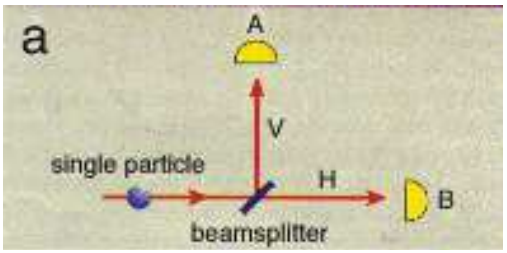
# Poglavje 1

# Kvantno procesiranje

*Kvantno procesiranje* (angl. *quantum computation*) je definirano kot kakršnokoli procesiranje, ki ga vrši *kvantni računalnik* (angl. *quantum computer*). Če delovanje klasičnega računalnika temelji na zakonih klasične fizike (klasične mehanike), bo delovanje kvantnega računalnika temeljilo na zakonih *kvantne fizike* ali *kvantne mehanike* [1].

Osnovna ideja kvantnega procesiranja izhaja iz enostavnega fizikalnega poizkusa. Predpostavimo, da vir svetlobe, ki je sestavljen iz nedeljivih delcev fotonov, naleti na zrcalo. V tem primeru se del svetlobe odbija proti točki A, del pa proti točki B. Intuitivno bi lahko sklepali, da se del fotonov, ki so načeloma nedeljivi, odbije v eni, del fotonov pa v drugi smeri. Vsak posamezni foton, bi bil usmerjen tako na lokacijo A ali na lokacijo B. Pri tem je uporaba besedice "ali" v predhodnjem stavku mišljena kot ekskluzivna (XOR) disjunkcija. Kvantna fizika pojasnjuje, da se vsak foton odbije v obeh smereh, čeprav gre za nedeljiv delec [2]. Tako lahko sklepamo, da se isti delec lahko po odboju nahaja na večih pozicijah hkrati. Če tovrstnemu delcu zaupamo vlogo *nosilca stanj* in njegovo stanje $q(t)$ v času $t$ izenačimo z njegovo pozicijo, lahko sklepamo, da je tovrstni delec lahko istočasno v več stanjih hkrati. Slednjo značilnost imenujemo za *superpozicijo* (angl. *superposition*). Opisani eksperiment je predstavljen na sliki 1.1 povzeti po viru [3]. V nadaljevanju definiramo pojem




Slika 1.1: Odboj fotona na lokaciji A in B (slika je povzeta po viru [3]).

*kvantnega računalnika* [4].

**Definicija 1** *Kvantni računalnik je kakršnakoli procesna naprava, ki izkorišča fenomene kvantne mehanike (npr. lastnosti superpozicije) za izvajanje operacij nad podatki.*

Osnova kvantnega računalnika je lahko *dvostanjski* ali *večstanjski kvantni sistem*. V pričujočem poglavju se bomo ukvarjali le z kvantnimi sistemi, ki temeljijo na *dveh osnovnih kvantnih stanjih*. Če je v klasični dvovrednostni logiki osnovna manipulativna enota ali nosilec informacije *bit*, slednjo vlogo v sistemu z dvemi osnovnimi kvantnimi stanji prevzame *qubit*, ki ga opišemo v naslednjem razdelku.

## 1.1 Qubit

V današnjih klasičnih elektronskih računalnikih je osnovna entiteta procesiranja, pomnjenja in prenašanja *bit*. Pri procesiranju si njegovo vrednost ali stanje, v katerem se nahaja, interpretiramo z napetostnimi nivoji. Osnovna entiteta procesiranja, pomnjenja in prenašanja v kvantnem sistemu z dvema osnovnima kvantnima stanjema je *kvantni bit* ali *qubit* (angl. *quantum binary digit*) [5]. Z razliko od bita, ki lahko hrani logično vrednost 0 ali 1, qubit lahko hrani osnovni logični vrednosti $|0\rangle$ ali $|1\rangle$ (slednji sovpadata z logičnima vrednostima 0 in 1), ali pa linearno kombinacijo obeh logičnih vrednosti hkrati (se nahaja v obeh stanjih hkrati in je *superpozicioniran*) [1]. Kvantni logični vrednosti $|0\rangle$ in $|1\rangle$ poimenujemo za *osnovni kvantni stanji*, vse njune linearne kombinacije pa za *superpozicionirana stanja*.

Notacija označevanja stanja qubita temelji na Diracovi *bra*/*ket* notaciji stanj v kvantnem sistemu [5]. Pri tem pod oznako *ket* smatramo zapis $|x\rangle$, ki ga interpretiramo kot *stolpični vektor* in ponazarja *kvantno stanje* enega ali več qubitov, pod oznako *bra* pa zapis $\langle x|$, ki ga tretiramo kot *vrstični vektor*. Za dvostanjski kvantni sistem bi bila tako notacija osnovnih stanj sledeča:

- $|0\rangle$: qubit je v osnovnem stanju, ki ponazarja bitno vrednost 0;
- $|1\rangle$: qubit je v osnovnem stanju, ki ponazarja bitno vrednost 1;

Kvantno stanje $|q\rangle$ posameznega opazovanega qubita na osnovi *ket* notacije zapišemo z izrazom

$$|q\rangle = a\,|0\rangle + b\,|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}, \tag{1.1}$$

pri čemer sta $a$ in $b$ kompleksni števili ($a, b \in \mathbb{C}$), $|0\rangle$ in $|1\rangle$ pa ortonormalna bazna vektorja v dvodimenzionalnem kompleksnem prostoru [5]. Parametra $a$ in $b$ imenujemo tudi za *amplitudi superpozicioniranega stanja*. V primeru, da

imamo opravka s pari parametrov ($a = 1,\ b = 0$) ali ($a = 0,\ b = 1$), se qubit nahaja v enem od dveh osnovnih stanj, v primeru pa da sta vrednosti parametrov drugačni, se qubit nahaja v superpozicioniranem stanju. Za superpozicioniranost stanja qubita bomo v nadaljevanju podali še dodatno zahtevo, ki ju morata izpolnjevati parametra $a$ in $b$.

Stanje qubita je tako enolično predstavljeno s *stolpičnim vektorjem*. Izraz (1.1) stanja imenujemo tudi za *valovno funkcijo* qubita [6]. Glede na definicijo zapisa stanja v vektorski obliki se tako qubit lahko nahaja v enem od osnovnih stanj $|0\rangle$ ali $|1\rangle$, ali pa v superpoziciji obeh stanj. Za parametra $a$ in $b$ po virih [5], [6] in [7] veljata izraza

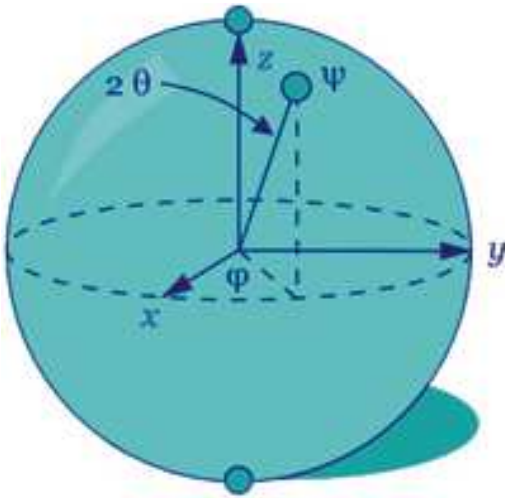
$$a = x_0 + iy_0,\ b = x_1 + iy_1,\ x_0, y_0, x_1, y_1 \in \mathbb{R}, \tag{1.2}$$

$$|a| = \sqrt{x_0^2 + y_0^2},\ |b| = \sqrt{x_1^2 + y_1^2}, \tag{1.3}$$

pri čemer mora biti veljavna relacija po izrazu

$$|a|^2 + |b|^2 = 1. \tag{1.4}$$

V matematičnem smislu si tako lahko zapis stanja posameznega qubita $|q\rangle$ interpretiramo kot *enotski vektor* v Blochovi sferi, ki vodi od središča sfere do njenega plašča. Na sliki 1.2 je v Blochovi sferi predstavljeno stanje qubita $|\psi\rangle$. Z različnimi vrednostmi parametrov $a$ in $b$ stolpičnega vektorja, ki ponazarja




Slika 1.2: Prikaz stanja qubita $|\psi\rangle$ z enotskim vektorjem v Blochovi sferi (vir: Wikipedia).

kvantno stanje posameznega qubita, je mogoče doseči vse lokacije na Blochovi sferi.

Na koncu pričujočega razdelka še formalno definirajmo termin qubita [8].

**Definicija 2** *Qubit je dvostanjski kvantni dinamični sistem, ki si ga v logičnem smislu interpretiramo kot dvodimenzionalni Hilbertov prostor. V njem imamo fiksno bazo* $B = \{|0\rangle, |1\rangle\}$*, stanji* $|0\rangle$ *in* $|1\rangle$ *pa poimenujemo za osnovni stanji. Meritev (branje) stanja qubita nam vrne vrednosti* $|a|^2$ *in* $|b|^2$*. Prva predstavlja verjetnost nahajanja qubita v osnovnem stanju* $|0\rangle$*, druga pa verjetnost nahajanja qubita v osnovnem stanju* $|1\rangle$*.*

## 1.2 Qubitni register

*Qubitni register* je sestavni del dvostanjskega kvantnega računalnika, ki vrši funkcijo delovne lokacije, v kateri se izvajajo logične operacije nad qubiti. Qubitni register je sestavljen iz $n$ pozicij na katerih se nahajajo vrednosti $n$ qubitov in ima funkcijo hrambe in obdelave *kvantne besede* dolžine $n$. V klasičnih računalniških sistemih je dolžina binarnih besed običajno 8, 16, 32 ali 64 bitov. Ob že znani predpostavki, da se posamezni qubiti lahko nahajajo tudi v superpozicioniranih stanjih, veljata naslednji ugotovitvi:

- qubitni register dolžine $n$ qubitov smatramo kot $2^n$ dimenzionalni kompleksni vektor;
- z razliko od bitnega registra dolžine $n$ bitov, ki hrani le eno od $2^n$ možnih različnih stanj, qubitni register dolžine $n$ qubitov lahko hrani do $2^n$ možnih različnih stanj istočasno; število stanj je odvisno od števila superpozicioniranih qubitov;

Glede na povedano qubitni register sestavljen iz $n$ qubitov omogoča dosti efektivnejši zapis podatkov, hkrati pa je efektivnejše tudi izvajanje operacij nad njim, saj se ena operacija ne izvede nad enim podatkom (enim stanjem registra), temveč nad večjo množico superpozicioniranih stanj. Družba D-Wave Inc., ki se ukvarja z razvojem kvantnih računalnikov, na svoji spletni strani (www.dwavesys.com) navaja, da bi qubitni register dolžine 300 qubitov predstavljal ekvivalent bitnemu registru dolžine $10^{90}$ bitov. Slednje število je večje, kot je predvidevano število atomov v vesolju. Po njihovih ocenah bi bil kvantni računalnik s qubitnim registrom dolžine 30 qubitov ekvivalenten računalniku z nekaj 10 TFlops-i procesne zmogljivosti.

Predpostavimo, da imamo opravka s kvantnim registrom dolžine treh qubitov. Če bi bil to klasičen bitni register, bi vanj lahko shranili eno od 8 različnih vrednosti iz množice zapisov $\{000, 001, 010, 011, 100, 101, 110, 111\}$ . Če iz navedenega nabora potencialnih vrednosti izberemo zapisa 110, 111, bi ju lahko v kvantnem registru hranili istočasno. Zadnji LSQ (angl. *least significant qubit*) qubit bi tako zapisali s superpozicioniranim zapisom

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{1.5}$$

stanje celotnega qubitnega registra pa s tenzorskim produktom vseh treh qubitov

$$|1\rangle \otimes |1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{1.6}$$

V primeru, da bi v qubitnem registru hoteli istočasno pomniti vseh osem različnih vrednosti, bi to zapisali s tenzorskim produktom

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) =$$
$$(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \otimes (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \otimes (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle). \tag{1.7}$$

## 1.3 Enovhodne kvantne logične operacije

Na začetku zapišimo formalno definicijo *kvantne logične operacije.*

**Definicija 3** *Kvantna logična operacija je definirana kot unitarna preslikava U, definirana po izrazu*

$$H2 \to H2, \tag{1.8}$$

*pri čemer H2 predstavlja dvodimenzionalni Hilbertov prostor.*

Kvantna logična operacija tako izvede *unitarno preslikavo* po izrazih

$$|0\rangle \to x_1|0\rangle + x_2|1\rangle, \tag{1.9}$$

$$|1\rangle \to x_3|0\rangle + x_4|1\rangle. \tag{1.10}$$

Unitarnost preslikave vektorja stanja zagotavlja, da se njegova značilnost enotskosti ohranja. Unitarnost preslikave je zagotovljena z unitarno preslikovalno matriko

$$U = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}. \tag{1.11}$$

Unitarnost matrike je izpolnjena, ko je matrika $U$ reda $nxn$ in velja izraz

$$U * U^T = U^T * U = I, \tag{1.12}$$

pri čemer je $U^T$ transponirana verzija matrike $U$, $I$ pa enotska matrika.

Logično operacijo nad enim qubitom ($|q\rangle = a|0\rangle + b|1\rangle$) bi tako zapisali z izrazom

$$U * \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} c \\ d \end{bmatrix}, \tag{1.13}$$

pri čemer je $U$ unitarna matrika reda 2x2, rezultat pa stolpični vektor reda 2x1.

Lastnost unitarnosti matrike omogoča *inherentno*[1] *reverzibilnost* kvantnih logičnih operacij.

[1] Inherentno - neločljivo, nerazdružno povezano s čim (Vir: SSKJ).

### 1.3.1 Kvantni negator

Najenostavnejši primer logične operacije nad enim qubitom je *kvantni negator*. Upoštevajoč zapis stanja qubita z izrazom

$$|q\rangle = a\,|0\rangle + b\,|1\rangle\,, \tag{1.14}$$

operacijo negacije ponazorimo z unitarno matriko

$$U_{neg} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{1.15}$$

Slednja daje kvantni negaciji pomen $NEG(|q\rangle)$ preko matematičnega izraza

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix}. \tag{1.16}$$

Tako negacijo stanja qubita $q$ ($|q\rangle = a\,|0\rangle + b\,|1\rangle$) zapišemo z izrazom

$$|\overline{q}\rangle = b\,|0\rangle + a\,|1\rangle\,. \tag{1.17}$$

### 1.3.2 $Z$ funkcija in Hadamardova funkcija

Kompleksnejši funkciji nad posameznim qubitom sta $Z$ funkcija in Hadamardova funkcija podani z unitarnima matrikama

$$U_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, U_{Hadamard} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{1.18}$$

$Z$ funkcija pusti $|0\rangle$ nespremenjen, na $|1\rangle$ pa izvede fazni premik (angl. *phase shift*) s spremembo predznaka. Hadamardova funkcija je ena od najpomembnejših kvantnih logičnih funkcij, saj izvede superpozicijo nad stanjem qubita, istočasno pa ima lastnosti reverzibilnosti. V izrazih (1.19) in (1.20) sta predstavljena rezultata omenjenih logičnih operacij.

$$U_Z * \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} * \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ -b \end{bmatrix} \tag{1.19}$$

$$U_{Hadamard} * \begin{bmatrix} a \\ b \end{bmatrix} = \frac{1}{\sqrt{2}} * \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} * \begin{bmatrix} a \\ b \end{bmatrix} = \frac{1}{\sqrt{2}} * \begin{bmatrix} a+b \\ a-b \end{bmatrix} \tag{1.20}$$

Čeprav imamo na prvi pogled možnih neskončno logičnih operacij nad qubitom, poljubna dvodimenzionalna unitarna matrika ne predstavlja logične operacije. Pogoj, ki omejuje možni prostor funkcij, je relacija $|a|^2 + |b|^2 = 1$, ki mora veljati za izhodiščno stanje, nad katerim deluje preslikava [5].

## 1.4 Superpozicija dveh ali več qubitov

Predpostavimo, da imamo opravka s sistemom, ki ga tvorita dva qubita. Množico *osnovnih stanj* takšnega sistema tvorijo stanja $|00\rangle$, $|01\rangle$, $|10\rangle$ in $|11\rangle$, lahko pa sta qubita tudi v superpoziciji $|q\rangle$ teh štirih osnovnih stanj, kar po viru [1] zapišemo z izrazom

$$|q\rangle = c_0\,|00\rangle + c_1\,|01\rangle + c_2\,|10\rangle + c_3\,|11\rangle\,,\ c_0, c_1, c_2, c_3 \in \mathbb{C}, \tag{1.21}$$

pri čemer so parametri $c_0$,...,$c_3$ pridobljeni s pomočjo *tenzorskega produkta*[2] po izrazih

$$|q\rangle = |q_1\rangle \otimes |q_2\rangle = |q_1, q_2\rangle = \begin{bmatrix} a_1 \\ b_1 \end{bmatrix} \otimes \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} = \tag{1.22}$$

$$\begin{bmatrix} a_1 \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} \\ b_1 \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_1a_2 \\ a_1b_2 \\ b_1a_2 \\ b_1b_2 \end{bmatrix}, \tag{1.23}$$

$$c_0 = a_1a_2,\ c_1 = a_1b_2,\ c_2 = b_1a_2,\ c_3 = b_1b_2. \tag{1.24}$$

Tudi v tem primeru velja relacija

$$|c_0|^2 + |c_1|^2 + |c_2|^2 + |c_3|^2 = 1. \tag{1.25}$$

V primeru, da imamo oprava s sistemom, ki ga tvori $n$ qubitov, njihovo superpozicionirano stanje zapišemo z izrazom

$$|q\rangle = \sum_{i=0}^{2^n-1} c_i\,|b_{i,n-1}b_{i,n-2}...b_{i,0}\rangle\,. \tag{1.26}$$

## 1.5 Večvhodne kvantne logične operacije

Tudi v primeru logičnih operacij na več qubitih, ki jih izvajajo večvhodne kvantne logične funkcije, morajo biti funkcijske matrike unitarne. V nadaljnjih razdelkih si bomo ogledali primere večvhodnih kvantnih logičnih funkcij Controlled NOT, Swaping gatein Controlled U gate.

### 1.5.1 Controlled NOT funkcija

Controlled NOT funkcija je dvovhodna in sicer vanjo vstopata qubita $q_1$ in $q_2$. Prvi qubit predstavlja *kontrolni qubit* (angl. *control qubit*), drugi pa *ciljni qubit* (angl. *target qubit*). V primeru, da je prvi qubit v osnovnem stanju $|0\rangle$, se stanje drugega qubita ne spremeni, če pa je prvi qubit v osnovnem stanju $|1\rangle$, se drugi qubit negira. V tem primeru na vhodna qubita gledamo kot na kvantni sistem,

[2] Več informacij o tenzorskem produktu bralec najde v matematičnih priročnikih [9], [10] ali na spletu (https://sl.wikipedia.org/wiki/Tenzorski_produkt).

tako da njuni stanji združimo v enoten zapis kvantnega stanja $|q_1 q_2\rangle$. Prehode iz osnovnih stanj para qubitov zapišemo z izrazom

$$|00\rangle \rightarrow |00\rangle\,,$$

$$|01\rangle \rightarrow |01\rangle\,,$$

$$|10\rangle \rightarrow |11\rangle\,,$$

$$|11\rangle \rightarrow |10\rangle\,. \tag{1.27}$$

Controlled NOT funkcijo lahko zapišemo tudi na osnovi XOR logične operacije ali seštevanja po modulu dva, ki jo zapisujemo s simbolom $\oplus$. Tako lahko zapišemo izraz

$$|A, B\rangle \rightarrow |A, A \quad \text{XOR} \quad B\rangle\,, \tag{1.28}$$

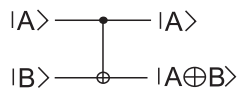
pri čemer $A$ predstavlja logično spremenljivko, katere vrednost ponazarja stanje qubita $|q_1\rangle$ in $B$ logično spremenljivko, katere vrednost ponazarja stanje qubita $|q_2\rangle$. Unitarno matriko, ki predstavlja Controlled NOT funkcijo zapišemo z izrazom

$$U_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \tag{1.29}$$

samo Controlled NOT logično operacijo nad dvema qubitoma v osnovnih stanjih pa z izrazom

$$U_{CNOT} * (|q_1\rangle \otimes |q_2\rangle) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} * \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}. \tag{1.30}$$

Na sliki 1.3 je predstavljen grafičen prikaz logičnega vezja Controlled NOT funkcije, ki smo ga predhodno že spoznali v poglavju o reverzibilnosti logičnih funkcij. Velja, da kakršnokoli logično operacijo nad več qubiti lahko realiziramo z




Slika 1.3: Grafična ponazoritev logičnega vezja Controlled NOT funkcije.

Controlled NOT funkcijami in operacijami nad enim qubitom. Omenjeni nabor predstavlja poln funkcijski nabor v svetu qubitnih logičnih operacij.

### 1.5.2 Swaping gate funkcija

Swaping gate funkcija zamenja stanji dveh qubitov (angl. *swaping the states*). V izrazu (1.31) je prikazan razvoj funkcije.

$$|A,B\rangle \rightarrow |A, A \quad \text{XOR} \quad B\rangle$$

$$\rightarrow |A \quad \text{XOR} \quad (A \quad \text{XOR} \quad B), A \quad \text{XOR} \quad B\rangle = |B, A \quad \text{XOR} \quad B\rangle\,,$$

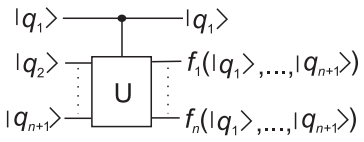
$$\rightarrow |B, (A \quad \text{XOR} \quad B) \quad \text{XOR} \quad B\rangle = |B, A\rangle\,. \tag{1.31}$$

Na sliki 1.4 je predstavljen grafičen prikaz logičnega vezja Swaping gate funkcije.


Slika 1.4: Grafična ponazoritev logičnega vezja Swaping gate funkcije (levo) in njen krajši grafični zapis (desno).

### 1.5.3 Controlled U-gate funkcija

Controlled U-gate funkcija predstavlja posplošitev Controlled NOT funkcije. Vhod funkcije vsebuje en kontrolni qubit in $n$ ciljnih qubitov. V primeru, da je kontrolni qubit v osnovnem stanju $|0\rangle$, se ciljni qubiti ne transformirajo, v primeru pa da je kontrolni qubit v osnovnem stanju $|1\rangle$, se izvede nad ciljnimi qubiti poljubno kvantno logično operacijo podano z unitarno matriko $U$. Iz opisa lahko pridemo do sklepa, da je Controlled NOT funkcija le poseben primer Controlled U-gate funkcije. Grafična predstavitev logičnega vezja Controlled U-gate funkcije je podana na sliki 1.5.



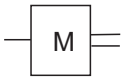

Slika 1.5: Grafična ponazoritev logičnega vezja Controlled U-gate funkcije.

## 1.6 Invazivnost branja qubita

V kvantnih sistemih so praviloma vsa branja ali meritve superpozicioniranih stanj qubitov *invazivna* [11], [1]. Slednje pomeni, da meritev transformira superpozicionirano stanja qubita bodisi v osnovno stanje $|0\rangle$, bodisi v osnovno

stanje $|1\rangle$, vsa dodatna informacijska vsebina o superpozicioniranosti pa se ob meritvi izgubi.

Za potrebe ponazarjanja kvantnih vezij vpeljemo posebno operacijo meritve $M$, ki je grafično ponazorjena na sliki 1.6. Predpostavljamo, da nam meritev $M$ za opazovano superpozicionirano stanje qubita $|q\rangle = a\,|0\rangle + b\,|1\rangle$ vrne vrednosti $|a|^2$ in $|b|^2$, pri čemer $|a|^2$ predstavlja verjetnost nahajanja v osnovnem stanju $|0\rangle$, $|b|^2$ pa verjetnost nahajanja v osnovnem stanju $|1\rangle$. Po izvedeni meritvi stanje $|q\rangle$ ni več superpozicionirano, temveč zasede eno od obeh možnih osnovnih stanj. O njem so podane le verjetnosti nahajanja v osnovnih stanj $|0\rangle$ in $|1\rangle$ in na ta način so amplitude superpozicioniranega stanja z izvedbo meritve za nadaljnje procesiranje nad sistemom kvantnega stanja izgubljene. Eventuelne ponovne meritve tako ne bodo več vrnile verjetnosti $|a|^2$ in $|b|^2$.




Slika 1.6: Grafična ponazoritev operacije meritve $M$, v katero z leve strani vstopa superpozicionirani qubit, na desni pa dobimo eno od obeh stabilnih stanj in verjetnosti osnovnih stanj qubita.

Ker je proces meritve ireverzibilen, bi moralo kvantno procesiranje potekati brez prisotnosti meritev (branj qubitov), ali pa bi meritve morali uporabljati samo za proces branja izhodnih vrednosti, pri katerem pričakujemo kot izhod samo eno od dveh možnih osnovnih stanj. Seveda moramo v tem primeru z vidika izbire kvantnih logičnih funkcij zagotoviti, da na izhodu dobimo samo eno od dveh osnovnih možnih stanj, ne pa superpozicioniranih, če le ta nosijo neko „dodano informacijsko vrednost“.

Zaradi invazivnosti branja se vsebine superpozicioniranega qubita ne da kopirati (angl. *no cloning theorem*). Slednje dejstvo poleg slabosti prinaša tudi prednosti, saj se nam s tem ponujajo nove možnosti uporabe kvantnih postopkov na različnih aplikacijskih področjih (npr. na področju varnega prenosa podatkov).

## 1.7 Kvantna vezja

*Kvantna vezja* (angl. *quantum circuit*) so sestavljena iz *kvantih vodil* (angl. *quantum wires*) in *kvantnih logičnih vrat* (angl. *quantum logic gates*), ki temeljijo na *kvantnih logičnih funkcijah* ali operacijah (angl. *quantum logical functions*, *quantum logical operations*). Pod pojmom kvantnega vodila nimamo primarno v mislih nekega fizičnega prenosnega medija, temveč nek virtualni kanal z njemu pripadajočo časovno latenco prenosa kvantnega stanja [1]. Nekaj primerov kvantnih vezij smo v grafičnem smislu že predstavili na slikah 1.3, 1.4 in 1.5.

Osnovna pravila za sestavljanje kvantnih vezij so sledeča:

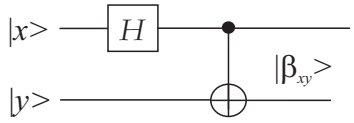
| In | Out |
|---|---|
| $\|00\rangle$ | $\frac{\|00\rangle+\|11\rangle}{\sqrt{2}} = \|\beta_{00}\rangle$ |
| $\|01\rangle$ | $\frac{\|01\rangle+\|10\rangle}{\sqrt{2}} = \|\beta_{01}\rangle$ |
| $\|10\rangle$ | $\frac{\|00\rangle-\|11\rangle}{\sqrt{2}} = \|\beta_{10}\rangle$ |
| $\|11\rangle$ | $\frac{\|01\rangle-\|10\rangle}{\sqrt{2}} = \|\beta_{11}\rangle$ |

Tabela 1.1: Pravilnostna tabela preslikave osnovnih stanj za pridobivanje Bellovih stanj.

- kvantna vezja z razliko od klasičnih vezij ne smejo vsebovati povratnih povezav (angl. *feedback*) in zank (angl. *loop*); slednje pomeni, da morajo biti kvantna vezja *aciklična*;
- v klasičnih vezjih lahko vodila združujemo (angl. *fanin*), kar nam omogoča izvajanje OR logične operacije na bitnem nivoju; ker je slednja operacija z logičnega vidika nereverzibilna, je združevanje vodil v kvantnih vezjih po dogovoru prepovedano;
- v klasičnih vezjih uporabljamo tudi operacijo multipliciranja nosilcev signalov (angl. *fanout*), s čimer dobimo več kopij logične vrednosti spremenljivke; tudi tovrstno množenje vrednosti logičnih spremenljivk je v kvantnih vezjih z samimi kvantnimi vodili prepovedano, nenazadnje zaradi invazivnosti procesa meritve, ki bi bil hipotetično sestavni del kopiranja superpozicioniranega stanja;

## 1.8 Bellova stanja in kvantna teleportacija

Poseben pomen v domeni kvantnega procesiranja imajo tako imenovana *Bellova stanja* (angl. *Bell states*). Do njih pridemo na osnovi kvantnega logičnega vezja prikazanega na sliki 1.7, iz katere je razvidno, da v kvantno vezje vstopata qubita $|x\rangle$ in $|y\rangle$, samo vezje pa vsebuje eno Hadamardovo operacijo in eno Controlled NOT operacijo. V primeru, da v vezje vstopata qubita v osnovnih




Slika 1.7: Shema logičnega vezja za tvorbo Bellovih stanj.

stanjih, kvantno vezje formira preslikave predstavljene v tabeli 1.1. Za primer izračunajmo odziv kvantnega vezja pri vstopajočih osnovnih stanjih $|x\rangle = |0\rangle$ in

$|y\rangle = |0\rangle$, ki ga predstavlja prva vrstica tabele 1.1. Izračun je povzet v izrazih

$$U_H |0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{1.32}$$

$$U_{CNOT}(\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix}) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1/\sqrt{2} \\ 0 \\ 1/\sqrt{2} \\ 0 \end{bmatrix} =$$

$$= \begin{bmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1/\sqrt{2} \end{bmatrix} = |\beta_{00}\rangle . \tag{1.33}$$

Bellova stanja imenujemo tudi za EPR stanja ali EPR pare. V splošnem lahko posamezni EPR par zapišemo z izrazom

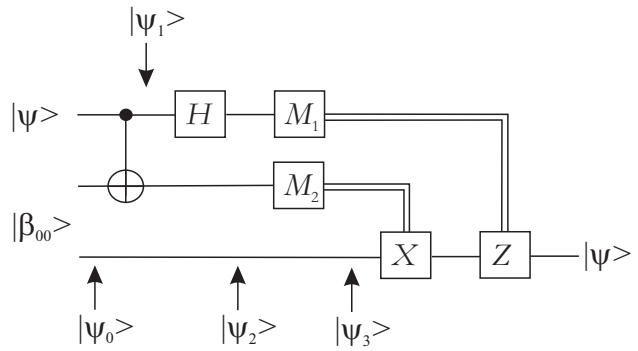
$$\beta xy \equiv \frac{|0, y\rangle + (-1)^x |1, \overline{y}\rangle}{\sqrt{2}}. \tag{1.34}$$

Ključni pomen Bellovih stanj je v omogočanju *kvantne teleportacije*[3]. Na tem mestu za razjasnitev pojma kvantne teleportacije povzemimo referenčni zgled prenosa qubita med Alice in Bobom. Predpostavimo, da Alice in Bob živita ločeno na točkah A in B. Ob zadnjem srečanju sta zgenerirala EPR par in vsak od njiju je iz EPR para vzel en qubit. Referenčni zgled odgovarja na vprašanje, kako naj Alice dostavi Bobu nek nov qubit $|\psi\rangle$ ($|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$), pri čemer Alice njegovega stanja ne pozna in Bobu lahko pošlje le klasične nesuperpozicionirane podatke. Alice stanja qubita $|\psi\rangle$ zaradi invazivnosti branja ne sme prebrati, saj bo s tem superpozicija qubita izgubljena. Zgled je povzet po viru [1], najdemo pa ga v večini virov o kvantnem procesiranju.

Osnovna ideja rešitve je sledeča. Alice mora svoj novi qubit $|\psi\rangle$ interaktirati s svojim delom EPR para (qubitom) in v nadaljevanju opraviti meritev obeh qubitov. Z meritvijo bo par qubitov prešel v eno od štirih možnih osnovnih stanj $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. V nadaljevanju mora Alice Bobu po klasičnem kanalu poslati rezultate meritev Bobu. Bob rezultate meritev interaktira s svojo polovico EPR para (qubitom) in tako pride do stanja qubita $|\psi\rangle$. Na ta način je Bob od Alice prejel kvantni qubit $|\psi\rangle$, pri čemer se slednji ni prenašal med točkama A in B. Med njima so se prenašali zgolj klasični - nesuperpozicionirani podatki.

Kvantno vezje za izvedbo kvantne teleportacije je predstavljeno na sliki 1.8. V kvantno vezje vstopa qubit $|\psi\rangle$ ter vezana qubita $|\beta_{00}\rangle$, pri čemer prvi vezani qubit poseduje Alice, drugega pa Bob. Tako prvi dve liniji v vezju smatramo kot Alicin del tretmaja qubita $|\psi\rangle$ (odpošiljanje qubita), tretjo linijo v vezju

[3] Teleportacija - Hipotetični transfer snovi ali energije med dvema točkama v prostoru brez prečkanja tega prostora (Vir: Wikipedia).




Slika 1.8: Shema logičnega vezja za teleportacijo qubita na osnovi posedovanja Bellovega stanja. Dvojne povezave med bloki predstavljajo medij za prenos klasičnih bitov.

pa kot Bobov del tretmaja qubita $|\psi\rangle$ (sprejemanje qubita). Izvedbe kvantnih operacij v vezju zapišemo z izrazi

$$|\psi_0\rangle = |\psi\rangle\,|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|00\rangle + |11\rangle)\right], \tag{1.35}$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|10\rangle + |01\rangle)\right], \tag{1.36}$$

$$|\psi_2\rangle = \frac{1}{2}\left[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\right] =$$

$$= \frac{1}{2}\left[|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle) + |10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) + |11\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle)\right]; \tag{1.37}$$

Na osnovi vezanega kvantnega stanja $\psi_2$ Alice izvede meritev v blokih $M_1$ in $M_2$. Osnovna stanja, v katera lahko preideta vezana qubita, so po vrsti $|00\rangle$, $|01\rangle$, $|10\rangle$ in $|11\rangle$. Alice v nadaljevanju Bobu pošlje osnovno stanje (eno od kombinacij $|00\rangle$, $|01\rangle$, $|10\rangle$ in $|11\rangle$), Bobove možne naloge (glej tretjo linijo v vezju) glede na prejeto osnovno stanje pa so sledeče:

- Bob prejme osnovno stanje $|00\rangle$: Bobu ni potrebno storiti ničesar, saj se na tretji liniji pojavi prvi člen izraza (1.37) z desne, ki že vsebuje qubit $|\psi\rangle$ ($\psi = \alpha\,|0\rangle + \beta\,|1\rangle$);
- Bob prejme osnovno stanje $|01\rangle$: ker se na tretji liniji pojavi drugi člen izraza (1.37) z desne ($\psi_3 = \alpha\,|1\rangle + \beta\,|0\rangle$), mora Bob stanje qubita popraviti z operacijo $X$ (negacijo);
- Bob prejme osnovno stanje $|10\rangle$: ker se na tretji liniji pojavi tretji člen izraza (1.37) z desne ($\psi_3 = \alpha\,|0\rangle - \beta\,|1\rangle$), mora Bob stanje qubita popraviti z operacijo $Z$ (faznim zamikom in spremembo predznaka);

- Bob prejme osnovno stanje $|11\rangle$: ker se na tretji liniji pojavi četrti člen izraza (1.37) z desne ($\psi_3 = \alpha|1\rangle - \beta|0\rangle$), mora Bob stanje qubita popraviti najprej z izvedbo operacije $Z$ in v nadaljevanju še z izvedbo operacije $X$;

Po izvedbi svojih nalog Bob pride do pravilnega stanja $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, ki mu ga je želela posredovati Alice.

Na sliki 1.8 sta uporabljeni dve dvojni povezavi, po katerih se preneseta osnovni stanji na pozicijo Boba. Vsako od osnovnih stanj se prenese kot klasični bit po klasičnem vodilu, kar pomeni, da je kvantna teleportacija s hitrostnega vidika izvedbe omejenena - se ne more izvesti hitreje od hitrosti potovanja svetlobe.

## 1.9 Kvantni algoritem

V pričujočem razdelku definiramo pojem kvantnega algoritma[4].

**Definicija 4** *Kvantni algoritem je algoritem, ki s svojimi ukazi kakorkoli izkorišča možnosti superpozicije v kvantnih računalniških strukturah. Z operacijskega vidika takšen algoritem vrši modifikacijo ali množenje unitarne matrike z vsebino kvantnega registra.*

Del razvoja na področju kvantnega računalništva je šel v preteklosti v smeri postavljanja modelov in simulatorjev že obstoječih klasičnih računalniških sistemov. V ta namen je bila v tovrstnih rešitvah mnogokrat uporabljena Toffolijeva funkcija, implementirana v obliki Toffolijevih kvantnih logičnih vrat. Uporabljana je bila predvsem zaradi tega, ker v dvovrednostnem svetu klasične logike samostojno predstavlja poln nabor logičnih funkcij.

Toffolijevo funkcijo že poznamo iz poglavja o reverzibilnosti logičnih funkcij in jo bomo zlahka prevedli v jezik kvantnega računalništva. Gre za reverzibilno logično funkcijo s tremi vhodi in tremi izhodi, pri čemer se na izhodni strani ohranjajo logične vrednosti iz istoležečih vhodov, kar pa ne velja v primeru, ko sta prvi dve vhodni vrednosti $|1\rangle$. V tem primeru pride do negacije tretjega qubita. Tako bi lahko zapisali sledeča izraza

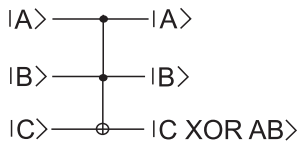
$$|000\rangle \to |000\rangle, |001\rangle \to |001\rangle, |010\rangle \to |010\rangle, |011\rangle \to |011\rangle, \tag{1.38}$$

$$|100\rangle \to |100\rangle, |101\rangle \to |101\rangle, |110\rangle \to |111\rangle, |111\rangle \to |110\rangle. \tag{1.39}$$

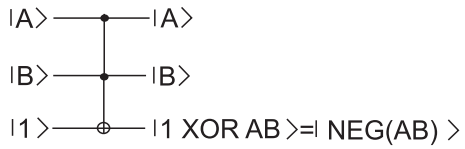
Grafična predstavitev logičnega vezja Toffoli funkcije je podana na sliki 1.9.

Ker Toffolijeva funkcija predstavlja poln funkcijski nabor v domeni dvovrednostne logike v nadaljevanju prikažemo, kako lahko z Toffolijevo funkcijo realiziramo NAND (slika 1.10) in FanOut (slika 1.11) funkcijo.

[4] Algoritem je postopek, ki enolično definira izvedbo nekega opravila v obliki zaporedja ukazov. Algoritem mora biti nedvoumen in končen.




Slika 1.9: Grafična ponazoritev logičnega vezja Toffoli funkcije.




Slika 1.10: Grafična ponazoritev logičnega vezja NAND funkcije.

Jedro raziskav na področju kvantnih algoritmov trenutno poteka na področju iskanja kvantnih algoritmov kot alternativ za algoritme, ki so danes z vidika izvedbe časovno prepotratni. Na tem mestu imamo v mislih raziskave o možnostih izkoriščanja *kvantnega paralelizma*. V nadaljevanju si kot primer slednjega ogledamo zgled Deutschevega kvantnega algoritma.

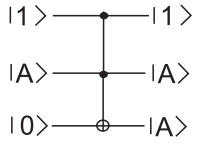
## 1.10 Deutschev algoritem

Predpostavimo, da imamo opravka z enovhodno logično funkcijo $f(x)$

$$f : \{0,1\} \to \{0,1\} \tag{1.40}$$

in si zastavimo vprašanje, ali funkcija ne glede na vrednosti vhodne spremenljivke na izhodu poraja konstanten odziv (funkcija je *konstanta*, angl. *constant*), ali pa sta izhoda ob različnih vrednostih vhodne spremenljivke različna (funkcija je *uravnotežena*, angl. *balanced*). Slednje lahko formalno zapišemo z izrazom

$$\begin{aligned} f(0) = f(1) &\Rightarrow f(x) \text{ je konstanta,} \\ f(0) \neq f(1) &\Rightarrow f(x) \text{ je uravnotežena.} \end{aligned} \tag{1.41}$$



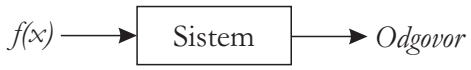

Slika 1.11: Grafična ponazoritev logičnega vezja FanOut funkcije.

| $x$ | $f(x_1)$ | $f(x_2)$ | $f(x_3)$ | $f(x_4)$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 1 | 0 | 1 |

Tabela 1.2: Pravilnostna tabela delovanja vseh možnih enovhodnih logičnih funkcij.

Delovanje vseh možnih enovhodnih logičnih funkcij predstavlja pravilnostna tabela 1.2. Iz nje je razvidno, da sta funkciji $f(x_1)$ in $f(x_4)$ konstanti, funkciji $f(x_2)$ in $f(x_3)$ pa glede na različne vhodne vrednosti spremenljivi in zaradi tega uravnoteženi.

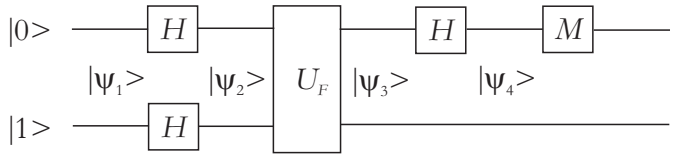
Na tem mestu predpostavimo, da imamo opravka s sistemom, ki nam ob podani enovhodni funkciji $f(x)$ zna odgovoriti na vprašanje, ali je opazovana funkcija konstanta, ali pa je uravnotežena. Shema tovrstnega sistema je predstavljena na sliki 1.12. Klasični računalniški sistem bi odgovor formiral po sle-




Slika 1.12: Shema sistema, ki nam odgovori na vprašanje, ali je $f(x)$ uravnotežena, ali konstanta.

dečem postopku. Najprej bi izračunal odziv opazovane funkcije $f(x)$ pri $x = 0$, v nadaljevanju odziv pri $x = 1$, na koncu pa bi oba funkcijska izhoda primerjal in glede na izid primerjave po izrazu (1.41) formiral odgovor. David Deutsch l.1992 predstavi kvantno rešitev omenjenega problema, v kateri se izogne zaporedju evaluacij funkcije $f(x)$ in ju izvede paralelno [12]. Omenjeno rešitev imenujemo za Deutschev algoritem, ki ga opišemo v nadaljevanju.

Deutsch svoj algoritem[5] predstavi v obliki kvantnega vezja, ki je prikazano na sliki 1.13. Pri tem blok $H$ predstavlja Hadamardovo funkcijo, blok pa $M$

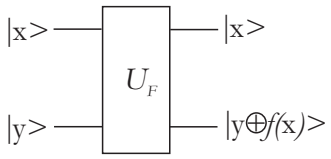



Slika 1.13: Shema sistem, ki nam odgovori na vprašanje, ali je $f(x)$ uravnotežena, ali konstanta.

pa meritev. Blok $U_F$ predstavlja dvovhodno kvantno operacijo, ki prvi qubit

[5]Opis Deutschevega algoritma je deloma povzet po spletni strani http://dkopczyk.quantee.co.uk/deutschs-algorithm/ (avtor: Dawid Kopczyk).

preslika na izhod ($|x\rangle \rightarrow |x\rangle$), drugi qubit pa transformira v izhod $|y \oplus f(x)\rangle$ ($|y\rangle \rightarrow |y \oplus f(x)\rangle$), kar je predstavljeno na sliki 1.14, sama funkcija $U_F$ pa je




Slika 1.14: Shema bloka $U_F$.

opisana z matriko po izrazu

$$U_F = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{1.42}$$

V kvantno vezje, ki implementira Deutschev algoritem paralelno vstopata qubita $|0\rangle$ in $|1\rangle$. Povezana qubita predstavlja qubitni par, katerih spreminjajoče stanje skozi vezje ponazarjamo z zaporedjem sestavljenih stanj $\psi_1$, $\psi_2$, $\psi_3$ in $\psi_4$. Na osnovi slike 1.13 lahko zaporedje izvedenih operacij formalno zapišemo z izrazom

$$(H \otimes I) U_F (H \otimes H) \, |01\rangle \,, \tag{1.43}$$

pri čemer znak $\otimes$ predstavlja tenzorski produkt, $I$ pa enotsko matriko. Samo procesiranje lahko zapišemo z naslednjimi koraki:

- stanje $|\psi_1\rangle$: kvatno stanje dveh qubitov pred vstopom v prvi segment procesiranja lahko zapišemo z izrazom

$$|\psi_1\rangle = |01\rangle \,; \tag{1.44}$$

- izračun stanja $|\psi_2\rangle$: tenzorski produkt dveh matrik dimenzije $2 \times 2$ se izračuna po izrazu

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \otimes \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} & a_{12} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \\ a_{21} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} & a_{22} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \end{bmatrix} =$$

$$= \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{bmatrix}, \tag{1.45}$$

tenzorski produkt dveh vektorjev pa po izrazu

$$\begin{bmatrix} a \\ b \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix}; \tag{1.46}$$

odtod lahko izračunamo $|\psi_2\rangle$ po izrazih

$$|\psi_2\rangle = (H \otimes H)\,|01\rangle = \tag{1.47}$$

$$= \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \left( \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) = \tag{1.48}$$

$$= \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} = \tag{1.49}$$

$$= \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2} = \left( \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right); \tag{1.50}$$

s tem postaneta tako prvi, kot tudi drugi qubit superpozicionirana;

- izračun stanja $|\psi_3\rangle$: izvedemo ga na osnovi izraza

$$|\psi_3\rangle = U_F\,|\psi_2\rangle\,; \tag{1.51}$$

zaradi preglednosti zapisa začasno predpostavimo, da prvi qubit ni superpozicioniran (predpostavimo da je ta qubit v stanju $|x\rangle$); tako delovanje operacije $U_F$ zapišemo z izrazom

$$|\psi_3\rangle = |x\rangle \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \oplus f(x) \right) = |x\rangle \left( \frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} \right); \tag{1.52}$$

upoštevajoč dve možni vrednosti funkcije $f(x)$ pridemo do izraza

$$|\psi_3\rangle = \begin{cases} |x\rangle \frac{|0\oplus 0\rangle - |1\oplus 0\rangle}{\sqrt{2}} = |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}, & \text{if } f(x) = 0 \\ |x\rangle \frac{|0\oplus 1\rangle - |1\oplus 1\rangle}{\sqrt{2}} = |x\rangle \frac{|1\rangle - |0\rangle}{\sqrt{2}}, & \text{if } f(x) = 1 \end{cases}, \tag{1.53}$$

ki ga lahko enovrstično zapišemo z izrazom

$$|\psi_3\rangle = (-1)^{f(x)}\,|x\rangle\,\frac{|0\rangle - |1\rangle}{\sqrt{2}}; \tag{1.54}$$

če sedaj vstavimo v predhodni izraz še superpozicionirani prvi qubit iz stanja $|\psi_2\rangle$ za katerega vemo, da ga $U_F$ enostavno preslikuje na izhod, pridemo do izraza

$$|\psi_3\rangle = (-1)^{f(x)} \left( \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) =$$

$$= \left( \frac{(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle}{\sqrt{2}} \right) \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right); \tag{1.55}$$

glede na to, da je $f(x)$ lahko konstanta ali uravnotežena, predhodni izraz splošneje zapišemo z izrazom

$$|\psi_3\rangle = \begin{cases} (\pm 1) \left( \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right), & \text{if } f(x) \text{ je konstanta;} \\ (\pm 1) \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right), & \text{if } f(x) \text{ je uravnotežena;} \end{cases} \tag{1.56}$$

- izračun stanja $|\psi_4\rangle$: izvedemo ga na osnovi izraza

$$|\psi_4\rangle = (H \otimes I) |\psi_3\rangle, \tag{1.57}$$

ki predstavlja izvedbo Hadamardove operacije nad prvim qubitom; rezultat omenjene operacije zapišemo z izrazom

$$|\psi_4\rangle = \begin{cases} (\pm 1)|0\rangle \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right), & \text{if } f(x) \text{ je konstanta;} \\ (\pm 1)|1\rangle \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right), & \text{if } f(x) \text{ je uravnotežena;} \end{cases} \tag{1.58}$$

- na zadnjem koraku algoritma izvedemo še meritev prvega qubita; v primeru, da nam meritev vrne osnovno stanje 0 je funkcija konstanta, v primeru pa da nam meritev vrne stanje 1 je funkcija uravnotežena;

## 1.11 Delovanje in prednosti kvantnega računalnika

Kvantni računalniki naj bi delovali po principu *pripravi- razvij - izmeri*. Slednje termine si po vrsti razlagamo na sledeče načine:

- *pripravi*: postavitev kvantnega registra v začetno stanje (vsi qubiti registra se postavijo v ustrezna stanja $|q_i\rangle$);
- *razvij*: izvaja se zaporedje operacij, ki spremeni začetno stanje registra v nova potencialna superpozicionirana stanja, kar predstavlja sprejemljive rešitve;
- *izmeri*: vrne vrednost izhodnega stanja, ki pa naj ne bi bilo superpozicionirano;

Glede na možno nahajanje qubita v obeh stanjih se izredno poveča njegova "informacijska moč". Na ta način z njim lahko rešujemo dosti kompleksnejše algoritme, kot smo jih vajeni reševati z današnjimi računalniki. Tipični zgledi področij, kjer pričakujemo izrazito pospešitev reševanja problemov na osnovi kvantnih vezij in kvantnih algoritmov, so sledeči:

- hitro iskanje podatkov (Grover l.1996 predstavi kvantni algoritem, ki glede na število podatkov $n$ kompleksnost iskanja z vidika časovne potratnosti iz $O(\frac{n}{2})$ zniža na $O(\sqrt{n})$);
- hitri enkripcijski postopki;
- hitra faktorizacija velikih števil (Shorov kvantni algoritem iz l.1994, ki časovno kompleksnost zniža iz časovne kompleksnosti $O(e^{L^{\frac{1}{3}}})$ na $O\left(L^2\right)$, pri čemer $L$ predstavlja število digitov);
- generiranje naključnih števil,
- kvantna teleportacija itd.;

## 1.12 Kvantni programski jeziki in simulacijska orodja

Kvantni programski jeziki so se razvili kot razširjave že obstoječih programskih jezikov, ki vsebujejo visoko nivojske programske ukaze vezane na izvajanje kvantnih operacij. V dveh izpisih kode v nadaljevanju, zapisani v jeziku QCL, ki predstavlja razširjavo programskega jezika C, najdemo primer deklaracije kvantnega registra in Hadamardove funkcije, ter definicijo kompleksnejše funkcije diffuse(qureg q).

```
qureg x1[2]; // 2-qubit quantum register x1
qureg x2[2]; // 2-qubit quantum register x2
H(x1); // Hadamard operation on x1
H(x2[1]); // Hadamard operation on the first qubit of the register
    x2
```

Listing 1.1: Primer deklaracije dveh qubitnih registrov in Hadamardove funkcije (vir: Wikipedia).

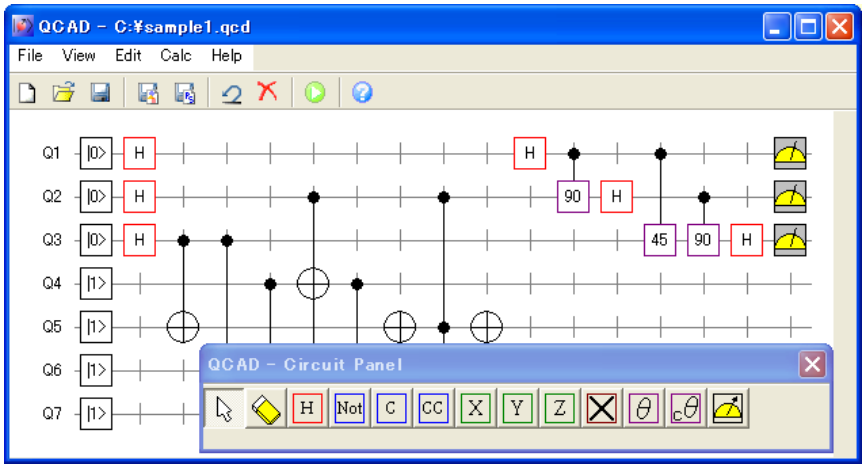
```
operator diffuse (qureg q) {
     H(q);                  // Hadamard Transform
     Not(q);                // Invert q
     CPhase(pi, q);         // Rotate if q=1111..
     !Not(q);               // undo inversion
     !H(q);                 // undo Hadamard Transform
   }
```

Listing 1.2: Primer definicije kompleksnejše funkcije diffuse(qureg q) (vir: Wikipedia).

Najbolj znani primeri jezikov so QCL, LanQ, QPL in QML. Sicer starejši, a temeljit pregled področja kvantnih programskih jezikov najdemo na spletni strani navedeni v viru [13].

Za postavitve in simulacije delovanja struktur kvantnih računalnikov je na razpolago kar nekaj programskih orodij. Nekatera od njih temeljijo na splošno uveljavljenih jezikih in okoljih, kot so C/C++, Java, Mathematica, MATLAB, Python, Haskell itd., nekatera od njih pa so samostojna in običajno opremljena

z grafičnim urejevalnim vmesnikom za enostavnejše postavljanje struktur. Najbolj razširjeni so QCAD [14], C++ Quantum Library in jQuantum. Povezavo na spletno stran z razvrstitvijo orodij najdemo v viru [15]. Primer delovnega področja orodja QCAD, iz katerega je razvidna metodologije gradnje strukture, je prikazan na sliki 1.15.




Slika 1.15: Predstavitev metodologije gradnje kvantne procesne strukture.

## 1.13 Realizacije kvantnih računalnikov

Realizacije kvantih računalnikov so zaradi težavnosti tehnološke izvedbe danes praktično šele na samem začetku razvoja. V nadaljevanju naštejemo nekaj najbolj znanih začetnih izvedb kvantnih računalnikov:

- družina kvantnih računalnikov kanadskega proizvajalca D-Wave Systems Inc.[6]: ena od prvih komercialnih izvedenk kvantnih računalnikov je bila družina računalnikov proizvajalca D-Wave Systems Inc., ki so performančno v letu 2008 temeljile na 64.000 paralelnih operacijah in 28 qubitnem registru, samo procesiranje pa je potekalo v tekočem heliju pri izredno nizkih temperaturah; leta 2010 proizvajalec na tržišče postavi prvo komercialno izvedenko kvantnega računalnika D-Wave One, leta 2013 pa je bila na tržišču naprodaj 512 qubitna realizacija računalnika; proizvajalec izpostavlja, da je D-Wave eksplicitno namenjen predvsem reševanju problemov, ki zahtevajo masovni paralelizem izvajanja operacij nad podatki; v tem smislu izpostavlja hitro reševanje problemov s področja bioinformatike, razporejanja resursov, finančnih analiz, optimizacije, strojnega

[6] Več podatkov o proizvajalcu D-Wave Systems najdemo na spletni strani http://www.dwavesys.com/, zgled programiranja kvantnega računalnika pa na spletni strani https://www.dwavesys.com/software.

učenja itd.; zadnja izvedenka (l.2019) nosi ime **DWave2000Q**; procesiranje se v njej izvaja blizu absolutne temperaturne ničle (blizu -273°C) ob umetno zmanjšanem tlaku in vzpostavljenih pogojih, v katerih praktično ni prisotnega šuma; DWave2000Q sestavlja približno 2.000 qubitov, katerih vloga v osnovni konfiguraciji sistema ni jasno opisana; v vsakem primeru to vsekakor ni število vhodnih linij ali dolžina registra qubitov, nad katerim se izvajajo hipotetične operacije;

- kvantni program korporacije Google: oktobra l.2019[7] je Google objavil, da je s svojim 54 qubitnim kvantnim računalnikom **SYCAMORE** uspel nekatere specifične algoritme izvesti v rekordnih časih;

- kvantni program korporacije IBM: omenjena korporacija trenutno omogoča kvantnim programerjem brezplačen dostop do svojega 16 qubitnega sistema **IBM QX5**; z odprtostjo dostopa do platforme se v okviru njenega kvantnega programa zbirajo kvantni algoritmi in njihovim problemom usmerjen nadaljnji razvoj kvantnega računalnika;

- poleg omenjenih korproracij danes v takšni ali drugačni obliki posedujejo kvantne računalnike tudi korporacije kot so Microsoft, Intel, Toshiba, NTT, HoneyWell, Alibaba, Rigetti, Airbus in Lockhead Martin;

Po mnenju avtorja pričujočega dela za vse izvedenke omenjenih proizvajalcev velja, da so ozko problemsko usmerjene, tako da je njihovo programiranje izredno zapleteno in v veliki meri odvisno od ciljne platforme. Ključni problemi trga kvantnih računalnikov so danes sledeči:

- ni javno dostopnih podatkov o arhitekturah kvantnih računalnikov;

- ni enotnih metrik, na osnovi katerih bi lahko kvantne računalnike primerjali med seboj; ena od možnih metrik je število qubitov, ki pa je danes v luči nejasnih arhitektur popolnoma nezanesljiva z vidika zmogljivostne ocene opazovanega kvantnega računalnika;

- proste prodaje kvantnih računalnikov trenutno ni, vsi računalniki pa so namensko razviti za različne korporacije;

Pozitivne plati kvantnega računalništva so trenutno v njegovi odprtosti preko množice organiziranih neinstitucionalnih kvantnih iniciativ, javno dostopnih projektov korporacij, ki omogočajo odprti dostop do platform (npr. projekti IBM-a, Microsoft-a itd.) ter množice brezplačnih razvojnih okolij, kot so grafična snovalska orodja, jeziki, prevajalniki itd.

[7] https://siol.net/digisvet/novice/kaj-google-dela-s-strojem-o-katerem-ta-teden-govorijo-vsi-510464

## 1.14 Povzetek poglavja

Realizacij kvantnih računalnikov v današnjem času ne najdemo v široki uporabi. Temu primerno je seveda tudi težko določljivo, v kolikšni meri bo realizacija zanesljivega kvantnega računalnika resnično vplivala na kvalitativni preskok procesiranja. Vsekakor pa vsi modeli kažejo, da gre v primeru uspešne realizacije kvantnega računalnika pričakovati eksponentno povečanje hitrosti reševanja določenih specifičnih algoritmičnih problemov.

# Literatura


[1] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, UK, 2009.

[2] C. Calude and G. Păun, *Computing with cells and atoms, An introduction to quantum, DNA and membrane computing*. Taylor and Francis, London, 2001.

[3] "Single particle interference." `http://player.slideplayer.com/26/8574538/#`, December 2017.

[4] "Quantum computing." `http://en.wikipedia.org/wiki/Quantum_computing`, Maj 2015.

[5] M. Nagy and S. G. Akl, "Quantum computation and quantum information," tech. rep., 2005. Technical report, 2005-496.

[6] "Elementary quantum notation." `http://www-users.cs.york.ac.uk/schmuel/comp/node6.html`, Maj 2015.

[7] J. Virant, *Načrtovanje nanoračunalniških struktur*. Didakta, Slovenija, 2007.

[8] M. Hirvensalo, *Quantum Computing*. Springer Verlag, 2001.

[9] H. Stöcker, *Matematični priročnik z osnovami računalništva*. Tehniška založba, Slovenija, 2006.

[10] O. Bronštejn, K. Semendjajev, G. Musiol, and H. Mühlig, *Matematični priročnik*. Tehniška založba, Slovenija, 1997.

[11] A. Pittenger, *An Introduction to Quantum Computing Algorithms*. Birkhäuser, ZDA, 2000.

[12] D. Deutsch and R. Jozsa, "Rapid solutions of problems by quantum computation," *Proceedings of the Royal Society of London*, vol. 439, no. 1907, pp. 553–558, 1992.

[13] "Quantum programming languages." `http://www.dcs.gla.ac.uk/~simon/quantum/`, November 2015.

[14] "GUI environment for Quantum Computer Simulator." http://qcad.osdn.jp/, November 2015.

[15] "Quantiki homepage." http://www.quantiki.org/wiki/list-qc-simulators, November 2015.