# 7. prednáška

## Kvantové pčítanie I – reverzibilné brány, Toffoliho brána a Fredkinova brány,

Budeme študovať elementárne zariadenia na kvantové počítanie, ktoré sú založené na predpoklade, že uskutočňuje unitárnu transformáciu $U$, ktorá sa rovná súčinu elementárnych unitárnych transformácií

$$U = U_n U_{n-1} ... U_2 U_1$$

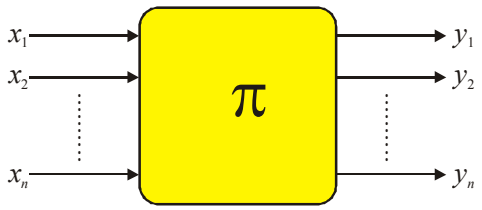
Každá elementárna transformácia $U_i$ je priradená nejakému kroku elementárneho zariadenia na kvantové počítanie. To znamená, že toto klasické výpočtové zariadenia sa budeme snažiť naformulovať pomocou unitárnych transformácií. Pretože unitárne transformácie sú invertibilné (pre unitárnu transformáciu platí $U^+ = U^{-1}$), potom môžeme povedať, že len také klasické výpočtové zariadenia môžu byť formálne diskutované ako kvantové výpočtové zariadenia, ktoré sú reverzibilné. Ak nejaké klasické výpočtové zariadenia je a-priori ireverzibilné, potom nemôže byť interpretované ako nejaká forma kvantového výpočtového zariadenia. Len reverzibilné klasické výpočtové zariadenia má šancu byť implementované na kvantovej úrovni. V nasledujúcej časti tejto kapitoly budeme postupne študovať klasické výpočtové zariadenia, ktoré sú implementované pomocou Boolových funkcií (ich konkretná realizácia ako výpočtových brán môžete byť uskutočnená pomocou niekoľkých elementárnych brán pre logické spojky AND, OR a NOT), v nasledujúcej časti budeme diskutovať reverzibilné verzie týchto klasických zariadení. V konečnej tretej časti kapitoly budeme diskutovať kvantové brány, ktoré sú implementované pomocou unitárnych operátorov a pôsobia na stavové vektory kvantového systému.

### 7.1 Klasické výpočtové zariadenie

Uvažujeme klasické výpočtové zariadenie, ktoré je formálne interpretované ako zobrazenie

$$\pi : \{0,1\}^n \to \{0,1\}^m \qquad (7.1)$$

ktoré zobrazuje binárny reťazec $x \in \{0,1\}^n$ dĺžky $n$ na binárny reťazec $y \in \{0,1\}^m$ dĺžky $m$, pozri obr. 7.1



**Obrázok 7.1.** Grafická interpretácia klasického výpočtového zariadenia, ktoré chápeme ako Boolovu funkciu (3.1), ktorá priradí *n* binárnym premenným $x_1, x_2, ..., x_n$ *n* binárných argumentov $y_1, y_2, ..., y_m$.

Boolova algebra poskytuje formálne prostriedky k simulácii ľubovoľnej Boolovej funkcie typu (3.1) pomocou DNF tvaru

$$f(x_1, x_2, ..., x_n) = \bigvee_{\boldsymbol{e} \in \{0,1\}^n} f(e_1, e_2, ..., e_n) \wedge x_1^{e_1} \wedge x_2^{e_2} \wedge ... \wedge x_n^{e_n} \tag{7.2a}$$

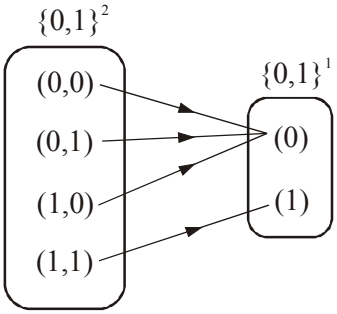
kde

$$x_i^{e_i} = \begin{cases} x_i & (e_i = 1) \\ \overline{x}_i & (e_i = 0) \end{cases} \tag{7.2b}$$

$x_i^{e_i}$ je literál *i*-tej premennej $x_i$. Na pravej strane (3.2a) sú aktívne len jednotkové funkčné hodnoty $f(e_1, e_2, ..., e_n) = 1$, členy s nulovými funkčnými hodnotami, $f(e_1, e_2, ..., e_n) = 0$, môžu byť ignorované ako nepodstatné. To znamená, že pri konštrukcii Boolovej funkcie pomocou (7.2a) z príslušnej tabuľky funkčných hodnôt berieme používame len riadky s jednotkovou funkčnou hodnotou (čo môže byť výhodné vtedy, ak daná Boolova funkcia obsahuje len niekoľko jednotkových funkčných hodnôt, vo väčšine prípadov má nulové funkčné hodnoty).

## 7.2 Reverzibílne klasické výpočty

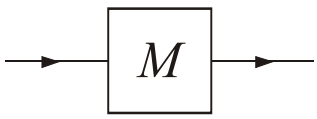
Hlavným nedostatkom Boolovej funkcie zostrojenej v predchádzajúcej kapitole 3.1 je, že nie je reverzibilná, t. j. z jej funkčných hodnôt nie sme schopný jednoznačne priradiť argumenty, pozri obr. 7.2. Podmienka reverzibilita danej funkcie je veľmi dôležitá pre jej implementáciu v prostredí kvantovej teórie, ktorá požaduje, aby daná funkcia bola realizovaná pomocou unitárneho operátora, ktorý je automaticky invertibílny. Tento pomerne tvrdú požiadavku zoslabíme tak, že každá funkcia, ktorá sa použije vo výpočte je invertibílna.




**Obrázok 7.2**. Znázornenie Boolovej funkcie AND ako zobrazenia $f: \{0,1\}^2 \to \{0,1\}^1$, k tomuto zobrazeniu neexistuje inverzné zobrazenie, t. .j. funcia AND nie je reverzibílna.

### 7.2.*1 Reverzibílne1-bitové brány*

Tieto najjednoduchšie brány sú určené transformáciou $\pi: \{0,1\} \to \{0,1\}$, pozri obr. 7.3.




**Obrázok 7.3.** Grafická reprezentácia 1-bitovej reverzibilnej brány.

Existujú dve reverzibílne 1-bitové brány, brána identity $I$ a brána negácie $N$, ktoré sú znázornené pomocou tabuľky

| $x$ | *Identita* ($I$) | *Negácia* ($N$) |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

### *7.2.2 Rreverzibílne 2-bitové brány*

Tieto brány sú určené transformáciou $\pi : \{0,1\}^2 \to \{0,1\}^2$, pozri obr. 7.4.


**Obrázok 7.4.**

2-bitovú bránu môžeme špecifikovať pomocou tabuľky

| # | *argumenty* | |
|---|---|---|
| 1 | 0 | 0 |
| 2 | 0 | 1 |
| 3 | 1 | 0 |
| 4 | 1 | 1 |

| $M_1$ | |
|---|---|
| 0 | 0 |
| 0 | 1 |
| 1 | 0 |
| 1 | 1 |
| $P$=$I$ | |

| $M_2$ | |
|---|---|
| 0 | 0 |
| 1 | 0 |
| 0 | 1 |
| 1 | 1 |
| $P$=(1,2) | |

.....

| $M_{24}$ | |
|---|---|
| 1 | 1 |
| 1 | 0 |
| 0 | 1 |
| 0 | 0 |
| $P$=(1,4)(2,3) | |

Z tejto tabuľky vyplýva, že existuje 4!=24 rôznych 2-bitových reverzibílnych brán, ktoré sú jednoznačne určené permutáciou 4 objektov špecifikujúcich dvojicu funkčných hodnôt danej brány.

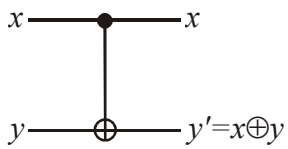
Z binárnych Boolových funkcií môžeme vyjadriť pomocou reverzibílnych brán logickú spojku XOR

$$M_{XOR} : (x, y) \to (x, x \oplus y) \tag{7.3}$$

V tabuľke sú uvedené jednoduché ilustračné príklady 2-bitových brán, ktoré sú priradené logickým spojkám AND, OR a IMP

| # | (x,y) | $(x, f_{XOR}(x,y))$ |
|---|---|---|
| 1 | (0,0) | (0,0) |
| 2 | (0,1) | (0,1) |
| 3 | (1,0) | (1,1) |
| 4 | (1,1) | (1,0) |

Grafická interpretácia tohto reverzibílneho obvodu je znázornená na obr. 7.5. Alternatívny názor tohto 2-bitovej brány je brána riadenej negácie ($C_{NOT}$), hodnota prvej premennej $x$ špecifikuje, či druhá premenná $y$ bude negovaná (pre $x$ = 1) alebo nebude negovaná (pre $x$ = 0).




**Obrázok 7.5.**

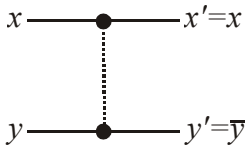
Každá reverzibílna 2-bitová brána môže byť kompletne popísaná pomocou permutácie vstupných binárnych dvojíc na výstupné binárne dvojice. Tak napríklad, 2-bitová brána $C_{NOT}$ je charakterizovaná permutáciou (pozri vyššie uvedenú tabuľku) $P$ = (3,4). Pre ilustráciu tohto prístupu uvažujme permutácie P = (1,2)(3,4), tabuľka vstupných a výstupných binárnych dvojíc pre túto permutáciu má tvar

| # | $(x,y)$ | $(x',y')$ |
|---|---|---|
| 1 | (0,0) | (0,1) |
| 2 | (0,1) | (0,0) |
| 3 | (1,0) | (1,1) |
| 4 | (1,1) | (1,0) |

kde tretí stĺpec sme zostrojili z druhého stĺpca ta, že sme prehodili prvý - druhý a tretí – štvrtý riadky. Výstupné premenné sú ohodnotené Boolovými funkciami, ktoré sú zostrojené štandardným postupom

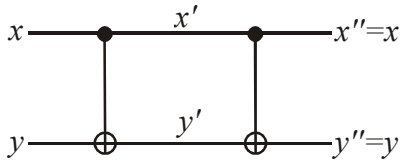
$$x' = x\overline{y} + xy = x$$
$$y' = \overline{x}\,\overline{y} + x\overline{y} = \overline{y}$$

To znamená, že tánto reverzibílna 2-bitová brána na prvom výstupe má vstupnú premennú $x$ a na druhom výstupe negovanmú premennú $\overline{y}$, pozri obr. 7.6.

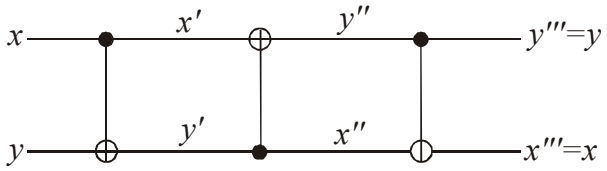



**Obrázok 7.6.**

Bránu $C_{NOT}$ môžeme medzi sebou kombinovať rôznymi spôsobmi. Napríklad opakované prepojenie tejto brány dáva identitu, pozri obr. 7.7.




**Obrázok 7.7.** Medzi výsledok je špecifikovaný $x' = x,\ y' = x \oplus y$, potom pre konečné výsledky platí $x'' = x,\ y'' = x \oplus (x \oplus y)$. Pretože operácia XOR je asociatívna, formulu pre $y''$ môžeme zjednodušiť, $y'' = x \oplus (x \oplus y) = \underbrace{(x \oplus x)}_{0} \oplus y = y$.



**Obrázok 7.8**. Trojnásobné použitie brány $C_{NOT}$, ktoré vedie k „transpozícii“ binárneho výstupu.

Trojnásobné použitie brány $C_{NOT}$ znázornené na obr. 7.8 vedie k transpozícii vstupných binárnych argumentov ako výstupných binárnych premenných. Dôkaz tejto vlastnosti je pomerne jednoduchý, postupne (pomocou troch krokov) budeme počítať binárne veličiny $(x',y')$, $(x'',y'')$ a $(x''',y''')$:

1. krok: $$x' = x,\ y' = x \oplus y$$

2. krok: $$x'' = y' = x \otimes y,\quad y'' = y' \oplus x' = (x \otimes y) \oplus x = y$$

3. krok: $$x''' = y'' \oplus x'' = y \oplus (x \oplus y) = x,\quad y''' = y'' = y$$

### *7.2.3 Reverzibílne 3-bitové brány*

Konštrukcia 3-bitových reverzibilných brán $\pi : \{0,1\}^3 \to \{0,1\}^3$, bola navrhnutá Toffolim a Fredkinom. Ich postup vysvetlíme pomocou jednoduchého ilustračného príkladu funkcie AND, ktorá je špecifikovaná na obr. 7.1. Táto funkcia $f_{AND} : \{0,1\}^2 \to \{0,1\}$ je v explicitnom tvare určená formulou $f_{AND}(x_1,x_2) = y$, kde $x_1, x_2$ sú binárne argumenty – premenné a $y$ je funkčná hodnota. Definujme funkciu $\tilde{f}_{AND} : \{0,1\}^3 \to \{0,1\}^3$, ako rozšíreniu pôvodnej funkcie $f_{AND}$ takto

$$\tilde{f}(x_1,x_2,z) = (x_1,x_2,z \oplus f(x_1,x_2)) \tag{3.3}$$

kde symbol $\oplus$ reprezentuje binárnu operáciu XOR (eXclusive OR). Tento prístup môžeme pomocou dvoch tabuliek vyjadriť takto

| $x_1$ | $x_2$ | $z$ | # |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 2 |
| 1 | 0 | 0 | 4 |
| 1 | 1 | 0 | 6 |
| 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 3 |
| 1 | 0 | 1 | 5 |
| 1 | 1 | 1 | 7 |

| $x_1$ | $x_2$ | $z \oplus f_{AND}(x_1,x_2)$ | # |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 2 |
| 1 | 0 | 0 | 4 |
| 1 | 1 | 1 | 7 |
| 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 3 |
| 1 | 0 | 1 | 5 |
| 1 | 1 | 0 | 6 |

Ľavá tabuľka rozšírenie dvoch argumentov $x_1$ a $x_2$ o ďalší tretí pomocný argument $z$, ktorý „riadi“ výsledky uvedené v pravej tabuľke pomocou binárnej operácie XOR. Ak pomocný argument $z = 0$ ($z = 1$), potom v treťom stĺpci pravej tabuľky sú uvedené výsledky binárnej operácia AND (Negácie AND, ktorá sa preto občas nazýva NAND, alebo v klasickej logike sa nazýva Shefferov symbol). Pravá a aj ľavá tabuľka v poslednom stĺpci (označenom symbolom #) obsahujú celočíselnú interpretáciu prvých troch binárnych čísel, potom symbol (3.3) môžeme interpretovať pomocou súčinu transpozícií jednotlivých riadkov v tabuľke, napríklad v tomto prípade tabuľka je jednoznačne špecifikovaná permutáciou symbolom

$$P = (6,7) \tag{7.4}$$

To znamená, že tabuľku môžeme zostrojiť tak, že vedľa seba napíšeme všetkých 8 binárnych trojíc (argumentov resp. funkčných hodnôt) a prehodíme medzi sebou dva riadky, ktoré majú celočíselnú interpretáciu 6 a 7.

Na rozdiel od 2-bitových reverzibílnych brán, Toffoliho brána je univerzálna pre výrokovú logiku, Pre zjednodušenie formulácie tejto skutočnosti definujme funkciu *T*, ktorá ma tri argumenty

$$T(x_1, x_2, y) = (x_1, x_2, y \oplus x_1 x_2)$$

kde súčin $x_1 x_2$ reprezentuje konjunkciu daných binárnych premenných (výrokov). Ľahko sa presvedčíme, že Toffoliho brána má iniverzálny charakter, pomocou nej môžeme zostrojiť základné logické spojky:

spojka NOT $$T(1,1,y) = \left(1,1,\boxed{\overline{y}}\right)$$

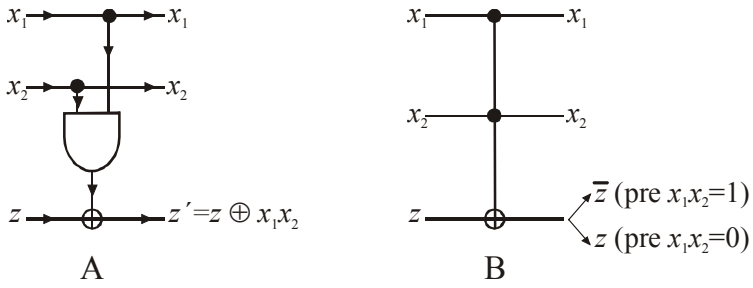
spojka AND $$T(x_1, x_2, 0) = \left(x_1, x_2, \boxed{x_1 x_2}\right)$$

spojka OR (dvojkroková konštrukcia)

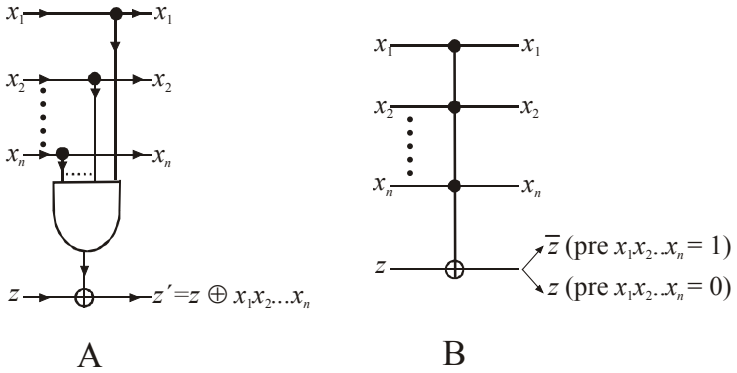
$$T(\overline{x}, \overline{y}, 0) = \left(\overline{x}, \overline{y}, \boxed{\overline{x}\,\overline{y}}\right) \Rightarrow T(1,1,\overline{x}\,\overline{y}) = \left(1,1,\boxed{x+y}\right)$$

Týmto sme dokázali, že pomocou Toffoliho 3-bitovej reverzibílnej brány sme schopný simulovať ľubovolnú Boolovu funkciu.

Diagramatické znázornenie Toffoliho brány je na obr. 7.9.

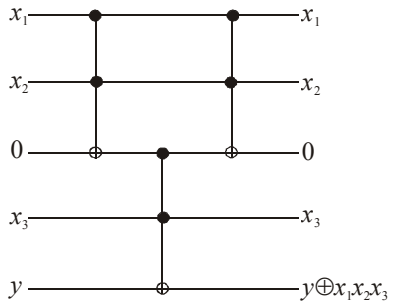



**Obrázok 7.9.** Znázornenie Toffoliho brány (taktiež často nazývaná $CC_{NOT}$ brána, dvakrát kontrolované NOT). Diagram (A) znázorňuje „klasickú“ realizáciu Toffoliho brány, ktorá je založená na použití brány konjunkcie (dobre známej z teórie logických obvodov). Diagram (B) je zjednodušenie diagramu (A).



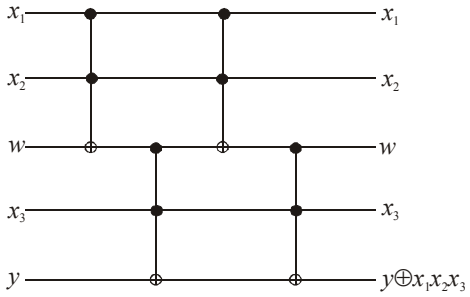

**Obrázok 7.10.** Zovšeobecnená Toffoliho reverzibílna brána obsahujúca (*n*+1) vstupných binárnych premenných, posledná vstupná premenná *z* je negovaná vtedy a len vtedy, ak konjunkcia prvých *n* vstupných premenných sa rovná 1.

Univerzálnosť Toffoliho brány môže byť chápaná nielen ako možnosť vyjadrenia pomoc nej základných logických spojok, ale taktiež aj možnosť vyjadriť každú reverzibílnu n-bitovú funkciu pomocou kombinácie Toffoliho 3-bitových brán. K tomu, aby sme demonštrovali túto skutočnosť, vykonáme formuláciu zovšeobecnených *n*-bitových Toffoliho brán. Táto univerzálnosť spočíva v tom, že pomocou tejto „elementárnej“ bráni sme schopný zostrojiť *n*-bitovú Toffoliho bránu (kde $n > 3$), pozri obr. 7.11.




**Obrázok 7.11.** Znázornenie rekonštrukcie zovšeobecnenej Toffoliho brány pre $n = 3$, pričom brána obsahuje prostredný spoj s nulovou premennou. Cieľom tretej Toffoliho brány je vynulovanie premennej späť do jej nulovej hodnoty.

Ak túto schému z obr. 7.11 rozšírime o štvrtú Toffoliho bránu, potom výsledky celkovej siete nebudú závislé od skutočnosti, či počiatočná hodnota prostredného bitu je nulová alebo nie, pozri obr. 7.12.




**Obrázok 7.12.** Modifikovaná rekonštrukcia z obr. 7.11, ktorá má navyše štvrtú Toffoliho bránu, potom výsledok celkovej brány už nie je závislý od hodnoty binárnej premennej *w*.

Pre úplnosť budeme študovať ešte Fredkinovu 3-bitovú reverzibílnu bránu, ktorá má použitie v ilustrácii reverzibílnych brán pomocou biliardových gúľ (pozri nasledujúcu kapitolu). ***Fredkinova brána*** je špecifikovaná tabuľkou

| $x$ | $y$ | $z$ | $x'$ | $y'$ | $z'$ |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 | 0 |
| 0 | 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 | 0 | 1 |
| 1 | 1 | 0 | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 |

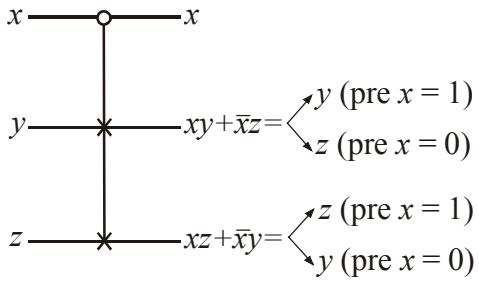
Prvá vstupná premenná $x$ je riadiaca, podľa jej hodnoty (ak $x$ = 1) dochádza na výstupe k transpozícii premenných $y$ a $z$, t. j. $z' = y, y' = z$, pozri obr. 7.13. Pomocou výrokových formúl môžeme Fredkinovu bránu vyjadriť takto:

$$F(x,y,z) = (x, \bar{x}z + xy, \bar{x}y + xz)$$

$$x' = x,$$

$$y' = \bar{x}\,\bar{y}z + \bar{x}yz + xy\bar{z} + xyz = \bar{x}(\bar{y} + y)z + xy(z + \bar{z}) = \bar{x}z + xy$$

$$z' = \bar{x}y\bar{z} + \bar{x}yz + x\bar{y}z + xyz = \bar{x}y(\bar{z} + z) + x(\bar{y} + y)z = \bar{x}y + xz$$




**Obrázok 7.13.** Diagramatická špecifikácia Fredkinovej brány, ktorá pôsobí ako podmienený prepínač, ak vstupná premenná $x$ = 0 ($x$ = 1) , potom na výstupe druhá a tretia premenná sú prehodené. $y \to z, z \to y$, (zostávajú zachované , $y \to y, z \to z$ ).

Podobne ako Toffoliho brána, aj Fredkinova brána má univerzálny charakter, pomocou tejto brány môžeme generovať základne logické spojky:

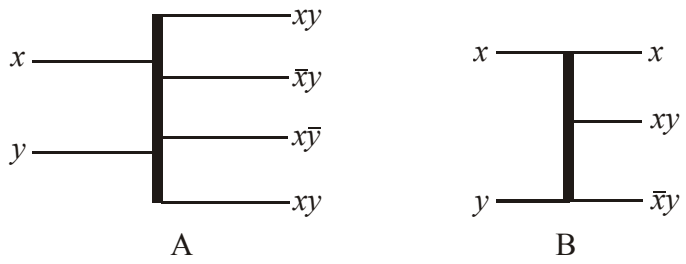
spojka OR: $F(x,1,z) = (x, \boxed{x+z}, \bar{x}+z)$,

spojka AND $F(x,y,0) = (x, \boxed{xy}, \bar{x}y)$,

spojka NOT $F(x,1,0) = (x, x, \boxed{\bar{x}})$.

Výstupné argumenty Fredkinovej brány, ktoré sú zarámované obdĺžnikom, sú interpretované ako výsledok brány, ostatne výstupné argumenty sú interpretované ako „odpad“.

Fredkinova brána sa obvykle interpretuje pomocou dvoch jednoduchších reverzibílnych brán, ktoré sa nazývajú interakčná brána a prepínaná brána, pozri obr. 3.13.



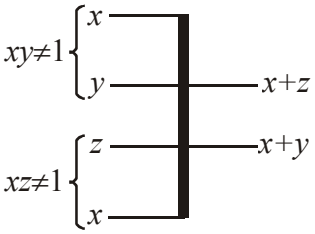

**Obrázok 7.14.** Reverzibílna (A) interakčná brána a (B) prepínaná brána.

Je potrebné zdôrazniť, že obe tieto brány, aj keď majú rozdielny počet vstupov a výstupov, sú reverzibílne, čo sa jednoducho overí z ich tabuľkových špecifikácií.

| *argumenty* | | | | *interakčná brána* | | | | | *prepínaná brána* | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| # | $x$ | $y$ | | $xy$ | $\bar{x}y$ | $x\bar{y}$ | $xy$ | | $x$ | $xy$ | $\bar{x}y$ |
| 1 | 0 | 0 | | 0 | 0 | 0 | 0 | | 0 | 0 | 0 |
| 2 | 0 | 1 | | 0 | 1 | 0 | 0 | | 0 | 0 | 1 |
| 3 | 1 | 0 | | 0 | 0 | 1 | 0 | | 1 | 0 | 0 |
| 4 | 1 | 1 | | 1 | 0 | 0 | 1 | | 1 | 1 | 0 |

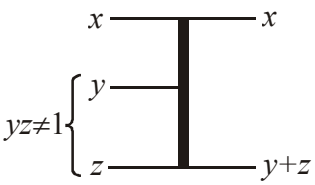
Z tejto tabuľky vyplýva, že vzťah medzi argumentmi a funkčnými hodnotami je 1-1-značný, čiže obe tieto brány sú reverzibílne.

Inverzná interakčná brána je znázornená na obr. 7.15.



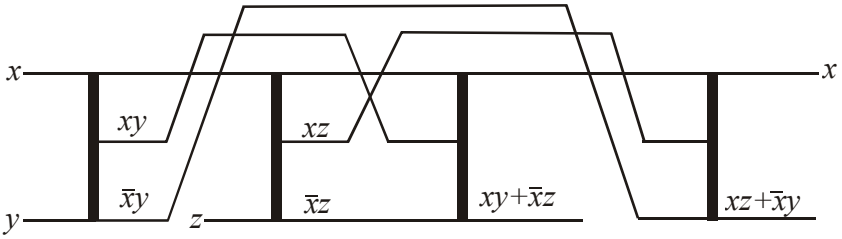

**Obrázok 7.15.** Inverzná interakčná brána vytvára súčet prvého a tretieho resp. prvého a druhého argumentu, vstupné argumenty sú ohraničené podmienkami $xy \neq 1$ a $xz \neq 1$.

Podobným spôsobom môžeme zostrojiť aj inverznú prepínanú bránu, ktorá taktiež môže slúžiť pre tvorbu súčtu druhého a tretieho argumentu, $y + z$, za predpokladu, že ich súčin sa nerovná jednej, $yz \neq 1$, pozri obr. 7.16.




**Obrázok 7.16.** Inverzná prepínaná brána slúži pre tvorbu súčtu druhého a tretieho argumentu, pričom ich súčin sa nerovná 1.

Pomocou štyroch prepínaných brán môžeme vytvoriť Fredkinovu bránu tak, že najprv použijeme dve „priame“ prepínané brány pre tvorbu súčinov argumentov a ich negácií, potom použijeme dve inverzné prepínané brány pre tvorbu súčtov, ktoré boli vytvorené predtým, pozri obr. 7.17. Ľahko sa presvedčíme, že podmienka nerovnosti súčinu druhého a tretieho argumentu jednej je v tomto prípade splnená. Podobným spôsobom môžeme zostrojiť aj Fredkinovu bránou pomocou štyroch (dvoch priamych a dvoch inverznych) inverzných brán.




**Obrázok 7.17**. Konštrukcia Fredkinovej brány pomocou štyroch prepínaných brán.