Základy kvantového počítání, Deutschův algoritmus

Martin Štefaňák

12. května 2021

Přehled

Kvantový bit — Qubit

- Kvantový systém, který má dva bazické stavy $|0\rangle$, $|1\rangle$

$$\mathscr{H} = [|0\rangle, |1\rangle]_\lambda \simeq \mathbb{C}^2$$

- Obecný stav qubitu — superpozice

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

- Ve stavu superpozice není hodnota qubitu určená
- Musíme provést měření ve výpočetní bázi $\{|0\rangle, |1\rangle\}$

$$|\psi\rangle = a|0\rangle + b|1\rangle \implies \begin{cases} W_{|\psi\rangle\to|0\rangle} = |\langle 0|\psi\rangle|^2 = |a|^2 \\ W_{|\psi\rangle\to|1\rangle} = |\langle 1|\psi\rangle|^2 = |b|^2 \end{cases}$$

- Po měření musíme změnit popis stavu podle odpovídajícího výsledku

Kvantový registr

- Soubor n qubitů — výpočetní báze má 2^n stavů

$$\mathscr{H} = [|i_1 \dots i_n\rangle | i_k = 0 \vee 1]_\lambda \simeq \mathbb{C}^{2^n} = \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2$$

- Obecný stav registru — superpozice

$$|\psi\rangle = \sum_{k=1}^{n} \sum_{i_k=0}^{1} a_{i_1 \dots i_n} |i_1 \dots i_n\rangle$$

- $a_{i_1 \dots i_n}$ je amplituda pr. naměření hodnoty registru $i_1 \dots i_n$

$$W_{|\psi\rangle \to |i_1 \dots i_n\rangle} = |\langle i_1 \dots i_n | \psi \rangle|^2 = |a_{i_1 \dots i_n}|^2$$

Počet parametrů nutných k popisu stavu registru roste exponenciálně

Využít řízený vývoj kvantového systému pro výpočet

Výpočet na kvantovém počítači

- Registr v počátečním stavu $|0 \ldots 0\rangle$
- Aplikujeme kvantové brány — unitární operátory $\hat{U}$
- Unitární — nemění se velikost vektoru
- V principu vystačíme s 1- a 2-qubitovými bránami
- Počáteční stav registru se změní do superpozice
- Nakonec provedeme měření ve výpočetní bázi
- Ze superpozice se náhodně vybere jedna z možností — výsledek

Využít princip superpozice a interference amplitud pravděpodobnosti tak, že správný výsledek najdeme s velkou pravděpodobností rychleji, než na klasickém počítači

- Unitární operace lze invertovat ($\hat{U}^{-1} = \hat{U}^{\dagger}$) — kvantový výpočet je reverzibilní
- Běžné operace (AND atd.) na klasickém počítači reverzibilní nejsou
- Výpočet na klasickém počítači lze efektivně udělat reverzibilní
- Kvantové počítače jsou alespoň tak silné jako klasické

1-qubitové kvantové brány

X-brána

- Prohodí hodnotu qubitu

$$\hat{X}|0\rangle = |1\rangle,\ \hat{X}|1\rangle = |0\rangle$$

- Maticový zápis

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

- Unitární a hermitovská transformace

$$\hat{X} = \hat{X}^\dagger = \hat{X}^{-1},\ \hat{X}^2 = \hat{I}$$

Z-brána

- Změní fázi u $|1\rangle$ o π

$$\hat{Z}|0\rangle = |0\rangle,\ \hat{Z}|1\rangle = -|1\rangle$$

- Maticový zápis

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- Unitární a hermitovská transformace

$$\hat{Z} = \hat{Z}^\dagger = \hat{Z}^{-1},\ \hat{Z}^2 = \hat{I}$$

Hadamardova transformace

- Z vektorů standardní báze vytvoří rovnoměrnou superpozici

$$\hat{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad \hat{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- Maticový zápis

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- Unitární a hermitovská transformace

$$\hat{H} = \hat{H}^\dagger = \hat{H}^{-1}, \ \hat{H}^2 = \hat{I}$$

2-qubitové brány

CNOT (CX)

- Prohodí hodnotu 2. qubitu, pokud první má hodnotu 1

$$\hat{CX}|00\rangle = |00\rangle, \quad \hat{CX}|01\rangle = |01\rangle, \quad \hat{CX}|10\rangle = |11\rangle, \quad \hat{CX}|11\rangle = |10\rangle$$

- Maticový zápis

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

- Unitární a hermitovská transformace

$$\hat{CX} = \hat{CX}^{\dagger} = \hat{CX}^{-1}, \ \hat{CX}^2 = \hat{I}$$

- Kontrolní qubit ve stavu superpozice — CX vytvoří provázaný stav

$$\hat{CX}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle$$

Přehled

Deutschův algoritmus

Oracle

- Neznámá funkce $f : \{0,1\} \to \{0,1\}$ — 4 možnosti

$$f_a(0) = 0,\ f_a(1) = 0, \qquad f_b(0) = 1,\ f_b(1) = 1$$
$$f_c(0) = 0,\ f_c(1) = 1, \qquad f_d(0) = 1,\ f_d(1) = 0$$

- f_a a f_b jsou konstantní, f_c a f_d jsou vyvážené

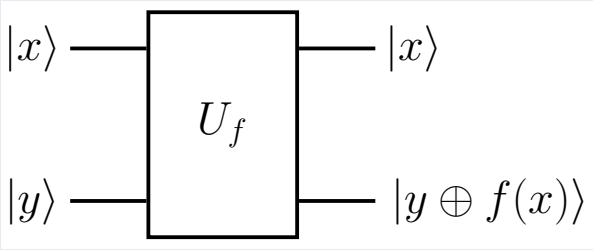
Je oracle f konstantní, nebo vyvážená funkce?

- Klasicky musíme použít oracle 2x
- Na kvantovém počítači stačí jedna iterace oracle

Oracle jako kvantová brána

- Unitární operátor — potřebujeme 2 qubity

Schéma kvantového oracle



- Obdoba brány CNOT — první qubit je kontrolní
- Hodnota druhého qubitu se změní z y na $y \oplus f(x)$
- $\oplus$ je sčítání modulo 2

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0$$

Hilbertův prostor dvou qubitů

- 2 qubity — $\mathscr{H} = \mathbb{C}^4$
- Výpočetní báze — standardní báze $\mathbb{C}^4$

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

- Oracle je popsán nějakou permutační maticí — je unitární

Konstantní oracle

$$y \longrightarrow y \oplus f(x)$$

Oracle f_a

$$f_a(x) = 0, \quad x = 0, 1$$

$$U_{f_a}|xy\rangle = |xy\rangle$$

$$U_{f_a} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = I \otimes I$$

Oracle f_b

$$f_b(x) = 1, \quad x = 0, 1$$

$$U_{f_b}|xy\rangle = |x\overline{y}\rangle$$

$$U_{f_b} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = I \otimes X$$

Vyvážené oracle

$$y \longrightarrow y \oplus f(x)$$

Oracle f_c

$$f_c(x) = x, \quad x = 0, 1$$

$$U_{f_c}|0y\rangle = |0y\rangle$$

$$U_{f_c}|1y\rangle = |1\overline{y}\rangle$$

$$U_{f_c} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = CX$$

Oracle f_d

$$f_d(x) = \overline{x}, \quad x = 0, 1$$

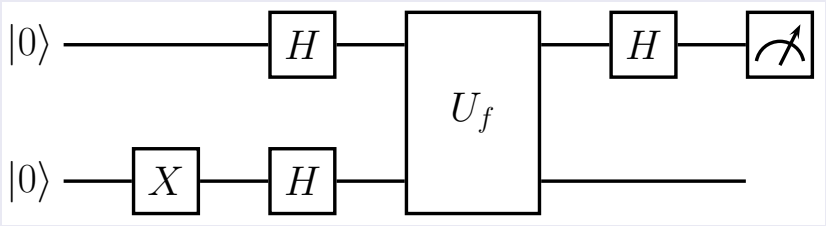
$$U_{f_d}|0y\rangle = |0\overline{y}\rangle$$

$$U_{f_d}|1y\rangle = |1y\rangle$$

$$U_{f_d} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = (X \otimes I)CX(X \otimes I)$$

Deutschův algoritmus

Schéma Deutschova algoritmu



Měření hodnoty 1. qubitu

- 1. qubit má hodnotu 0 $\iff$ f je konstantní
- 1. qubit má hodnotu 1 $\iff$ f je vyvážená

Jednotlivé kroky Deutschova algoritmu

1. Aplikujeme X-bránu na 2. qubit

$$|\psi_1\rangle = |0\rangle \otimes (X|0\rangle) = |01\rangle$$

2. Aplikujeme Hadamardovu bránu na oba qubity

$$\begin{aligned} |\psi_2\rangle &= (H|0\rangle) \otimes (H|1\rangle) = \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) \\ &= \frac{1}{2}\big(\,|0\rangle \otimes (|0\rangle - |1\rangle) + |1\rangle \otimes (|0\rangle - |1\rangle)\,\big) \end{aligned}$$

Jednotlivé kroky Deutschova algoritmu

3. Aplikujeme oracle

$$
\begin{aligned}
|\psi_3\rangle &= U_f|\psi_2\rangle = \frac{1}{2}U_f\big(|0\rangle\otimes(|0\rangle-|1\rangle)+|1\rangle\otimes(|0\rangle-|1\rangle)\big)\\
&= \frac{1}{2}\big(|0\rangle\otimes(|0\oplus f(0)\rangle-|1\oplus f(0)\rangle)+|1\rangle\otimes(|0\oplus f(1)\rangle-|1\oplus f(1)\rangle)\big)\\
&= \frac{1}{2}\big(|0\rangle\otimes(|f(0)\rangle-|1\oplus f(0)\rangle)+|1\rangle\otimes(|f(1)\rangle-|1\oplus f(1)\rangle)\big)
\end{aligned}
$$

Stav registru pro konstantní oracle

$$\frac{1}{2}\big(|0\rangle \otimes (|f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle \otimes (|f(1)\rangle - |1 \oplus f(1)\rangle)\big)$$

$f_a(x) = 0, \quad x = 0, 1$

$$|\psi_{3a}\rangle = \frac{1}{2}\big(|0\rangle \otimes (|0\rangle - |1\rangle) + |1\rangle \otimes (|0\rangle - |1\rangle)\big) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$f_b(x) = 1, \quad x = 0, 1$

$$|\psi_{3b}\rangle = \frac{1}{2}\big(|0\rangle \otimes (|1\rangle - |0\rangle) + |1\rangle \otimes (|1\rangle - |0\rangle)\big) = -\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- Qubity jsou ve faktorizovaném stavu, stejném pro f_a i f_b až na globální fázi
- V prvním qubitu relativní fáze mezi $|0\rangle$ a $|1\rangle$ je nulová

Stav registru pro vyvážené oracle

$$\frac{1}{2}\big(|0\rangle \otimes (|f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle \otimes (|f(1)\rangle - |1 \oplus f(1)\rangle)\big)$$

$f_c(x) = x, \quad x = 0, 1$

$$|\psi_{3c}\rangle = \frac{1}{2}\big(|0\rangle \otimes (|0\rangle - |1\rangle) + |1\rangle \otimes (|1\rangle - |0\rangle)\big) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$f_d(x) = \overline{x}, \quad x = 0, 1$

$$|\psi_{3d}\rangle = \frac{1}{2}\big(|0\rangle \otimes (|1\rangle - |0\rangle) + |1\rangle \otimes (|0\rangle - |1\rangle)\big) = -\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- Qubity jsou ve faktorizovaném stavu, stejném pro f_c i f_d až na globální fázi
- Stav druhého qubitu je stejný jako pro konstantní oracle
- V prvním qubitu relativní fáze mezi $|0\rangle$ a $|1\rangle$ je rovna π

Stav registru po aplikaci oraclu

- Pro všechny případy oracle lze zapsat stav registru ve tvaru

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

- 2. qubit nás dále nezajímá
- Stav 1. qubitu bez irelevantní globální fáze

$$|\psi'_3\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{f(1)-f(0)}|1\rangle\right)$$

f je konstantní

$$f(1) - f(0) = 0$$

$$|\psi'_{3ab}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

f je vyvážená

$$f(1) - f(0) = \pm 1$$

$$|\psi'_{3cd}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Stavy jsou ortogonální, nějakou unitární transformací je můžeme převést na $|0\rangle$ a $|1\rangle$

Poslední krok algoritmu

4. Na 1. qubit aplikujeme Hadamardovu bránu

$$
\begin{aligned}
|\psi_4\rangle &= H|\psi_3'\rangle = \frac{1}{\sqrt{2}} H \left(|0\rangle + (-1)^{f(1)-f(0)} |1\rangle \right) \\
&= \frac{1}{2} \left((|0\rangle + |1\rangle) + (-1)^{f(1)-f(0)} (|0\rangle - |1\rangle) \right) \\
&= \frac{1}{2} \left(1 + (-1)^{f(1)-f(0)} \right) |0\rangle + \frac{1}{2} \left(1 - (-1)^{f(1)-f(0)} \right) |1\rangle
\end{aligned}
$$

Stav 1. qubitu na konci algoritmu

$$|\psi_4\rangle = \frac{1}{2}\left(1 + (-1)^{f(1)-f(0)}\right)|0\rangle + \frac{1}{2}\left(1 - (-1)^{f(1)-f(0)}\right)|1\rangle$$

f je konstantní

- Amplitudy u $|0\rangle$ mají stejnou fázi - konstruktivní interference
- Amplitudy u $|1\rangle$ mají opačnou fázi - destruktivní interference

$$|\psi_4\rangle = |0\rangle$$

- S jistotou naměříme hodnotu qubitu 0

f je vyvážená

- Amplitudy u $|0\rangle$ mají opačnou fázi - destruktivní interference
- Amplitudy u $|1\rangle$ mají stejnou fázi - konstruktivní interference

$$|\psi_4\rangle = |1\rangle$$

- S jistotou naměříme hodnotu qubitu 1

Přehled

Deutschův - Jozsův algoritmus

- Rozšíření Deutschova algoritmu na $f : \{0,1\}^n \to \{0,1\}$
- Předem víme, že f je buď konstantní, nebo vyvážená
- Vyvážená — 0 na polovinu vstupů

Je oracle f konstantní, nebo vyvážená funkce?

- Klasicky musíme použít oracle $2^{n-1}+1$ pro jednoznačnou odpověď
- Na kvantovém počítači stačí jedna iterace oracle

- Exponenciální urychlení oproti klasickému deterministickému algoritmu
- Klasický pravděpodobnostní algoritmus také dokáže problém vyřešit v počtu iterací oracle nezávislém na n (ale závislém na toleranci chyby)

Kvantový oracle

- Kvantová brána na $n+1$ qubitech
- Prvních n qubitů je kontrolních
- Poslední qubit se změní z y na $y \oplus f(x)$

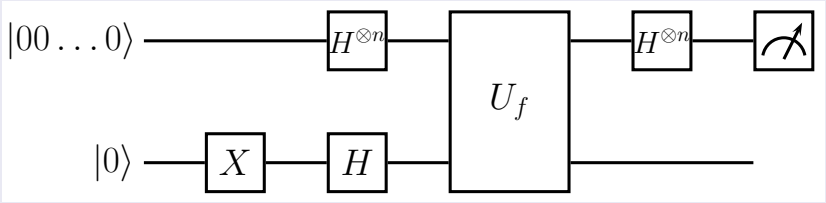
$$U_f|x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus f(x)\rangle, \quad x \in \{0, 1, \ldots 2^n - 1\}, \quad y \in \{0, 1\}$$

- Zjednodušení zápisu

$$x \equiv x_{n-1} \ldots x_1 x_0, \quad x = x_{n-1} 2^{n-1} + \ldots + x_1 2^1 + x_0 2^0$$

Deutschův - Jozsův algoritmus

Schéma Deutschova - Jozsova algoritmu



Měření hodnoty prvních *n* qubitů

- Všechny mají hodnotu 0 $\iff$ *f* je konstantní
- Alespoň jeden má hodnotu 1 $\iff$ *f* je vyvážená

Jednotlivé kroky Deutschova - Jozsova algoritmu

1. Aplikujeme X-bránu na poslední qubit

$$|\psi_1\rangle = |0\ldots0\rangle \otimes (X|0\rangle) = |0\ldots0\rangle \otimes |1\rangle$$

2. Aplikujeme Hadamardovu bránu na všechny qubity

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{\sqrt{2}} \underbrace{(|0\rangle + |1\rangle) \otimes \ldots \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)}_{n\times} \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\ &= \frac{1}{\sqrt{2^n}} \left(\sum_{x=0}^{2^n-1} |x\rangle \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \end{aligned}$$

Jednotlivé kroky Deutschova - Jozsova algoritmu

3. Aplikujeme oracle

$$
\begin{aligned}
|\psi_3\rangle &= U_f\left[\frac{1}{\sqrt{2^n}}\left(\sum_{x=0}^{2^n-1}|x\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)\right] = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\otimes\frac{1}{\sqrt{2}}\left(|f(x)\rangle-|1\oplus f(x)\rangle\right)\\
&= \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\otimes\frac{1}{\sqrt{2}}(-1)^{f(x)}\left(|0\rangle-|1\rangle\right)\\
&= \left(\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)
\end{aligned}
$$

- Stav prvních n qubitů

$$
|\psi_3'\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle
$$

Na každý qubit aplikujeme Hadamardovu bránu

- Působení Hadamardovy brány na bazické stavy qubitu

$$H|a\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^a|1\rangle\right), \quad a \in \{0,1\}$$

- Působení n Hadamardových bran na bazické stavy n qubitů

$$\begin{aligned} H^{\otimes n}|x\rangle &= H|x_{n-1}\rangle \otimes \ldots \otimes H|x_0\rangle \\ &= \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_{n-1}}|1\rangle\right) \otimes \ldots \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_0}|1\rangle\right) \\ &= \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x\cdot y}|y\rangle, \quad x \cdot y = \sum_{i=0}^{n-1} x_i y_i \end{aligned}$$

Stav registru na konci algoritmu

4. Aplikujeme Hadamardovu bránu na všechny qubity

$$
\begin{aligned}
|\psi_4\rangle &= H^{\otimes n}\left(\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle\right) \\
&= \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\left(\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}|y\rangle\right) \\
&= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\left(\sum_{x=0}^{2^n-1}(-1)^{f(x)+x\cdot y}\right)|y\rangle
\end{aligned}
$$

- Amplituda pravděpodobnosti naměření hodnoty registru y

$$\langle y|\psi_4\rangle = \frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)+x\cdot y}$$

Měření registru

- Pravděpodobnost naměření hodnoty 0 na všech qubitech

$$W_0 = |\langle 0|\psi_4\rangle|^2 = \frac{1}{2^{2n}} \left| \sum_{x=0}^{2^n-1} (-1)^{f(x)} \right|^2$$

f je konstantní

- Amplitudy mají stejnou fázi
- Konstruktivní interference

$$W_0 = 1$$

- Všechny qubity mají hodnotu 0

f je vyvážená

- Polovina amplitud je $+1$, polovina -1
- Destruktivní interference

$$W_0 = 0$$

- Alespoň jeden qubit má hodnotu 1