

Photonen als Qubits für den Quantencomputer?

W. Dultz, E. Frins*, B. Hils, H. Schmitzer**

Univ. Frankfurt, *Univ. de la República, Uruguay, **Xavier Univ. Cincinnati

requelivahanus@t-online.de

Die Anzahl der bekannten Algorithmen für den Quantenrechner hat sich in den letzten Jahrzehnten nicht wesentlich vergrößert, vielleicht auch weil vielen Praktikern die Theorie zu ungewohnt ist. Wir wollen am Beispiel des Deutsch-Problems, einem der ältesten Algorithmen, einen leichten Zugang finden und dabei zeigen warum Photonen, die viele der nötigen Eigenschaften für Qubits haben nur bedingt zum Quantenrechnen taugen; dabei stützen wir uns wesentlich auf zwei Arbeiten [1,2].

Photonen haben mehrere Eigenschaften, die man für Qubits braucht: Ihre Quantenzustände mit den beiden Basiszuständen der linearen Polarisation x,y kann man überlagern und zwei Photonen lassen sich im Sinne der Quantenmechanik miteinander verschränken. Außerdem sind sie durch Linsen, Spiegel aber auch innerhalb der integrierten Optik leicht zu manipulieren.

DEUTSCH PROBLEM Connection diagram

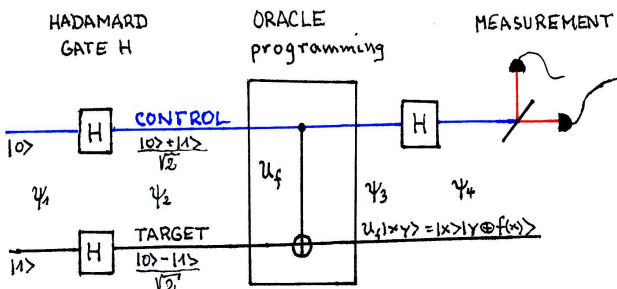


Abb.1 Deutsch-Problem Schaltplan

Abb.1 zeigt den Schaltplan des Deutsch-Problems der drei Ein-Qubit Hadamard Gatter H sowie das Zwei-Qubit Gatter Orakel U_f enthält und der uns als Lehrbeispiel dient. Für die Berechnung verwenden wir die IBM-Konvention; statt dessen könnte man auch die grüne Matrizendarstellung wählen (F1) [1,2].

Deutsch Algorithm Gates; also with matrices

Hadamard gate H (one qubit gate) (F1)

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

$$H|0\rangle = H\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$H|1\rangle = H\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Oracle U_f , CNOT, XOR gate, a two qubit gate; Function $f(x)$

All states must be normalized

constant: $f=(00), (11)$ balanced: $f=(01), (10)$

$$U_f|xy\rangle = |x\rangle|y \oplus f(x)\rangle$$

Summation: $y \oplus f(x) \equiv y + f(x) \pmod{2}$

$$|xy\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

$$U_f|xy\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ -\delta \end{pmatrix}$$

Deutsch Algorithm formulas

(F2)

Summation of $a \oplus f(b) \equiv (a+f(b)) \pmod{2}$

$$\psi_1 = |0\rangle|1\rangle = |01\rangle$$

$$\psi_2 = H\psi_1 = H|0\rangle H|1\rangle = \frac{1}{\sqrt{2}}|0+1\rangle \frac{1}{\sqrt{2}}|0-1\rangle = \frac{1}{2}|00-01+10-11\rangle$$

Programming $f(01)$ of the oracle U_f ; $U_f|xy\rangle = |x\rangle|y \oplus f(x)\rangle$

$$\psi_3 = U_f\psi_2 = \frac{1}{2}(|0\rangle|0 \oplus f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|0 \oplus f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle)$$

$$\psi_3 = \frac{1}{2}(|0\rangle|f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle)$$

$$\text{constant } f(0)=f(1)=0; \psi_{3c} = \frac{1}{2}(|0\rangle|1\rangle|f(0)\rangle - |0\rangle|1\rangle|1 \oplus f(0)\rangle)$$

$$\psi_{3c} = \frac{1}{2}|00-01+10-11\rangle = \frac{1}{2}(|0+1\rangle|0\rangle - |0+1\rangle|1\rangle) = \frac{1}{\sqrt{2}}|0+1\rangle \frac{1}{\sqrt{2}}|0-1\rangle$$

$$\psi_{4c} = H\psi_{3c} = H \text{ first qubit} \times \text{second qubit} = |0\rangle \frac{1}{\sqrt{2}}|0-1\rangle$$

$$\text{constant } f(0)=f(1)=1; \psi_{3c} = \frac{1}{2}(|0\rangle|1\rangle|f(0)\rangle - |0\rangle|1\rangle|1 \oplus f(0)\rangle)$$

$$\psi_{3c} = \frac{1}{2}|01+11-00-10\rangle = \frac{1}{2}(|0+1\rangle|1\rangle - |0+1\rangle|0\rangle) = \frac{1}{\sqrt{2}}|0+1\rangle \frac{1}{\sqrt{2}}|1-0\rangle$$

$$\psi_{4c} = H\psi_{3c} = H \text{ first qubit} \times \text{second qubit} = |0\rangle(-1) \frac{1}{\sqrt{2}}|0-1\rangle = -|0\rangle \frac{1}{\sqrt{2}}|0-1\rangle$$

balanced $f(0) \neq f(1) = (01)$

$$\psi_{3b} = \frac{1}{2}(|0\rangle|f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle) = \frac{1}{2}(|00-01+11-10\rangle)$$

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

$$\psi_{4b} = H\psi_{3b} = H \text{ first qubit} \times \text{second qubit} = |1\rangle \frac{1}{\sqrt{2}}|0-1\rangle$$

balanced $f(0) \neq f(1): f=(10)$

$$\psi_{3b} = (|0\rangle|f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle) = \frac{1}{2}(|01-00+10-11\rangle)$$

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

$$\psi_{3b} = -\frac{1}{\sqrt{2}}|0-1\rangle \frac{1}{\sqrt{2}}|0-1\rangle$$

$$\psi_{4b} = H\psi_{3b} = H \text{ first qubit} \times \text{second qubit} = -|1\rangle \frac{1}{\sqrt{2}}|0-1\rangle$$

Wir beginnen mit zwei Qubits mit den beiden Basiszuständen 0,1 in getrennten Kanälen ψ_1 (control, target), die durch die beiden Hadamard-Gatter H in Überlagerungszustände ψ_2 gebracht werden (F1). Im optischen Bild bedeutet das, daß zwei Photonen mit x- bzw. y-Polarisation in der xy-Ebene durch je ein $\lambda/2$ -Blättchen jeweils um 45° gedreht werden. Mit ψ_2 gehen wir ins Orakel Abb.1, (F2), das für unsere Fragestellung programmiert werden muß: Gefragt wird, ob eine zweiwertige Funktion $f(0,1)$ "constant", d.h. $f(0) = f(1) = 0$ oder 1, oder aber "balanced" d.h. $f(0)$ ungleich $f(1)$ entweder 0,1 oder 1,0 ist. Man stelle

sich vor es sei die Frage nach einer Münze mit gleichen Seiten (falsch) oder unterschiedlichen Seiten (richtig)[3]. Dazu wird die Funktion f binär (d.h. modulo 2) zum Targetbit addiert und man erhält ψ_3 im Ausgang des Orakels; die Rechnung ist einfach aber länglich (F2). Diese Operation U_f kann nicht mit einzelnen Photonen durchgeführt werden, da diese nicht miteinander wechselwirken! (F3) faßt die Ergebnisse der Quantenzustände vor und nach dem Orakel zusammen. Es zeigt sich, daß sich in jedem der 4 Fälle von f ψ_3 als Produkt von Überlagerungszuständen des Controlbits (blau) und des Targetbits darstellen läßt.

Oracle input		(F3)	
$\psi_2 = \frac{1}{\sqrt{2}} 0+1\rangle + \frac{1}{\sqrt{2}} 0-1\rangle = \frac{1}{2} +$		00 - 01 + 10 - 11)	
Oracle program		Oracle output	
$f=(00)$	$\psi_{3f} = \frac{1}{\sqrt{2}} 0+1\rangle + \frac{1}{\sqrt{2}} 0-1\rangle = \frac{1}{2} +$	00 - 01 + 10 - 11)	
$f=(10)$	$\psi_{3f} = -\frac{1}{\sqrt{2}} 0+1\rangle + \frac{1}{\sqrt{2}} 0-1\rangle = \frac{1}{2} -$	00 + 01 - 10 + 11)	
$f=(01)$	$\psi_{3f} = \frac{1}{\sqrt{2}} 0-1\rangle + \frac{1}{\sqrt{2}} 0-1\rangle = \frac{1}{2} +$	00 - 01 - 10 + 11)	
$f=(11)$	$\psi_{3f} = -\frac{1}{\sqrt{2}} 0-1\rangle + \frac{1}{\sqrt{2}} 0-1\rangle = \frac{1}{2} -$	00 + 01 + 10 - 11)	

Damit ist ψ_3 faktorisiert ebenso wie ψ_2 und eine Verschränkung der Qubits ist für das Deutsch-Problem nicht notwendig. Wendet man jetzt noch ein Hadamard-Gatter auf das erste (blaue) Qubit von ψ_3 an, so erhält man dafür den Zustand 0 (rot) für ein konstantes f und 1 (rot) für ein "ballanced" f (F2), ein Ergebnis, das durch eine einzige Messung erhalten wird. Letztere kann man sich am besten wieder optisch durch einen polarisierten Strahlteiler mit zwei Photonenanzählern vorstellen, Abb.1. Man braucht also um die Qualität der "Münze" festzustellen nur eine Anfrage und muß nicht auf den beiden Münzseiten nachschauen.



Abb.2 Zeitungsausschnitt FAZ Februar 2026

Hadamard-Gatter und Orakel sind die Grundbausteine vieler Quantenalgorithmien, wenn man auch meistens ganze Kaskaden dieser Gatter dazu braucht; z.B. Zigtausende um eine moderne Verschlüsselung zu knacken. Soweit ist man heute anscheinend noch nicht, wären ja sonst weder Bankkonten noch Kryptowährungen sicher (Abb. 2 FAZ). Die Rechnungen sind im Prinzip ähnlich, dabei aber zunehmend unübersichtlich, wären aber vermutlich eine gute Aufgaben für die KI. Einen allgemeineren Zugang bietet das Kickback-

Verfahren (F4). Man beweist die rote Formel, indem man die Basiszustände $(0,1)$ getrennt für x einsetzt. Die Funktion f erscheint dann als Exponent. Die Formel erweist sich in größeren Schaltkreisen als nützlich [1,2].

$$\begin{aligned}
 &\text{Phase Kickback} & (F4) \\
 &\psi_{2k} = |x\rangle \frac{1}{\sqrt{2}}|0-1\rangle \\
 &\psi_{3k} = U_f \psi_2 = U_f |x\rangle \frac{1}{\sqrt{2}}|0-1\rangle = \frac{1}{\sqrt{2}} (U_f |x\rangle |0\rangle - U_f |x\rangle |1\rangle) \\
 &\psi_{3k} = \frac{1}{\sqrt{2}} (|x\rangle |0 \oplus f(x)\rangle - |x\rangle |1 \oplus f(x)\rangle) = |x\rangle \frac{1}{\sqrt{2}} (|f(x)\rangle - |1 \oplus f(x)\rangle) \\
 &\psi_{3k} = (-1)^{f(x)} |x\rangle \frac{1}{\sqrt{2}} |0-1\rangle \text{ with } a \oplus f(b) \equiv (a + f(b)) \bmod 2 \\
 &\text{Deutsch's Algorithm with Phase Kickback} \\
 &\psi_2 = \frac{1}{\sqrt{2}}|0+1\rangle + \frac{1}{\sqrt{2}}|0-1\rangle \\
 &\psi_3 = U_f \psi_2 = \frac{1}{\sqrt{2}} ((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle) \frac{1}{\sqrt{2}}|0-1\rangle \\
 &\text{constant: } f(0)=f(1)=0; \psi_{3c} = \frac{1}{\sqrt{2}}|0+1\rangle + \frac{1}{\sqrt{2}}|0-1\rangle \\
 &\psi_{4c} = H_1 \psi_{3c} = H \text{ first qubit} \times \text{second qubit} = H_1 \frac{1}{\sqrt{2}}|0+1\rangle + \frac{1}{\sqrt{2}}|0-1\rangle \\
 &\psi_{4c} = |0\rangle \frac{1}{\sqrt{2}}|0-1\rangle \\
 &\text{constant: } f(0)=f(1)=1; \psi_{3c} = (-1) \frac{1}{\sqrt{2}}|0+1\rangle + \frac{1}{\sqrt{2}}|0-1\rangle \\
 &\psi_{4c} = H_1 \psi_{3c} = H \text{ first qubit} \times \text{second qubit} = -H_1 \frac{1}{\sqrt{2}}|0+1\rangle + \frac{1}{\sqrt{2}}|0-1\rangle \\
 &\psi_{4c} = -|0\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
 &\text{balanced: } f(0) \neq f(1); f(0)=0, f(1)=1 \\
 &\psi_{3b} = \frac{1}{\sqrt{2}} ((-1)^0|0\rangle + (-1)^1|1\rangle) \frac{1}{\sqrt{2}}|0-1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \frac{1}{\sqrt{2}}|0-1\rangle \\
 &\psi_{4c} = H_1 \psi_{3b} = H \text{ first qubit} \times \text{second qubit} = H_1 \frac{1}{\sqrt{2}}|0-1\rangle + \frac{1}{\sqrt{2}}|0-1\rangle \\
 &\psi_{4c} = |1\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
 &\text{balanced: } f(0) \neq f(1); f(0)=1, f(1)=0 \\
 &\psi_{3b} = \frac{1}{\sqrt{2}} ((-1)^1|0\rangle + (-1)^0|1\rangle) \frac{1}{\sqrt{2}}|0-1\rangle = \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle) \frac{1}{\sqrt{2}}|0-1\rangle \\
 &\psi_{4b} = H_1 \psi_{3b} = H \text{ first qubit} \times \text{second qubit} = -H_1 \frac{1}{\sqrt{2}}|0-1\rangle + \frac{1}{\sqrt{2}}|0-1\rangle \\
 &\psi_{4b} = -|1\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
 \end{aligned}$$

Optische Zweiqubit-Gatter auf der Grundlage von nichtlinearen optischen Kristallen, die eine Wechselwirkung von Photonen erlauben, wurden erfolgreich erprobt [4]. Allerdings lassen sie sich nicht kaskadieren, da alle folgenden Gatter dieser Art mit dem Zweiqubit Ausgang des ersten zu wenig Lichtintensität für weitere nichtlineare optische Wechselwirkungen erhalten.

Danksagung

E.F. thanks CSIC and PEDECIBA in Uruguay and H.S. the John Hauck Foundation for their Support.

Literatur

- [1] S.Gharibian, Introduction to Quantum Computing 2020, uni-paderborn.de
- [2] C.Hughes et al., Quantum Computing for the Quantum Curious 2021, ISBN 978-3-03061600-4
- [3] J.Gruska, Quantum Computing S.104
- [4] S.Barz al., Scientific Reports 4:6115;doi:10.1038/srep06115; 2017.