VERSENY! – NOVEMBER 20., 14:00-16:00, IE007

A versenyen négyféle feladattal találkoznak a részvevők:

- Esszé kérdés: a témakörhöz kapcsolódó algoritmusról/protokollról, műszaki megoldásról kell áttekintést/értelmezést adni.
- Totó: feleletválasztós kérdéssorozat a témakörből, mely az általános tájékozottságot teszteli beleértve szakmai és tudománytörténeti kérdéseket is.
- Számítási feladat: kvantumregiszterek és logikai kapuk működésének elemzése.
- Tervezési feladat: adott specifikációnak megfelelő kvantum algoritmus/protokoll/berendezés blokkvázlatának megtervezése, a működés leírása.
- https://vik.hk/verseny/kvantuminformatika-es-kommunikacio/

- **Kvantumhálózatok nyomában – A kommunikáció jövője a BME-n**
- Időpont: november 26., 14:00-15:30
- Helyszín: BME I épület, IB028 (1117 Budapest, Magyar Tudósok ktr. 2.)
- Neves szakemberek járják körül a kvantumhálózatok megvalósítását és a kapcsolódó szabályozói kihívásokat, s bepillantást kaphatunk nemzetközi kvantumkommunikációs hálózatépítési projektekbe és az adiabatikus kvantumszámítógépek helyzetébe.

DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES

Kvantumos algoritmus tervezése, Deutsch-Jozsa algoritmus

Kvantuminformatikai alkalmazások

Dr. Imre Sándor , Dr. Bacsárdi László

BME Hálózati Rendszerek és Szolgáltatások Tanszék

imre@hit.bme.hu

MŰEGYETEM 1782

Hol is tartunk?

A KVANTUMMECHANIKA POSZTULÁTUMAI

- 1. Posztulátum: kvantumbit
  - Hilbert-tér
- 2. Posztulátum: logikai kapuk
  - Unitér transzformáció
  - Elemi kvantum logikai kapuk
- 3. Posztulátum: Q/C átalakítás
  - Mérési statisztika
  - Mérés utáni állapot
- 4. Posztulátum: regiszterek
  - Tenzor szorzás

$$|\varphi\rangle = \sum_{i=0}^{2^n-1} \varphi_i |i\rangle$$

$$U^\dagger \equiv U^{-1}$$

$$P(m \mid |\varphi\rangle) = \langle\varphi|M_m^\dagger M_m|\varphi\rangle$$

$$|\varphi'\rangle = \frac{M_m|\varphi\rangle}{\sqrt{\langle\varphi|M_m^\dagger M_m|\varphi\rangle}}$$

$$|\varphi\rangle = |0\rangle \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

KÖVETKEZMÉNYEK

- Kvantuminterferométer működése
- No clonig tétel
- Tetszőleges kvantumállapot létrehozása
- Szupersűrű tömörítés
- Teleportálás
- Kvantumos kulcsszétosztás

DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES

Kvantumos algoritmus tervezése, Deutsch-Jozsa algoritmus

Kvantuminformatikai alkalmazások

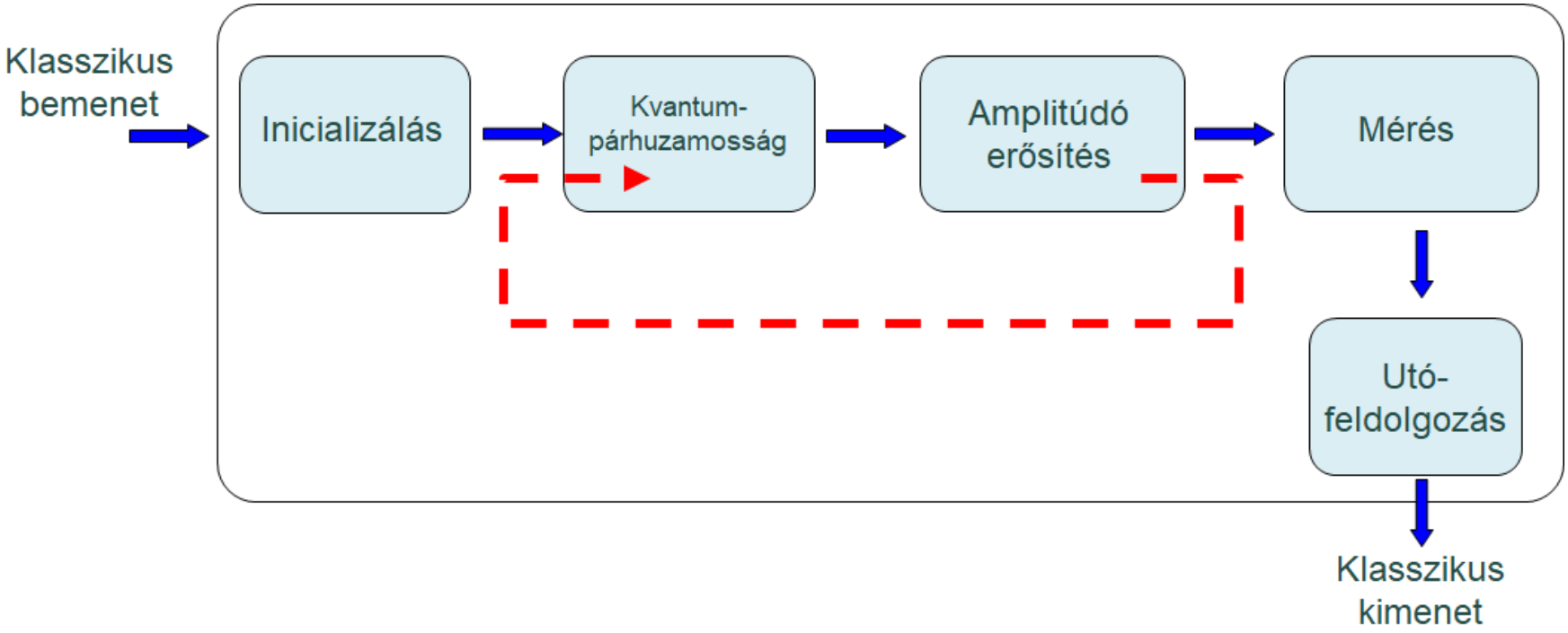
Dr. Imre Sándor , Dr. Bacsárdi László

BME Hálózati Rendszerek és Szolgáltatások Tanszék

imre@hit.bme.hu

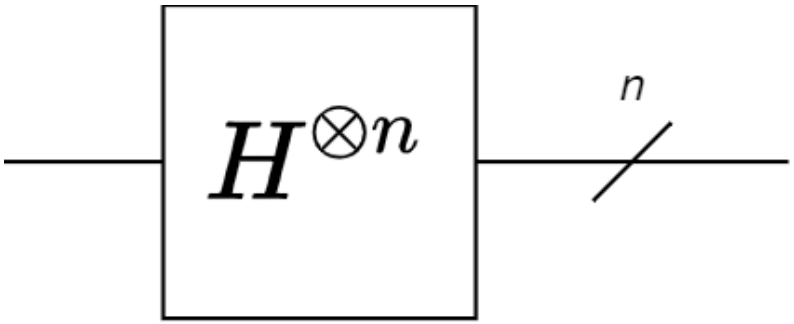
MŰEGYETEM 1782

KVANTUMALGORITMUSOK TERVEZÉSI RECEPTJE

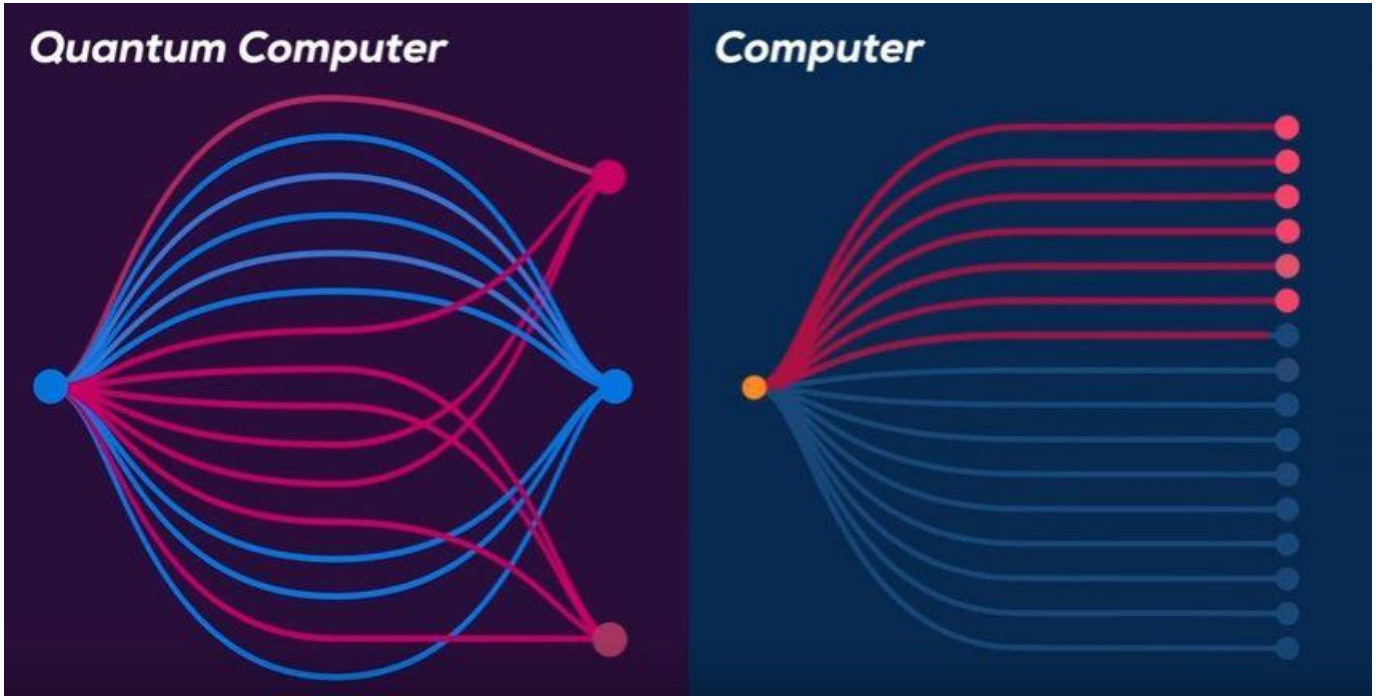


INICIALIZÁLÁS

- Hadamard-kapu segítségével az összes lehetséges bemeneti bázisállapotot (egész számot 0 és *N*-1 között) egyetlen **egyenletes** szuperpozícióba tesszük.
- Így egyforma esélye lesz mindegyiknekmegnyerni a “versenyt”.



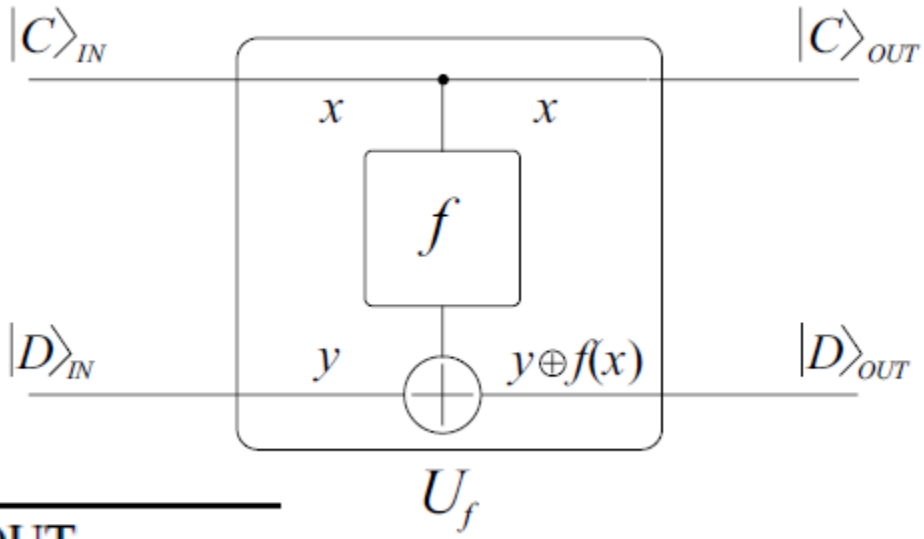
Kvantumpárhuzamosság



steemit

KVANTUMOS PÁRHUZAMOSSÁG – A CNOT KAPU

$$U_f : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$$



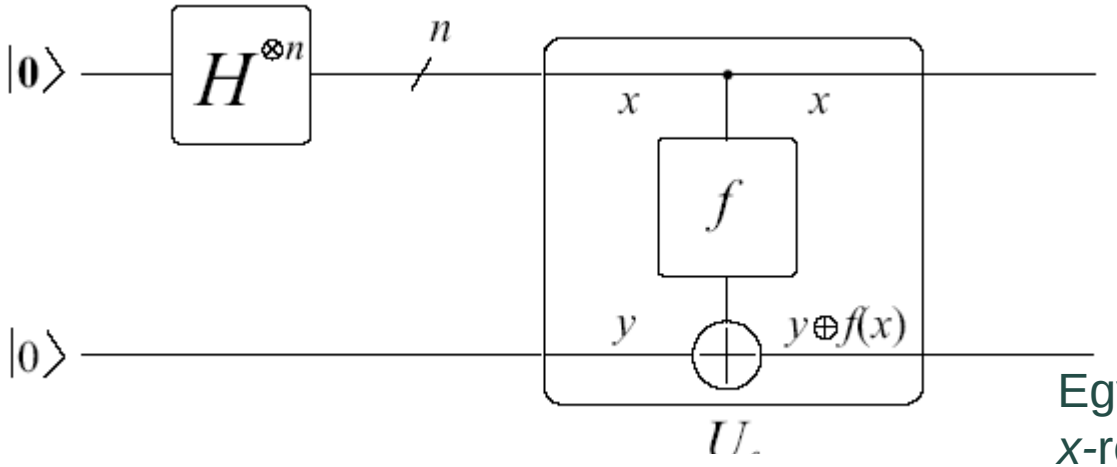
IN		OUT	
x	y	x	$y \oplus f(x)$
0	0	0	$0 \oplus f(0) = f(0)$
0	1	0	$1 \oplus f(0)$
1	0	1	$0 \oplus f(1) = f(1)$
1	1	1	$1 \oplus f(1)$

$$U_f \frac{|00\rangle + |10\rangle}{\sqrt{2}} = \frac{|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle}{\sqrt{2}}$$

KVANTUMOS PÁRHUZAMOSSÁG

Egy lépesben kiszámoltuk valamennyi *x*-re!

$$U_f : |x\rangle_N |y\rangle \rightarrow |x\rangle_N |y \oplus f(x)\rangle$$



Egy lépésben minden *x*-re!

$$U_f \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|0 \oplus f(x)\rangle$$

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

AMLITÚDÓ ERŐSÍTÉS

- Úgy módosítja a szuperpozíciót, hogy a megjelölt/kért egész szám/bázisvektor 1 vagy ahhoz közeli valószínűségi amplitúdót kapjon.
- Ez garantálja, hogy a mérés nagy valószínűséggel adja vissza a vágyott egész számot.
- Az amplitúdóerősítés a legtöbb esetben egyetlen lépésben elérhető a Hadamard-transzformáció vagy a kvantum-Fourier-transzformáció segítségével. De iteratív is lehet (azaz több lépést igényelhet).
- Nincs egyértelmű recept az amplitúdóerősítésre. Csak példákat tudunk mutatni. Ez a lépés komoly kreativitást és intuíciót igényel.

MÉRÉS

- Már tárgyaltuk a kvantummechanika posztulátumai között.
- A gondosan beállított mérési operátorok garantálják a helyes mérési eredményt.

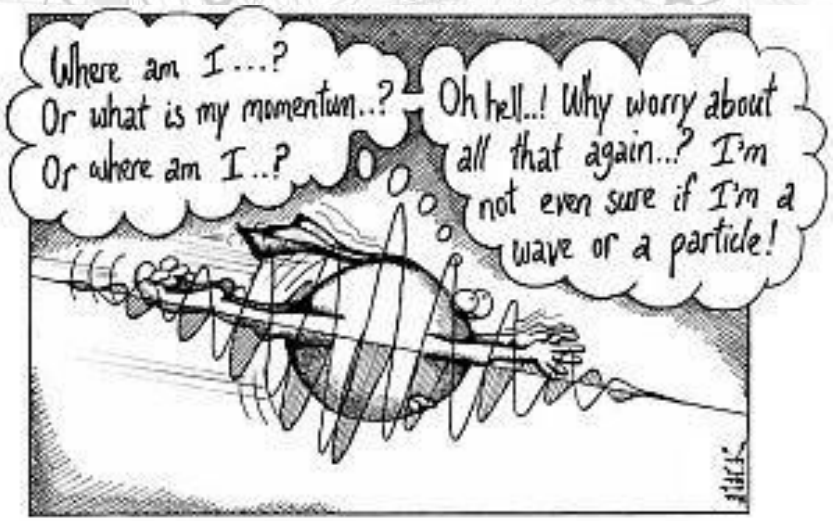
$$P(m \mid |\varphi\rangle) = \langle\varphi|M_m^\dagger M_m|\varphi\rangle$$

$$|\varphi'\rangle = \frac{M_m|\varphi\rangle}{\sqrt{\langle\varphi|M_m^\dagger M_m|\varphi\rangle}}$$

KLASSZIKUS UTÓFELDOLGOZÁS

- Az utófeldolgozás során a mérési eredményt a kezdeti probléma megoldásává alakítjuk.
- A legtöbb esetben az utófeldolgozás egyszerűen a mért érték közléséből áll.
- Azonban néha összetett matematikai levezetésekre van szükség.

DEPARTMENT
NETWORKED
AND SERVICES



Photon self-identity problems.

A Deutsch-Józsa algoritmus

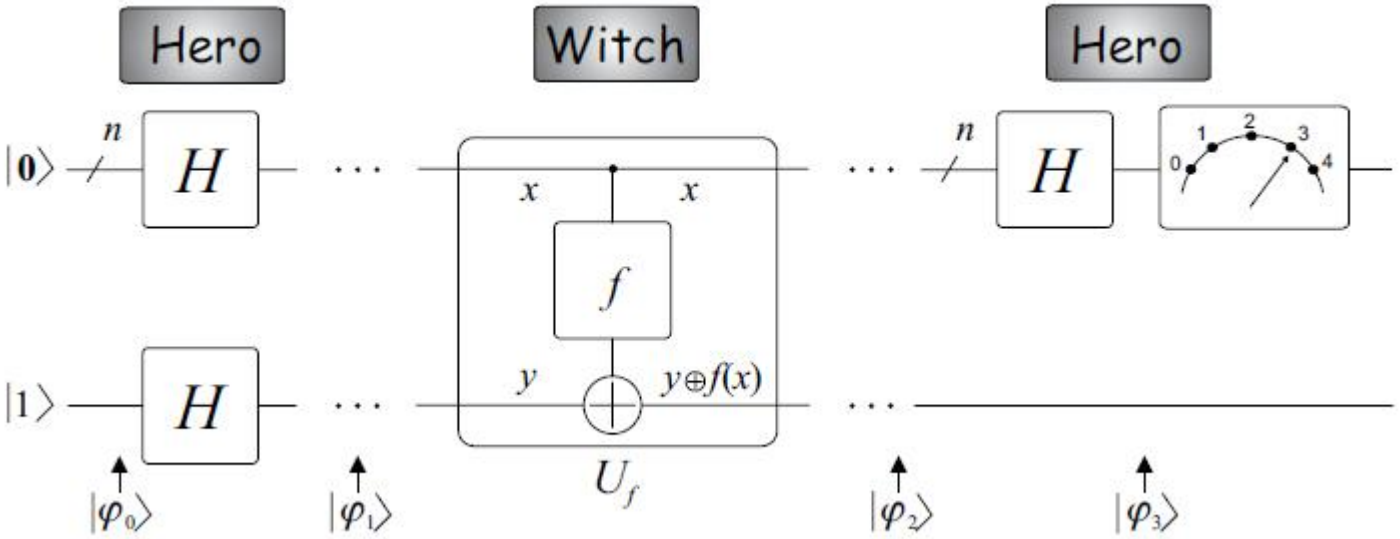
MŰEGYETEM 1782

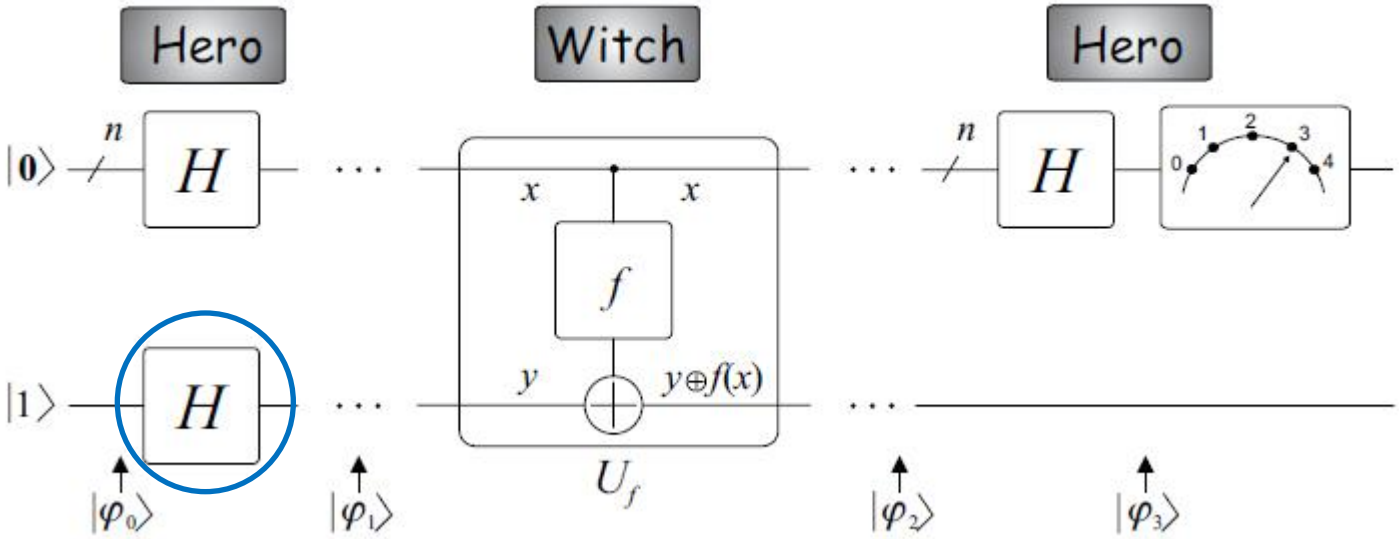
A DEUTSCH-JÓZSA ALGORITMUS

- Konstans vagy kiegyenlített?
- A legjobb klasszikus megoldás?

$$x \in \{0,1\}^n$$

$$f(x) : \{0,1\}^n \rightarrow \{0,1\}^1$$

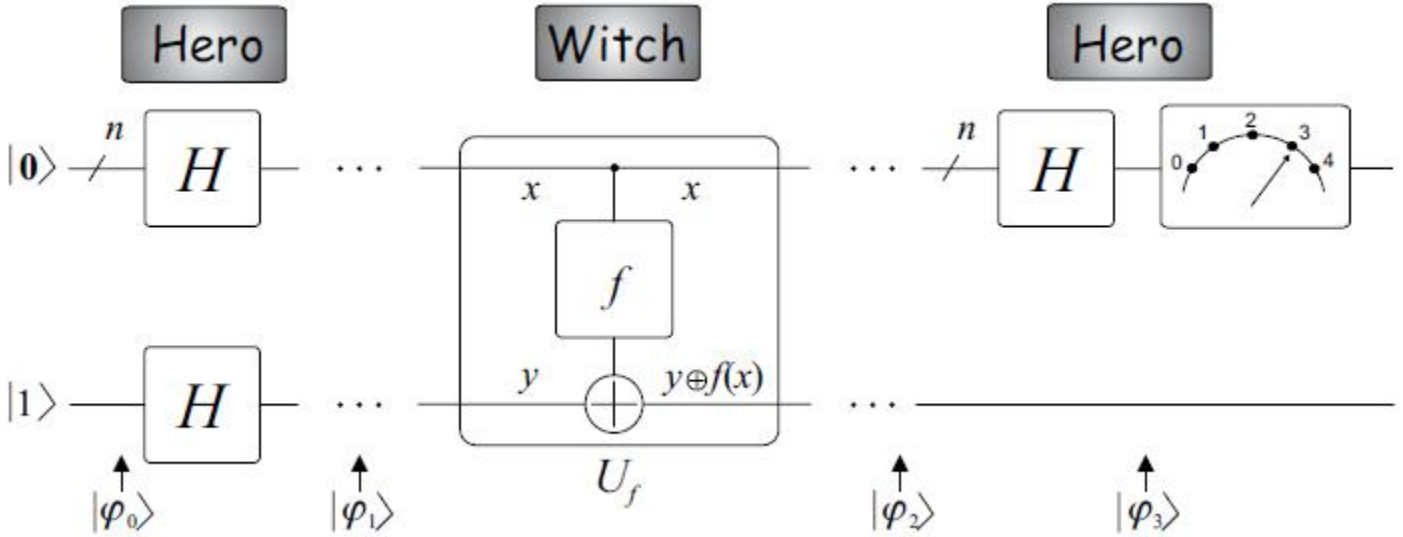




$$|\varphi_0\rangle = |0\rangle_N|1\rangle$$

$$|\varphi_1\rangle = H^{\otimes(n+1)}|\varphi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

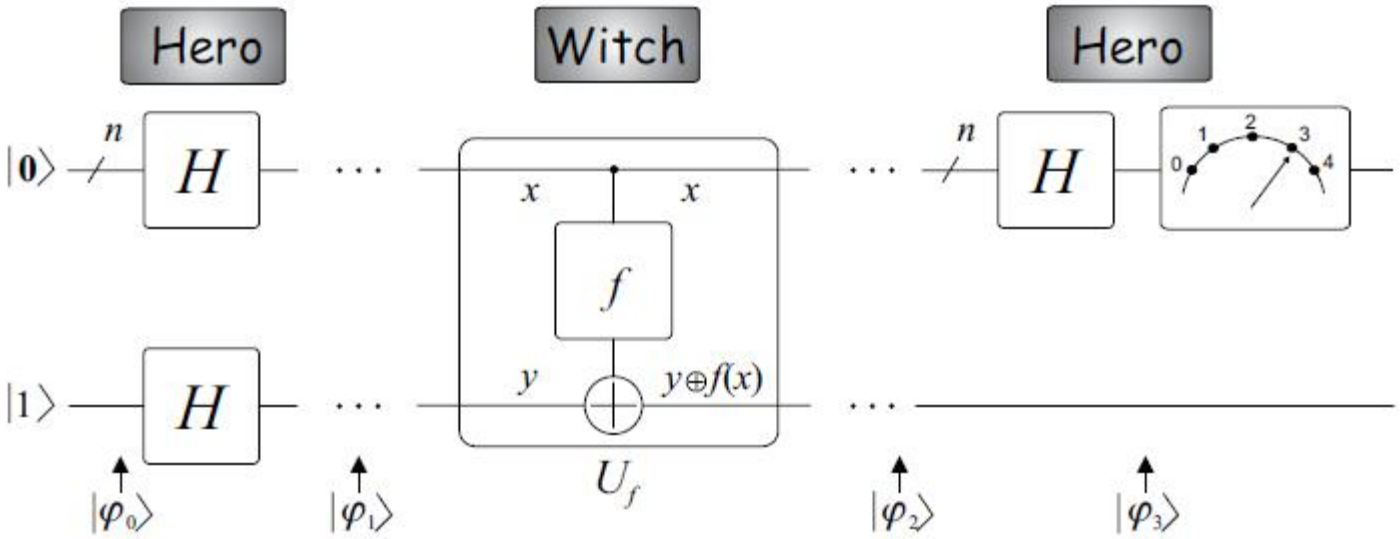
$$= \frac{1}{\sqrt{2^{(n+1)}}} \sum_{x\in\{0,1\}^n} |x\rangle|0\rangle - \frac{1}{\sqrt{2^{(n+1)}}} \sum_{x\in\{0,1\}^n} |x\rangle|1\rangle$$



- Az első tag (már ismert):

$$U_f \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|0 \oplus f(x)\rangle$$

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



- A második tag:

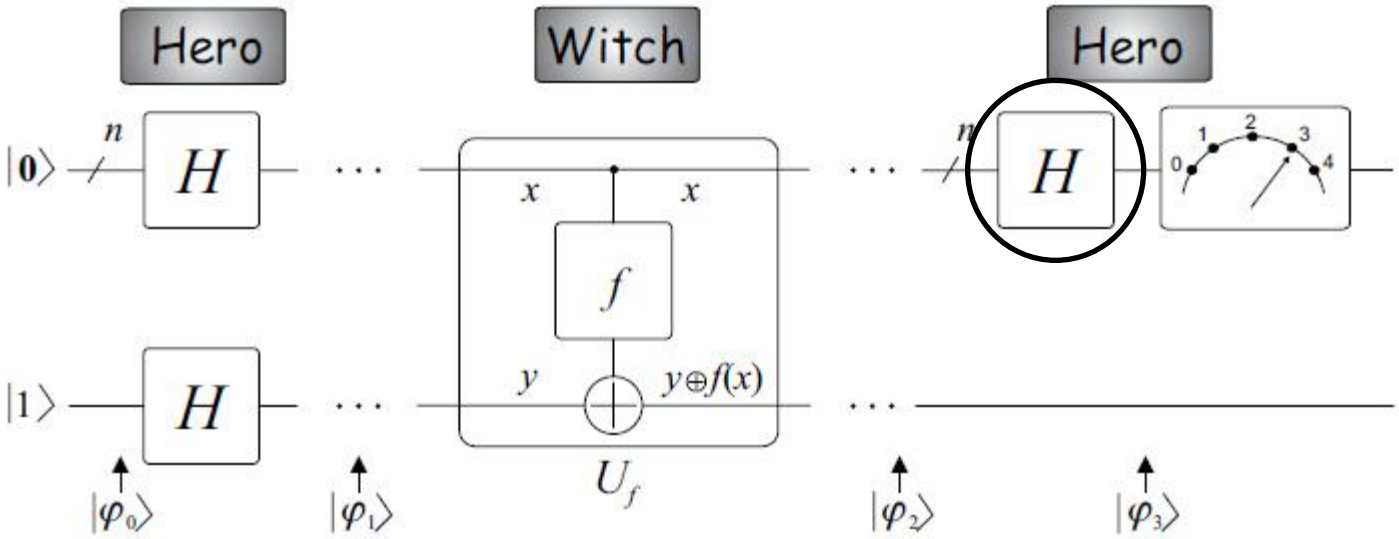
$$U_f \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|1 \oplus f(x)\rangle$$

$$|\varphi_2\rangle = U_f|\varphi_1\rangle = \frac{1}{\sqrt{2^{(n+1)}}} \sum_{x \in \{0,1\}^n} |x\rangle|f(x)\rangle - \frac{1}{\sqrt{2^{(n+1)}}} \sum_{x \in \{0,1\}^n} |x\rangle|1 \oplus f(x)\rangle$$

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

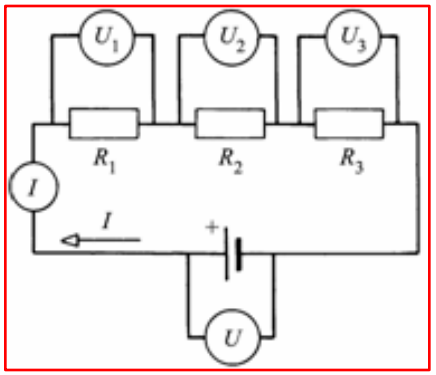
$$= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

HF



$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{xz}|z\rangle$$

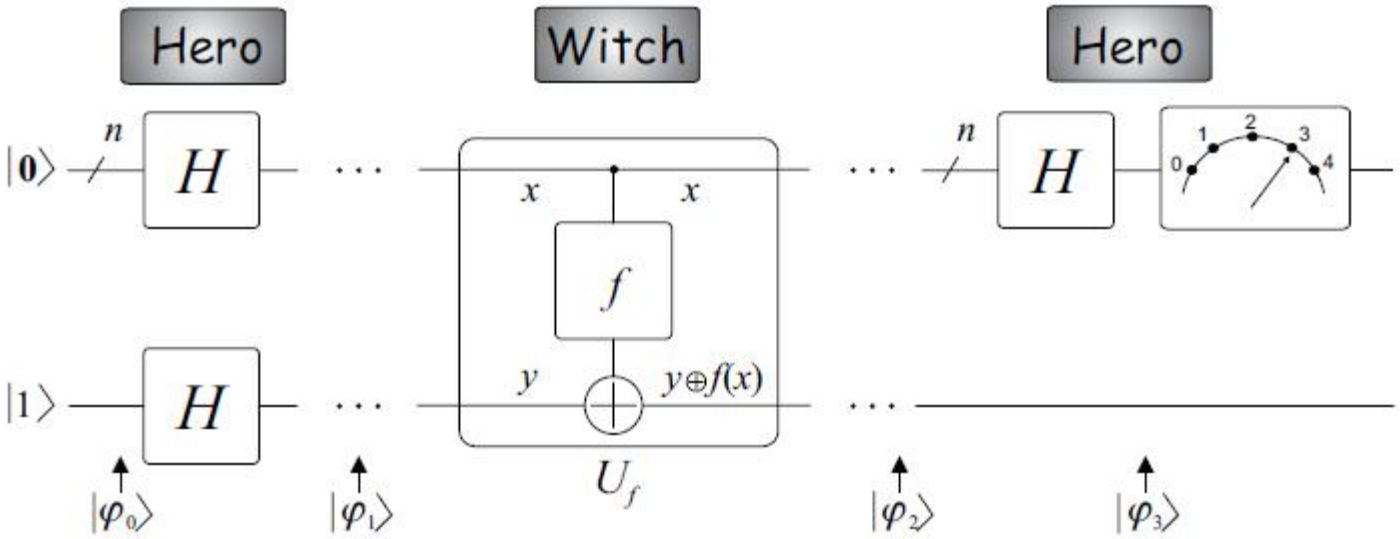
A szuperpozicós elvet alkalmazva



$$|\varphi_3\rangle = (H^{\otimes n} \otimes I)|\varphi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} H^{\otimes n}|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

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

$$= \sum_{x'\in\{0,1\}^n} \underbrace{\left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{xx'+f(x)} \right)}_{c_{x'}} |x'\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$



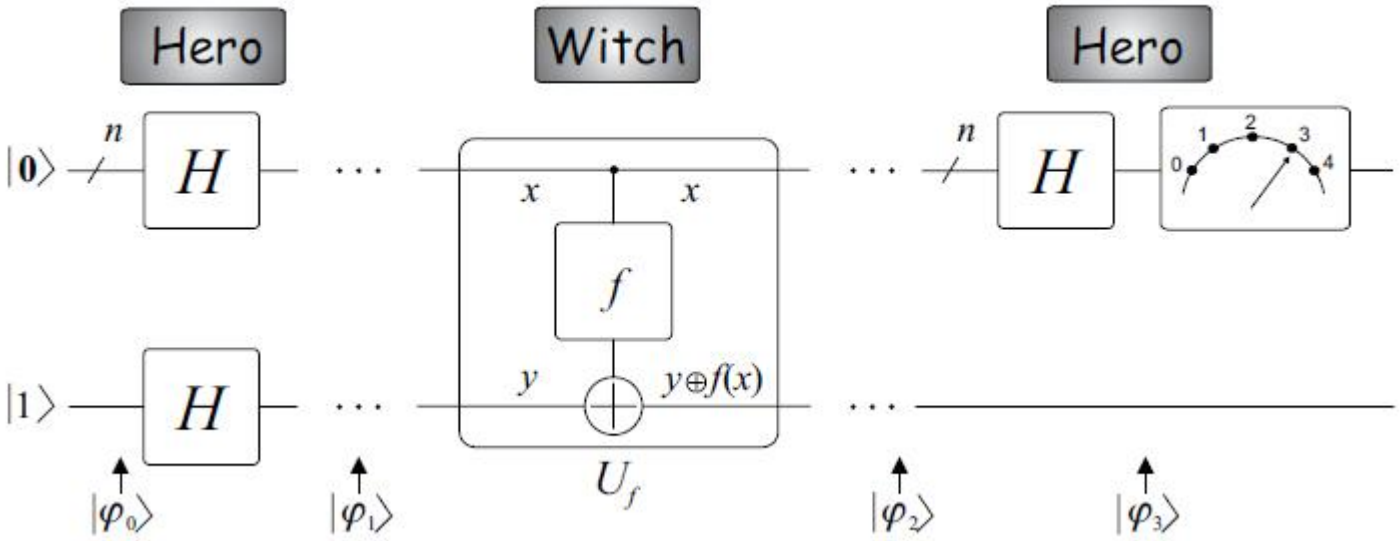
$$c_{\mathbf{0}} = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{xx'+f(x)} = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)}$$

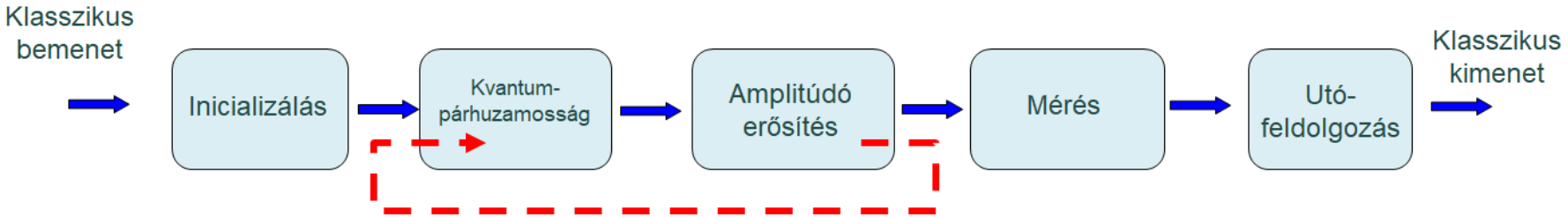
since $xx' = x\mathbf{0} \equiv 0$. Now let us investigate (5.10) when $f(x)$ is *constant*, then

$$c_{\mathbf{0}} = \begin{cases} -1 & \text{if } f(x) \equiv 1 \\ 1 & \text{if } f(x) \equiv 0. \end{cases}$$

Concerning the *balanced* scenario $c_{\mathbf{0}} = 0$ since we have the same number of positive (+1) and negative (-1) terms in the sum.

AZ ALGORITMUS TERVEZÉSI RECEPT

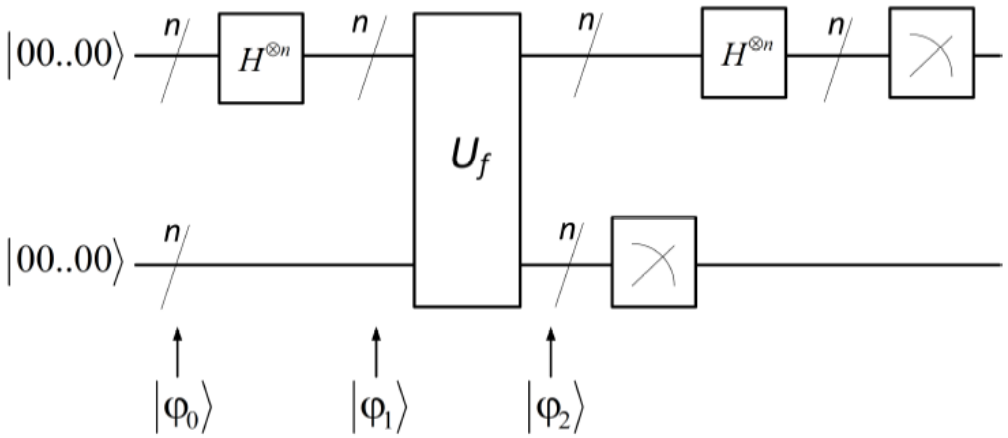




SIMON-ALGORITMUS

Let us modify the function f and the related question under discussion in the Deutsch–Jozsa problem in the following way: $f : \{0,1\}^n \to \{0,1\}^n$, i.e. Simon's algorithm deals with a binary vector valued function which is constrained by a special condition. f is periodical in terms of $f(x) = f(y)$ if and only if $x = y$ or $x = y \oplus r$, where $r \neq 0$ stands for the binary period of f. There are two obvious questions, namely how and in how many steps (evaluation of f) can r be computed. These questions can answered both classically and quantum computationally but with a major difference. A traditional computer requires an exponential number of queries while Simon's solution is able to find r after $O(n)$ iterations with high probability.

$$x \in \{0,1\}^n$$
$$f(x) : \{0,1\}^n \to \{0,1\}^n$$
$$f(x) = x \oplus s$$



The development of this course material has received funding from the European Union under grant agreement No 101081247 (QCIHungary project) and has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund.