Univerza v Ljubljani
Fakulteta
za računalništvo
in informatiko

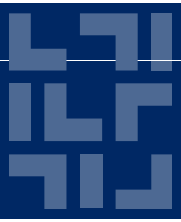


# 3. Kvantno procesiranje (angl. Quantum Computing)

Vsebina 3. poglavja predavanj (II.st.RI)

Avtor: izr.prof.dr. Miha Mraz

Štud.leto: 2012/2013

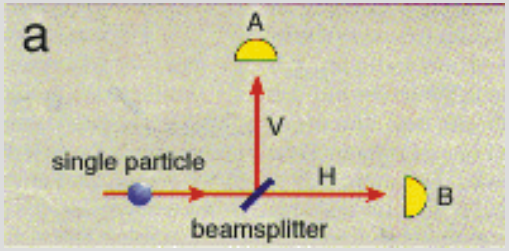


# 3.1.Uvod v kvantno procesiranje

- *Kvantno procesiranje*: kakršnokoli procesiranje, ki ga vrši kvantni računalnik
- Definicija *kvantnega računalnika*: kakršnakoli procesna naprava, ki izkorišča fenomene kvantne mehanike (npr. lastnosti superpozicije, zapleta, itd.) za izvajanje operacij nad podatki
- Kvantni fenomeni: temeljijo na teoriji kvantne fizike
- Konvencionalni rač.sistemi temeljijo na mehanskih (zgod.), elektromehanskih (zgod.) in elektronskih fizikalnih zakonitostih (sedanjost)
- Napovedi: kvantni računalniki bodo omogočali eksponentno povečanje hitrosti reševanja problemov (ne pa samega takta ure delovanja)

# Osnovna ideja: superpozicija

- Klasična fizika: pot fotona od izvora v A ali B (ali = XOR); foton nedeljiv delec; verjetnosti nahajanja v A ali B sta enaki
- Kvantna mehanika: pot fotona bo vodila v A in B
- Klasični računalniki:
  - Osnovna entiteta pomnjenja bit
  - Njegova vrednost izražena z napetostnimi nivoji



# 3.2. Kvantni bit ali Qubit

•Kvantni računalniki: kakršenkoli dvostanjski kvantni sistem je sposoben pomnjenja **qubita** (angl. *qubit*)

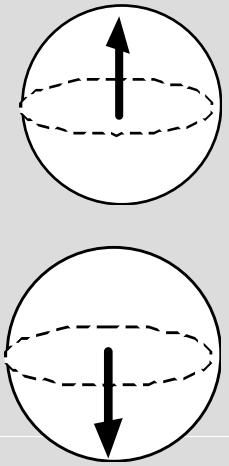
• bra/ket notacija:

$|q\rangle$ **ket notacija**: stolpični vektor (zapis **kvantnega stanja**)

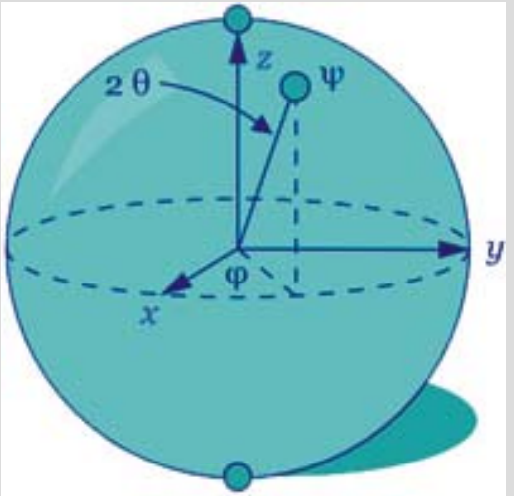
$\langle q|$ **bra notacija**: vrstični vektor

• $|0\rangle$ : qubit je v fizikalnem stanju, ki ponazarja bitno vrednost 0 (interpretacija s spinom elektrona: grafično v sferi navzgor obrnjen vektor -slika zgoraj)

• $|1\rangle$ : qubit je v fizikalnem stanju, ki ponazarja bitno vrednost 1 (grafično v sferi navzdol obrnjen vektor – slika spodaj)



- Qubit ima namesto dveh stabilnih stanj (0 ali 1) stanja definirana z vektorjema $a|0\rangle$ in $b|1\rangle$, ki popišejo vse možne lokacije v sferi, a in b sta amplitudi superpozicioniranega stanja
- Splošen zapis kvantega stanja (stanje imenujemo tudi za valovno funkcijo):
  - $|q\rangle = a|0\rangle + b|1\rangle$



- Kvantni sistem se lahko nahaja v dveh osnovnih stanjih $|0\rangle$ , $|1\rangle$, ali v SUPERPOZICIJI (v obeh potencialnih stanjih HKRATI)
- Veljajo izrazi:

$$|q\rangle = a|0\rangle + b|1\rangle,$$

$$|a|^2 + |b|^2 = 1,$$

$$a = x_0 + iy_0, b = x_1 + iy_1,$$

$$|a| = \sqrt{x_0^{\,2} + y_0^{\,2}}, |b| = \sqrt{x_1^{\,2} + y_1^{\,2}}.$$

$|0\rangle$

$|1\rangle$

- Definicija: *Qubit je dvostanjski kvantni dinamični sitem, ki si ga v logičnem smislu interpretiramo kot dvo-dimenzionalen Hilbertov prostor. V njem imamo fiksno bazo B= ( |0⟩, |1⟩), stanji pa poimenujemo za osnovni.*
- Opazovanje (branje) qubita nam bo vrnilo vrednosti a in b.

# 3.3. Kvantni register

- Kvantni register: sekvenca qubitov
- Funkcija: hranjenje in obdelava kvantne besede
- *n* bitov v klasičnem bitnem registru: register je **v enem** od $2^n$ možnih stanj
- *n* qubitov v klasičnem registru: register se hipotetično zaradi superpozicije lahko nahaja **v vseh možnih** $2^n$ stanjih -> efektivnejši zapis podatkov in višja efektivnost izvajane operacije (velika stopnja paralelizma, koncept SIMD)

# 3.4. Kvantna logična operacija (kvantna logična vrata)

- Definicija: *Kvantna logična operacija je unitarna preslikava U: H2->H2.*
- $|0\rangle$-> a $|0\rangle$ + b $|1\rangle$
- $|1\rangle$-> c $|0\rangle$ + d $|1\rangle$
- U je unitarna <->
  - $U^*U^T=U^T*U=I$
  - U je reda *n*n*
  - I je enotska matrika

$$U = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

- Izvedba preslikave stanja $|q\rangle = a|0\rangle + b|1\rangle$ na osnovi logičnih vrat f (predstavljena z U)

$$U * \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} c \\ d \end{bmatrix}$$

- Negator: $U_{neg}$

$$U_{neg} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- Z funkcija: $U_z$

$$U_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Hadamard: $U_H$

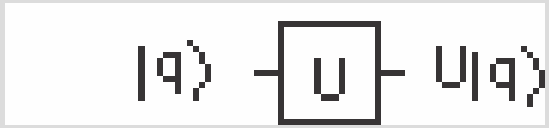
$$U_H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

- Unitarna transformacija, ki deluje na manjšem število kubitov (npr.1, 2 ali 3)
- Hadamardova vrata (delujejo nad 1 kubitom):
  - $|0\rangle$ -> 1/sqrt(2)( $|0\rangle$ + $|1\rangle$ )
  - $|1\rangle$ -> 1/sqrt(2)( $|0\rangle$ - $|1\rangle$ )
- Toffolijeva vrata (negacija tretjega qubita, če sta prva dva po vrednosti 1
  - $|0,0,0\rangle$ -> $|0,0,0\rangle$, $|0,0,1\rangle$ -> $|0,0,1\rangle$,
  - $|0,1,0\rangle$ -> $|0,1,0\rangle$, $|0,1,1\rangle$ -> $|0,1,1\rangle$,
  - $|1,0,0\rangle$ -> $|1,0,0\rangle$, $|1,0,1\rangle$ -> $|1,0,1\rangle$,
  - $|1,1,0\rangle$ -> $|1,1,1\rangle$, $|1,1,1\rangle$ -> $|1,1,0\rangle$

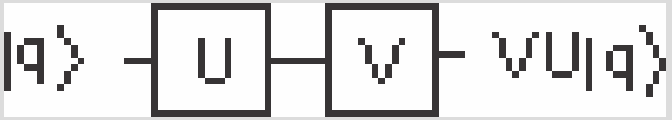
- Hadamardova in Toffolijeva vrata skupaj tvorita **Univerzalni** nabor kvantni vrat (to je vse kar potrebujemo za kvantni računalnik)
- S tem naborom lahko modeliramo poljubna druga kvantna vrata

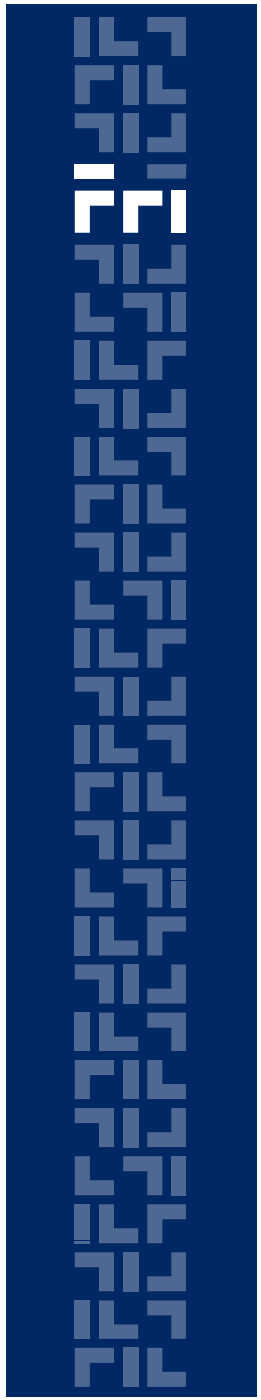
Grafično ponazarjanje kvantnih vezij:

- 1.Operacija U nad $|q\rangle$




- 2.Operaciji U in V nad $|q\rangle$

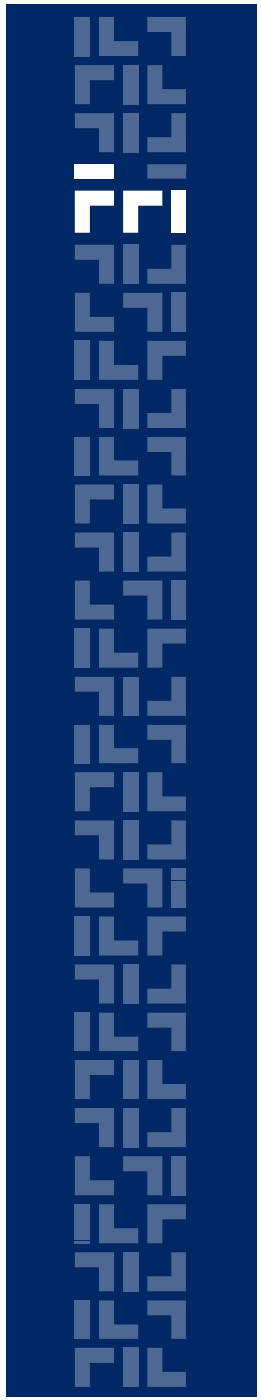




- Definicija: *Kvantni algoritem je algoritem, ki s svojimi napotki kakorkoli izkorišča značilnosti superpozicije. Z operacijskega vidika vrši modifikacijo (množenje) kvantnega registra z unitarno matriko.*
- Unitarnost matrike omogoča reverzibilnost procesa.

# 3.5. Invazivnost branja qubitov v stanju superpozicije

- Praviloma so vse meritve superpozicioniranih qubitov invazivne, kar pomeni, da qubit “preide” zgolj v eno od dveh osnovnih stanj. Ta proces je ireverzibilen. Meritev pa vseeno vrne kvadrat amplitud a in b, kar si intepretiramo kot verjetnosti nahajanja v stanju $|0\rangle$ in $|1\rangle$.
- Prednosti invazivnosti:
  - Varen prenos podatkov
  - Brez kopiranja

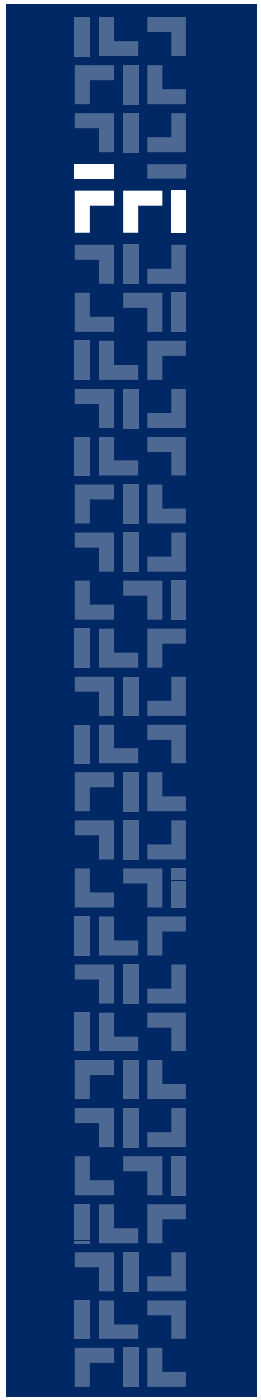


# 3.6. Osnovne značilnosti kvantnega procesiranja

- Poleg superpozicije so lastnosti še:
  - Interferenca
  - Zaplet (angl. entaglement)
  - Kvantna nedeterminističnost
  - Neklonirnost

# 3.7. Delovanje kvantnega računalnika

- Koncept delovanja *pripravi – razvij - izmeri*:
  - Pripravi: postavitev kvantnega registra v začetno stanje (npr. vsi qubiti se postavijo v stanje $|0\rangle$ )
  - Razvij: izvaja se zaporedje operacij, ki spremeni začetno stanje registra v potencialna superpozicionirana stanja (sprejemljive rešitve)
  - Izmeri: vrne eno od stanj superpozicije



# 3.8. Aplikativne prednosti kvantnega procesiranja

- Hitro iskanje podatkov
- Hitri enkripcijski postopki
- Hitra faktorizacija števil (Shorov algoritem)
- Kvantna teleportacija

# 3.9. Realizacije kvantnega računalnika

Družina D-Wave: prve komercialne izvedenke

- Leto 2008: 28 kubitni delovni register
- Leto 2010 (plan) 128 kubitni del.register
- http://www.dwavesys.com/
- Reklama na desni: 24.10.11
- Apl.področje **D-wave One**: „Markov random field“

# 3.10. Literatura poglavja


[1] M.Hirvensalo: Quantum computing (knjigo si lahko sposodite pri prof.Mrazu)

[2] A.O. Pittenger: An Introduction to Quantum Computing Algorithms (knjigo si lahko sposodite pri prof.Mrazu)

[3] http://www-users.cs.york.ac.uk/schmuel/comp/

[4] M.Nagy, S.G.Akl: Quantum computation and Quantum information (Technical report 2005-496)