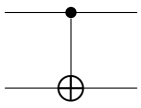
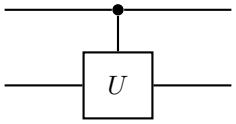
Univerzální množiny hradel

V této kapitole ukážeme, základní princip stavby kvantových počítačů, totiž fakt, že libovolný unitární operátor lze zkonstruovat s pomocí jednokubitových operátorů a jediného dvoukubitového operátoru CNOT, tedy kontrolované negace, kterou značíme



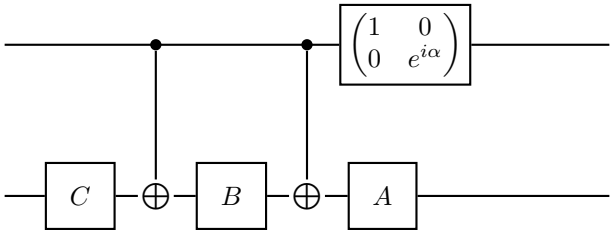
Kontrolované jednokubitové operátory. Prvním krokem je konstrukce libovolných kontrolovaných jednokubitových operátorů. Ty odpovídají podmíněné instrukci „pokud je první kubit jedna, proveď na druhém kubitu operaci U“, schematicky:



Klíčem k řešení je rozklad libovolného operátoru pomocí X a nějakých operátorů A, B a C takových, že platí

$$U = e^{i\alpha} AXBXC, \qquad\qquad ABC = E.$$

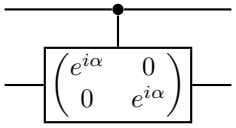
Díky tomuto rozkladu dostáváme kontrolovaný operátor U pomocí obvodu



Je přímočaré ověřit, že $|0\rangle \otimes |\varphi\rangle$ se zobrazí na $|0\rangle \otimes |\varphi\rangle$ a $|1\rangle \otimes |\varphi\rangle$ se zobrazí na $|1\rangle \otimes U|\varphi\rangle$. Všimněte si, že matice

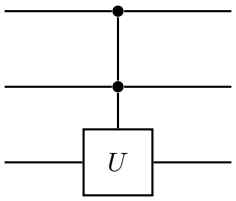
$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$

aplikovaná na první kubit je ekvivalentní kontrolovanému násobení skalární maticí $e^{i\alpha}$:

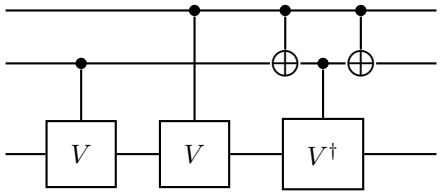


Dvoukontrolované jednokubitové operátory. Dalším důležitým krokem je konstrukce dvoukontrolovaných operátorů, tedy operátorů, které se provedou, právě

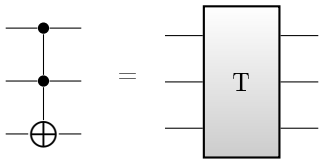
když jsou obě kontrolující hodnoty jedna. Schematicky:



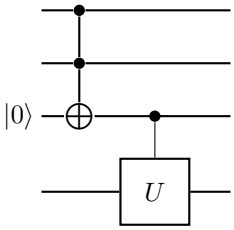
K tomu je třeba odmocniny z operátoru U, tedy operátoru $V = \sqrt{U}$, splňujícího $V^2 = U$ (viz níže). Dvoukontrolovaný operátor U je pak realizován obvodem



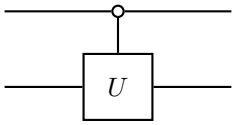
Dvoukontrolovaný operátor je vlastně operátor kontrolovaný konjunkcí dvou hodnot. Jeho konstrukci bychom tedy nemuseli zvlášť zdůrazňovat, pokud bychom uměli realizovat obvod pro AND, což je, jak víme, možné reversibilně pomocí Toffoliho hradla. To je ale samo vlastně dvoukontrolovaná negace (a proto se někdy také značí CCNOT):



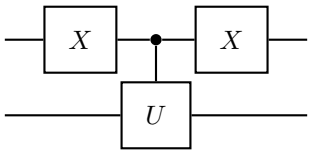
Toffoliho hradlo je tedy speciálním případem uvedené konstrukce a máme díky ní k dispozici všechny booleovské funkce, protože Toffoliho hradlo je univerzální. Dvoukontrolovaný operátor U bychom tedy také mohli vyjádřit složitějším obvodem s jedním pomocným kubitem jako:



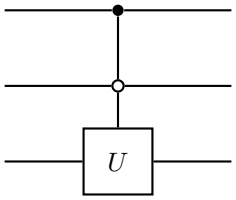
Podobně lze zkonstruovat operátory kontrolované libovolnou booleovskou funkcí. Pokud chceme, aby se operátor provedl, pokud je hodnota kontrolujícího kubitu nula, nikoli jedna, budeme schematicky psát



což je vlastně zkratkou pro



Zápisy můžeme také kombinovat, např. jako



Na příkladu Toffoliho hradla si ukažme konstrukci operátoru V , tedy „odmocniny z negace“. Nalezení takového operátoru je speciálním případem funkce aplikované na normální operátor. Pro libovolnou funkci $f : \mathbb{R} \to \mathbb{C}$ a pro normální operátor A definujme $f(A)$ jako operátor splňující

$$f(A)|u_\lambda\rangle = f(\lambda)|u_\lambda\rangle$$

pro každý vlastní vektor u_λ operátoru A, kde λ je příslušné vlastní číslo. Negace je dána Pauliho operátorem

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

který lze pomocí projekcí na vlastní vektory zapsat jako

$$X = |+\rangle\langle +| - |-\rangle\langle -|,$$

kde

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

Odtud dostáváme

$$V = \sqrt{1}|+\rangle\langle +| + \sqrt{-1}|-\rangle\langle -|\,.$$

Máme čtyři možnosti jak dvojici odmocnin zvolit. Pro $\sqrt{1} = 1$ a $\sqrt{-1} = i$ dostáváme

$$V = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \frac{i}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \frac{1-i}{2} \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix}.$$

Převod dvouúrovňových operátorů na jednokubitové kontrolované. Uvažme unitární operátor U na čtyřdimenzionálním prostoru daný maticí

$$U = \begin{pmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

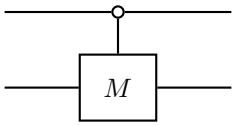
Operátor působí neidenticky pouze na bázových vektorech $|00\rangle$ a $|01\rangle$, a to takto

$$|0\rangle \otimes |0\rangle \mapsto |0\rangle \otimes (a|0\rangle + c|1\rangle), \qquad |0\rangle \otimes |1\rangle \mapsto |0\rangle \otimes (b|0\rangle + d|1\rangle).$$

Označíme-li

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

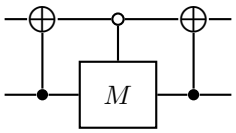
lze tedy U zkonstruovat jako



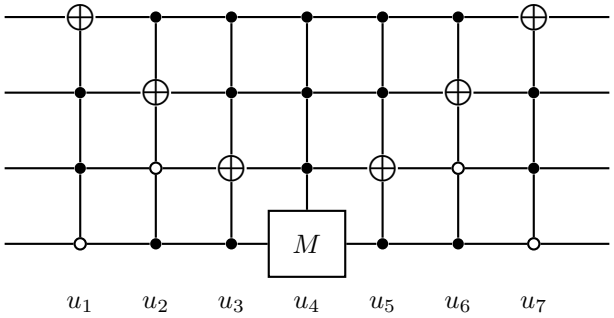
Operátory působící neidenticky pouze na dvou bázových vektorech se nazývají dvouúrovňové. Ne každý dvouúrovňový operátor má ale tak jednoduchý obvod jako operátor U. Např. operátor

$$U' = \begin{pmatrix} a & 0 & 0 & b \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ c & 0 & 0 & d \end{pmatrix}$$

působí neidenticky na bázových vektorech $|00\rangle$ a $|11\rangle$, které se liší na více než jednom místě, a proto ho nelze jednoduše zapsat jako kontrolovanou matici M. Je nutné nejprve provést změnu báze, tak aby se neidenticky zobrazované vektory lišily pouze na jednom místě. Provedeme tedy permutaci, která prohazuje $|11\rangle$ a $|01\rangle$, což je CNOT na prvním kubitu kontrolovaný druhým kubitem. Pak už můžeme postupovat jako v případě U a následně zpět vyměnit $|11\rangle$ a $|01\rangle$. Celý obvod vypadá takto



V případě obecné dvouúrovňové matice působící neidenticky na bázových vektorech $\mathbf{b} = |k_{n-1}k_{n-2}\dots k_0\rangle$ a $\mathbf{b'} = |\ell_{n-1}\ell_{n-2}\dots \ell_0\rangle$, musíme tyto vektory zobrazit na bázové prvky, které se liší jen v jednom kubitu. Na něm pak provedeme kontrolovanou operaci a bázi převedeme zpět do původní podoby. Celkem to znamená sérii operací kontrolovaných všemi kubity až na jeden, který se mění. Předpokládejme např., že matice M působí neidenticky na kubitech $\mathbf{b} = |0110\rangle$ a $\mathbf{b} = |1001\rangle$. Můžeme si vybrat bázové vektory, lišící se jen v jednom kubitu, na kterých budeme provádět kontrolovanou operaci M; zvolme např. $|1110\rangle$ a $|1111\rangle$. Musíme tedy změnit první tři kubity: první v bázovém vektoru $\mathbf{b}$, druhý a třetí v bázovém vektoru $\mathbf{b'}$. Obvod bude vypadat takto



- u_1 a u_7: transpozice $|0110\rangle \leftrightarrow |1110\rangle$
- u_2 a u_6: transpozice $|1001\rangle \leftrightarrow |1101\rangle$
- u_3 a u_5: transpozice $|1101\rangle \leftrightarrow |1111\rangle$

- u_4: transformace $|1110\rangle \mapsto a|1110\rangle + b|1111\rangle$; $|1111\rangle \mapsto c|1110\rangle + d|1111\rangle$

Rozklad na dvouúrovňové operátory. Zbývá ukázat, že libovolný unitární operátor je možné rozložit na unitární dvouúrovňové operátory. Proces takového rozkladu je podobný Gaussově eliminaci a hledané dvouúrovňové matice jsou matice příslušných elementárních transformací. Ty jsou vždy dvouúrovňové: manipulují jen se dvěma řádky. Oproti klasické Gaussově eliminaci ale ještě musíme zajistit, aby byly unitární. To jistě platí, pokud pouze prohazujeme řádky (abychom na diagonálu dostali nenulový prvek). Studujme případ, kdy chceme odečíst prvek mimo diagonálu. Nechť je upravovaná matice tvaru

$$U = \begin{pmatrix} a & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ b & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix},$$

kde $U_{1,1} = a \neq 0$ a $U_{j,1} = b \neq 0$ a ostatní prvky jsou libovolné. Nenulovost prvku a jsme případně zajistili permutací řádků. Chceme se nyní zbavit prvku b, tedy vynulovat pozici $(j, 1)$. Můžeme to udělat přičtením vhodného násobku prvního řádku k řádku j-tému. V případě klasické Gaussovy eliminace bychom použili matici elementární transformace

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ -b/a & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Poznamenejme, že chceme-li se vyhnout dělení (např. při úpravě celočíselné matice), lze také použít matici

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ b & 0 & 0 & -a & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Ani jedna z těchto matic sice není unitární, ale není těžké ji na unitární doplnit znormováním j-tého řádku a změnou prvního řádku na kolmý jednotkový vektor:

$$U_1 = \begin{pmatrix} a^*/c & 0 & 0 & b^*/c & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ b/c & 0 & 0 & -a/c & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

kde $c = \|(a,b)\| = \sqrt{aa^* + bb^*}$. Vynásobením dostaneme

$$U_1 \cdot U = \begin{pmatrix} c & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix} .$$

Takto postupně převedeme matici U na

$$U' = \begin{pmatrix} a' & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix} .$$

Vzhledem k tomu, že vzniklá matice je stále unitární (násobili jsme ji unitárními maticemi), musí být $|a'| = 1$. Z posledního kroku eliminace je navíc zřejmé, že $a' = 1$. Protože i řádky unitární matice mají normu jedna, je U' ve skutečnosti tvaru

$$U' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix} .$$

Opakováním postupu pro menší matici dostaneme nakonec matici jednotkovou. Máme tedy

$$U_k \cdots U_2 U_1 \cdot U = I \,,$$

kde U_i jsou dvouúrovňové unitární operátory (některé z nich mohou být permutační matice vyměňující řádky). Máme tedy kýžený rozklad U na dvouúrovňové operátory

$$U = U_1^\dagger U_1^\dagger \cdots U_k^\dagger \,.$$