Kvantni algebrajski učinki

Strah

26. 5. 2022

mentor: doc. dr. Matija Pretnar

Motivacija

Kvantno programiranje

- Novi problemi za teorijo programskih jezikov
- Enakost programov

Motivacija

Kvantno programiranje

- Novi problemi za teorijo programskih jezikov
- Enakost programov

1. Dva izziva:
   - Strojna oprema
   - Programska oprema
2. Kloniranje
   - Linearnost

Pregled

- Kratek opis kvantne mehanike
- Definiramo algebrajski jezik
- Podamo model za ta jezik
- ”Dokažemo” polnost

Kvantni vektorji

Definicija (Binarni vektorji)

Binarni vektorji so elementi prostora $\mathbf{B}_n := 2^n$ *in jih pišemo kot nize.*

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

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 ($n = 1$)

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

Primer ($n = 2$)

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

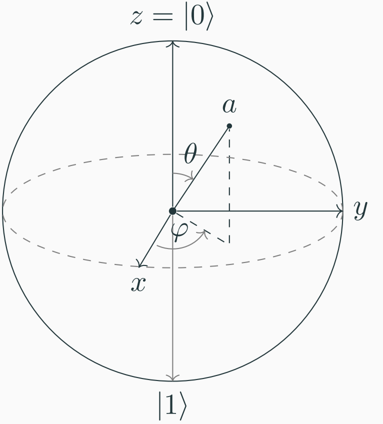
Primer (Hadamardov vektor)

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

Blochova sfera

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

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



Tenzorski produkt

Definicija (Tenzorski produkt)

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

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

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

Primeri

Primer

$$\mathbf{h}_n = \mathbf{h}^{\otimes n} = \rho^n \underbrace{(|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle)}_{n}.$$

$$\mathbf{H}_n = \mathbf{H}^{\otimes n}.$$

Definicija

Če lahko vektor $a \in \mathbf{H}_n$ zapišemo kot $\bigotimes_{j=1}^{n} a_j$ z $a_j \in \mathbf{H}$ pravimo, da je enostaven ali separabilen, sicer je pa sestavljen ali kvantno prepleten.

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)

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

Primeri

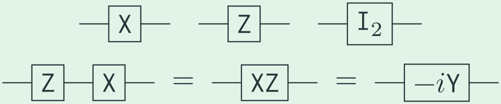
Primer (Paulijeve matrike)

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)



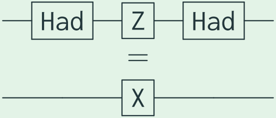
Primeri

Primer (Hadamardova matrika)

Predstavlja rotacijo okrog $x = z, y = 0$ premice.

$$\text{Had} = \rho \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \text{Had}(|0\rangle) = \mathbf{h}$$

Primer (Hadamardova matrika)

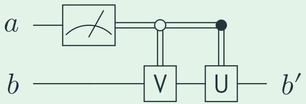


Kvantna meritev

Definicija (Kvantna meritev)

Meritev kubita $a = a_0 |0\rangle + a_1 |1\rangle$ *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)



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

Kvantna kontrola

Definicija

Kontrola "na ena" in "na nič".

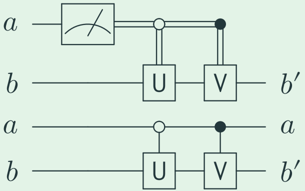
$$C_{r,s}(U)\,|j\rangle = \begin{cases} |j\rangle & ; \quad j_r = 0 \\ |j_1 \ldots\rangle\,|Uj_s\rangle\,|\ldots j_n\rangle & ; \quad j_r = 1 \end{cases}$$

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

Posebej za $U \in \mathrm{U}_2$ označimo

$$\mathsf{cU} := C_{1,2}(U) = D(\mathtt{I}_2, \mathsf{U}), \quad \bar{\mathsf{c}}\mathsf{U} := \overline{C}_{1,2}(U) = D(\mathsf{U}, \mathtt{I}_2).$$

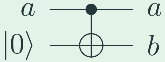
Primer



$$\texttt{\textbf{if}}\ \underline{\mathsf{measure}}(a) = 0\ \texttt{\textbf{then}}\ (a, Ub)\ \texttt{\textbf{else}}\ (a, Vb)$$

Primer (Prepleteni pari kubitov)

$$\mathsf{cX}(a \otimes |0\rangle) = "a \otimes b" = a_0\,|00\rangle + a_1\,|11\rangle$$



Algebrajski jezik

- Tip kubitov `qubit`. Funkcije dostopanja:
  - new$(a.t)$: Dodeli nov kubit, z začetno vrednostjo $|0\rangle$
  - apply$_{\mathsf{U}}(a;\, b.t)$: Uporabi vrata U na danem vektorju
  - measure$(a;\, t, u)$: Izmeri kubit, nadaljuje v t ali u
  - discard$(a;\, t) \coloneqq$ measure$(a;\, t, t)$
- Za tipa A in B obstaja tip $A \otimes B$ prepletenih parov.

Aksiomi

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

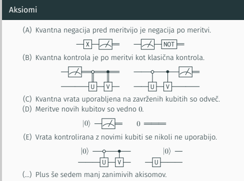
(B) Kvantna kontrola je po meritvi kot klasična kontrola.

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

(D) Meritve novih kubitov so vedno 0.

(E) Vrata kontrolirana z novimi kubiti se nikoli ne uporabijo.

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



Lahko prestavim malo kasneje

1. Kvantna negacija in kontrola se obnašata kot klasični verziji.
2. discard dela kot pričakujemo.
3. Novi kubiti so vedno $|0\rangle$ glede na meritev in kontrolo.
4. Sklopa sta
   4.1 apply se razume z matrikami.
   4.2 Stvari komutirajo, kolikor lahko, do vezave spremenljivk.

Algebrajska teorija

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*-ti veže* m_i *parametrov. Pišemo O :* $(p \mid m_1, ..., m_k)$*.*

$$\mathsf{new} : (0 \mid 1) \qquad \mathsf{measure} : (1 \mid 0, 0) \qquad \mathsf{apply}_{\mathsf{U}} : (n \mid n)$$

$$\frac{\Gamma \mid \Delta, a \vdash t}{\Gamma \mid \Delta \vdash \mathsf{new}(a.t)} \qquad \frac{\Gamma \mid \Delta \vdash t \qquad \Gamma \mid \Delta \vdash u}{\Gamma \mid \Delta, a \vdash \mathsf{measure}(a;\, t, u)}$$

$$\frac{\Gamma \mid \Delta, a_1, ..., a_n \vdash t}{\Gamma \mid \Delta, a_1, ..., a_n \vdash \mathsf{apply}_{\mathsf{U}}(a_1, ..., a_n;\, t)}$$

C^*-algebre

Definicija

A je C^*-algebra, če:

- *je normiran $\mathbb{C}$-vektorski prostor,*
- *ima množenje in enoto,*
- *ima involucijo, za katero velja $\|x\|^2 = \|x^* x\|$*

Za nas so $\mathbf{M}_n := M_n(\mathbb{C})$ unitarne $n \times n$ matrike.

Definicija

Za $A, B \in \mathbf{Cstar}$ je $f : A \to B$ $*$-homomorfizem, če je linearna preslikava, ki ohranja množenje, enoto, in involucijo.

C^*-algebre

Definicija

A je C^*-algebra, če:

- *je normiran $\mathbb{C}$-vektorski prostor,*
- *ima množenje in enoto,*
- *ima involucijo, za katero velja $\|x\|^2 = \|x^*x\|$*

Za nas so $\mathbf{M}_n := M_n(\mathbb{C})$ unitarne $n \times n$ matrike.

Definicija

Za $A, B \in \mathbf{Cstar}$ je $f : A \to B$ $*$-homomorfizem, če je linearna preslikava, ki ohranja množenje, enoto, in involucijo.

1. Involucija je hermitsko transponiranje

Matrike

Trditev

Velja $M_n(\mathbf{M}_p) = \mathbf{M}_{np}$

Vsaka linearna preslikava $f : X \to Y$ *se naravno razširi do* $M_n(f) : M_n(X) \to M_n(Y)$.

Velja $M_n(X \oplus Y) \cong M_n(X) \oplus M_n(Y)$

Trditev

Izraze algebrajske teorije interpretiramo z unitarnimi matrikami: Izraz $x_1 : m_1, ..., x_k : m_k \mid a_1, ..., a_p \vdash t$ *interpretiramo kot linearno preslikavo* $[\![t]\!] : \mathbf{M}_{2^{m_1}} \oplus \cdots \oplus \mathbf{M}_{2^{m_k}} \to \mathbf{M}_{2^p}$.

Trditev

Velja $M_n(\mathbf{M}_p) = \mathbf{M}_{np}$

Vsaka linearna preslikava $f : X \to Y$ *se naravno razširi do* $M_n(f) : M_n(X) \to M_n(Y)$.

Velja $M_n(X \oplus Y) \cong M_n(X) \oplus M_n(Y)$

Trditev

Izraze algebrajske teorije interpretiramo z unitarnimi matrikami: Izraz $x_1 : m_1, \ldots, x_k : m_k \mid a_1, \ldots, a_p \vdash t$ *interpretiramo kot linearno preslikavo* $[\![t]\!] : \mathbf{M}_{2^{m_1}} \oplus \cdots \oplus \mathbf{M}_{2^{m_k}} \to \mathbf{M}_{2^p}$.

$M_n(X)$ predstavlja n prepletenih parov X

Osnovne operacije

Definicija

Operaciji measure in apply$_{\mathsf{U}}$ *interpretiramo z* $*$*-homomorfizmoma measure* : $\mathbf{M}_{2^0} \oplus \mathbf{M}_{2^0} \to \mathbf{M}_{2^1}$ *in apply*$_{\mathsf{U}}$: $\mathbf{M}_{2^p} \to \mathbf{M}_{2^p}$, *s predpisoma*

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

$$\text{measure} : (1 \mid 0, 0) \qquad \text{apply}_{\mathsf{U}} : (p \mid p)$$

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* $\Gamma \mid \Delta \vdash t = u$.

Dokaz

Definicija

Množica Bratelijevih diagram za signaturo $(p \mid m_1, \ldots, m_k)$ *je množica* k*-teric* $(s_i)_i$*, tako da velja* $\sum_{i=1}^k s_k m_k = p$*.*

Izrek

$*$*-homomorfizmi* $\mathbf{M}_k \to \mathbf{M}_n$ *so oblike* $A \mapsto U^* D(A, \ldots, A, 0) U$ *za neko unitarno matriko* U*.*

Izrek

$\mu : \mathbf{Brat}(p \mid m_1, \ldots, m_k) \leftrightarrow \mathbf{Cstar}(\mathbf{M}_{2^{m_1}} \oplus \cdots \oplus \mathbf{M}_{2^{m_k}}, \mathbf{M}_{2^p}) : \rho$ *obstajata in* $\rho\mu = \mathrm{id}$*.*

Enakost $\rho(f) = \rho(g)$ *velja natanko tedaj, ko obstaja unitarna matrika* U*, tako da za vsak* $\underline{A}$ *velja* $f(\underline{A}) = U^* g(\underline{A}) U$*.*

Dokaz

Definicija

Množica Bratelijevih diagram za signaturo $(p \mid m_1, ..., m_k)$ je množica k-teric $(s_i)_i$, tako da velja $\sum_{i=1}^{k} s_k m_k = p$.

Izrek

$*$-homomorfizmi $\mathbf{M}_k \to \mathbf{M}_n$ so oblike $A \mapsto U^* D(A, ..., A, 0) U$ za neko unitarno matriko U.

Izrek

$\mu : \mathbf{Brat}(p \mid m_1, ..., m_k) \leftrightarrow \mathbf{Cstar}(\mathbf{M}_{2^{m_1}} \oplus \cdots \oplus \mathbf{M}_{2^{m_k}}, \mathbf{M}_{2^p}) : \rho$ obstajata in $\rho\mu = \mathrm{id}$.

Enakost $\rho(f) = \rho(g)$ velja natanko tedaj, ko obstaja unitarna matrika U, tako da za vsak $\underline{A}$ velja $f(\underline{A}) = U^* g(\underline{A}) U$.

1. $k \leq n, n = mk + r$
2. $\mu(s_1, ..., s_k)(A_1, ..., A_k) = D(A_1, ..., A_1, A_2, ..., A_k)$.
3. Dokaz: znamo prehajat med $\mathbf{Brat}$ in $\mathbf{Cstar}$, želimo iz T v $\mathbf{Cstar}$, gremo prek $\mathbf{Brat}$, znamo v $\mathbf{Brat}$, iz $\mathbf{Brat}$ gremo z measure
4. Tako dobimo točno, kar želimo (obliko apply(measure(...)))
5. Ostane pokazati, da je to surjekcija, sledi, ker lahko uporabimo aksiome, da preuredimo vsak izraz v tako obliko, te pa dobimo vse

new

Definicija

Operacijo new interpretiramo kot linearno preslikavo new : $\mathbf{M}_{2^1} \to \mathbf{M}_{2^0}$*, s predpisom 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.*

Pišemo $\mathbf{Cstar}_{\mathrm{CPU}}$.

Dokaz, da ni $*$-homomorfizem: $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

new

Definicija

Operacijo new interpretiramo kot linearno preslikavo new : $\mathbf{M}_{2^1} \to \mathbf{M}_{2^0}$, *s predpisom 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.

Pišemo $\mathbf{Cstar}_{\mathrm{CPU}}$.

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

Izrek (o minimalnosti dilacije)

Lahko izberemo minimalno dilacijo; če je $r \geq p$ in $h : \mathcal{A} \to \mathbf{M}_p$ $*$-homomorfizem tak, da je $h(-)|_p = f(-)$ je $r \geq q$ in $g(-) = Uh(-)U^*|_q$.

Dokaz

Izrek (Stinespringov izrek o dilaciji)
Naj bo $f : \mathcal{A} \to \mathbf{M}_p$ CPU. Tedaj obstaja $q \geq p$ in $*$-homomorfizem $g : \mathcal{A} \to \mathbf{M}_q$, tako da je $f(A) = g(A)|_p$.

Izrek (o minimalnosti dilacije)
Lahko izberemo minimalno dilacijo; če je $r \geq p$ in $h : \mathcal{A} \to \mathbf{M}_p$ $*$-homomorfizem tak, da je $h(-)|_p = f(-)$ je $r \geq q$ in $g(-) = Uh(-)U^*|_q$.

Diagrami