Kvantová informace - zápočtové úlohy

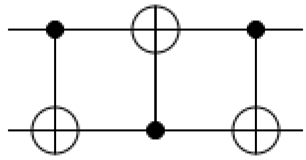
Jan Oupický

1

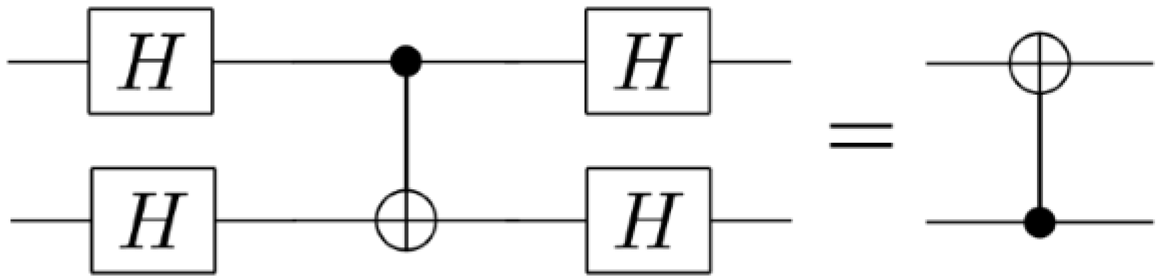
idk

2

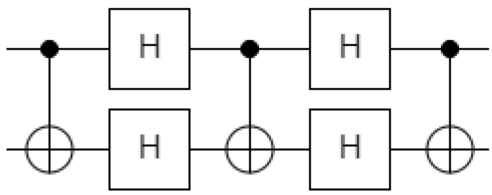
Klasický SWAP vypadá takto:



Použítím této ekvivalence CNOT pomocí Hadamardových matic:



se zbavíme prostředního CNOT, který je v jiném směru. Výsledný obvod je tedy:



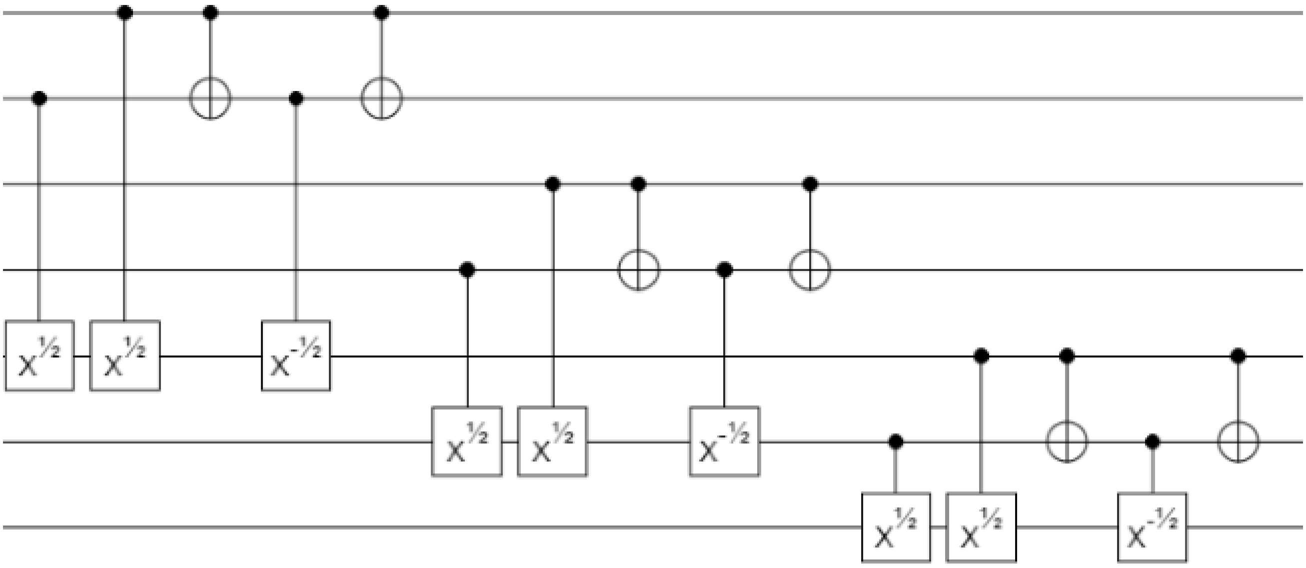
3

Řešení je v principu spočítat AND prvního a druhého qubitu samostatně a zároveň stejně třetího a čtvrtého. A spočítat výsledný AND těchto výsledků, který je ekvivalentní ANDu všech 4 „najednou“.

Použijeme tedy 3x CNOT. Ten ale potřebujeme rozložit pomocí dvoukubitových bran. Použijeme postup ve skriptech, jak rozložit dvoukontrolovaný jednokubitový operátor na jednokontrolované jednokubitové. Použijeme tedy matici X a spočítáme její odmocninu $\sqrt{X}$ a její hermitovsky sdruženou $\sqrt{X}^{-1}$. Matice jsou:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sqrt{X} = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}, \sqrt{X}^{-1} = \frac{1}{2}\begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix}$$

Výsledný obvod tedy vypadá takto:

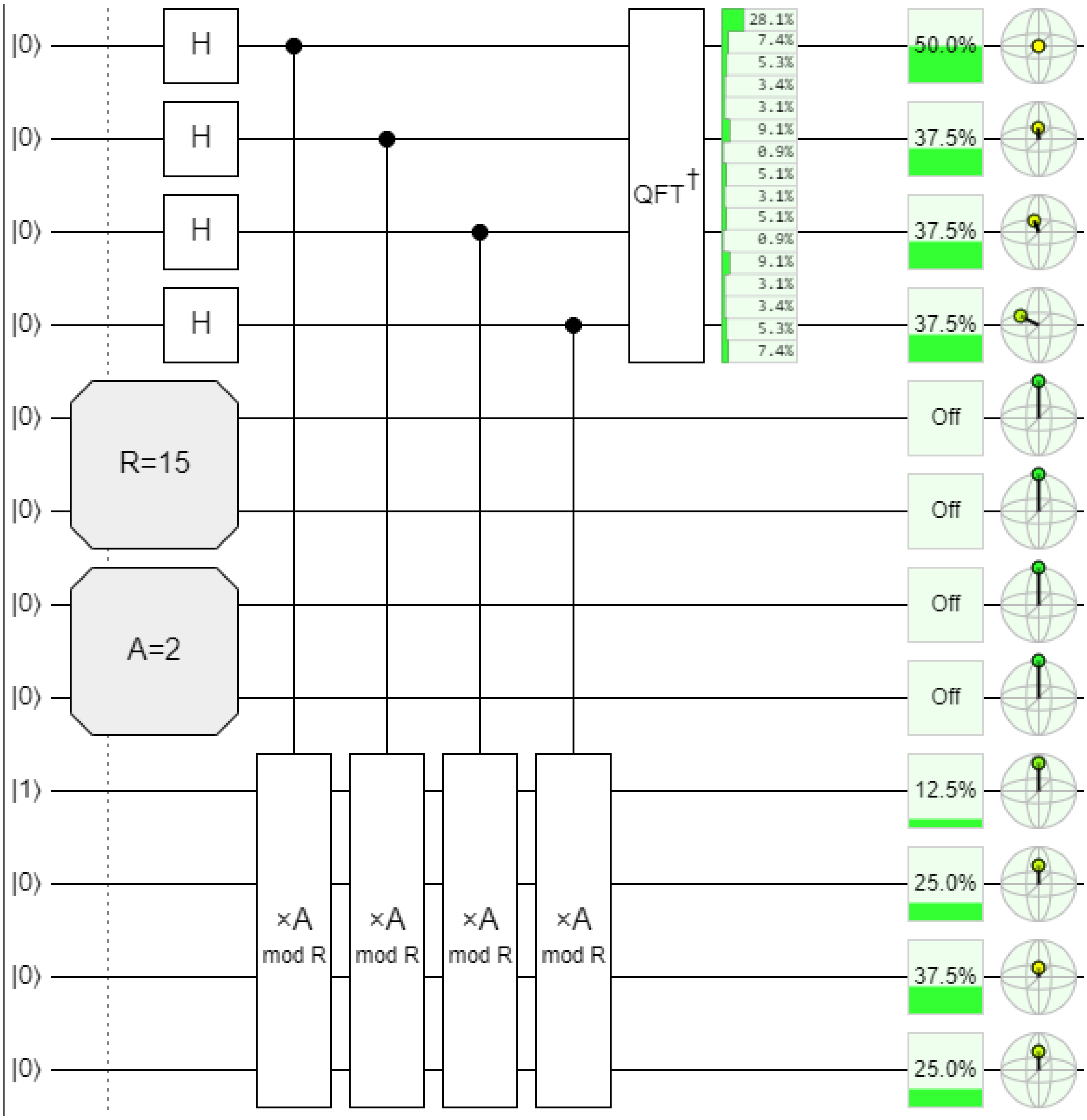


První 4 dráty jsou vstupní 4 qubity. V 5. drátě je výsledek AND prvního a druhého, v 6. je 3. a 4. a v posledním se spočítá AND 5. a 6., což je požadovaný výsledek.

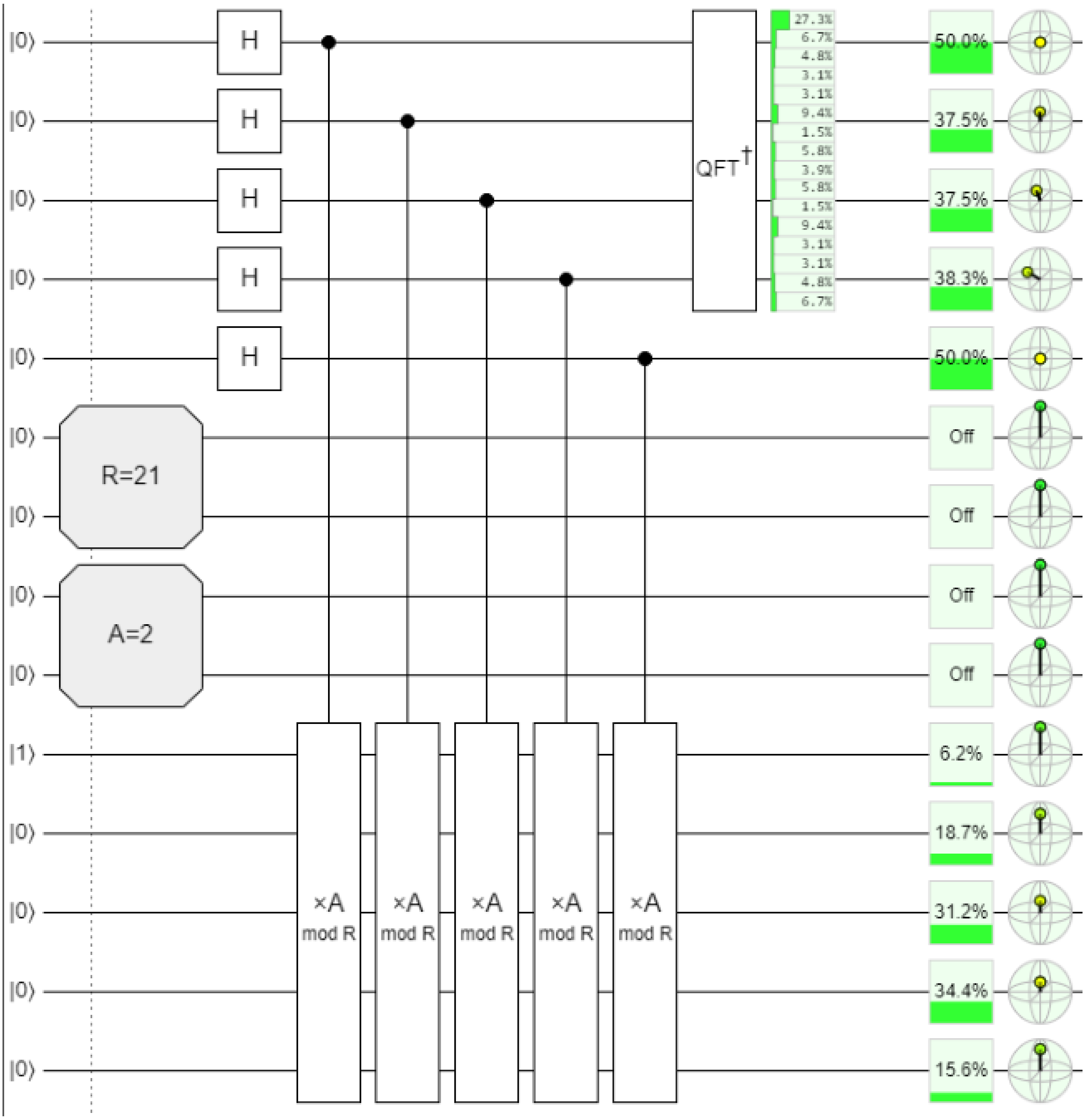
4

Postupujeme dle skript. Pro 15 volíme $n = 4$ a pro 21 $n = 5$, v obou případěch $m = n$ (značí řád, který jistě $\leq n$). Obvod pro 21 se liší od 15 pouze počtem použitých drátů. Jako a je v obou případech zvoleno $a = 2$.

Obvod pro 15:


|0⟩
|0⟩
|0⟩
|0⟩
|0⟩
|0⟩
|0⟩
|0⟩
|1⟩
|0⟩
|0⟩
|0⟩
H
H
H
H
R=15
A=2
×A
mod R
×A
mod R
×A
mod R
×A
mod R
QFT†
28.1%
7.4%
5.3%
3.4%
3.1%
9.1%
0.9%
5.1%
3.1%
5.1%
0.9%
9.1%
3.1%
3.4%
5.3%
7.4%
50.0%
37.5%
37.5%
37.5%
Off
Off
Off
Off
12.5%
25.0%
37.5%
25.0%

Obvod pro 21:



5

Chceme N t.ž. $\phi(N) = 2^i, i \in \mathbb{N}$, protože $\phi(N) = |\mathbb{Z}_N^*|$. Předpokládáme, že N je složené, liché a bezčtvercové. Tedy $N = p_1 p_2 \dots p_n, p_i \neq p_j$ pro $j \neq i$, zároveň z vlastností eulerovy funkce plyne, že $\phi(N) = \phi(p_1)\phi(p_2)\dots\phi(p_n) = (p_1-1)(p_2-1)\dots(p_n-1) = 2^i$ neboli pro každé p_i musí existovat $e_i \in \mathbb{N}$ t. ž. $p_i = 2^{e_i} + 1$.

Hledáme tedy čísla, která jsou o jedno větší než nějaká mocnina 2 a jsou prvočísla. Nalezl jsem: 3, 5, 17, 257. Dále je můžeme kombinovat díky vlastnostem uvedeným výše, máme tedy například čísla: $17 \cdot 3 = \underline{51}$, $17 \cdot 5 = \underline{85}, 17 \cdot 5 \cdot 3 = \underline{255}$, $257 \cdot 3 = \underline{771}$, $257 \cdot 5 = \underline{1285}$.

Vzhledem k otázce „Kolik takových čísel existuje?“ odpověď neznám. Prvočísla, která mají tvar $2^i + 1$, se nazývají Fermatova prvočísla a dle Wikipedie je jich známo pouze

5. Čísla co hledáme jsou právě všechny možné násobky těchto prvočísel, problémy tedy přímo souvisí, ale odpověď se asi neznámá v tuto chvíli.

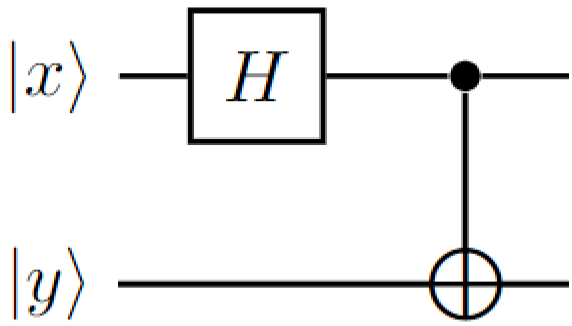
6

Dle přechozího cvičení víme, že $N = p_1 p_2 \dots p_n, p_i \neq p_j$ pro $j \neq i$, kde $\forall p_i \exists e_i \in \mathbb{N} : p_i = 2^{e_i} + 1$. Zřejmě máme omezení na možná $e_i < \lfloor \log_2(N) \rfloor$. Algoritmus tedy vyzkouší všechny možné exponenty $e \in \mathbb{N} : e < \lfloor \log_2(N) \rfloor$ jejichž počet je omezen $\log(N)$, pro každý exponent spočítej $x \coloneqq \gcd(N, 2^e + 1)$, pokud $x = 1$ inkrementuj e, pokud $x \neq 1$, tak máme faktor N, který je $2^e + 1$.

Nechť $n = \log(N)$ (počet cifer N). Složitost je $n \cdot n^2$, kde n je výše zmíněný počet kandidátů na e a n^2 je složitost výpočtu GCD. Výsledná složitost je tedy n^3.

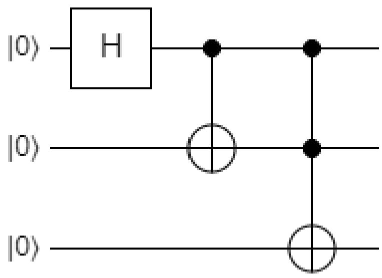
7

Ze skript víme, jak udělat obvod, který „proplete“ 2 qubity. Obvod vypadá následovně:



Pokud $x = 0, y = 0$, tak dostaneme stav $\frac{|00\rangle + |11\rangle}{\sqrt{(2)}}$, který je propletený. Rozšířením obvodu o jeden CCNOT dostaneme stav $\frac{|000\rangle + |111\rangle}{\sqrt{2}}$, který si ukážeme, že je propletený.

Obvod tedy vypadá:



Výpočet správnosti:

$$|0\rangle \otimes |0\rangle \otimes |0\rangle \overset{H \otimes id \otimes id}{=} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle \otimes |0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}} \otimes |0\rangle \overset{CNOT \otimes id}{=} \frac{|00\rangle + |11\rangle}{\sqrt{2}} \otimes |0\rangle =$$
$$\frac{|000\rangle + |110\rangle}{\sqrt{2}} \overset{CCNOT}{=} \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

Dokážeme, že je to propletený stav. Ukážeme, že nelze napsat jako tenzorový součin vektorů z prostorů $\mathbb{H}_2$. BÚNO můžeme ignorovat $\frac{1}{\sqrt{2}}$ (normalizační faktor):

$$a, b, c, d, e, f, g \in \mathbb{C}, (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \otimes (e|0\rangle + f|1\rangle) = ace|000\rangle + acf|001\rangle + ade|010\rangle + adf|011\rangle + bce|100\rangle + bcf|101\rangle + bde|110\rangle + bdf|111\rangle$$

Abychom získali vektor $|000\rangle + |111\rangle$ musí platit: $ace \neq 0 \implies a \neq 0, c \neq 0, e \neq 0 \wedge bdf \neq 0 \implies b \neq 0, d \neq 0, f \neq 0$. Potřebujeme ale nulové koeficienty u ostatních bázových vektorů což je spor, jelikož již předpokládáme, že všechny koeficienty jsou nenulové. Stav je tedy propletený.

8

Postupujeme dle vzorce ze skript pro matici $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Nechť $|\phi\rangle = \begin{pmatrix} 2-i \\ i \end{pmatrix} \implies |\phi\rangle' := \frac{|\phi\rangle}{\||\phi\rangle\|} = \frac{1}{\sqrt{6}} \begin{pmatrix} 2-i \\ i \end{pmatrix}$.

$$E(X) = \langle\phi|' X |\phi\rangle' = \frac{1}{6}(2i + i^2 - 2i + i^2) = \frac{-1}{3}$$

9

Dle vzorce ze skript chceme spočítat $\langle\phi| P_1 |\phi\rangle$. Ze zadání víme, jak bude vypadat P_1. Potřebujeme nejprve z daných vektorů udělat ON bázi, která je

$$b_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, b_2 = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix} \implies P_1 = |b_1\rangle\langle b_1| + |b_2\rangle\langle b_2| \implies$$

$$P_1 = \begin{pmatrix} \frac{3}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{-1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{-1}{4} \\ \frac{1}{4} & \frac{-1}{4} & \frac{-1}{4} & \frac{3}{4} \end{pmatrix}$$

Dále potřebujeme spočítat zadaný vektor jako prvek $\mathbb{H}_4$. To spočítáme pomocí vlastností tenzorového součinu:

$$\begin{pmatrix} 1+i \\ i \end{pmatrix} \otimes \begin{pmatrix} 1-i \\ 2i \end{pmatrix} = ((1+i)|0\rangle + i|1\rangle) \otimes ((1-i)|0\rangle + 2i|1\rangle) =$$

$$(1+i)(1-i)|00\rangle + 2i(1+i)|01\rangle + i(1-i)|10\rangle + 2i^2|11\rangle =$$

$$2|00\rangle + (2i-2)|01\rangle + (1+i)|10\rangle - 2|11\rangle = \begin{pmatrix} 2 \\ -2+2i \\ 1+i \\ -2 \end{pmatrix} \xrightarrow{\text{znormování}} |\phi\rangle := \frac{1}{3\sqrt{2}} \begin{pmatrix} 2 \\ -2+2i \\ 1+i \\ -2 \end{pmatrix}$$

Výsledná pravděpodobnost se tedy spočítá:

$$\frac{1}{36} \begin{pmatrix} 2 & -2-2i & 1-i & -2 \end{pmatrix} \begin{pmatrix} \frac{3}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{-1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{-1}{4} \\ \frac{1}{4} & \frac{-1}{4} & \frac{-1}{4} & \frac{3}{4} \end{pmatrix} \begin{pmatrix} 2 \\ -2+2i \\ 1+i \\ -2 \end{pmatrix} = \frac{1}{4} \tag{1}$$