Kvantni algebrajski učinki

Rok Strah

mentor: doc. dr. Matija Pretnar

22. 11. 2021

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

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

Definicija (Kvantna vrata)

Kvantna vrata reda n *so unitarne matrike dimenzije* 2^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 ($n = 2$)

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

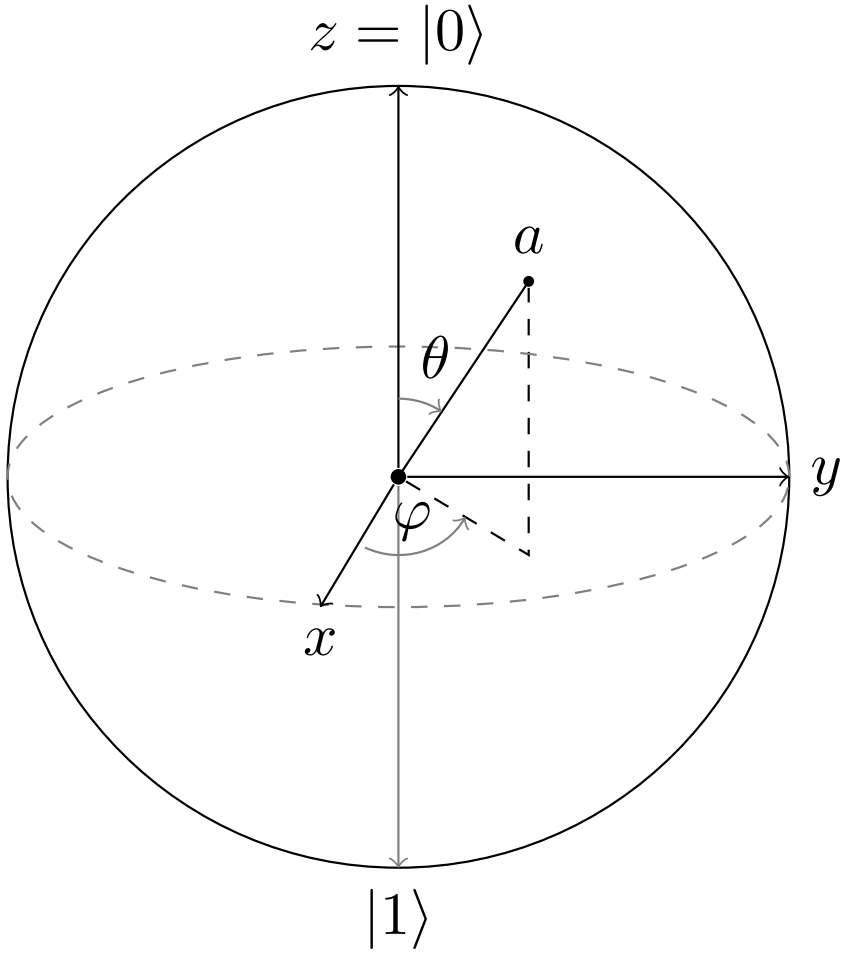
Primer (Hadamardov vektor)

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

Blochova sfera

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

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



Primeri

Primer (Paulijeve matrike)

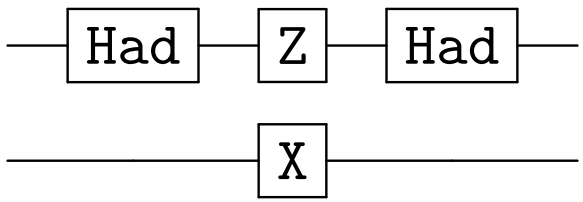
To so matrike zrcaljenja okrog osi na Blochovi sferi:

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

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

Primer (Hadamardova matrika)

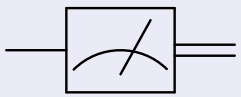
$$\texttt{Had} = \rho \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \texttt{Had}(|0\rangle) = \mathbf{h}$$



Kvantna meritev

Definicija (Kvantna meritev)

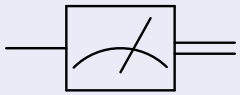
Meritev kubita $a = a_0 |0\rangle + a_1 |1\rangle$ *označimo* $M(a)$ *in je* 0 *z verjetnostjo* $|a_0|^2$ *in* 1 *z verjetnostjo* $|a_1|^2$. *To "uniči" kubit* a.



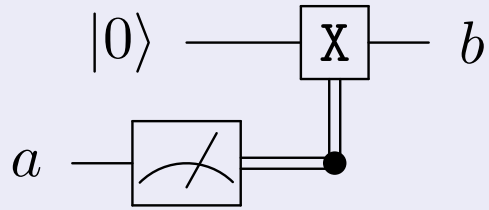
Kvantna meritev

Definicija (Kvantna meritev)

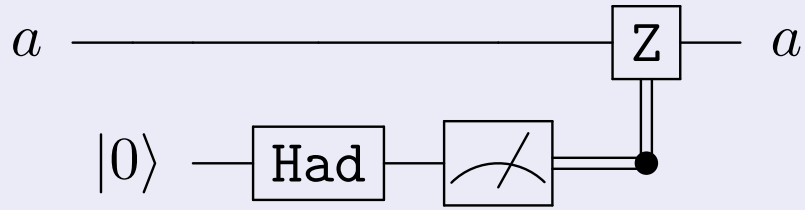
Meritev kubita $a = a_0 |0\rangle + a_1 |1\rangle$ *označimo* $M(a)$ *in je* 0 *z verjetnostjo* $|a_0|^2$ *in* 1 *z verjetnostjo* $|a_1|^2$*. To "uniči" kubit* a*.*



Primer (Projekcija na Z os)



Primer (Naključna rotacija faze)



Algebrajski učinki

Definicija (Računski učinki)

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

Algebrajski učinki

Definicija (Računski učinki)

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

Definicija (Algebrajski učinki)

So računski učinki, ki jih lahko predstavimo z algebrajsko teorijo.

Motivacija

- Kvantni programski jeziki predstavljajo nove probleme za teorijo programskih jezikov.
  - Linearnost
  - Učinki

Motivacija

- Kvantni programski jeziki predstavljajo nove probleme za teorijo programskih jezikov.
  - Linearnost
  - Učinki
- Dober način razumevanja je, da razumemo enakost programov.

Pregled

- Predstavimo algebrajsko teorijo za kvantne izračune
  - Zgrajena na unitarnih vratih in meritvah
  - Ima linearne parametre
- Dokažemo polnost v tej teoriji
- Iz algebre izpeljemo pravila za enakost kvantnih programov

Kvantno računalništvo

Kaj sploh imamo?

- Tip kubitov `qubit`. Funkcije dostopanja:
  - new: dodeli nov kubit, z začetno vrednostjo $|0\rangle$.
  - apply_U: Uporabi vrata U na danem kubitu.
  - measure: izvede meritev na kubitu, vrne element tipa `bit`.

Kvantno računalništvo

Kaj sploh imamo?

- Tip kubitov `qubit`. Funkcije dostopanja:
  - new: dodeli nov kubit, z začetno vrednostjo $|0\rangle$.
  - apply_U: Uporabi vrata U na danem kubitu.
  - 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 t.i. kontrolirana vrata, na primer `cX`. $\text{apply}_{\texttt{cX}}(a, b)$ *se obnaša kot* ***if*** $\text{measure}(a) = 0$ ***then*** (a, b) ***else*** $(a, \neg b)$.

Pretvorba v algebrajske izraze

Primer (Projekcija na Z os in naključna rotacija faze)

1. ***if*** $\underline{\text{measure}}(a) = 0$ ***then*** $\underline{\text{new}}()$ ***else*** $\underline{\text{apply}_{\texttt{X}}}(\underline{\text{new}}())$
2. ***if*** $\underline{\text{measure}}(\underline{\text{apply}_{\texttt{Had}}}(\underline{\text{new}}())) = 0$ ***then*** a ***else*** $\underline{\text{apply}_{\texttt{Z}}}(a)$

Pretvorba v algebrajske izraze

Primer (Projekcija na Z os in naključna rotacija faze)

1. $\textit{if}\ \underline{\mathsf{measure}}(a) = 0\ \textit{then}\ \underline{\mathsf{new}}()\ \textit{else}\ \underline{\mathsf{apply}_{\mathtt{X}}}(\underline{\mathsf{new}}())$
2. $\textit{if}\ \underline{\mathsf{measure}}(\underline{\mathsf{apply}_{\mathtt{Had}}}(\underline{\mathsf{new}}())) = 0\ \textit{then}\ a\ \textit{else}\ \underline{\mathsf{apply}_{\mathtt{Z}}}(a)$

- $\mathsf{new}(a.x(a)) := \mathtt{let}\ a \leftarrow \underline{\mathsf{new}}()\ \mathtt{in}\ x(a)$
- $\mathsf{apply}_{\mathtt{U}}(a.x(a)) := \underline{\mathsf{apply}_{\mathtt{U}}}(a);\ x(a)$
- $\mathsf{measure}(a; t, u) := \mathtt{if}\ \underline{\mathsf{measure}}(a) = 0\ \mathtt{then}\ t\ \mathtt{else}\ u$
- $\mathsf{discard}(a.t) := \mathsf{measure}(a; t, t)$

Pretvorba v algebrajske izraze

Primer (Projekcija na Z os in naključna rotacija faze)

1. $\mathbf{if}\ \underline{\mathsf{measure}}(a) = 0\ \mathbf{then}\ \underline{\mathsf{new}}()\ \mathbf{else}\ \underline{\mathsf{apply}_{\mathtt{X}}}(\underline{\mathsf{new}}())$
2. $\mathbf{if}\ \underline{\mathsf{measure}}(\underline{\mathsf{apply}_{\mathtt{Had}}}(\underline{\mathsf{new}}())) = 0\ \mathbf{then}\ a\ \mathbf{else}\ \underline{\mathsf{apply}_{\mathtt{Z}}}(a)$

- $\mathsf{new}(a.x(a)) := \mathbf{let}\ a \leftarrow \underline{\mathsf{new}}()\ \mathbf{in}\ x(a)$
- $\mathsf{apply}_{\mathtt{U}}(a.x(a)) := \underline{\mathsf{apply}_{\mathtt{U}}}(a);\ x(a)$
- $\mathsf{measure}(a; t, u) := \mathbf{if}\ \underline{\mathsf{measure}}(a) = 0\ \mathbf{then}\ t\ \mathbf{else}\ u$
- $\mathsf{discard}(a.t) := \mathsf{measure}(a; t, t)$

Primer (Projekcija na Z os in naključna rotacija faze)

1. $\mathsf{measure}\big(a; \mathsf{new}(b.x(b)), \mathsf{new}\big(b.\mathsf{apply}_{\mathtt{X}}(b.x(b))\big)\big)$
2. $\mathsf{new}\big(b.\mathsf{apply}_{\mathtt{Had}}\big(b.\mathsf{measure}\big(b; x(a), \mathsf{apply}_{\mathtt{Z}}(a.x(a))\big)\big)\big)$

Pretvorba v algebrajske izraze

Primer (Projekcija na Z os in naključna rotacija faze)

1. $\mathsf{measure}\big(a; \mathsf{new}(b.x(b)), \mathsf{new}\big(b.\mathsf{apply}_{\mathtt{X}}(b.x(b))\big)\big)$
2. $\mathsf{new}\big(b.\mathsf{apply}_{\mathtt{Had}}\big(b.\mathsf{measure}\big(b; x(a), \mathsf{apply}_{\mathtt{Z}}(a.x(a))\big)\big)\big)$

Pretvorba v algebrajske izraze

Primer (Projekcija na Z os in naključna rotacija faze)

1. $\mathsf{measure}\big(a; \mathsf{new}(b.x(b)), \mathsf{new}\big(b.\mathsf{apply}_{\mathtt{X}}(b.x(b))\big)\big)$
2. $\mathsf{new}\big(b.\mathsf{apply}_{\mathtt{Had}}\big(b.\mathsf{measure}\big(b; x(a), \mathsf{apply}_{\mathtt{Z}}(a.x(a))\big)\big)\big)$

- $\nu a.\, t := \mathsf{new}(a.t)$
- $\mathtt{U}_a(t) := \mathsf{apply}_{\mathtt{U}}(a.t)$
- $t \mathbin{?}_a u := \mathsf{measure}(a; t, u)$
- $\mathsf{disc}_a(t) := \mathsf{discard}(a.t)$

Pretvorba v algebrajske izraze

Primer (Projekcija na Z os in naključna rotacija faze)

1. $\mathsf{measure}\big(a; \mathsf{new}(b.x(b)), \mathsf{new}\big(b.\mathsf{apply}_{\mathtt{X}}(b.x(b))\big)\big)$
2. $\mathsf{new}\big(b.\mathsf{apply}_{\mathtt{Had}}\big(b.\mathsf{measure}\big(b; x(a), \mathsf{apply}_{\mathtt{Z}}(a.x(a))\big)\big)\big)$

- $\nu a.\, t := \mathsf{new}(a.t)$
- $\mathtt{U}_a(t) := \mathsf{apply}_{\mathtt{U}}(a.t)$
- $t \mathbin{?}_a u := \mathsf{measure}(a; t, u)$
- $\mathsf{disc}_a(t) := \mathsf{discard}(a.t)$

Primer (Projekcija na Z os in naključna rotacija faze)

1. $(\nu a.\, x(a)) \mathbin{?}_b (\nu a.\, \mathtt{X}_a(x(a)))$
2. $\nu a.\, \mathtt{Had}_a(x(b) \mathbin{?}_a \mathtt{Z}_b(x(b)))$

Aksiomi

Osnovni aksiomi na kratko:

1. Kvantna negacija pred meritvijo je negacija po meritvi.
2. Kvantna kontrola je po meritvi kot klasična kontrola.
3. Kvantna vrata uporabljena na zavrženih kubitih so odveč.
4. Meritve novih kubitov so vedno 0.
5. Vrata kontrolirana z novimi kubiti se nikoli ne uporabijo.
6. Plus še sedem manj zanimivih akisomov.

Uporaba

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