m_k \mid a_1, ..., a_p \vdash t$ in $[\![t]\!] = f$.*
2. *Če $\Gamma \mid \Delta \vdash t, u$ ne vsebujeta* new *in $[\![t]\!] = [\![u]\!]$ lahko izpeljemo $\Gamma \mid \Delta \vdash t = u$.*

Dodeljevanje novih kubitov

Definicija

Dodeljevanje novih kubitov interpretiramo kot linearno preslikavo new : $\mathbf{M}_2 \to \mathbf{M}_1$, *s predpisom*

$$\text{new}\begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} = \alpha_{11}.$$

Dodeljevanje novih kubitov

Definicija

Dodeljevanje novih kubitov interpretiramo kot linearno preslikavo new : $\mathbf{M}_2 \to \mathbf{M}_1$, *s predpisom*

$$\text{new}\begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} = \alpha_{11}.$$

Definicija

Element x C^*-algebre je pozitiven, če obstaja kak element y, da je $x = y^*y$.

Definicija

Preslikava f je popolnoma pozitivna, če za vsak $k \in \mathbb{N}$ preslikava $M_k(f)$ ohranja pozitivnost elementov.

Polnost 2: Electric boogaloo

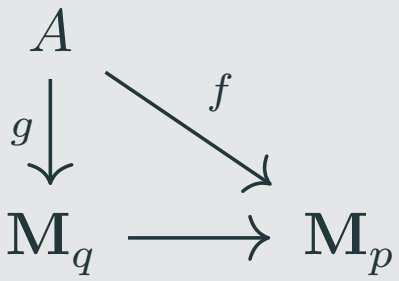
Izrek (Polnost v splošnem)

1. *Za vsako linearno preslikavo* $f : \mathbf{M}_{2^{m_1}} \oplus \cdots \oplus \mathbf{M}_{2^{m_k}} \to \mathbf{M}_{2^p}$, *ki je popolnoma pozitivna in enotska, obstaja izraz v algebrajski teoriji, tako da je* $t : (p \mid m_1, ..., m_k)$ *in* $[\![t]\!] = f$.
2. *Če* $\Gamma \mid \Delta \vdash t, u$ *in* $[\![t]\!] = [\![u]\!]$ *lahko izpeljemo* $\Gamma \mid \Delta \vdash t = u$.

Dokaz

Izrek (Stinespringov izrek o dilaciji)

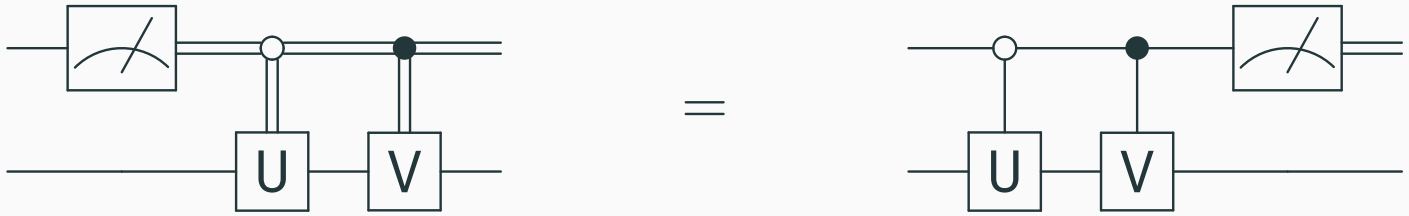
Naj bo $f : \mathcal{A} \to \mathbf{M}_p$ popolnoma pozitivna in naj ohranja enoto. Tedaj obstaja $q \geq p$ in $*$-homomorfizem $g : \mathcal{A} \to \mathbf{M}_q$, tako da je $f(A) = g(A)|_p$.



Aksiomi

(A) Kvantna negacija pred meritvijo je negacija po meritvi.

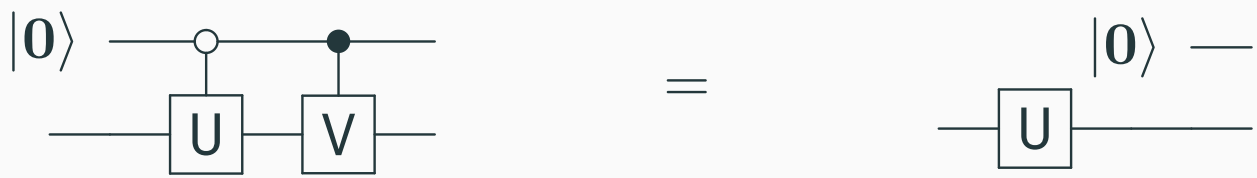
(B) Kvantna kontrola je po meritvi kot klasična kontrola.



(C) Kvantna vrata uporabljena na zavrženih kubitih so odveč.

(D) Novi kubiti so $|\mathbf{0}\rangle$ glede na meritev.

(E) Novi kubiti so $|\mathbf{0}\rangle$ glede na kontrolo.



(...) Plus še sedem manj zanimivih akisomov.

Uporaba

$$
\begin{aligned}
&(\nu a.\, x(a)) \;?_b\; (\nu a.\, \mathsf{X}_a(x(a))) \\
&\quad = \nu a.\, x(a) \;?_b\; \mathsf{X}_a(x(a)) && \text{komutativnost} \\
&\quad = \nu a.\, \mathsf{cX}_{b,a}(x(a) \;?_b\; x(a)) && (2) \\
&\quad = \nu a.\, \mathsf{cX}_{b,a}(\mathsf{disc}_b(x(a))) \\
&\quad = \nu a.\, \mathsf{cX}_{a,b}\big(\mathsf{cX}_{b,a}(\mathsf{disc}_a(x(b)))\big) \\
&\quad = \nu a.\, \mathsf{cX}_{b,a}(\mathsf{disc}_a(x(b))) && (5) \\
&\quad = \nu a.\, \mathsf{Had}_a\big(\mathsf{cZ}_{a,b}(\mathsf{Had}_a(\mathsf{disc}_a(x(b))))\big) \\
&\quad = \nu a.\, \mathsf{Had}_a\big(\mathsf{cZ}_{a,b}(\mathsf{disc}_a(x(b)))\big) && (3) \\
&\quad = \nu a.\, \mathsf{Had}_a(x(b) \;?_a\; \mathsf{Z}_b(x(b))) && (2)
\end{aligned}
$$