Einfache Quantenalgorithmen

- Die wesentlichen Charakteristiken von Quantenalgorithmen sollen anhand einfacher Beispiele veranschaulicht werden.

Gliederung

- Einführung
- Algorithmus von Deutsch
- Deutsch-Jozsa-Algorithmus
  - Verschränkungsmaß
- Elitzur-Vaidman
- Zusammenfassung

Einführung

- Algorithmen von klassischer Logik auf Quantencomputer übertragbar
  (QC = Universelle Turingmaschine, physikalische Grundlage)
  Werkzeug: Toffoli-Gatter (Simulation von NAND möglich)

  ABER: kein Vorteil -> sinnlos.
- Also quantenmechanische Effekte ausnutzen.
- bereits bekannte Eigenschaften von Q.-Alg:
  - no copy-Theorem
    => keine Verzweigungen, Zusammenführungen
    => Alle benötigten Qubits sind bereits am Anfang des Alg. vorhanden und können auch nicht entfernt werden.
  - keine Schleifen

Algorithmus von Deutsch
- Quantenparallelismus -

Motivation:

- Nutze Superposition der Basiszustände $|0\rangle; |1\rangle$ um mehrere Zustände simultan mit einer Operation auszuwerten:

  Man betrachte dazu eine „teure“ Funktion f(x), exemplarisch: $f(x): \{0,1\} \rightarrow \{0,1\}$

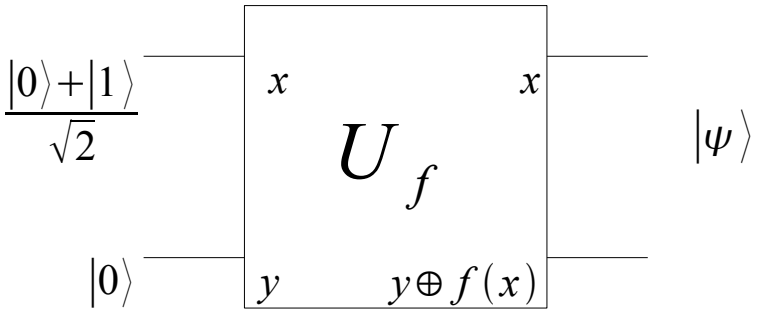
  (->einfacher Fall: 1bit Definitions- und Wertebereich)

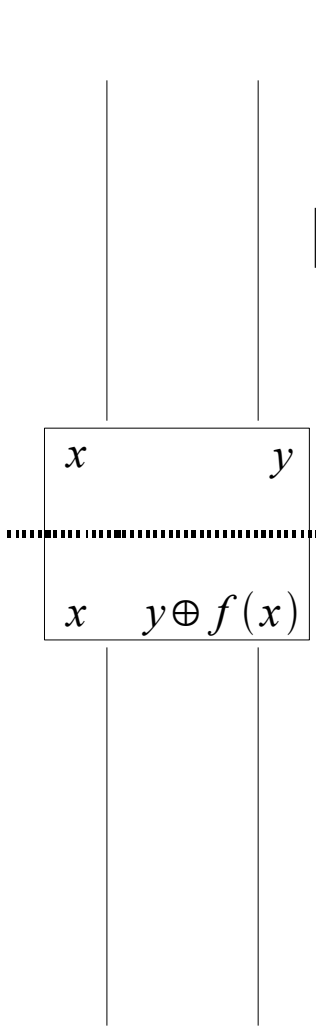
  Es gibt Gatterkombination zu:

  $$U_f: |Argument - Register\, x\,,\, Ziel - Register\, y\rangle \rightarrow |x\,,\, y \oplus f(x)\rangle$$

  Anwendung auf superpositionierten Zustand:

  $$|+\rangle := \frac{|00\rangle + |10\rangle}{\sqrt{2}} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} |0\rangle$$





$$|\psi_1\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}$$

$$|\psi_2\rangle = \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$$

Eingabe:

Ausgabe:

- beide Zustände simultan ausgewertet
- Sowohl f(0) als auch f(1) sind enthalten!

Problem:

- Bei Messung tritt Zustandsreduktion ein: Man misst zu je 50% einen der folgenden Zustände:

$$|0, f(0)\rangle \quad ; \quad |1, f(1)\rangle$$

- Mehrfachausführung nötig? Kompensation: Quantenparallelismus sinnlos?
- Nein: Es gibt Möglichkeiten dennoch Nutzen daraus zu ziehen: zB. Algorithmus von Deutsch

Algorithmus von Deutsch

Problemstellung:

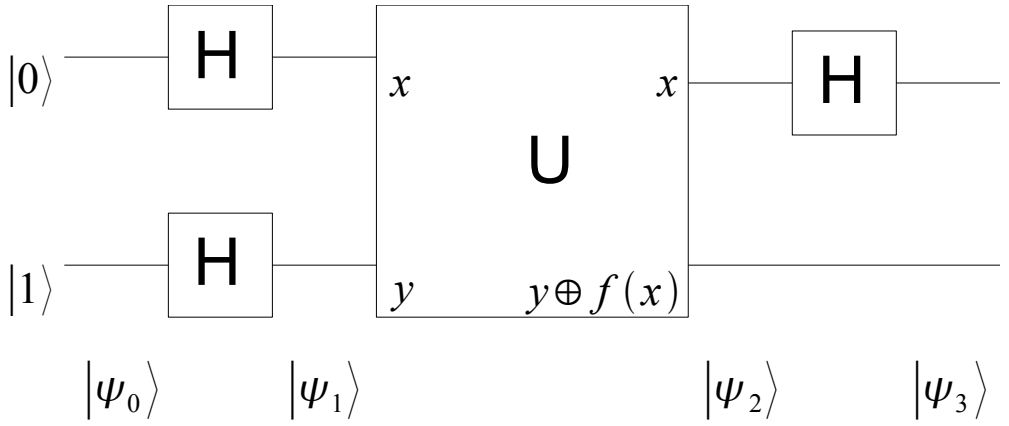
- bestimmen, ob Funktion f(x)=konstant: $f(x):\{0,1\}\rightarrow\{0,1\}$
- f(x) möglichst wenig ausführen (f ist teuer)

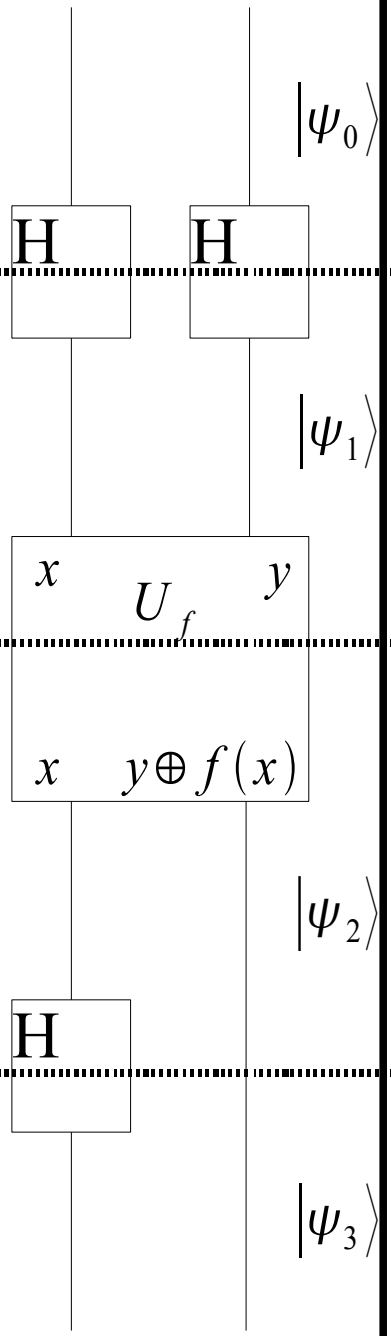
Algorithmus:

- 3 Zusätzliche Hadamard-Gatter:
  - Superposition im Argument-Zustand wird erzeugt:
  - Zielzustand wird auch superpositioniert:
  - Auswertung

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

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





$|\psi_0\rangle$

$|\psi_1\rangle$

$|\psi_2\rangle$

$|\psi_3\rangle$

$$|\psi_0\rangle = |0\rangle|1\rangle$$

$$|\psi_1\rangle = \left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

$$U_f|x\rangle\left[|0\rangle-|1\rangle\right]/\sqrt{2} = (-1)^{f(x)}|x\rangle\left[|0\rangle-|1\rangle\right]/\sqrt{2}$$

$$|\psi_2\rangle = \pm\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \quad ; f(0)=f(1)$$

$$|\psi_2'\rangle = \pm\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \quad ; f(0)\neq f(1)$$

$$|\psi_3\rangle = \pm|0\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \quad ; f(0)=f(1)$$

$$|\psi_3'\rangle = \pm|1\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \quad ; f(0)\neq f(1)$$

Eingabe:
klassische Basiszustände

Erzeugung der Superposition
durch Hadamard-Gatter

Falls f(x)=1, dann invertiert $\oplus f(x)$
$1\ XOR\ f(x)=0;\quad 0\ XOR\ f(x)=1$

Da $f(0)\neq f(1)$
wird nur das VZ eines Teilzustandes
gewechselt .

da H unitär, werden wieder die
reinen Argument-Zustände
erzeugt.

Ausgabe:
Messung des 1. Qubits
$\Rightarrow f(0)\oplus f(1)$

Algorithmus von Deutsch

Auswertung:

- Zeitvorteil:
  - f nur einmal ausgeführt, klassische 2x notwendig:
    Die verschiedenen Zustände existieren parallel, können miteinander in Wechselwirkung treten und am Ende z.B. durch Hadamard zusammengeführt werden („Interferenz“).
  - linear: f kann eventuell klassisch leichter evaluiert werden.
    =>Zeitvorteil aufgebraucht.
- Verallgemeinerung auf n Qubits möglich:
  - Deutsch-Jozsa: wirklicher Zeitvorteil

Deutsch – Jozsa – Algorithmus
- n Qubits -

Motivation:

- Verallgemeinerung des Algorithmuses von Deutsch auf n Qubits um eindeutigen Zeitvorteil gegenüber klassischen Umsetzungen zu erhalten.
- Für die Funktion $f(x):\{0,1\}_1,\ldots,\{0,1\}_n \rightarrow \{0,1\}$ gilt $f(x)=const$ oder $\sum_x f(x)=2^n/2$
- klassisch müssen schlimmstenfalls $2^n/2+1$ verschiedene Argumente ausgewertet werden um die Fälle zu unterscheiden
  => Quantenparallelismus nutzen um Aufwand zu senken

Problemstellung:

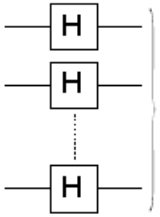
- Für die Funktion gilt $f(x):\{0,1\}^n \rightarrow \{0,1\}$ gilt $f(x)=const$ oder $\sum_x f(x)=2^n/2$.
- Welcher Fall liegt vor?
- f(x) möglichst wenig ausführen (f ist teuer)

Deutsch – Jozsa – Algorithmus

Algorithmus:

- Da das Argumenten-Register nun n Qubits fasst, muss die Superpositionsoperation verallgemeinert werden:

  Die (Walsh-)Hadamard-Transformation $H^{\otimes n}$ wirkt parallel auf n Qubits:



n Stück; erzeugt 2^n-fache Superposition
=> effiziente Umsetzung

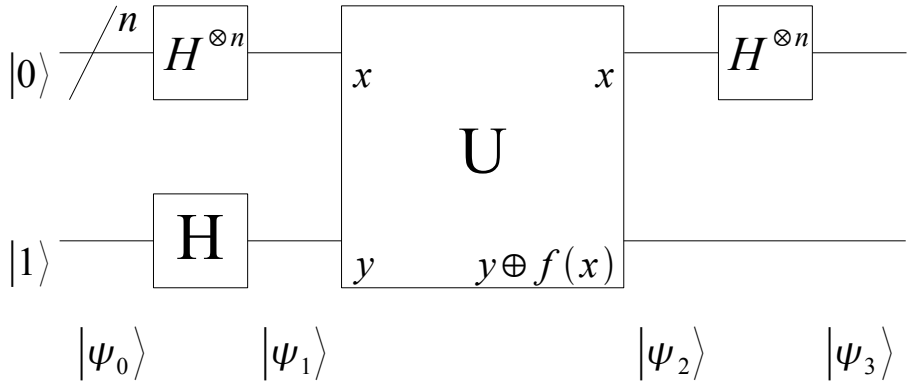
$$H^{\otimes n}\left|x_0 \ldots x_n\right\rangle = H\left|x_1\right\rangle \cdot \ldots \cdot H\left|x_n\right\rangle$$

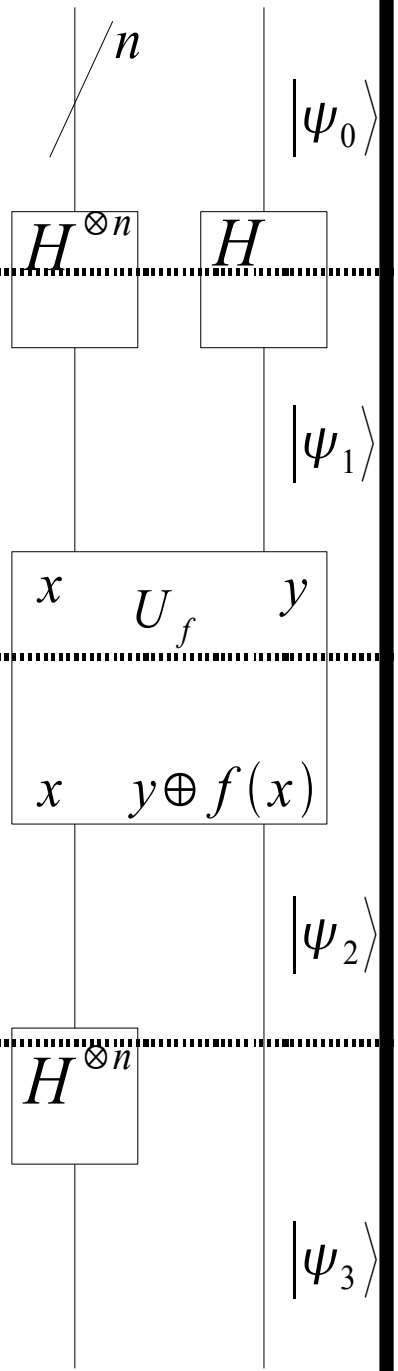
Produkt der n 2-Superpositionen ergibt Superposition aller 2^n Basiszustände

- Parallelauswertung einer Fkt:

$$U_f \;\; H^{\otimes n}\left|0\right\rangle^{\otimes n}\left|0\right\rangle = \sum_{x\in\{0,1\}^n} \frac{\left|x\right\rangle}{\sqrt{2^n}}\left|f(x)\right\rangle$$

- Deutsch – Jozsa – Algorithmus:





$$|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle$$

Eingabe:
n+1 klassische Basiszustände

$$|\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

Erzeugung der Superposition durch Hadamard-Transformation

$$U_f |x\rangle [|0\rangle - |1\rangle]/\sqrt{2} = (-1)^{f(x)} |x\rangle [|0\rangle - |1\rangle]/\sqrt{2}$$

Falls f(x)=1, dann invertiert $\oplus f(x)$
$1\ XOR\ f(x) = 0;\quad 0\ XOR\ f(x) = 1$

$$|\psi_2\rangle = \sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

wenn f nicht konstant ist, gibt es wieder negative Summanden

$$H|b\rangle = \sum_{z \in \{0,1\}^1} \frac{(-1)^{bz}}{\sqrt{2^1}} |z\rangle$$

Der Zustand nach Anwendung des 1-Bit Hadamards auf Basiszustand b...
...ist einer von n Faktoren des n-Bit-Hadamards.

$$H^{\otimes n} |b_1 \ldots b_n\rangle = \sum_{z \in \{0,1\}^n} \frac{(-1)^{bz}}{\sqrt{2^n}} |z_1 \ldots z_n\rangle$$

$$|\psi_3\rangle = \sum_{x,z \in \{0,1\}^n} \frac{(-1)^{xz + f(x)}}{2^n} |z_1 \ldots z_n\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

$|\psi_2\rangle$ eingesetzt:
-Wurzel quadriert sich weg
-Exponenten von (-1) summiert

$$|\psi_3\rangle = \sum_{x,z\in\{0,1\}^n} \frac{(-1)^{xz+f(x)}}{2^n} |z_1 \ldots z_n\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

Nun wird nur die Amplitude $\sum_{x\in\{0,1\}^n} \frac{(-1)^{xz+f(x)}}{2^n}$ des Zustandes $|z_1=0 \ldots z_n=0\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$ betrachtet:

- wenn f konstant ist erhält man: $\sum_{x\in\{0,1\}^n} \frac{(-1)^{xz+f(x)}}{2^n} = \sum_{x\in\{0,1\}^n} \frac{(-1)^{x\cdot 0+f}}{2^n} = (-1)^f \sum_{x\in\{0,1\}^n} \frac{1}{2^n} = (-1)^f$

  Da der Betrag 1 ist und die Wellenfunktion normiert sein muss:

$$\Rightarrow |\psi_3{}'\rangle = |z_1=0 \ldots z_n=0\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

- wenn f balanciert ist: $\sum_{x\in\{0,1\}^n} \frac{(-1)^{x\cdot 0+f(x)}}{2^n} = \sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)}}{2^n} = 2^n/2 \frac{1}{2^n} + 2^n/2 \frac{-1}{2^n} = 0$

  Also tritt der zugehörige Zustand nicht auf.

Ausgabe:

Messung des Argumenten-Registers ergibt...

- 0 für jedes Qubit ,wenn $f(x) = const$
- 1 mindestens für ein Qubit ,wenn $\sum_x f(x) = 2^n/2$

Auswertung:

- Der Quantenparallelismus = Grund für höhere Rechenleistung gegenüber klassischem Computer:
  Einmaligen Anwendung eines Gatters auf einen Zustand von n Qubits führt zu 2^n Manipulationen (klassisch: nur eine) .
  <=>exponentiell schneller!

  (Abgesehen von n Messungen am Register, die bei teurem f wenig ins Gewicht fallen.)

- ABER:
  - Die Umsetzung von f(x) im Quantencomputer schlecht zu vergleichen mit der klassichen Variante – möglicherweise deutlich ineffizienter.
  - Deutsch(-Jozsa)-Algorithmus besitzt keine sinnvolle Anwendung
- Neben Quantenparallelismus ist die Verschränkung, der Qubits miteinander ein weiterer Vorteil gegenüber klassischen Algorithmen.
  Dies wird beim Deutsch-Jozsa ebenfalls genutzt.
  =>Verschränkung untersuchen.

Einschub: U_f effizient umsetzbar?

- f nur näherungsweise aus unitären Gattern durch sehr lange Gatterperioden darstellbar (-> schon im 1bit Fall schlecht)
- n Bits: f skaliert schlecht mit n, da viele (unbenachbarte) Verknüpfungen der Bits untereinander

Entropie

- klassisch: Shanon H:
  - Maß für Informationsgewinn bei Erkenntnis des Wertes einer Zufalls Variable - oder: Maß für die Unbestimmtheit der Var ^= deren „Unordnung“
  - H(p_1,...,p_n)=-Sum from x p_x log p_x; 0 log 0:=0; log zur Basis 2, da binär
  - lim p_x to inf p_x log p_x =0; da hier Sicherheit herrscht
  - Rechtfertigung:
    - quantisiert Ressourcen , die nötig sind um Inform. zu speichern.
    - H(q p_1 + (1-q) p_2)>= q H(p_)1 + (1-q) H(p_2) // die verketteter Zufall 2er Systeme: erst q oder (1-q), dann p_1 bzw p_2. -> Superposition hat mehr Möglichkeiten als jeweils beide einzeln.
      (H konkav, folgt aus Def. H)
    - Wie viel Information von Quelle E: I(E) mit
      - I(E)=I(p(E)) wenn E nur ein Zufallsereignis
      - I ist stetige Fkt von p
      - I(p q) =I(p) + I(q) (p, q gehören zu unabh. Ereignissen)
        =>I(p_i)=k log p_; ; I(p)Sum from k p_i p log P_i
  - rel. Entropie: H(p||q):=-Sum from x p(x) log p(x)/q(x) //p relativ zu q => Wichtung erfolgt mit p

Entropie H: Eigenschaften

- H(x,y)=- Sum from x p(x,y) log p(x,y)//(^=Vereinigungsinformationsmenge)
- H(x|y)=H(x,y)-H(y) //(^=Menge x ohne y) y schon bekannt, dh von y unabhängiges: da log(p_x*p_y) =log p_x + log p_y, wird p_y so entfernt
- H(x:y)=H(x)+H(y)-H(x,y)//(^=Schnittmenge)Schnittinformationen: Inf, die in beiden enthalten, bleibt über da die GesamtInf einmal abgezogen wird
  Es gilt auch H(x:y)=H(x)-H(x|y)
- Folgerungen:
  1. H(x,y)=H(y,x); H(x:y)=H(y:x)
  2. H(y|x)>=0 & H(x:y)<=H(y); „=“ bei y=f(x)
  3. H(x)<=H(y,y); „=“ bei y=f(x)
  4. Subadditivität: H(x,y)<=H(x) +H(y); „=“ bei x unabh. y //wegen H(x:y)!= i.A.
  5. H(y|x)<=H(y) & H(x:y)>=0; „=“ bei x unabh. y
  6. starke Subadditivität: H(x,y,z)+H(y)<=H(x,y) +H(y,z); „=“ bei z->y->x Markov-Kette
  7. reduzierte Entropie: H(x|(y,z))<=H(x|y) //durch Neuanordnung folgt Starke Subadditivität

Von Neumann Entropie

- Maß für Informationsgewinn durch Erkennen des Wertes einer Zufallsvariable – oder: Misst Ressourcen, die nötig sind um Information zu speichern.
  - Von Neumann Entropie S einer Dichtematrix $\rho = |\psi\rangle\langle\psi|$:

    $$S(\rho) \equiv -tr(\rho \log \rho);\quad 0 \log 0 \equiv 0;\quad \log x \equiv \log_2 x$$

  - In Eigenwertbasis ergibt sich die klassische Entropie

    $$S(\rho) = -\sum_i \lambda_i \log \lambda_i$$

- Eigenschaften:
  - nicht negativ; $S = 0 \Leftrightarrow reiner\ Zustand$
  - höchstens log d im d-dimensionalen Hilbertraum; $S = -\log d \Leftrightarrow \rho = I/d$
  - Für Kombinierte Systeme A,B: $S(A,B) = -tr\,\rho_{AB} \log \rho_{AB}$
    - Wenn man nur die Entropie von A wissen möchte:

      $$S(A) = -tr\,\rho_A \log \rho_A;\qquad mit\ \rho_A = tr_B\,\rho_{AB}$$

Verschränkung im Deutsch-Jozsa-Algorithmus

Es wird die Verschränkung des 1. Qubits im Argumenten-Register mit den restlichen untersucht:

- Der Eingabe-Zustand ist offensichtlich nicht verschränkt:

$$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle = |0\rangle\otimes\ldots|0\rangle\otimes|1\rangle$$

1.Umschreiben auf vollständige Dichtematrix

$$\rho_0 = |\psi_0\rangle\langle\psi_0| = |0\rangle\langle 0|\otimes\ldots\otimes|0\rangle\langle 0|\otimes|1\rangle\langle 1|$$

2.ausspuren der 2,...,n+1 Qubits ergibt 1, da reiner Zustand

$$\rho_0^1 = tr_{2,\ldots,n+1}\{\rho_0\} = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

3.Dichtematrix des 1. Qubits verbleibt

$$S = -\sum_i \lambda_i \log \lambda_i = -1\log 1 - 0\log 0 = 0$$

4.Verschränkungsentropie des 1. Qubits

- Zustand nach Hadamard-Transformation:

$$|\psi_1\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

1.Umschreiben auf vollständige Dichtematrix:

$$\rho_1 = |\psi_1\rangle\langle\psi_1|$$

$$= \left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{\langle 0|+\langle 1|}{\sqrt{2}}\right] \otimes \ldots \otimes \left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{\langle 0|+\langle 1|}{\sqrt{2}}\right] \otimes \left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{\langle 0|-\langle 1|}{\sqrt{2}}\right]$$

2.ausspuren der 2,...,n+1 Qubits ergibt:

$$\rho_1^1 = tr_{2,\ldots,n+1}\{\rho_1\} = 1/2\left[|0\rangle+|1\rangle\right]\left[\langle 0|+\langle 1|\right]$$

(da Spur =1 - Eigentlich offensichtlich, da die Qbits auch hier nicht verschränkt sind.)

$$Spur = \sum_{x_{2,\ldots}, x_n=0}^{1} 1/2\langle x_2|\left[|0\rangle+|1\rangle\right]\left[\langle 0|+\langle 1|\right]|X_2\rangle \cdot \ldots \cdot \sum_{x_{n+1}} \langle x_{n+1}|\text{-}\rangle\langle\text{-}|x_{n+1}\rangle$$

$$= \prod_{i=2}^{n} \sum_{x_i=0}^{1} 1/2\langle x_i|\left[|0\rangle+|1\rangle\right]\left[\langle 0|+\langle 1|\right]|X_i\rangle \cdot \ldots \cdot 1 = 1$$

3.Dichtematrix des 1. Qubits verbleibt:

$$= \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix} \qquad \Rightarrow \lambda_1 = 1;\ \ \lambda_2 = 0$$

4.Verschränkungsentropie des 1. Qubits:

$$S = -\sum_i \lambda_i \log \lambda_i = -1\log 1 - 0\log 0 = 0$$

=>keine Verschränkung. Sinnvoll, da Hadamard-Transformation lokal ist.

- Zustand nach Anwenden von U_f (Modulo 2 Addition von f(x) auf Ziel-Register):

$$|\psi_2\rangle = \sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

1.Umschreiben auf vollständige Dichtematrix:

$$\rho_2 = |\psi_2\rangle\langle\psi_2|$$

$$= \sum_{l_{1,\dots}, l_n=0}^{1} \sum_{r_{1,\dots}, r_n=0}^{1} (-1)^{f(l)}(-1)^{f(r)} \frac{|l_1\rangle}{\sqrt{2}} \frac{\langle r_1|}{\sqrt{2}} \otimes \dots \otimes \frac{|l_n\rangle}{\sqrt{2}} \frac{\langle r_n|}{\sqrt{2}} \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\left[\frac{\langle 0| - \langle 1|}{\sqrt{2}}\right]$$

2.ausspuren der 2,...,n+1 Qubits:

$$tr\{|l_i\rangle\langle r_i|\} = \langle 0|r_i\rangle\langle l_i|0\rangle + \langle 1|r_i\rangle\langle l_i|1\rangle = \delta_{r_i, l_i} + 0$$

$$Spur = \sum_{l_{2,\dots}, l_n=0}^{1} \sum_{r_{2,\dots}, r_n=0}^{1} (-1)^{f(l)+f(r)} \frac{1}{2}\left[\langle 0|r_2\rangle\langle l_2|0\rangle + \langle 1|r_2\rangle\langle l_2|1\rangle\right] \cdot \dots \cdot \frac{1}{2}\left[\langle 0|r_n\rangle\langle l_n|0\rangle + \langle 1|r_n\rangle\langle l_n|1\rangle\right] \cdot 1$$

$$= \sum_{l_{2,\dots}, l_n=0}^{1} \sum_{r_{2,\dots}, r_n=0}^{1} (-1)^{f(l)+f(r)} \frac{1}{2} \delta_{l_2, r_2} \cdot \dots \cdot \delta_{l_n, r_n} \cdot = \frac{1}{2^{n-1}} \sum_{l_{2,\dots}, l_n=0}^{1} (-1)^{f(l_1, l_{2,\dots}, l_n) + f(r_1, l_{2,\dots}, l_n)}$$

Durch die Delta-Funktionen in der Spur entfällt eine Summe (r) ab der 2. Stelle:
(Die Summe der 1. Stelle wird ausgeschrieben.)

$$\rho_2^1 = tr_{2,\dots,n+1}\{\rho_2\} = \frac{1}{2^n} \sum_{l_{1,\dots}, l_n=0}^{1} (-1)^{f(l_{1,\dots}, l_n) + f(0, l_{2,\dots}, l_n)} |l_1\rangle\langle 0| + (-1)^{f(l_{1,\dots}, l_n) + f(1, l_{2,\dots}, l_n)} |l_1\rangle\langle 1|$$

3.Dichtematrix des 1. Qubits verbleibt:

$$= \frac{1}{2^n} \sum_{l_2, \dots, l_n=0} \begin{pmatrix} (-1)^{2f(0, l_2, \dots, l_n)} = 1 & (-1)^{f(0, l_2, \dots, l_n) + f(1, l_2, \dots, l_n)} \\ (-1)^{f(1, l_2, \dots, l_n) + f(0, l_2, \dots, l_n)} & (-1)^{2f(1, l_2, \dots, l_n)} = 1 \end{pmatrix}$$

$$\rho_2^1 = \frac{1}{2^n} \sum_{x_2,\ldots,x_n=0} \begin{pmatrix} 1 & (-1)^{f(0,x_2,\ldots,x_n)+f(1,x_2,\ldots,x_n)} \\ (-1)^{f(0,x_2,\ldots,x_n)+f(1,x_2,\ldots,x_n)} & 1 \end{pmatrix}$$

mit $\sum_{x_2,\ldots,x_n=0} 1 = 2^{n-1}$ ergibt sich durch Auflösen der Summen:

$$= \begin{pmatrix} 1/2 & \frac{1}{2^n} \sum_{x_2,\ldots,x_n=0} (-1)^{f(0,x_2,\ldots,x_n)+f(1,x_2,\ldots,x_n)} \\ \frac{1}{2^n} \sum_{x_2,\ldots,x_n=0} (-1)^{f(0,x_2,\ldots,x_n)+f(1,x_2,\ldots,x_n)} & 1/2 \end{pmatrix}$$

- Beispiel 1: $f(x_1,\ldots,x_n) = \begin{cases} x_2 & wenn \quad x_1 = 0 \\ 1 - x_3 & wenn \quad x_1 = 1 \end{cases}$

$$\rho_2^1 = \begin{pmatrix} 1/2 & 1/8\left[(-1)^{0+1}+(-1)^{0+0}+(-1)^{1+1}+(-1)^{1+0}\right] \\ 1/8\left[(-1)^{0+1}+(-1)^{0+0}+(-1)^{1+1}+(-1)^{1+0}\right] & 1/2 \end{pmatrix}$$

$$= \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix} \qquad \Rightarrow \lambda_1 = 1/2; \quad \lambda_2 = 1/2$$

Verschränkungsentropie des 1. Qubits:

$$S = -\sum_i \lambda_i \log \lambda_i = -2 \cdot 1/2 \log 1/2 \neq 0$$

=> 1. Qubit ist maximal mit den ausgespurten verschränkt.

$$\rho_2^1 = \begin{pmatrix} 1/2 & \frac{1}{2^n}\sum_{x_2,\ldots,x_n=0}(-1)^{f(0,x_2,\ldots,x_n)+f(1,x_2,\ldots,x_n)} \\ \frac{1}{2^n}\sum_{x_2,\ldots,x_n=0}(-1)^{f(1,x_2,\ldots,x_n)+f(0,x_2,\ldots,x_n)} & 1/2 \end{pmatrix}$$

- Beispiel 2: $f(x_1,\ldots,x_n)=x_1$

$$\rho_2^1 = \begin{pmatrix} 1/2 & 1/4\left[(-1)^{0+1}+(-1)^{0+1}\right] \\ 1/4\left[(-1)^{1+0}+(-1)^{1+0}\right] & 1/2 \end{pmatrix}$$

$$= \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix} \qquad \Rightarrow \lambda_1 = 1\,;\ \ \lambda_2 = 0$$

Verschränkungsentropie des 1. Qubits:

$$S = -\sum_i \lambda_i \log \lambda_i = -1\log 1 - 0\log 0 = 0$$

=> keine Verschränkung

Auswertung:

- Die auftretende Verschränkung ist von f(x) abhängig.
- Sind alle Zustände separabel, so könnte das Problem, durch n Umsetzungen des Deutsch-Algorithmus ähnlich effizient gelöst werden.
- Sind die Zustände nicht separabel, so kann der Deutsch-Jozsa Algorithmus bis zu 2^n Dimensionen nutzen, um f zu charakterisieren.
  - => Verschränkung bietet einen exponentiellen Vorteil bei linear ansteigender Komplexität.
  - Quantenalgorithmen, die Verschränkung nutzen, können nicht klassisch effizient umgesetzt werden, da kein Analogon existiert.

- Neben dem Quantenparallelismus stellt die Möglichkeit zur Verschränkung also einen weiteren wichtigen Vorteil der Quantencomputer dar.

Überleitung (Folie wird nicht gezeigt)

- Algorithmus=genau definiertes Verfahren zur Lösung eines Problems.

- bisher: mathematische Eigenschaften bestimmen.
- Nun: bestimmen ob ein Objekt vorhanden ist ohne klassisch WzuW.
- Ähnelt sich prinzipiell: mathematisch f={0,1} ? Dies hier besitzt aber eine relevante physikalisch Entsprechung

Elitzur – Vaidmann – Verfahren
- „wechselwirkungsfreie“ Messung -

Motivation:

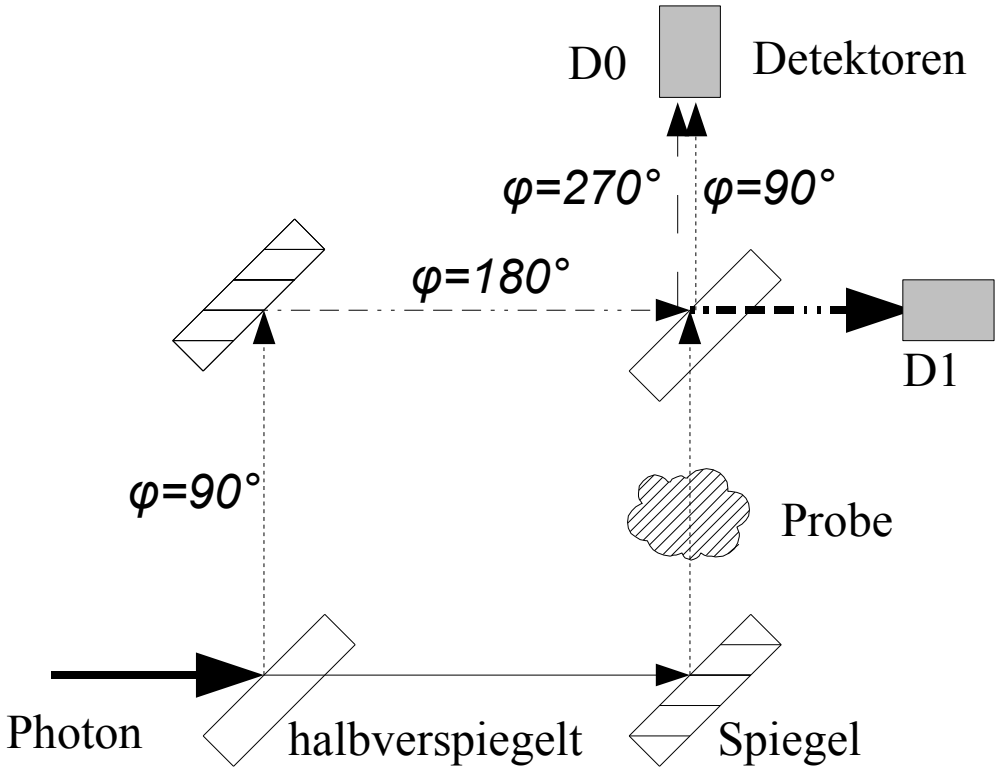
- Unter den Bomben in einem Vorratslager befinden sich einige, die keinen Zünder besitzen.
- Der Zünder der funktionstüchtigen Bomben ist so beschaffen, dass bereits ein einziges Photon genügt, um eine Detonation zu bewirken.
- Wenn man wissen möchte, ob eine Bombe funktioniert, so kann der Zünder betrachtet werden – falls sie explodiert, so handelte es sich um ein brauchbares Exemplar.
- Wie gelangt man an eine sicher funktionierende Bombe ohne diese zu zerstören?

Problemstellung:

- Feststellen, ob eine Bombe einen Zünder besitzt, ohne dabei auch nur in kleinste Wechselwirkung mit diesem zu treten.

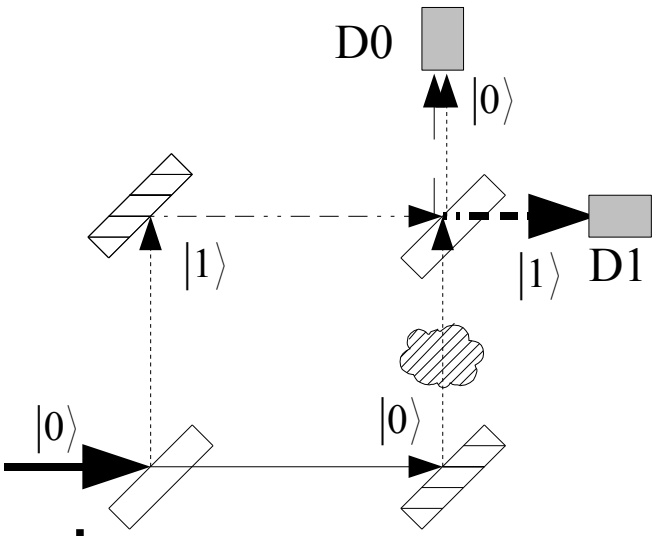
Algorithmus:

- Bei einem Mach-Zehner-Interferometer, wird die Wellenfunktion eines Photons über einen Strahlteiler aufgespalten.
- Die verschiedenen, gleichlangen Wege erzeugen bei Spiegelungen 90°-Phasensprünge.
- Die Teilwellenfunktionen werden durch einen weiteren Strahlteiler interferiert:
  - Auslöschung bei Detektor D2, da Phasendifferenz=180°.
  - => Photon bei D1.
- In einen Strahlengang wird der Bombensensor eingebracht.



Den Wellenfunkionen verschiedener Wege werden die Zustände zugeordnet: $|0\rangle$; $|1\rangle$

(transmittierte Anteile behalten ihre Zuordnung)



$|\psi_0\rangle$

$|\psi_0\rangle = |0\rangle$

Eingabe: 1 Photon

$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & i\\ i & 1\end{pmatrix}$

$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$

Strahlteiler:
Superposition der Wegzustände;
Der reflektierte Teil bekommt Phasensprung i

$|\psi_1\rangle$

$\begin{pmatrix}i & 0\\ 0 & i\end{pmatrix}$

$|\psi_2\rangle = \frac{1}{\sqrt{2}}(i|0\rangle - |1\rangle)$

Spiegel:
Je Phasensprung i

$|\psi_2\rangle$

$\begin{pmatrix}1 & 0\\ 0 & \{1, absorbiert\}\end{pmatrix}$

$|\psi_3\rangle = \frac{1}{\sqrt{2}}(i|0\rangle - |1\rangle)$

$|\psi_3'\rangle = \frac{1}{\sqrt{2}}(i|0\rangle - |absorbiert\rangle)$

Zünder:
Wenn der Zünder vorhanden ist, wird die entsprechende Teilwellenfunktion absorbiert.

$|\psi_3\rangle$

$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & i\\ i & 1\end{pmatrix}$

$|\psi_4\rangle = \frac{1}{2}(i|0\rangle - |1\rangle) - \frac{1}{2}(i|0\rangle + |1\rangle) = -|1\rangle$

$|\psi_4'\rangle = \frac{1}{2}(i|0\rangle - |1\rangle) - \frac{1}{\sqrt{2}}|absorbiert\rangle$

Strahlteiler:
Die Teilwellenfunktionen interferieren.

$|\psi_4\rangle$

$|\psi_4\rangle = -|1\rangle$ kein Zünder: Destruktive Interferenz vor Detektor D0; D1 klickt immer.

$|\psi_4'\rangle = \frac{1}{2}(i|0\rangle - |1\rangle) - \frac{1}{\sqrt{2}}|absorbiert\rangle$ mit Zünder:

- zu 25% klickt D0
- zu 25% klickt D1
- zu 50% trifft das Photon auf den Zünder
  => die Bombe explodiert.

Falls D0 klickt, hat man eine funktionierende Bombe gefunden, dabei war das Photon nicht am Zünder, denn es wurde am Detektor registriert. => „wechselwirkungsfreie Messung“

Solange D1 klickt muss die Messung wiederholt werden, bis man sich hinreichend sicher ist, dass kein Zünder vorhanden ist.

Auswertung:

- Durch Wiederholung können 1/3 der funktionierenden Bomben gefunden werden.
- Erfolgsrate kann, durch Modifikation der Reflektionskoeffizienten verbessert werden. Allerdings braucht man entsprechend mehr Versuche.
- Wie beim Deutsch (-Jozsa) - Algorithmus wurde Quantenparallelismus genutzt.
- Sowie die Zustandsreduktion des Ortes.
- Die Messung ist nicht wirklich wechselwirkungsfrei: Z.B. würde man ein QM-Teilchen als Probe verwenden, würde es in einen Orts-Eigenzustand kollabieren. => Die Wellenfunktionen wechselwirken.

Zusammenfassung

- Durch Ausnutzung von Quanteneffekten können Quantenalgorithmen effizienter sein, als klassische Versionen:
  - **Quantenparallelismus**:
    - basiert auf Superposition von Basiszuständen
    - nützlich um mehrere Varianten parallel auszuwerten
    - Problematisch ist es, aus den superpositionierten Evaluationen wieder einzelne Ergebnisse zu erhalten:
      - Beim Deutsch-Josza-Algorithmus. wurden auch nur eine globale Eigenschaften von $f(x_1, ..., x_n)$ ausgewertet.
    - Während beim Algorithmus von Deutsch nur ein linearer Zeitvorteil erzielt wurde, zeigt der Deutsch-Jozsa-Algorithmus , mit exponentiellem Vorteil, das Potential dieses Quanteneffektes.
  - **Verschränkung**:
    - nützlich um komplexe Probleme zu lösen: Durch Verschränkung von n Qubits können 2^n Werte gespeichert werden
    - Mit linear ansteigender Komplexität des Algorithmus könnte die der lösbaren Probleme exponentiell wachsen.
    - Deutsch-Jozsa-Algorithmus nutzt Verschränkung.
- Das Elitzur-Vaidman-Verfahren ermöglicht eine klassisch wechselwirkungsfreie Messung.