Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

4. Kvantno procesiranje

II.stopnja RI, 2014/2015

Nosilec: prof.dr.Miha Mraz

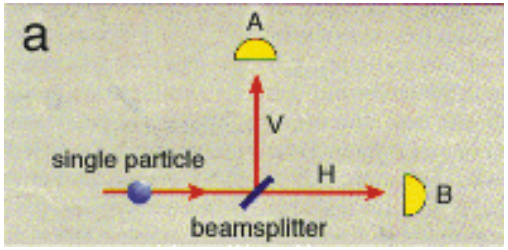
14. oktober 2014

1. Uvod

- Angl. *quantum computing*;
- *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)

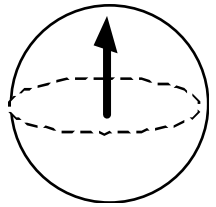
2. Ideja superpozicije

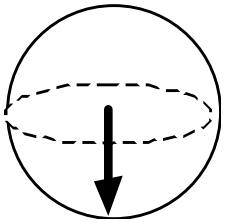
- Klasična fizika: pot fotona od izvora v A ali B (ali = XOR); foton nedeljiv delec; verjetnosti nahajanja v A ali B sta enaki
- Kvantna mehanika: pot fotona bo vodila v A in B
- Klasični računalniki:
  - Osnovna entiteta pomnjenja bit
  - Njegova vrednost izražena z napetostnimi nivoji



3. Kvantni bit ali qubit

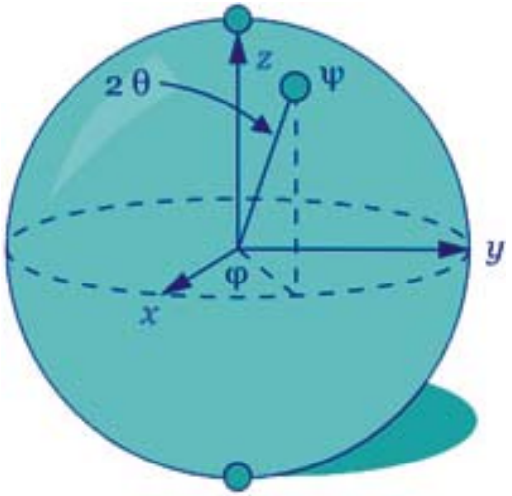
- Kvantni računalniki: kakršenkoli dvostanjski kvantni sistem je sposoben pomnjenja **qubita** (angl. *qubit*)
- bra/ket notacija: $|q\rangle$ **ket notacija**: stolpični vektor (zapis **kvantnega stanja**) $\langle q|$ **bra notacija**: vrstični vektor
- $|0\rangle$: qubit je v fizikalnem stanju, ki 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, ali linearno kombinacijo dveh osnovnih stanj):

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



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

$$|q\rangle = a|0\rangle + b|1\rangle,$$
$$|a|^2 + |b|^2 = 1,$$
$$a = x_0 + iy_0, b = x_1 + iy_1,$$
$$|a| = \sqrt{x_0{}^2 + y_0{}^2}, |b| = \sqrt{x_1{}^2 + y_1{}^2}.$$

- 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.

4. 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, kvantni paralelizem, koncept SIMD)

5. Kvantna logična operacija nad enim qubitom

- 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 mora biti unitarna <->
  - $U^*U^T=U^T*U=I$
  - U je reda *n*n*
  - I je enotska matrika
- Red matrike: odvisen od števila qubitov, nad katerimi se izvede operacija

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

- Izvedba preslikave stanja $|q\rangle = a|0\rangle + b|1\rangle$ na osnovi logičnih vrat f (predstavljena z U)
- Negator: U_{neg}
- Z funkcija: U_z ($|0\rangle$ ostaja nespremenjen, nad $|1\rangle$ se izvede fazni premik

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

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

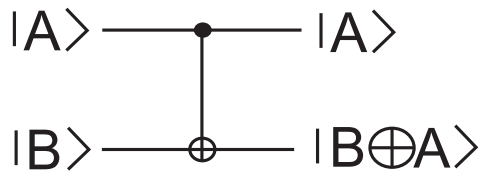
$$U_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Hadamard: U_H (izvede superpozicioniranje)
- Hadamardova vrata (delujejo nad 1 kubitom):
  - $|0\rangle$ -> 1/sqrt(2)($|0\rangle$ + $|1\rangle$)
  - $|1\rangle$ -> 1/sqrt(2)($|0\rangle$ - $|1\rangle$)

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

6. Kvantna logična operacija nad več qubiti

- Unitarne transformacije, ki delujejo na večjem številu kubitov (npr. 2 ali 3 treh)
- „Controlled NOT" (CNOT) vrata:
  - Prvi qubit $|A\rangle$ - kontrolni qubit
  - Drugi qubit $|B\rangle$ - ciljni (angl. target) qubit
  - Če je A=0, B ostaja nespremenjen
  - Če je A=1, se B negira
  - $|00\rangle$->$|00\rangle$, $|01\rangle$->$|01\rangle$, $|10\rangle$->$|11\rangle$, $|11\rangle$->$|10\rangle$
  - Splošneje; $|A,B\rangle$->$|A, B \text{ XOR } A\rangle$

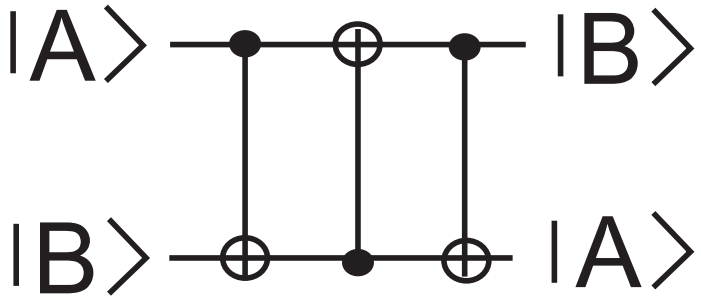


$$U_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

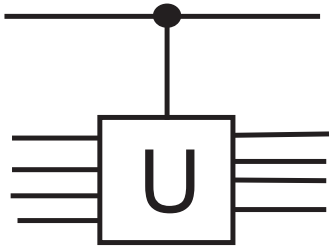
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} * \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}$$

- CNOT (nadaljevanje):
  - Posplošitev XOR vrat
  - **Kakršnakoli logična operacija nad več qubiti je lahko realizirana z CNOT vrati in operacijami nad enim qubitom (paralela z univerzalnostjo nabora NAND v klasični procesni logiki)**

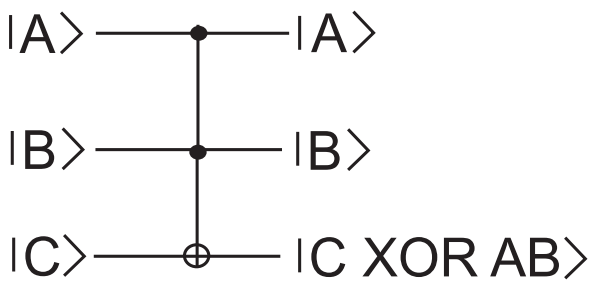
- Primer kvantnega vezja (angl. quantum circuit) – izmenjava stanj dveh qubitov (angl. swaping the states):
- $|A,B\rangle \rightarrow |A,A \text{ XOR } B\rangle$
  - $\rightarrow |A \text{ XOR } (A \text{ XOR } B), A \text{ XOR } B\rangle = |B, A \text{ XOR } B\rangle$
  - $\rightarrow |B, (A \text{ XOR } B) \text{ XOR } B\rangle = |B,A\rangle$
- Vezje s slike beremo od leve proti desni



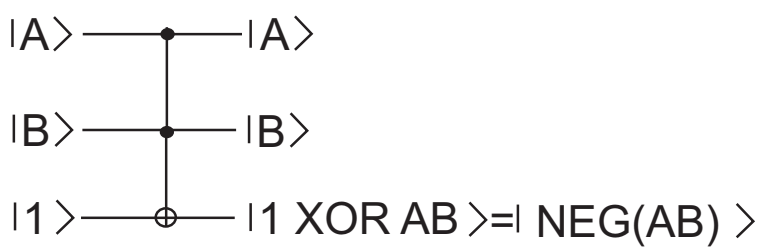
- „Controlled U-gate“:
  - Razširjava CNOT vrat;
  - En kontrolni qubit
  - N ciljnih (angl. *target*) qubitov
  - Kontrolni qubit = 0 -> ciljni qubiti se ne obdelajo
  - Kontrolni qubit = 1 –> U matrika izvede logično operacijo nad N qubiti (vrsta operacije je določena z matriko U)

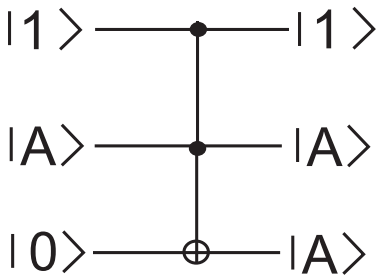


- Toffolijeva vrata (negacija tretjega qubita, če sta prva dva po vrednosti 1
  - $|0,0,0\rangle \rightarrow |0,0,0\rangle$, $|0,0,1\rangle \rightarrow |0,0,1\rangle$,
  - $|0,1,0\rangle \rightarrow |0,1,0\rangle$, $|0,1,1\rangle \rightarrow |0,1,1\rangle$,
  - $|1,0,0\rangle \rightarrow |1,0,0\rangle$, $|1,0,1\rangle \rightarrow |1,0,1\rangle$,
  - $|1,1,0\rangle \rightarrow |1,1,1\rangle$, $|1,1,1\rangle \rightarrow |1,1,0\rangle$
- (a,b,c)->(a,b,c XOR ab) -> (a,b,c) REVERZIBILNOST



- Univerzalnost Toffolijevih vrat – z njimi lahko realiziramo NAND vrata:
- FAN-OUT množenje signalov s pomočjo Toffolijevih vrat:

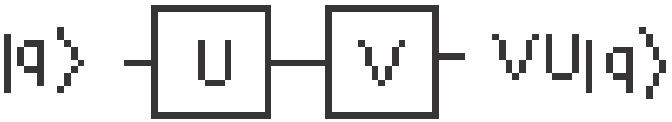




- Hadamardova in Toffolijeva vrata vsaka posebej tvorita **Univerzalni** nabor kvantnih vrat (to je vse kar potrebujemo za kvantni računalnik)
- S tem naborom lahko modeliramo poljubna druga kvantna vrata

- 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.

7. Invazivnost branja qubitov v stanju superpozicije

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

8. Osnovne značilnosti kvantnega procesiranja

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

9. Delovanje kvantnega računalnika

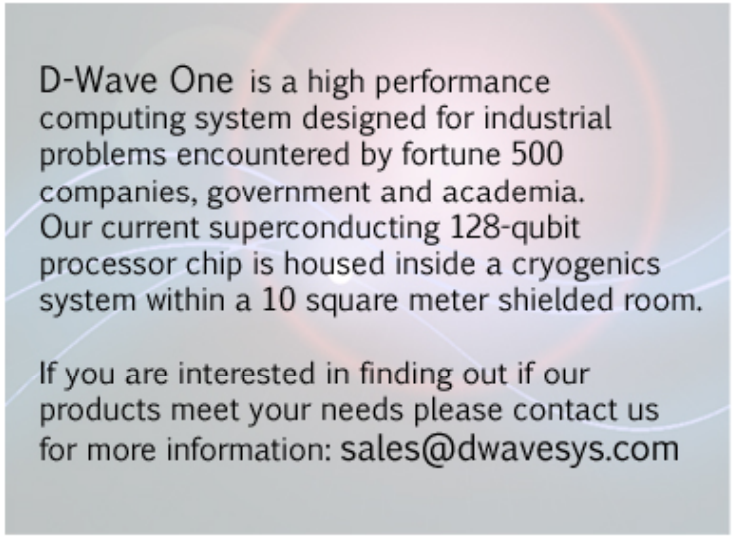
- Koncept delovanja *pripravi – razvij - izmeri*:
  - Pripravi: postavitev kvantnega registra v začetno stanje (npr. vsi qubiti se postavijo v stanje $|0\rangle$)
  - Razvij: izvaja se zaporedje operacij, ki spremeni začetno stanje registra v potencialna superpozicionirana stanja (sprejemljive rešitve)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

10. Aplikativne prednosti kvantnega procesiranja

- Hitro iskanje podatkov (Grover 1996: O(n/2) -> O(sqrt(n)), n – število podatkov
- Hitri enkripcijski postopki
- Hitra faktorizacija števil (Shorov algoritem 1994: $O(e^{L**(1/3)})$ -> $O(L^2)$, L – število digitov faktoriziranega števila
- Kvantna teleportacija

11. Realizacija 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 zgoraj (24.10.11), desno spodaj (21.10.13)
  - Apl.področje **D-wave One**: „Markov random field"



The D-Wave Two™ system is a high performance computing system designed for industrial problems encountered by Fortune 500 companies, government and academia. Our latest superconducting 512-qubit processor chip is housed inside a cryogenics system within a 10 square meter shielded room. If you are interested in finding out if this quantum computing system meets your needs please contact us for more information.

12. Orodja za snovanje kvantnih vezij

- http://qcraft.org/ (google)
- http://tph.tuwien.ac.at/~oemer/qcl.html (QCL - Quantum computing language
- Več povezav: http://en.wikipedia.org/wiki/Quantum_programming
- http://www.quantiki.org/wiki/List_of_QC_simulators

13. Literatura

- [1] M.A.Nielsen et.al.: Quantum Computation and Quantum Information, Cambridge Press, 2009 (9. izdaja)
- [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)
- [5] http://www.quantiki.org/ - več informacij