Princípy kvantových počítačov a perspektíva ich využitia

Ján Kollár

15.10.2020

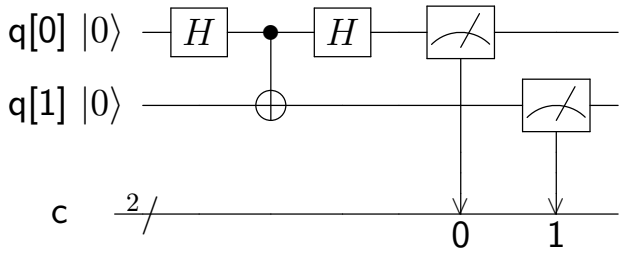
Ján Kollár: Princípy kvantových počítačov a perspektíva ich využitia/Principles of Quantum Computers and their Perspectives, KPI FEI TUKE, 2020, 46pp.

1. Úvod – porovnanie klasického a kvantového bitu

Klasický bit Fyzikálnou podstatou je elektrický signál – napätie. Stav klasického bitu je hodnotou napätia, preto klasický bit môže byť len v dvoch stavoch: 0 (pri $U = 0V$) a 1 (pri $U = 5V$).

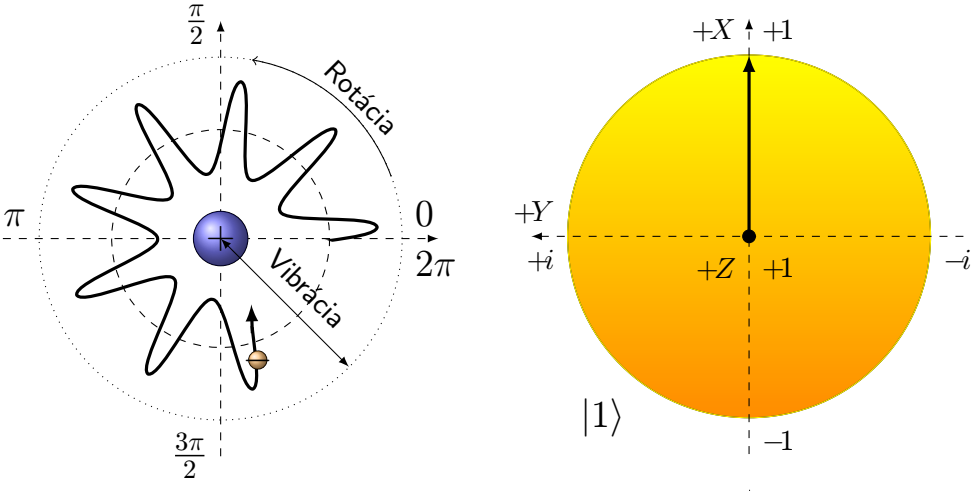
Kvantový bit Fyzikálnou podstatou je pohyb elementárnej častice. Stav kvantového bitu (kvantový stav) je hodnotou dvojzložkového vektora v dvojrozmernom Hilbertovom priestore $\mathbb{C}^2$, preto kvantový bit môže byť v stave patriacom do nekonečnej množiny stavov.

Stav bitu je teda hodnotou bitu.



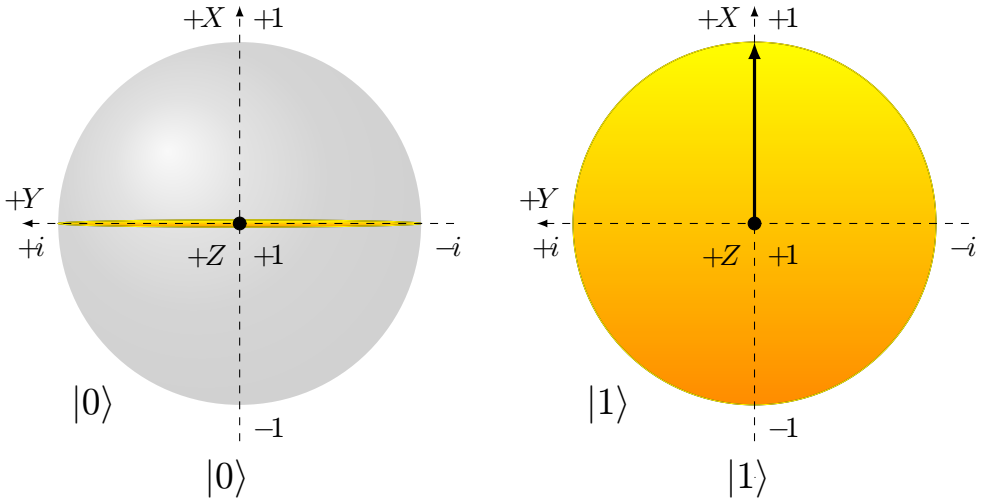
2. Kvantový bit, kvantový stav a bázy základných kvantových stavov

2.1. Mechanický model kvantového bitu a jeho kvantový stav



- Kvantový bit je zobrazený v stave $|1\rangle$ z pohľadu merania (os Z smeruje na meracie zariadenie) a je umiestnený v jednotkovej guli.
- XY je rovina $\mathbb{C}$ a ZX je rovina $\mathbb{R}$.
- Prechodom kvantového bitu cez kvantové hradlo (bránu, gate) dochádza k otočeniu kvantového bitu okolo osi X, Y a Z a teda k zmene jeho stavu.

2.2. Základné stavy štandardnej (výpočtovej) bázy $\{|0\rangle, |1\rangle\}$



- $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ je kvantový stav s minimálnou energiou (0.0).
- $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ je kvantový stav s maximálnou energiou (1.0).
- Kvantový stav $|0\rangle$ je vždy začiatočným stavom každého kvantového obvodu.

2.3. Definícia všeobecného kvantového stavu $|\psi\rangle$ jedného bitu vo vektorovom a Diracovom tvare

Definícia: Všeobecný kvantový stav $|\psi\rangle$ kvantového bitu patrí do dvojrozmerného Hilbertovho priestoru $\mathbb{C}^2$ a je teda dvojzložkovým vektorom komplexných čísel α a β, teda

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha\,|0\rangle + \beta\,|1\rangle\,,\ |\alpha|^2 + |\beta|^2 = 1$$

kde $|\alpha|$ a $|\beta|$ sú normy (veľkosti, magnitúdy, amplitúdy) komplexných zložiek α a β.

Vlastnosti kvantového stavu $|\psi\rangle$:

1. Norma $\|\,|\psi\rangle\,\|$ každého kvantového stavu je 1, pretože platí: $\|\,|\psi\rangle\,\| = \sqrt{|\alpha|^2 + |\beta|^2} = 1$.
2. $|\alpha|^2$ je pravdepodobnosť, že $|\psi\rangle = |0\rangle$, a teda bude nameraný do klasického bitu s hodnotou $c = 0$ a
3. $|\beta|^2$ je pravdepodobnosť, že $|\psi\rangle = |1\rangle$, a teda bude nameraný do klasického bitu s hodnotou $c = 1$.

2.4. Vyjadrenie všeobecného kvantového stavu $|\psi\rangle$ v polárnom tvare

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = e^{i\lambda} \begin{pmatrix} \cos(\theta/2) \\ e^{i\varphi} \sin(\theta/2) \end{pmatrix}$$

Kvantový stav v polárnom tvare je určený hodnotami fáz θ, φ a λ.

- $\theta/2$ – *otočenie vektora stavu v rovine reálnych čísel* $\mathbb{R}$, $\theta \in [-\pi, \pi]$.
- φ – *lokálna fáza*, t.j. relatívne otočenie zložky β oproti zložke α vektora stavu do roviny komplexných čísel $\mathbb{C}$, $\varphi \in [0, 2\pi]$.
- λ – *globálna fáza*, t.j. otočenie zložky β aj α do roviny komplexných čísel $\mathbb{C}$, $\lambda \in [0, 2\pi]$.

Platí aj

1. $\varphi = \varphi_\beta - \varphi_\alpha$, kde φ_β je otočenie β do roviny $\mathbb{C}$ a φ_α je otočenie α do roviny $\mathbb{C}$.
2. $\lambda = \varphi_\alpha$
3. Globálna fáza vyjadruje relatívne otočenie vektorov viacerých kvantových stavov vo viacbitovom kvantovom obvode, preto nemá význam v prípade jednobitového obvodu, čo vedie k zjednodušeniu $\lambda = 0$, $\varphi_\alpha = 0$ a $\varphi = \varphi_\beta$.

2.5. Odvodenie fáz základných stavov $|0\rangle$ a $|1\rangle$

$$|\psi\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = e^{i0} \begin{pmatrix} \cos(0) \\ e^{i0} \sin(0) \end{pmatrix} = e^{i\lambda} \begin{pmatrix} \cos(\theta/2) \\ e^{i\varphi} \sin(\theta/2) \end{pmatrix}$$

Fázy $|0\rangle$ sú teda $\theta = 0$ (lebo $\theta/2 = 0$), a $\lambda = \varphi = 0$.

$$|\psi\rangle = |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = e^{i0} \begin{pmatrix} \cos(\pi/2) \\ e^{i0} \sin(\pi/2) \end{pmatrix} = e^{i\lambda} \begin{pmatrix} \cos(\theta/2) \\ e^{i\varphi} \sin(\theta/2) \end{pmatrix}$$

Fázy $|1\rangle$ sú teda $\theta = \pi$ (lebo $\theta/2 = \pi/2$), a $\lambda = \varphi = 0$.

Vektory obidvoch základných stavov štandardnej bázy $\{|0\rangle, |1\rangle\}$ ležia teda v reálnej rovine a sú ortonormálne, pretože sú ortogonálne (navzájom kolmé) a zároveň normalizované (majú jednotkovú veľkosť).

2.6. Základné stavy štandardnej bázy $\{|0\rangle, |1\rangle\}$ – vektorový, Diracov a polárny tvar

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1\,|0\rangle + 0\,|1\rangle = e^{i0} \begin{pmatrix} \cos(0) \\ e^{i0}\ \sin(0) \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0\,|0\rangle + 1\,|1\rangle = e^{i0} \begin{pmatrix} \cos(\pi/2) \\ e^{i0}\ \sin(\pi/2) \end{pmatrix}$$

2.7. Základné stavy bázy $\{|+\rangle, |-\rangle\}$ a bázy $\{|\circlearrowright\rangle, |\circlearrowleft\rangle\}$

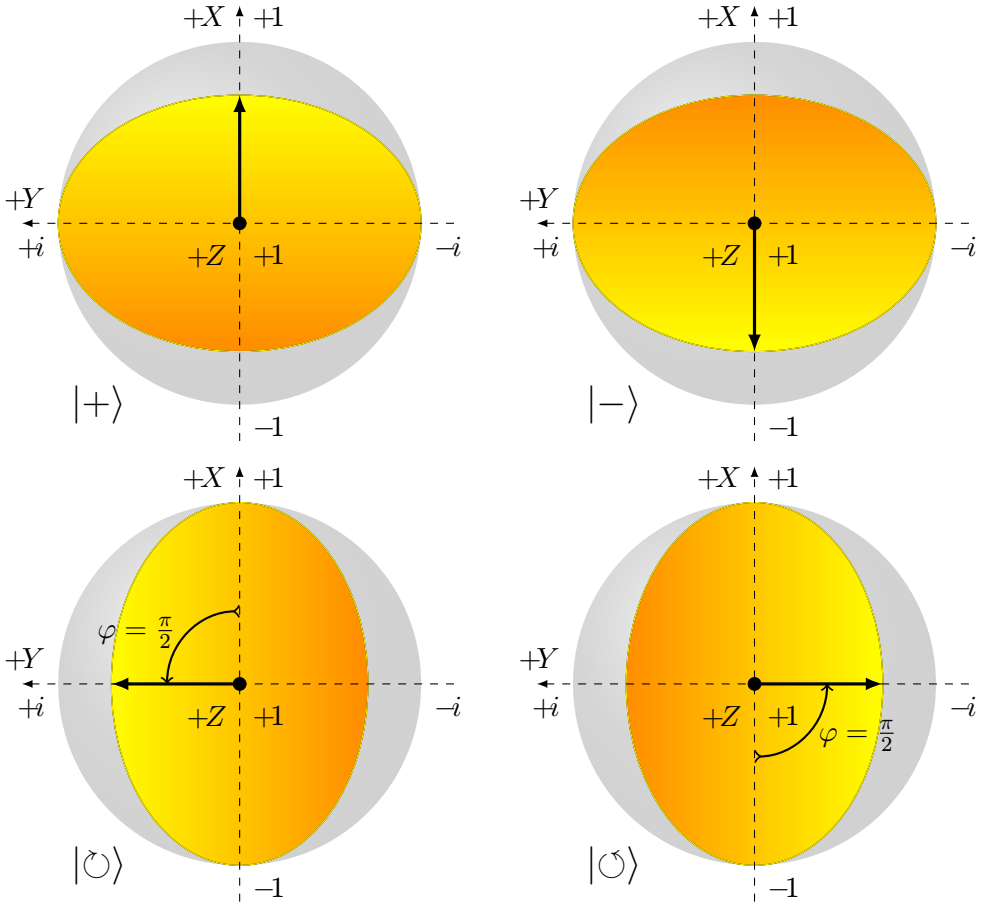
$$|+\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = e^{i0} \begin{pmatrix} \cos(\pi/4) \\ e^{i0}\ \sin(\pi/4) \end{pmatrix} \Rightarrow \theta/2 = \pi/4$$

$$|-\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = e^{i0} \begin{pmatrix} \cos(-\pi/4) \\ e^{i0}\ \sin(-\pi/4) \end{pmatrix} \Rightarrow \theta/2 = -\pi/4$$

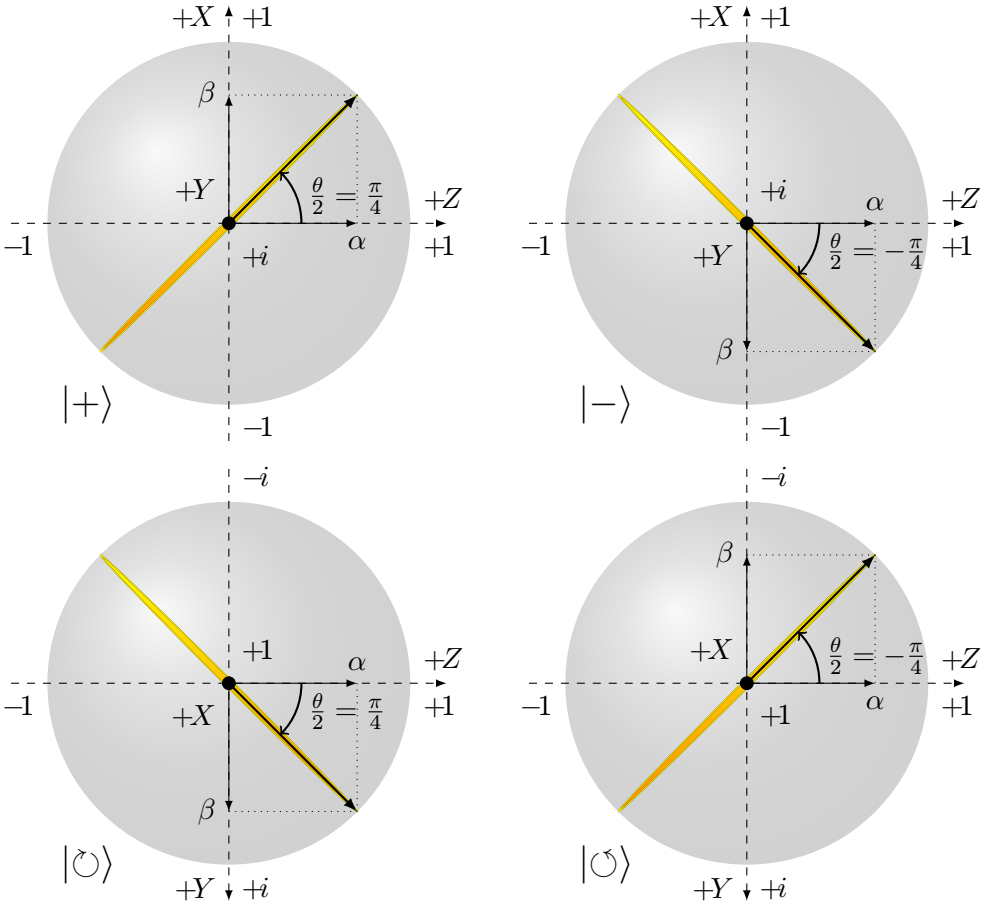
$$|\circlearrowright\rangle \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle = e^{i0} \begin{pmatrix} \cos(\pi/4) \\ e^{i\frac{\pi}{2}}\ \sin(\pi/4) \end{pmatrix} \Rightarrow \theta/2 = \pi/4,\ \varphi = \pi/2$$

$$|\circlearrowleft\rangle \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{i}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle = e^{i0} \begin{pmatrix} \cos(-\pi/4) \\ e^{i\frac{\pi}{2}}\ \sin(-\pi/4) \end{pmatrix} \Rightarrow \theta/2 = -\pi/4,\ \varphi = \pi/2$$

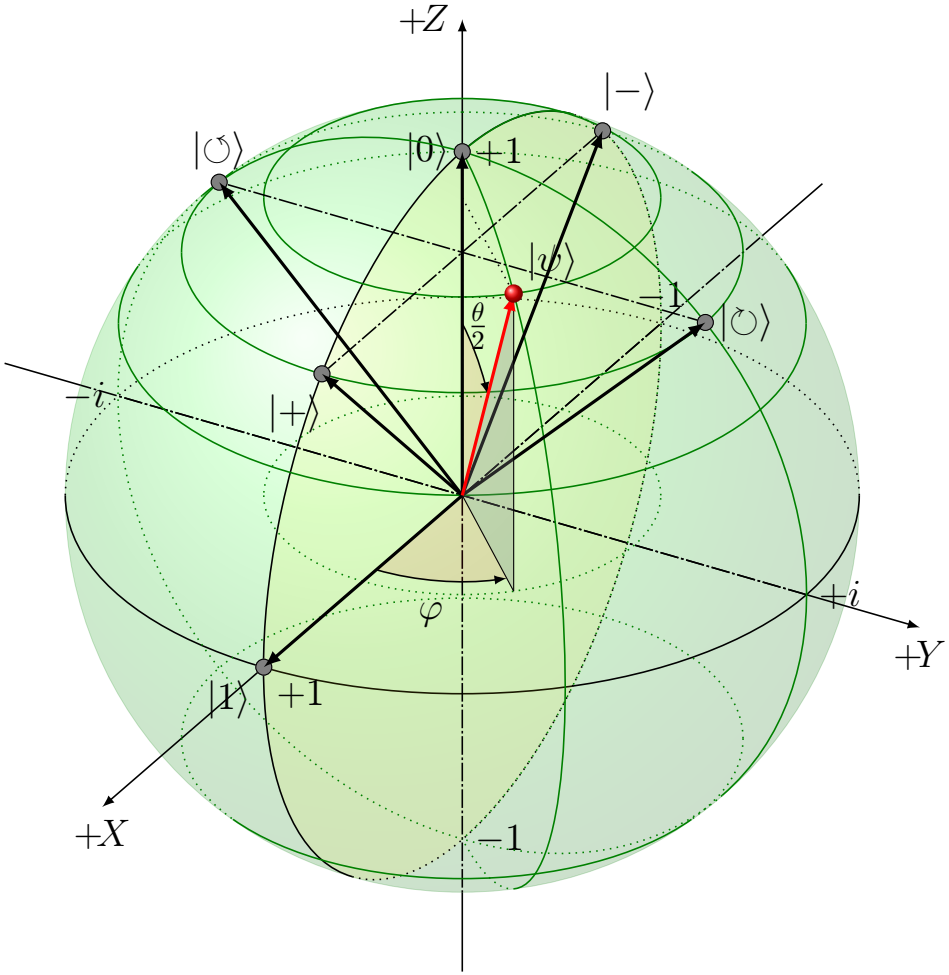
2.8. Zobrazenie stavov báz $\{|+\rangle, |-\rangle\}$ a $\{|\circlearrowright\rangle, |\circlearrowleft\rangle\}$ z pohľadu merania (z protismeru osi Z)

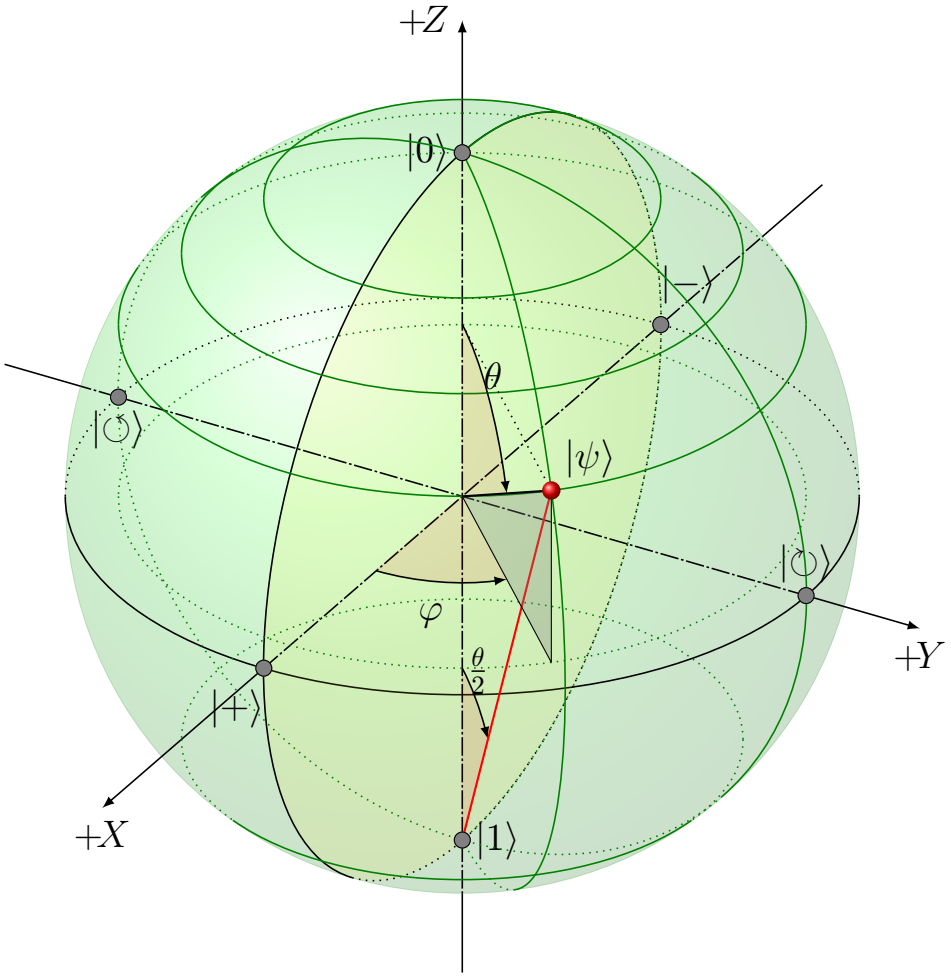


2.9. Zobrazenie stavov bázy $\{|+\rangle, |-\rangle\}$ z protismeru osi Y a bázy $\{|\circlearrowleft\rangle, |\circlearrowright\rangle\}$ z protismeru osi X



3. Zobrazenie kvantových stavov v priestore


+Z
|−⟩
|↺⟩
|0⟩
+1
|ψ⟩
−1
|↻⟩
θ/2
−i
|+⟩
+i
+Y
φ
|1⟩
+1
+X
−1


+Z
|0⟩
|−⟩
θ
|⟳⟩
|ψ⟩
|⟲⟩
φ
+Y
θ/2
|+⟩
+X
|1⟩

4. Superpozícia a meranie kvantového stavu

4.1. Princíp superpozície

Každý všeobecný kvantový stav jedného bitu $|\psi\rangle$

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

možno vyjadriť superpozíciou (t.j. lineárnou kombináciou) základných stavov v Diracovom tvare podľa vzťahu

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,,\ |\alpha|^2 + |\beta|^2 = 1,\ \alpha, \beta \in \mathbb{C},\ |\psi\rangle \in \mathbb{C}^2$$

kde $|\alpha|$, $|\beta|$ sú veľkosti komplexných zložiek α, β stavu $|\psi\rangle$.

4.2. Fyzikálny význam superpozície a pravdepodobnostná podstata kvantových stavov

Fyzikálnym významom superpozície je to, že kvantový stav $|\psi\rangle$ existuje súčasne v dvoch základných stavoch, pričom $|\alpha|^2$ je pravdepodobnosť, s akou bude stav $|\psi\rangle$ nameraný do klasického jednobitového registra c ako hodnota 0 a $|\beta|^2$ je pravdepodobnosť, s akou bude stav $|\psi\rangle$ nameraný do registra c ako hodnota 1.

Kľúčom k pochopeniu pravdepodobnostnej podstaty kvantových stavov danej fyzikálnym významom superpozície je príklad merania stavu $|+\rangle$ pri jednej strele prúdu fotónov na kvantový bit.

4.3. Princíp merania kvantového stavu

- Ostreľovanie kvantového bitu prúdom fotónov v dávke, zvyčajne 1000-10000 striel (angl. shots) – podobné osvetľovaniu predmetu v tme.
- Meranie odrazenej energie $\mathcal{E}$ – energie lúča dopadajúceho na plochu meracieho zariadenia – hradla merania.
- Meraním kvantový bit je zničený (alebo kolabuje do základného stavu $|0\rangle$).
- Meraná energia $\mathcal{E} = |\beta|^2$ je pravdepodobnosťou, s ktorou bude do klasického registra zapísaná hodnota 1.
- Meraná hodnota do klasického registra c je vždy buď 0 alebo 1:

$$c = \begin{cases} 0 \ / \ |\alpha|^2 \\ 1 \ / \ |\beta|^2 \end{cases}$$

4.4. Odvodenie pravdepodobností od počtu výstrelov

V prípade jediného výstrelu prúdu fotónov na kvantový bit v stave $|+\rangle$ dostaneme zaujímavý výsledok, a to:

$$\text{buď } (0): \; c = \begin{cases} 0/1.0 \\ 1/0.0 \end{cases} \quad \text{alebo } (1): \; c = \begin{cases} 0/0.0 \\ 1/1.0 \end{cases} .$$

Na základe jedného výstrelu s istotou (teda pravdepodobnosťou 1.0) bude $|+\rangle$ nameraný ako bit 0 (prípad (0)), alebo ako bit 1 (prípad (1)).

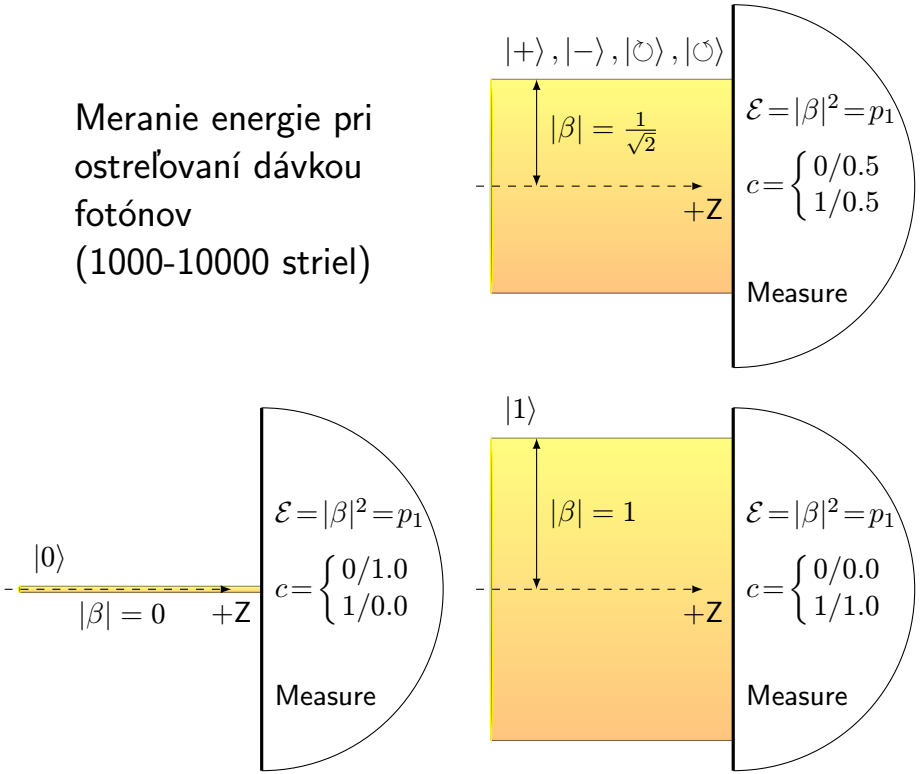
Čím viac výstrelov však použijeme, tým presnejšie zistíme pravdepodobnosti, s akými je $|+\rangle$ nameraný ako klasická hodnota 0 a 1, formálne

$$c = \begin{cases} 0/\frac{n_0}{(n_0+n_1)} \\ 1/\frac{n_1}{(n_0+n_1)} \end{cases}$$

kde n_0 je počet výstrelov s výsledkom (0), n_1 je počet výstrelov s výsledkom (1), a $(n_0 + n_1)$ je celkový počet výstrelov, zvyčajne 1000 až 10000.

4.5. Meranie kvantového stavu – príklady

Meranie energie pri ostreľovaní dávkou fotónov (1000-10000 striel)



Meraním je kvantový bit zničený.

5. Zmena kvantového stavu, kvantové hradlá a ich operácie

5.1. Zmena kvantového stavu

Prechodom kvantového bitu cez kvantové hradlo (bránu, gate) dôjde k skokovej zmene kvantového vstupného kvantového stavu $|\psi\rangle$ na výstupný stav $|\psi'\rangle$. Kvantové hradlo realizuje kvantovú operáciu U – rotáciu vstupného stavu do výstupného stavu, ktorá z matematického hľadiska je maticou 2×2 v tvare

$$U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}, \qquad u_{ij} \in \mathbb{C}$$

Kvantová operácia musí byť nielen unitárna (zachovávajúca $\| \, |\psi'\rangle \, \| = 1$), ale aj reverzibilná, t.j. musí k nej existovať matica $U^\dagger$

$$U^\dagger = \begin{pmatrix} \overline{u}_{11} & \overline{u}_{21} \\ \overline{u}_{12} & \overline{u}_{22} \end{pmatrix}$$

taká, že platí:

$$U \; U^\dagger = U^\dagger \; U = I, \qquad \text{kde } I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Potom prechod zo vstupného do výstupného stavu je definovaný maticovým násobením kvantovej operácie a vektora vstupného stavu (a naopak)

$$|\psi\rangle \mapsto |\psi'\rangle : \; |\psi'\rangle = U \; |\psi\rangle \;\; \text{a} \;\; |\psi'\rangle \mapsto |\psi\rangle : \; |\psi\rangle = U^\dagger \; |\psi'\rangle$$

5.2. Kvantové operácie

Všeobecná kvantová operácia $U = U_3$ je daná hodnotami fáz $\theta,\ \varphi,\ \lambda$

$$U_3\ \theta\ \varphi\ \lambda = \begin{pmatrix} \cos(\theta/2) & -e^{i\lambda}\sin(\theta/2) \\ e^{i\varphi}\sin(\theta/2) & e^{i\lambda+i\varphi}\cos(\theta/2) \end{pmatrix}$$

Operácie štandardných hradiel sú odvodené z $(U_3\ \theta\ \varphi\ \lambda)$, napr.

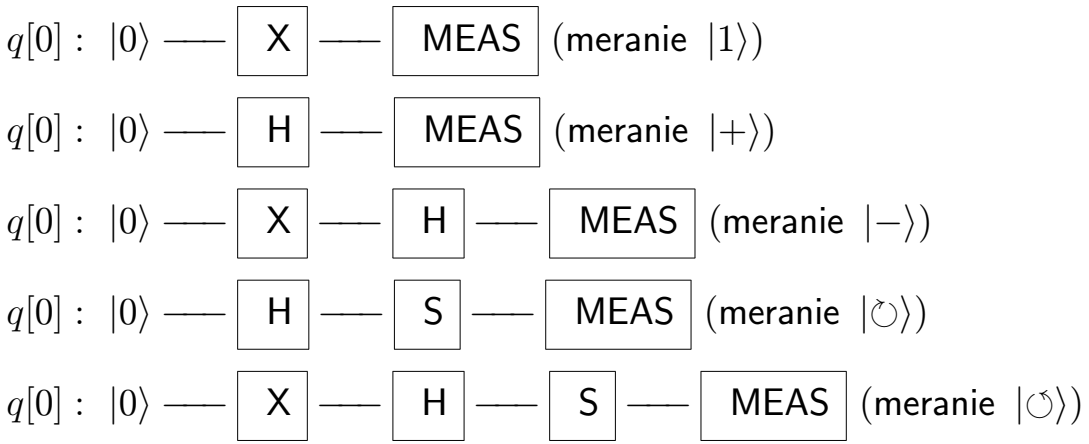
$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad S^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$$

Pretože platí:

$$
\begin{aligned}
|1\rangle &= X\,|0\rangle \\
|+\rangle &= H\,|0\rangle \\
|-\rangle &= H\,|1\rangle \\
|\circlearrowright\rangle &= S\,|+\rangle \\
|\circlearrowleft\rangle &= S\,|-\rangle
\end{aligned}
$$

možno vytvoriť napr. kvantové obvody



6. Kvantový systém viacerých nepreviazaných kvantových bitov

Napr. pre n=3, ak stav kvantového bitu $q[0]$ je $|\psi_0\rangle$, kv. bitu $q[1]$ je $|\psi_1\rangle$ a kv. bitu $q[2]$ je $|\psi_2\rangle$, a tieto bity navzájom nekorelujú (sú nepreviazané), potom celkový stav $|\psi\rangle$ je tenzorovým súčinom stavov $|\psi_0\rangle$, $|\psi_1\rangle$, $|\psi_2\rangle$:

$$|\psi\rangle = |\psi_0\psi_1\psi_2\rangle = |\psi_0\rangle \otimes |\psi_1\rangle \otimes |\psi_2\rangle = \binom{\alpha_0}{\beta_0} \otimes \binom{\alpha_1}{\beta_1} \otimes \binom{\alpha_2}{\beta_2} =$$

$$\begin{pmatrix} \alpha_0 \begin{pmatrix} \alpha_1 \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} \\ \beta_1 \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} \end{pmatrix} \\ \beta_0 \begin{pmatrix} \alpha_1 \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} \\ \beta_1 \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} \end{pmatrix} \end{pmatrix} \Rightarrow \begin{pmatrix} \alpha_0\ \alpha_1\ \alpha_2 \\ \alpha_0\ \alpha_1\ \beta_2 \\ \alpha_0\ \beta_1\ \alpha_2 \\ \alpha_0\ \beta_1\ \beta_2 \\ \beta_0\ \alpha_1\ \alpha_2 \\ \beta_0\ \alpha_1\ \beta_2 \\ \beta_0\ \beta_1\ \alpha_2 \\ \beta_0\ \beta_1\ \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_{000} \\ \alpha_{001} \\ \alpha_{010} \\ \alpha_{011} \\ \alpha_{100} \\ \alpha_{101} \\ \alpha_{110} \\ \alpha_{111} \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \\ \alpha_5 \\ \alpha_6 \\ \alpha_7 \end{pmatrix}$$

Celkový kvantový stav n bitov je 2^n zložkovým vektorom, patrí teda do 2^n rozmerného Hilbertovho priestoru $\mathbb{C}^{2^n}$.

Veľkosť vektora celkového stavu je 1 ($\| |\psi\rangle \| = 1$)!

6.2. Pravdepodobnosť meraných hodnôt celkového stavu nepreviazaných bitov

Pre $n = 3$ klasický 3 bitový register $c = c[2]c[1]c[0]$ nadobúda hodnoty indexov zložiek α_k vyjadrených v binárnom tvare, avšak v zrkadlovom usporiadaní bitov :

$$c[0]c[1]c[2] = \begin{cases} 000 \ / \ |\alpha_0|^2 \ |\alpha_1|^2 \ |\alpha_2|^2 \\ 001 \ / \ |\alpha_0|^2 \ |\alpha_1|^2 \ |\beta_2|^2 \\ 010 \ / \ |\alpha_0|^2 \ |\beta_1|^2 \ |\alpha_2|^2 \\ 011 \ / \ |\alpha_0|^2 \ |\beta_1|^2 \ |\beta_2|^2 \\ 100 \ / \ |\beta_0|^2 \ |\alpha_1|^2 \ |\alpha_2|^2 \\ 101 \ / \ |\beta_0|^2 \ |\alpha_1|^2 \ |\beta_2|^2 \\ 110 \ / \ |\beta_0|^2 \ |\beta_1|^2 \ |\alpha_2|^2 \\ 111 \ / \ |\beta_0|^2 \ |\beta_1|^2 \ |\beta_2|^2 \end{cases}$$

Napr. pri meraní 3 kvantových bitov $q[0] \mapsto c[0]$, $q[1] \mapsto c[1]$ a $q[1] \mapsto c[2]$, meraná hodnota v c bude mať hodnotu 001 s pravdepodobnosťou $|\beta_0|^2 \ |\alpha_1|^2 \ |\alpha_2|^2$.

Súčet pravdepodobností všetkých meraných hodnôt do klasického registra je rovný 1.

Pravdepodobnosť, že všetky klasické bity budú mať hodnotu 1 ($c = 111$) je $|\beta_0|^2 \ |\beta_1|^2 \ |\beta_2|^2$!

6.3. Zmena celkového kvantového stavu viacerých nepreviazaných bitov

Ak vstupné stavy vzájomne nekorelujúcich bitov $q[0]$, $q[1]$, $q[2]$ sú $|\psi_0\rangle$, $|\psi_1\rangle$, $|\psi_2\rangle$ a ich výstupné stavy sú $|\psi'_0\rangle = U_0\,|\psi_0\rangle$, $|\psi'_1\rangle = U_1\,|\psi_1\rangle$, $|\psi'_2\rangle = U_2\,|\psi_2\rangle$, potom celkový výstupný kvantový stav $|\psi'\rangle$ je daný tenzorovým súčinom

$$|\psi'\rangle = |\psi'_0\rangle \otimes |\psi'_1\rangle \otimes |\psi'_2\rangle = (U_0\,|\psi_0\rangle) \otimes (U_1\,|\psi_1\rangle) \otimes (U_2\,|\psi_2\rangle)$$

Možno ho však vypočítať aj maticovým násobením tenzorového súčinu operácii príslušných hradiel a celkového vstupného stavu, teda podľa vzťahu

$$|\psi'\rangle = (U_0 \otimes U_1 \otimes U_2)\,|\psi\rangle$$

ktorým bude celkový vstupný stav $|\psi\rangle$ zmenený na celkový výstupný stav $|\psi'\rangle$.

Pozn: V prípade previazaných kvantových bitov však nie je možné dosiahnuť celkový výstupný stav tenzorovým súčinom hradiel!

7. Kvantový systém previazaných kvantových bitov

7.1. Previazanosť (entanglement) kvantových bitov

Fyzikálna podstata: Kvantové stavy previazaných kvantových bitov sa ovplyvňujú – dochádza ku korelácii ich stavov (bez ohľadu na ich polohu a vzdialenosť v priestore).

Praktická realizácia: V systéme n kvantových bitov ($n \geq 2$) možno vybrať ľubovoľný (ale iba jeden) cieľový kvantový bit a definovať operáciu zmeny jeho stavu U. Ďalej možno vybrať zo zvyšných $n-1$ bitov ľubovoľnú podmnožinu $\{q[k_1], q[k_2], \ldots, q[k_m]\}$, m zdrojových kvantových bitov ($1 \leq m \leq n-1$).

Pozn: Výber zdrojových kvantových bitov môže byť obmedzený v reálnych kvantových systémoch štruktúrou grafu kvantových bitov.

7.2. Dôsledky previazanosti

1. Celkový výstupný stav $(m+1)$ bitov (m výstupných stavov zdrojových bitov a výstupného stavu cieľového bitu) je maticovým súčinom hradla C^mU a celkového vstupného stavu $(m+1)$ bitov (m vstupných stavov zdrojových bitov a vstupného stavu cieľového bitu).

2. Hradlo C^mU je teda maticou rozmeru $2^{(m+1)} \times 2^{(m+1)}$ a účinkuje na celkový stav $(m+1)$ bitov.

3. Výstupné bity sú už previazané, takže meraním (a zničením) jedného z nich vieme posúdiť stavy iných previazaných kvantových bitov.

4. Previazanosť rieši problém, že nemožno vytvoriť kópiu kvantového bitu (no-cloning theorem).

7.3. Podmienená operácia C^mU a jej prípad CX

V 2 bitovom kvantovom systéme $m = 1$, preto $C^mU = C^1U = CU$.

Podmienená operácia previazania zdrojového bitu $q[0]$ a operácie CU cieľového bitu $q[1]$ je definovaná maticou rozmerov $2^{(m+1)} \times 2^{(m+1)} = 2 \times 2$ aje v tvare:

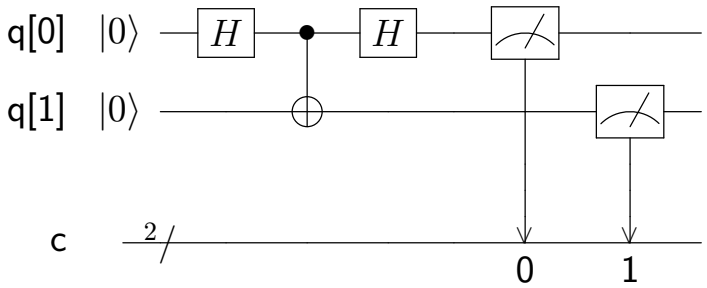
$$CU = \begin{pmatrix} I & \Theta \\ \Theta & U \end{pmatrix}$$

Ak $U = X$ potom $CU = CX$ v tvare

$$CX = \begin{pmatrix} I & \Theta \\ \Theta & X \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

CX je teda operácia podmienečného preklopenia stavu $|\psi_1\rangle$ do stavu $X|\psi_1\rangle$ s pravdepodobnosťou $|\beta_0|^2$.

7.4. Dvojica EPR: $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$



$\|\psi^0\rangle$	$\|\psi^1\rangle$	$\|\psi^2\rangle$	$\|\psi^3\rangle$	$c_0\ c_1$
$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$	$\begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{pmatrix}$	0 0 0 1 1 0 1 1

kde

$$
\begin{aligned}
|\psi^0\rangle &= |0\rangle \otimes |0\rangle \\
|\psi^1\rangle &= (H\,|0\rangle) \otimes |0\rangle \\
|\psi^2\rangle &= CX\,|\psi^1\rangle \\
|\psi^3\rangle &= (H \otimes I)\,|\psi^2\rangle
\end{aligned}
$$

8. Záver

1. Vlastnosti kvantového stroja a spôsob spracovania informácií
2. Kvantový stroj z hľadiska Computer Science
3. Súčasný stav a požiadavky

Literatúra

[1] Scott Aaronson and Andris Ambainis. Quantum search of spatial regions. In *44th Annual IEEE Symposium on Foundations of Computer Science, 2003. Proceedings.*, pages 200–209. IEEE, 2003.

[2] Scott Aaronson and Yaoyun Shi. Quantum lower bounds for the collision and the element distinctness problems. *Journal of the ACM (JACM)*, 51(4):595–605, 2004.

[3] Dorit Aharonov and Michael Ben-Or. Fault-tolerant quantum computation with constant error rate. *arXiv preprint quant-ph/9906129*, 1999.

[4] Andris Ambainis. Communication complexity in a 3-computer model. *Algorithmica*, 16(3):298–301, 1996.

[5] Andris Ambainis. Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences*, 64(4):750–767, 2002.

[6] Andris Ambainis. Polynomial degree vs. quantum query complexity. *Journal of Computer and System Sciences*, 72(2):220–238, 2006.

[7] Andris Ambainis. Quantum walk algorithm for element distinctness. *SIAM Journal on Computing*, 37(1):210–239, 2007.

[8] PK Aravind. A simple demonstration of bell's theorem involving two observers and no probabilities or inequalities. *arXiv preprint quant-ph/0206070*, 2002.

[9] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental tests of realistic local theories via bell's theorem. *Physical review letters*, 47(7):460, 1981.

[10] László Babai. Graph isomorphism in quasipolynomial time. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*, pages 684–697. ACM, 2016.

[11] László Babai and Eugene M Luks. Canonical labeling of graphs. In *Proceedings of the fifteenth annual ACM symposium on Theory of computing*, pages 171–183. ACM, 1983.

[12] Ziv Bar-Yossef, Thathachar S Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing*, pages 128–137. ACM, 2004.

[13] Robert Beals. Quantum computation of fourier transforms over symmetric groups. In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pages 48–53. Citeseer, 1997.

[14] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald De Wolf. Quantum lower bounds by polynomials. *Journal of the ACM (JACM)*, 48(4):778–797, 2001.

[15] John S Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.

[16] Aleksandrs Belovs. Span programs for functions with constant-sized 1-certificates. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 77–84. ACM, 2012.

[17] Paul Benioff. Quantum mechanical hamiltonian models of turing machines. *Journal of Statistical Physics*, 29(3):515–546, 1982.

[18] Charles H Bennett and Gilles Brassard. Quantum cryptography: public key distribution and coin tossing. *Theor. Comput. Sci.*, 560(12):7–11, 2014.

[19] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical review letters*, 70(13):1895, 1993.

[20] Charles H Bennett and Stephen J Wiesner. Communication via one-and two-particle operators on einstein-podolsky-rosen states. *Physical review letters*, 69(20):2881, 1992.

[21] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. *SIAM Journal on computing*, 26(5):1411–1473, 1997.

[22] Jean-François Biasse and Fang Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In *Proceedings of the twenty-seventh annual ACM-SIAM symposium on Discrete algorithms*, pages 893–902. Society for Industrial and Applied Mathematics, 2016.

[23] P Van Emde Boas. Machine models and simulations. *Handbook of Theoretical Computer Science, volume A*, pages 1–66, 2014.

[24] Michel Boyer, Gilles Brassard, Peter Høyer, and Alain Tapp. Tight bounds on quantum searching. *Fortschritte der Physik: Progress of Physics*, 46(4-5):493–505, 1998.

[25] Gilles Brassard, Richard Cleve, and Alain Tapp. Cost of exactly simulating quantum entanglement with classical communication. *Physical Review Letters*, 83(9):1874, 1999.

[26] Gilles Brassard, Peter Hoyer, and Alain Tapp. Quantum algorithm for the collision problem. *arXiv preprint quant-ph/9705002*, 1997.

[27] Harry Buhrman, Richard Cleve, Serge Massar, and Ronald De Wolf. Nonlocality and communication complexity. *Reviews of modern physics*, 82(1):665, 2010.

[28] Harry Buhrman, Richard Cleve, John Watrous, and Ronald De Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001.

[29] Harry Buhrman, Richard Cleve, and Avi Wigderson. Quantum vs. classical communication and computation. *arXiv preprint quant-ph/9802040*, 1998.

[30] Harry Buhrman and Robert Špalek. Quantum verification of matrix products. In *Proceedings of the seventeenth annual ACM-SIAM symposium on Discrete algorithm*, pages 880–889. Society for Industrial and Applied Mathematics, 2006.

[31] Mark Bun and Justin Thaler. Dual lower bounds for approximate degree and markov–bernstein inequalities. *Information and Computation*, 243:2–25, 2015.

[32] Andrew M Childs. Lecture notes on quantum algorithms. *Lecture notes at University of Maryland*, 2017.

[33] Boris S Cirel'son. Quantum generalizations of bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980.

[34] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Physical review letters*, 23(15):880, 1969.

[35] Richard Cleve. The query complexity of order-finding. In *Proceedings 15th Annual IEEE Conference on Computational Complexity*, pages 54–59. IEEE, 2000.

[36] Richard Cleve and Harry Buhrman. Substituting quantum entanglement for communication. *Physical Review A*, 56(2):1201, 1997.

[37] Richard Cleve, Artur Ekert, Chiara Macchiavello, and Michele Mosca. Quantum algorithms revisited. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 454(1969):339–354, 1998.

[38] Richard Cleve, Wim Van Dam, Michael Nielsen, and Alain Tapp. Quantum entanglement and the communication complexity of the inner product function. In *Quantum Computing and Quantum Communications*, pages 61–74. Springer, 1999.

[39] Ronald de Wolf. *Quantum Computing and Communication Complexity*. PhD thesis, 2001.

[40] D Deutsch. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society A*, 435:563–574, 1991.

[41] David Deutsch. Quantum theory, the church–turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117, 1985.

[42] David Elieser Deutsch. Quantum computational networks. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 425(1868):73–90, 1989.

[43] Andrew Drucker and Ronald de Wolf. Quantum proofs for classical theorems. *arXiv preprint arXiv:0910.3376*, 2009.

[44] Christoph Durr and Peter Høyer. A quantum algorithm for finding the minimum. *arXiv preprint quant-ph/9607014*, 1996.

[45] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[46] Mark Ettinger, Peter Høyer, and Emanuel Knill. The quantum query complexity of the hidden subgroup problem is polynomial. *Information Processing Letters*, 91(1):43–48, 2004.

[47] Lance Fortnow and John Rogers. Complexity limitations on quantum computation. *Journal of Computer and System Sciences*, 59(2):240–252, 1999.

[48] Peter Frankl and Vojtěch Rödl. Forbidden intersections. *Transactions of the American Mathematical Society*, 300(1):259–286, 1987.

[49] Rusins Freivalds. Probabilistic machines can use less running time. In *IFIP congress*, volume 839, page 842, 1977.

[50] Martin Fürer. Faster integer multiplication. *SIAM Journal on Computing*, 39(3):979–1005, 2009.

[51] Daniel Gottesman. An introduction to quantum error correction and fault-tolerant quantum computation. In *Quantum information science and its contributions to mathematics, Proceedings of Symposia in Applied Mathematics*, volume 68, pages 13–58, 2010.

[52] Michelangelo Grigni, Leonard J Schulman, Monica Vazirani, and Vazirani S. Quantum mechanical algorithms for the nonabelian hidden subgroup problem.

[53] Lov K Grover. A fast quantum mechanical algorithm for database search. *arXiv preprint quant-ph/9605043*, 1996.

[54] Lisa Hales and Sean Hallgren. An improved quantum fourier transform algorithm and applications. In *Proceedings 41st Annual Symposium on Foundations of Computer Science*, pages 515–525. IEEE, 2000.

[55] Sean Hallgren. Polynomial-time quantum algorithms for pell's equation and the principal ideal problem. *Journal of the ACM (JACM)*, 54(1):4, 2007.

[56] Sean Hallgren, Alexander Russell, and Amon Ta-Shma. The hidden subgroup problem and quantum computation using group representations. *SIAM Journal on Computin*, 32(4):916–934, 2003. Earlier version in STOC'00.

[57] G. H. Hardy and E. M. Wrigh. *An Introduction to the Theory of Numbers*. Oxford University Press, New York, fifth edition, 1979.

[58] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Experimental loophole-free violation of a bell inequality using entangled electron spins separated by 1.3 km. *Nature*, 526, 29 October 2015.

[59] A. S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973. English translation in *Problems of Information Transmission*, 9:177-183, 1973.

[60] Peter Høyer, Troy Lee, and Robert Špalek. Negative weights make adversaries stronger. In *Proceedings of 39th ACM STOC*, pages 526–535, 2007.

[61] Peter Høyer and Robert Špalek. Lower bounds on quantum query complexity. *Bulletin of the EATCS*, 87:78–108, October 2005.

[62] Gábor Ivanyos, Luc Sanselme, and Miklos Santha. An effcient quantum algorithm for the hidden subgroup problem in nil-2 groups. *Algorithmica*, 62(1–2):480–492, 2012.

[63] Stacey Jeffery, Robin Kothari, and Frederic Magniez. Nested quantum walks with quantum data structures. In *Proceedings of 24th ACM-SIAM SODA*, pages 1474–1485, 2013.

[64] Jonathan Katz and Luca Trevisan. On the effciency of local decoding procedures for error-correcting codes. In *Proceedings of 32nd ACM STOC*, pages 80–86, 2000.

[65] Iordanis Kerenidis and Ronald de Wolf. Exponential lower bound for 2-query locally decodable codes via a quantum argument. *Journal of Computer and System Sciences*, 69(3):395–420, 2004. Earlier version in STOC'03.

[66] A. Yu. Kitaev. Quantum measurements and the abelian stabilizer problem, 12 November 1995.

[67] Boaz Klartag and Oded Regev. Quantum one-way communication is exponentially stronger than classical communication. *Proceedings of 43rd ACM STOC*, 2011.

[68] Emanuel Knill, Raymond Laflamme, and Wojciech Zurek. Threshold accuracy for quantum computation, 15 October 1996.

[69] Donald E. Knuth. *The Art of Computer Programming. Volume 2: Seminumerical Algorithms*. Addison-Wesley, third edition, 1997.

[70] Francois Le Gall. Improved quantum algorithm for triangle finding via combinatorial arguments. In *Proceedings of 55th IEEE FOCS*, pages 216–225, 2014.

[71] Troy Lee, Frederic Magniez, and Miklos Santha. Improved quantum query algorithms for triangle finding and associativity testing. *Algorithmica*, 77(2):459–486, 2017.

[72] Arjen K. Lenstra and Hendrik W. Jr. Lenstra. *The Development of the Number Field Sieve*, volume 1554 of *Lecture Notes in Mathematics*. Springer, 1993.

[73] Hendrik W. Jr. Lenstra and Carl Pomerance. A rigorous time bound for factoring integers. *Journal of the American Mathematical Society*, 5:483–516, 1992.

[74] Hoi-Kwong Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances, 3 March 1998.

[75] Frederic Magniez, Miklos Santha, and Mario Szegedy. Quantum algorithms for the triangle problem. In *Proceedings of 16th ACM-SIAM SODA*, pages 1109–1117, 2005.

[76] Yuri Manin. *Vychislimoe i nevychislimoe (computable and noncomputable).* Soviet Radio, 1980. In Russian.

[77] Yuri Manin. Classical computing, quantum computing, and shor's factoring algorithm, 2 March 1999.

[78] Dominic Mayers. Unconditional security in quantum cryptography, 10 February 1998.

[79] Cristopher Moore, Daniel Rockmore, and Alexander Russell. Generic quantum fourier transforms. *ACM Transactions on Algorithms*, 2(4):707–723, 2006.

[80] Cristopher Moore, Alexander Russell, and Leonard J. Schulman. The symmetric group defies strong fourier sampling. *SIAM Journal on Computing*, 37(6):1842–1864, 2008. Earlier version in FOCS'05.

[81] Michele Mosca and Artur Ekert. The hidden subgroup problem and eigenvalue estimation on a quantum computer. In *Proceedings of 1st NASA QCQC conference*, volume 1509 of *Lecture Notes in Computer Science*, pages 174–188. Springer, 1998.

[82] Ashwin Nayak. Optimal lower bounds for quantum automata and random access codes. In *Proceedings of 40th IEEE FOCS*, pages 369–376, 1999.

[83] Ilan Newman. Private vs. common random bits in communication complexity. *Information Processing Letters*, 39(2):67–71, 1991.

[84] Ilan Newman and Mario Szegedy. Public vs. private coin ips in one round communication games. In *Proceedings of 28th ACM STOC*, volume 39, pages 561–570, 1996.

[85] Christos H. Papadimitriou. *Computational Complexity*. Addison-Wesley, 1994.

[86] Alexander Razborov. Quantum communication complexity of symmetric predicates. *Izvestiya of the Russian Academy of Sciences, mathematics*, 67(1):159–176, 2003.

[87] Ben Reichardt. Span programs and quantum query complexity: The general adversary bound is nearly tight for every boolean functio. In *Proceedings of 50th IEEE FOCS*, pages 544–551, 2009.

[88] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[89] R. L. Rivest. *Cryptography*, pages 717–755. In [100], 1990.

[90] Miklos Santha. Quantum walk based search algorithms. In *Proceedings of 5th TAMC*, pages 31–46, 2008.

[91] A. Schönhage and V. Strassen. Schnelle multiplikation grosser zahlen. *Computing*, 7:281–292, 1971.

[92] uwe Schöning. A probabilistic algorithm for k-sat and constraint satisfaction problems. In *proceedings of 40th IEEE FOCS*, pages 410–414, 1999.

[93] Alexander Sherstov. Approximating the and-or tree. *Theory of Computing*, 9(20):653–663, 2013.

[94] Peter Shor. Scheme for reducing decoherence in quantum memory. *Physical Review A*, 52:2493, 1995.

[95] Peter Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997. Earlier version in FOCS'94.

[96] Daniel Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26(5):1474–1483, 1997. Earlier version in FOCS'94.

[97] Barbara M. Terhal. Quantum error correction for quantum memories. *Reviews of Modern Physics*, 87:307, 2015.

[98] Luca Trevisan. Some applications of coding theory in computational complexity. *Quaderni di Matematica*, 13:347–424, 2004.

[99] Wim Van Dam. Quantum oracle interrogation: Getting all information for almost half the price. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)*, pages 362–367. IEEE, 1998.

[100] Jan van Leeuwen. *Handbook of Theoretical Computer Science. Volume A: Algorithms and Complexity*. MIT Press, Cambridge, MA, 1990.

[101] Lieven Vandersypen, Matthias Steffen, Gregory Breyta, Constantino Yannoni, Richard Cleve, and Isaac Chuang. Experimental realization of an order-finding algorithm with an nmr quantum computer. *Physical Review Letters*, 85(25):5452–545, 2000.

[102] John Watrous. Quantum algorithms for solvable groups. In *Proceedings of 33rd ACM STOC*, pages 60–67, 2001.

[103] John Watrous. Quantum computational complexity. In *Encyclopedia of Complexity and System Science*. Springer, 2009.

[104] W. K. Wootters and W. H. Zurek. A single quantum cannot be copied. *Nature*, 299:802–803, 1982.

[105] Andrew Chi-Chih Yao. Some complexity questions related to distributive computing. In *Proceedings of 11th ACM STOC*, pages 209–213, 1979.

[106] Andrew Chi-Chih Yao. Quantum circuit complexity. In *Proceedings of 34th IEEE FOCS*, pages 352–360, 1993.