Deutsch-Jozsa algorithm

A short intro into dirty tricks of quantum computing

Adolf Středa

Quantum Lambda; March 20, 2019

Promises you would write in a project description

- Can solve every[1] problem, like, really fast.
- Breaks all[2] the asymmetric cryptography.
- Quantum computers will be more efficient[3] and faster[4].

[1]Very specific problems I want money for.
[2]Mostly ones starting with "Let p, q be primes."
[3]Except staggering amount of ancilla bits.
[4]Yeah, sure...

Trick No. 1 – Linearity

- Complex vector space with inner product (Hilbert space)
- Inner product: $\langle u|v\rangle$ braket ($\langle u|$ bra, $|v\rangle$ ket)

Definition – inner product

Let $u, v, w \in \mathbb{C}^n$ and $\lambda \in \mathbb{C}$ then $\langle|\rangle$ is called inner product iff

- $\langle u + v|w\rangle = \langle u|w\rangle + \langle v|w\rangle$
- $\langle w|u + v\rangle = \langle w|u\rangle + \langle w|v\rangle$
- $\langle \lambda u|v\rangle = \lambda^* \langle u|v\rangle$
- $\langle u|\lambda v\rangle = \lambda \langle u|v\rangle$

Inner product also defines a norm $||u|| = \sqrt{\langle u|u\rangle}$

Trick No. 1 – Linearity

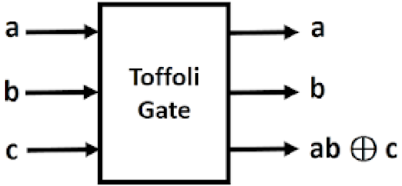
- Qubit = element of $\mathbb{C}^2$ of a norm 1
- Every operator A is unitary (linear, $A^* = A^{-1}$, preserves norm)

Examples

Qubit $e^{i\gamma}(\alpha|0\rangle + \beta|1\rangle)$, $\alpha^2 + \beta^2 = 1$
$|0\rangle = e_0$ and $|1\rangle = e_1$ canonical basis of $\mathbb{C}^2$

Trick No. 2 – Toffoli gate

Can provide reversible variant for every Boolean function.



Bigger system

To create bigger systems, we will need to use tensor product $\otimes$.

- $|a\rangle \otimes |b\rangle = |a\rangle\,|b\rangle = |ab\rangle$
- $\frac{|1\rangle + |0\rangle}{\sqrt{2}} \otimes \frac{|1\rangle + |0\rangle}{\sqrt{2}} = \frac{|1\rangle\,|1\rangle + |0\rangle\,|1\rangle + |1\rangle\,|0\rangle + |0\rangle\,|0\rangle}{2}$
- $\begin{bmatrix} \mathbf{a} & b \\ c & d \end{bmatrix} \otimes X = \begin{bmatrix} \mathbf{a}X & bX \\ cX & dX \end{bmatrix}$

Trick No. 3 – Hadamard gate

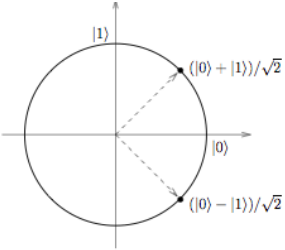
$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H \left|0\right\rangle = \frac{\left|0\right\rangle + \left|1\right\rangle}{\sqrt{2}} =: \left|+\right\rangle$$

$$H \left|1\right\rangle = \frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}} =: \left|-\right\rangle$$

Trick No. 3 – Hadamard gate

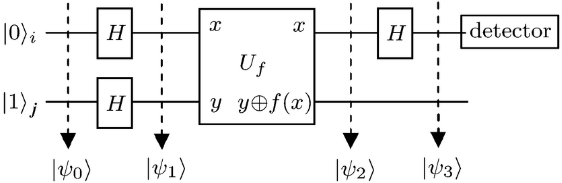
- Rotates the canonical basis.
- $H|0\rangle$ sum of elements from the canonical basis
- Works similarly in higher dimensions.
- Used to obtain LK of all possible states.



Warning

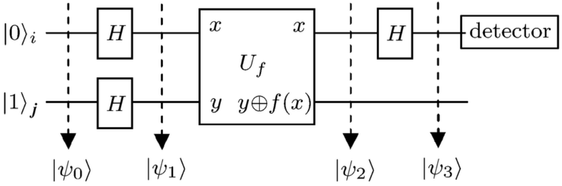
Following slides may contain algebra and other explicit content.

Deutsch Algorithm



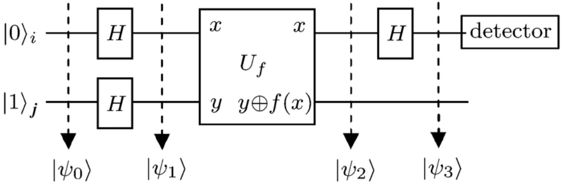
- Question: Given $f : \mathbb{F}_2 \to \mathbb{F}_2$, decide whether f is constant or balanced.
- Non-quantum solution: run it twice
- Quantum solution: run once only
- We will want to (ab)use Hadamard gate together with linearity

Deutsch Algorithm



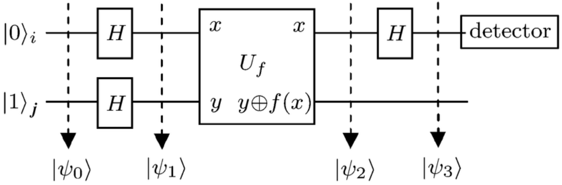
- $|\psi_0\rangle = |01\rangle$
- $|\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{2}(|00\rangle + |10\rangle - |01\rangle - |11\rangle)$
- Now observe that U_f is linear, i.e. we may apply it on each $|ab\rangle$ separately.

Deutsch Algorithm



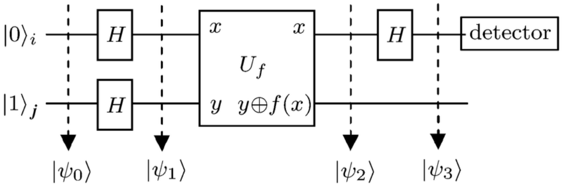
- Application of U_f changes the "second coordinate" only.
- $U_f(\frac{1}{2}\,|00\rangle) = \frac{1}{2}\,|0\rangle\,|0 + f(0)\rangle$
- $|\psi_1\rangle = \frac{1}{2}(\,|00\rangle + |10\rangle - |01\rangle - |11\rangle)$
- $|\psi_2\rangle = \frac{1}{2}(\,|0\rangle\,|0 \oplus f(0)\rangle + |1\rangle\,|0 \oplus f(1)\rangle -$
  $- \,|0\rangle\,|1 \oplus f(0)\rangle - |1\rangle\,|1 \oplus f(1)\rangle)$

Deutsch Algorithm



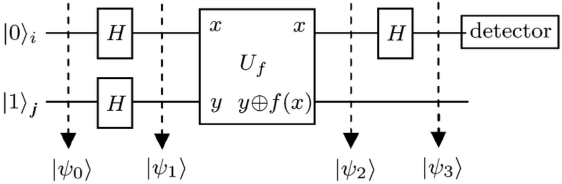
- $|\psi_2\rangle = \frac{1}{2}(|0\rangle|0 \oplus f(0)\rangle + |1\rangle|0 \oplus f(1)\rangle -$
  $- |0\rangle|1 \oplus f(0)\rangle - |1\rangle|1 \oplus f(1)\rangle)$
- $|\psi_2\rangle = \frac{1}{2}((-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle) + (-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle))$
- Forget second qubit: $\frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)$

Deutsch Algorithm



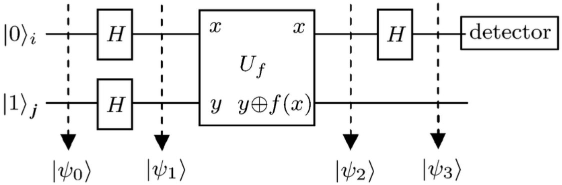
- Forget second qubit: $\frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)$
- f balanced, i.e. $f(0) \neq f(1)$: one of minus vanishes
  - $|\psi_2\rangle = \pm |-\rangle |.\rangle$
- f constant, i.e. $f(0) = f(1)$: both minuses either stay or both vanish
  - $|\psi_2\rangle = \pm |+\rangle |.\rangle$

Deutsch Algorithm



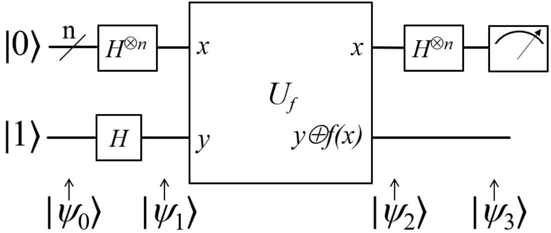
- f balanced, i.e. $f(0) \neq f(1)$: $|\psi_2\rangle = \pm |-\rangle |.\rangle$
- That is, after the application of H, we measure $|1\rangle$
- f constant, i.e. $f(0) = f(1)$: $|\psi_2\rangle = \pm |+\rangle |.\rangle$
- That is, after the application of H, we measure $|0\rangle$

Trick No. 4 – aggregation



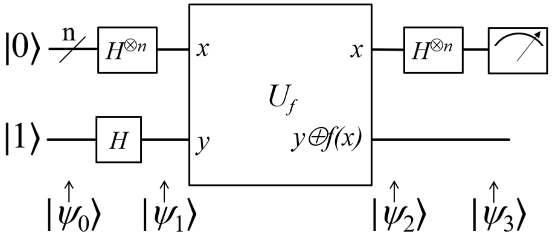
- While we were not able access specific outputs of f, we were able to aggregate them.
- This is a "standard" procedure – we want to lump together desirable results (i.e. add their probabilities heightening the probability that we will measure them).
- What if we had more dimensions?

Deutsch-Jozsa Algorithm



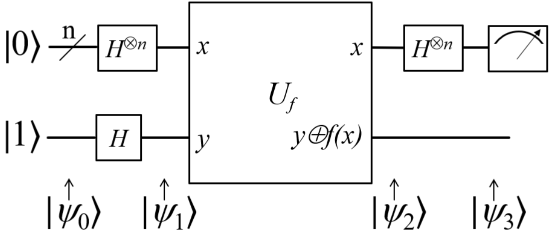
- What's the difference? It's the same, isn't it?

Deutsch-Jozsa Algorithm



- What's the difference? It's the same, isn't it?
- Oh right, you have got the picture in a better resolution.

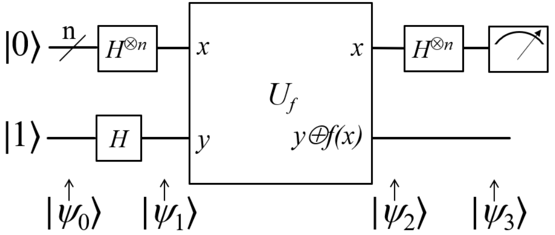
Deutsch-Jozsa Algorithm



- What's the difference? It's the same, isn't it?
- Oh right, you have got the picture in a better resolution.
- Exactly[5]!

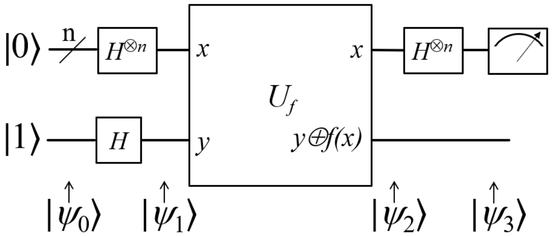
[5] Only causing worse headache. Consult a doctor if it persists for more than 2 days.

Deutsch-Jozsa Algorithm



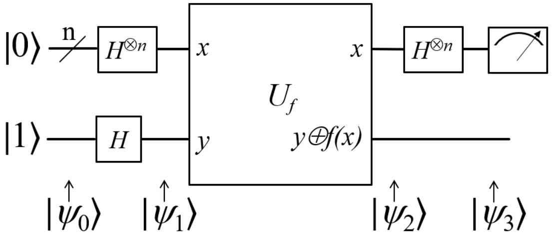
- $|\psi_0\rangle = |0\dots01\rangle$
- Hadamard trick: $|\psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x\rangle\left(|0\rangle - |1\rangle\right)$
- $|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x\rangle\left(|f(x)\rangle - |1\oplus f(x)\rangle\right)$

Deutsch-Jozsa Algorithm



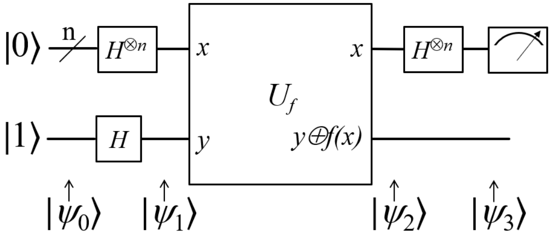
- $|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle \left(|f(x)\rangle - |1 \oplus f(x)\rangle \right)$
- Again, restructure the second qubit
  $|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \left(|0\rangle - |1\rangle \right)$

Deutsch-Jozsa Algorithm



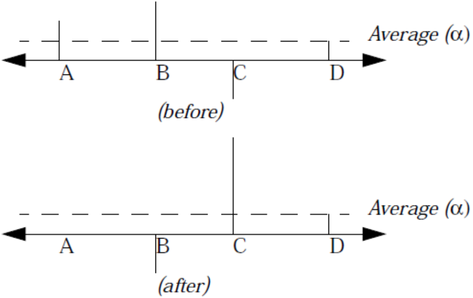
- $|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \left(|0\rangle - |1\rangle \right)$
- Let's ignore the last qubit and apply Hadamard transformation:
  $\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \sum_{y=0}^{2^n-1} (-1)^{x.y} |y\rangle$

Deutsch-Jozsa Algorithm



- $\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \sum_{y=0}^{2^n-1} (-1)^{x.y} \, |y\rangle$
- Probability of measuring $|0\rangle$: $|\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)}|^2$
  - f balanced $\Rightarrow 0$
  - f constant $\Rightarrow 1$

Grover's algorithm

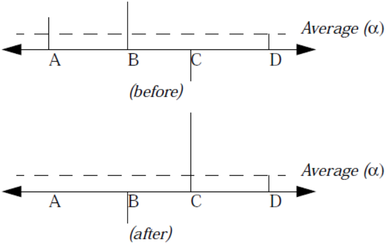


- Database lookup ($O(\sqrt{n})$)
- Usable also for pre-image search (hash functions, block ciphers)
- "Invert" the target ($|x\rangle \mapsto -|x\rangle$), inversion about average, rinse and repeat.

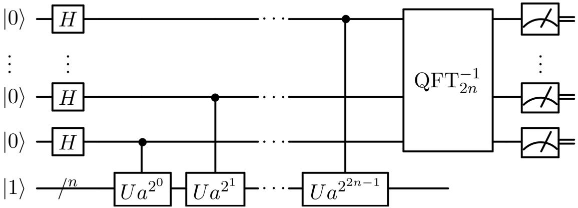
Grover's algorithm – 4-item example

Let the third item be our target.

- $\frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2}$
- $\frac{1}{2},\ \frac{1}{2},\ -\frac{1}{2},\ \frac{1}{2}$ (Oracle step)
- Average is $\frac{1}{4}$
  $0,\ 0,\ \frac{1}{2}+\frac{1}{4}+\frac{1}{4}=1,\ 0$
- $|3\rangle$ will be measured with probability 1



Shor's algorithm



- Factorization
- Main idea – calculate "a^k mod N" for many k at once; elements of the same order will lump together
- Quantum Fourier Transform hidden inside

Q&A

and an obligatory cliche picture.