Kvantni algebrajski učinki

Strah

26. februar 2022

Povzetek

Motivacija

Kvantni programski jeziki predstavljajo nove probleme za teorijo programskih jezikov, kot so linearnost tipov, (kvantni) fizikalni pojavi, in še mnogi drugi. V tej nalogi se bomo posvetili tema dvema. Naš cilj je razumeti, kako se kvantne programe, in dober način je razumevanje enakosti programov, tj. kdaj sta dva programa enaka?

Pregled

Najprej bomo predstavili algebrajsko teorijo za kvantne programe; ta je zgrajena na unitarnih vratih in meritvah ter ima linearne parametre. Nato bomo dokazali, da lahko s to teorijo predstavimo vse programe (polnost) in nato iz nje izpeljali pravila za enakost kvantnih programov.

I Kvantno računalništvo ter algebrajski učinki in diagrami

I.1 Kvantna mehanika

Ta del je povzet po [1].

Oznake

Skozi ta del bomo uporabljali naslednje oznake:

- $\mathbb{N} = \{0, \dots\}, \mathbb{N}_+ = \{1, \dots\}$,
- $n \in \mathbb{N}_+$, ki mu bomo pravili število kubitov,
- $j, k, \dots \in \{0, \dots, 2^n - 1\}$,
- $j = j_1 \dots j_n$ binarni zapis števila j,
- $\mathbf{n} = \{0, \dots, n-1\}$, na primer $\mathbf{2} = \{0, 1\}$.

I.1.1 Kvantni vektorji

Definicija 1. Binarni vektorji so elementi prostora $\mathbf{B}_n \coloneqq \mathbf{2}^n$ in jih pišemo kot nize v binarnem zapisu.

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

Opomba. 1 in 01 predstavljata različna vektorja.

Definicija 2 (Hilbertov prostor)**.** Elementom prostora $\mathbf{H}_n \coloneqq \mathbb{C}^{2^n}$ pravimo kvantni vektorji, elementom $\mathbf{H} \coloneqq \mathbf{H}_1$ pa kubiti. Prostoru $\mathbf{H}_n$ torej pravimo prostor kvantnih vektorjev reda n, njegovo standardno bazo pa označimo z $\{e_j\}$.

Definicija 3 (Braket notacija)**.** Naj bo $j \in \{0, \dots, 2^n - 1\}$, ter $\hat{\jmath} \in \mathbf{B}_n$ pripadajoč vektor v binarnem zapisu. Potem je $|j\rangle = |\hat{\jmath}\rangle \coloneqq e_j$.

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

Primer $(n = 1)$**.**

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

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)**.**

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

I.1.2 Tenzorski produkt

Definicija 4 (Tenzorski produkt)**.** Tenzorski produkt prostorov $\mathbf{H}_n$ in $\mathbf{H}_m$ je enak $\mathbf{H}_{n+m}$. Pišemo $\mathbf{H}_n \otimes \mathbf{H}_m$. Če sta $a \in \mathbf{H}_n$ in $b \in \mathbf{H}_m$ je $a \otimes b \in \mathbf{H}_n \otimes \mathbf{H}_m$.

Opomba. Operator $\otimes$ je res tenzorski produkt.

Primer ($n = m = 1$)**.**

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

Primer.

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

Primer (Hadamardov vektor kot tenzorski produkt)**.**

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

Primer (Hilbertov prostor kot tenzorski produkt)**.**

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

Definicija 5. Če lahko $a \in \mathbf{H}_n$ zapišemo kot $\bigotimes_{j=1}^{n} a_j$ za neke $a_j \in \mathbf{H}$ pravimo, da je enostaven ali separabilen, sicer je pa sestavljen oziroma kvantno prepleten.

I.1.3 Kvantne preslikave/Unitarna vrata

Definicija 6. Unitarna vrata reda n so unitarna matrika dimenzije 2^n. Tenzorski produkt vrat $U \otimes V \coloneqq [u_{jk} V]_{j,k}$ uporabljen na $a \otimes b$ je enak $Ua \otimes Vb$.

Primer (Tenzorski produkt vrat)**.**

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

Definicija 7. Za vrata $U_0, \ldots, U_n$ označimo njihovo bločno-diagnoalno matriko z $D(U_0, \ldots, U_n)$.

Izrek 1 (No cloning)**.** *Ne obstaja unitarna matrika (vrata reda 2), ki vsak vektor $a \otimes \left|0\right\rangle \in \mathbf{H} \otimes \mathbf{H}$ slika v $a \otimes a$.*

Dokaz. Naj bo U tak, da $\forall a \in \mathbf{H}$ velja $U(a \otimes \left|0\right\rangle) = a \otimes a$.
Potem za $\mathbf{h} \otimes \left|0\right\rangle = \rho(\left|00\right\rangle + \left|10\right\rangle)$ velja:

$$U(\rho(\left|00\right\rangle + \left|10\right\rangle)) = \begin{cases} \rho^2(\left|00\right\rangle + \left|01\right\rangle + \left|10\right\rangle + \left|11\right\rangle), \\ \rho U \left|00\right\rangle + U \left|10\right\rangle = \rho(\left|00\right\rangle + \left|11\right\rangle), \end{cases}$$

kar je protislovje. □

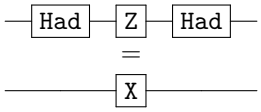
Primer (Paulijeve matrike)**.** To so matrike zrcaljenja okrog osi na Blochovi sferi:

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

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

Primer (Hadamardova matrika)**.**

$$\texttt{Had} = \rho \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \texttt{Had}(|0\rangle) = \mathbf{h}, \quad \texttt{Had}^{\otimes n}(|0^n\rangle) = \mathbf{h}_n.$$



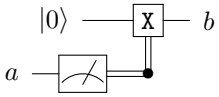
Primer (Fazni zamik)**.**

$$S_\alpha = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix}, \text{ posebej označimo } S := S_{\pi/2}\colon\ S^2 = X$$
$$S_\alpha \left(a_0 |0\rangle + a_1 |1\rangle\right) = a_0 |0\rangle + a_1 e^{i\alpha} |1\rangle .$$

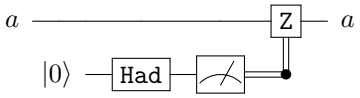
I.1.4 Kvantna meritev

Definicija 8 (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 (Projekcija na Z os)**.**



Primer (Naključna rotacija faze)**.**



I.2 Algebrajski učinki

Definicija 9 (Računski učinki)**.** Če ima funkcija ali operacija še kak navzven viden učinek poleg vrnjene vrednosti temu pravimo računski učinek (učinek računanja).

Definicija 10 (Algebrajski učinki)**.** So računski učinki, ki jih lahko predstavimo z algebrajsko teorijo.

I.3 Kvantno računalništvo

Kaj sploh imamo?

- Tip kubitov `qubit`. Funkcije dostopanja:
  - $\underline{\mathsf{new}}$: dodeli nov kubit, z začetno vrednostjo $|0\rangle$.
  - $\underline{\mathsf{apply}}_{\mathtt{U}}$: Uporabi vrata U na danem kubitu.
  - $\underline{\mathsf{measure}}$: izvede meritev na kubitu, vrne element tipa `bit`.
- Za tipa A in B obstaja tip $A \otimes B$ prepletenih parov.

Primer (Prepleteni pari kubitov)**.** Obstajajo ti. kontrolirana vrata, na primer `cX`. $\underline{\mathsf{apply}}_{\mathtt{cX}}(a, b)$ se obnaša kot **`if`** $\underline{\mathsf{measure}}(a) = 0$ **`then`** (a, b) **`else`** $(a, \neg b)$

Kvantni programski jezik	Algebrajski izrazi	Matematični simboli
`let` $a \leftarrow \underline{\mathsf{new}}()$ `in` t	$\mathsf{new}(a.\,t)$	$\nu a.\,t$
$\underline{\mathsf{apply}_{\mathtt{U}}}(a)\,;\ x\,(a)$	$\mathsf{apply}_{\mathtt{U}}(a.\,t)$	$\mathtt{U}_a(t)$
`if` $\underline{\mathsf{measure}}(a) = 0$ `then` t `else` u	$\mathsf{measure}(a.\,t; u)$	$t \mathbin{?_a} u$
`if` $\underline{\mathsf{measure}}(a) = 0$ `then` t `else` t	$\mathsf{discard}(a.\,t)$	$\mathsf{disc}_a(t)$

I.3.1 Pretvorba v algebrajske izraze

Primer (Projekcija na Z-os)**.**

1. `if` $\underline{\mathsf{measure}}\,(a) = 0$ `then` $\underline{\mathsf{new}}()$ `else` $\underline{\mathsf{apply}_{\mathtt{X}}}(\underline{\mathsf{new}}())$
2. $\mathsf{measure}\Big(a.\,\mathsf{new}(b.\,x\,(b)); \mathsf{new}\Big(b.\,\mathsf{apply}_{\mathtt{X}}(b.\,x\,(b))\Big)\Big)$
3. $(\nu a.\,x\,(a)) \mathbin{?_b} (\nu a.\,\mathtt{X}_a(x\,(a)))$

Primer (Naključna rotacija faze)**.**

1. `if` $\underline{\mathsf{measure}}\Big(\underline{\mathsf{apply}_{\mathtt{Had}}}(\underline{\mathsf{new}}())\Big) = 0$ `then` a `else` $\underline{\mathsf{apply}_{\mathtt{Z}}}(a)$
2. $\mathsf{new}\Big(b.\,\mathsf{apply}_{\mathtt{Had}}\Big(b.\,\mathsf{measure}\Big(b.\,x\,(a)\,; \mathsf{apply}_{\mathtt{Z}}(a.\,x\,(a))\Big)\Big)\Big)$
3. $\nu a.\,\mathtt{Had}_a(x\,(b) \mathbin{?_a} \mathtt{Z}_b(x\,(b)))$

I.3.2 Aksiomi

Osnovni aksiomi na kratko:

Kvantna negacija pred meritvijo je negacija po meritvi.

$$\mathtt{X}_a(x \mathbin{?_a} y) = y \mathbin{?_a} x \tag{1}$$

Kvantna kontrola je po meritvi kot klasična kontrola.

$$\mathtt{U}_b(x(b)) \mathbin{?_a} \mathtt{V}_b(y(b)) = D(\mathtt{U}, \mathtt{V})_{a,b}(x(b) \mathbin{?_a} y(b)) \tag{2}$$

Kvantna vrata uporabljena na zavrženih kubitih so odveč.

$$\mathtt{U}_a(\mathsf{disc}_a(t)) = \mathsf{disc}_a(t) \tag{3}$$

Meritve novih kubitov so vedno 0.

$$\nu a.\,x \mathbin{?_a} y = x \tag{4}$$

Vrata kontrolirana z novimi kubiti se nikoli ne uporabijo.

$$\nu a.\,D(\mathtt{U}, \mathtt{V})_{a,b}(x(a,b)) = \mathtt{U}_b(\nu a.\,x(a,b)) \tag{5}$$

Ostanejo še bolj „administrativni“ aksiomi.

Spoštovanje simetrične grupe.

$$\mathtt{swap}_{a,b}(x(a,b)) = x(b,a) \tag{6}$$
$$\mathtt{I}_a(x(a)) = x(a) \tag{7}$$
$$\mathtt{UV}_a(x(a)) = \mathtt{U}_a(\mathtt{V}_a(x(a))) \tag{8}$$
$$\mathtt{U} \otimes \mathtt{V}_{a,b}(x(a,b)) = \mathtt{U}_a(\mathtt{V}_b(x(a,b))) \tag{9}$$

Komutativnost.

$$(u \mathbin{?_b} v) \mathbin{?_a} (x \mathbin{?_b} y) = (u \mathbin{?_a} x) \mathbin{?_b} (v \mathbin{?_a} y) \tag{10}$$
$$\nu a.\,\nu b.\,x(a,b) = \nu b.\,\nu a.\,x(a,b) \tag{11}$$
$$\nu a.\,x(a) \mathbin{?_b} y(a) = (\nu a.\,x(a)) \mathbin{?_b} (\nu a.\,y(a)) \tag{12}$$

Primer.

$$
\begin{aligned}
&(\nu a.\, x\,(a))\ ?_b\ (\nu a.\, \mathtt{X}_a(x\,(a))) \\
&\quad = \nu a.\, x\,(a)\ ?_b\, \mathtt{X}_a(x\,(a)) && (12)\\
&\quad = \nu a.\, \mathtt{cX}_{b,a}(x\,(a)\ ?_b\, x\,(a)) && (2)\\
&\quad = \nu a.\, \mathtt{cX}_{b,a}(\mathsf{disc}_b(x\,(a))) && (\text{def.})\\
&\quad = \nu a.\, \mathtt{cX}_{a,b}\big(\mathtt{cX}_{b,a}(\mathsf{disc}_a(x\,(b)))\big)\\
&\quad = \nu a.\, \mathtt{cX}_{b,a}(\mathsf{disc}_a(x\,(b))) && (5)\\
&\quad = \nu a.\, \mathtt{Had}_a\big(\mathtt{cZ}_{a,b}(\mathtt{Had}_a(\mathsf{disc}_a(x\,(b))))\big)\\
&\quad = \nu a.\, \mathtt{Had}_a\big(\mathtt{cZ}_{a,b}(\mathsf{disc}_a(x\,(b)))\big) && (3)\\
&\quad = \nu a.\, \mathtt{Had}_a(x\,(b)\ ?_a\, \mathtt{Z}_b(x\,(b))). && (2)
\end{aligned}
$$

Literatura

[1] Sebastian Xambó Juanjo Rué. „Mathematical Essentials of Quantum Computing“. V: 2011.