CoveX: Quantum Circuit Simulator

Βασιλειάδης Βύρων

Πανεπιστήμιο Πελοποννήσου

Μάρτιος 2015

Περιεχόμενα

Κβαντική Πληροφορία

- Στους κλασικούς υπολογιστές η πληροφορία είναι αποθηκευμένη σε bits.
- Τα bits αυτά μπορούν να πάρουν τιμές 0 ή 1.
- Κλασική πληροφορία σημαίνει ότι μπορεί να αποθηκευτεί σε φυσικό μέσο που υπακούει τους νόμους της κλασικής μηχανικής και μπορεί να υπαρχει σε μία από δύο διακριτές καταστάσεις.
- Πχ. Flip Flop, θέσεις ενός διακόπτη, διακριτές τάσεις ηλεκτρικού ρεύματος, διακριτές εντάσεις φωτός κ.α.

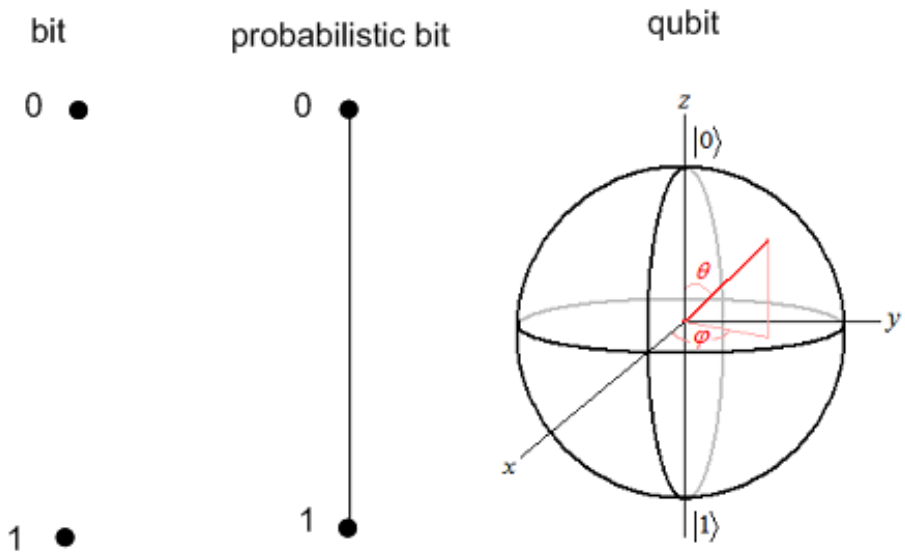
Κβαντική Πληροφορία

- Στους κβαντικούς υπολογιστές η πληροφορία αποθηκεύεται σε qubits.
- Το qubit μπορεί να πάρει τιμές 0, 1 αλλά και υπέρθεσης (superposition) των δυο καταστάσεων ταυτόχρονα.
- Κβαντική πληροφορία σημαίνει ότι μπορεί να αποθηκευτεί σε ένα φυσικό μέσο που υπακούει τους νόμους της κβαντικής μηχανικής και μπορεί να υπάρχει σε κάθε υπέρθεση μεταξύ δύο καταστάσεων.
- Πχ. σπιν σωματιδίου, πολικότητα φωτονίου κ.α.

Κβαντική Πληροφορία

- Για ένα qubit: $|\psi\rangle = a|0\rangle + b|1\rangle$, ισχύει ότι $a, b \quad \epsilon \mathbb{C}$ και $|a|^2 + |b|^2 = 1$
- Το qubit "ζεί" στον χώρο Hilbert 2 διαστάσεων (Hilbert Space). Ο χώρος Hilbert είναι ένας πλήρης μιγαδικός διανυσματικός χώρος με εσωτερικό γινόμενο.
- Το qubit είναι ένα διάνυσμα στον χώρο Hilbert.
- Το $|\psi\rangle$ προφέρεται "ket" και ο συμβολισμός αυτός λέγεται "Dirac Notation". Ενα ket συμβολίζει ένα διάνυσμα, ενώ το εσωτερικό γινόμενο δύο διανυσμάτων $|a\rangle$, $|b\rangle$ συμβολίζεται ως $\langle a|\, b\rangle$ (και προφέρεται "braket").

Κβαντική Πληροφορία



- Διαφέρει από το πιθανοτικό bit!
- Πολική μορφή: $|\psi\rangle = \cos(\frac{\theta}{2})|0\rangle + e^{i\phi}\sin(\frac{\theta}{2})|1\rangle$
- Οι τιμές ενός qubit ανήκουν στην επιφάνεια της σφαίρας. (Bloch Sphere)

Κβαντική Πληροφορία

- Κβαντικός καταχωρητής (quantum register)
- Αν $|\psi_1\rangle = a_1|0\rangle + b_1|1\rangle$ και $|\psi_2\rangle = a_2|0\rangle + b2|1\rangle$ τότε:

$$\begin{aligned}|\psi_1\rangle \otimes |\psi_2\rangle &= |\psi_1\rangle|\psi_2\rangle = |\psi_1\psi_2\rangle \\ &= (a_1|0\rangle + b_1|1\rangle)(a_2|0\rangle + b2|1\rangle \\ &= a_1a_2|0\rangle|0\rangle + a_1b_2|0\rangle|1\rangle + b_1a_2|1\rangle|0\rangle + b_1b_2|1\rangle|1\rangle \\ &= a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle\end{aligned}$$

- Η πράξη $\otimes$ είναι το τανυστικό γινόμενο (tensor product) μεταξύ διανυσμάτων.
- Ένας καταχωρητής μεγέθους n qubits "ζει" έναν χώρο Hilber 2^n διαστάσεων. Οι πιθανές καταστάσεις/τιμές του καταχωρητή είναι 2^n.
- Για n > 332, το 2^n είναι αριθμός μεγαλύτερος από το σύνολο όλων των σωματιδίων που υπάρχουν στο σύμπαν!

Κβαντική Πληροφορία

- Ας δούμε την κβαντική κατάσταση $|\psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$. Αυτή η κατάσταση έχει την ιδιότητα να μην μπορεί να γραφτεί ως σύνθεση δύο ξεχωριστών μονών καταστάστεων $|\psi_0\rangle, |\psi_1\rangle$, δηλαδή $|\psi\rangle = |\psi_0\rangle|\psi_1\rangle$.
- Για να γραφτεί ως σύνθεση καταστάσεων πρέπει

$$(a_0|0\rangle + b_0|1\rangle) \otimes (a_1|0\rangle + b_1|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$$

με $|a_0|^2 + |a_1|^2 = 1$ και $|b_0|^2 + |b_1|^2 = 1$.
- Το σύστημα εξισώσεων που προκύπτει είναι:

$$a_0b_0 = \frac{1}{\sqrt{2}}, \quad a_0b_1 = 0, \quad a_1b_0 = 0, \quad a_1b_1 = \frac{1}{\sqrt{2}}.$$

το οποίο δεν έχει λύση!

Κβαντική Πληροφορία

- Λέμε ότι η κατάσταση $|\psi\rangle$ είναι μή διαχωρίσιμη (non separable) ή αλλιώς *κβαντικά εναγκαλισμένη* (quantum entangled).
- Ο κβαντικός εναγκαλισμός ή κβαντική διεμπλοκή (quantum entanglement) είναι μία μοναδική ιδιότητα της κβαντικής πληροφορικής και παίζει πολύ μεγάλο ρόλο στους αλγορίθμους που αναπτύσσονται σε αυτούς.

Κβαντική Πληροφορία

- Η επεξεργασία της κβαντικής πληροφορίας γίνεται μέσω ορθομοναδιαίων τελεστών (unitary operators).
- Αν την χρονική στιγμή t_1 το σύστημα βρίσκεται στην κατάσταση $|\psi_1\rangle$, τότε την χρονική στίγμή t_2 μετά την εφαρμογή του τελεστή U θα βρίσκεται στην κατάσταση $|\psi_2\rangle = U|\psi_1\rangle$.
- Η ορθομοναδιαιότητα (unitarity) ενός τελεστή είναι το μοναδικό κριτήριο για το αν αυτός είναι ενας έγκυτος κβαντικός τελεστής!
- Αν $U^\dagger U = I$, τότε ο U είναι ορθομοναδιαίος και είναι έγκυρος κβαντικός τελεστής.

Κβαντική Πληροφορία

- Σε όλη τη φάση επεξεργασίας το σύστημα πρέπει να παραμένει *κλειστό*! Αυτό σημαίνει ότι δεν μπορούμε να παρατηρήσουμε την κατάσταση του καθώς αυτό θα εξουδετέρωνε τα κβαντικά χαρακτηριστικά του!
- Πως μπορούμε να πάρουμε αποτελέσματα από το σύστημα;
- Μέσω ειδικών τελεστών μέτρησης M_m.

Κβαντική Πληροφορία

- Για την μέτρηση ενός qubit στην υπολογιστική βάση (computational basis) οι τελεστές αυτοί είναι οι $M_0 = |0\rangle\langle 0|$ και $M_1 = |1\rangle\langle 1|$.
- Μετά την μέτρηση η πιθανότητα να βρεθεί το qubit $|\psi\rangle = a|0\rangle + b|1\rangle$ στην τιμή 0 είναι

$$p(0) = |a|^2,$$

ενώ να βρεθεί στην τιμή 1

$$p(1) = |b|^2.$$

- Τα αποτελέσματα που παίρνουμε είναι κλασική πληροφορία!

Κβαντική Πληροφορία

- Ένας χρήσιμος τρόπος αναπαράστασης είναι οι πίνακες (matrix form). Την αναπαράσταση αυτή είσήγαγε ο Werner Heisenberg.
- Ένα qubit, δηλαδή ένα διάνυσμα του χώρου Hilbert, συμβολίζεται με έναν πίνακα 2x1.
- Αν $|\psi\rangle = a|0\rangle + b|1\rangle$, τότε ισοδύναμα

$$|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$$

Κβαντική Πληροφορία

- Οι τελεστές που εκτελούνται πάνω σε ένα qubit συμβολίζονται με πίνακα 2x2.
- Για παράδειγμα ο τελεστής NOT ή αλλιώς Pauli X και συμβολίζεται συνήθως ως X, σε μορφή πίνακα γράφεται:

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

- Το αποτέλεσμα της πράξης $X|\psi\rangle$ είναι απλά το αποτέλεσμα του πολλαπλασιασμού τως αντίστοιχων πινάκων. Έχουμε δηλαδή

$$X \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix}$$

Κβαντική Πληροφορία

- Γενικά, ένα σύστημα n qubits αντιπροσωπεύεται από έναν πίνακα διαστάσεων $2^n \times 1$.
- Ένας τελεστής που εκτελείται σε m qubits αντιπροσωπεύεται από έναν πίνακα διαστάσεων $2^m \times 2^m$.
- Το αποτέλεσμα της μέτρησης ενός συστήματος n qubits είναι n bits.

Μοντέλο Κβαντικών Κυκλωμάτων

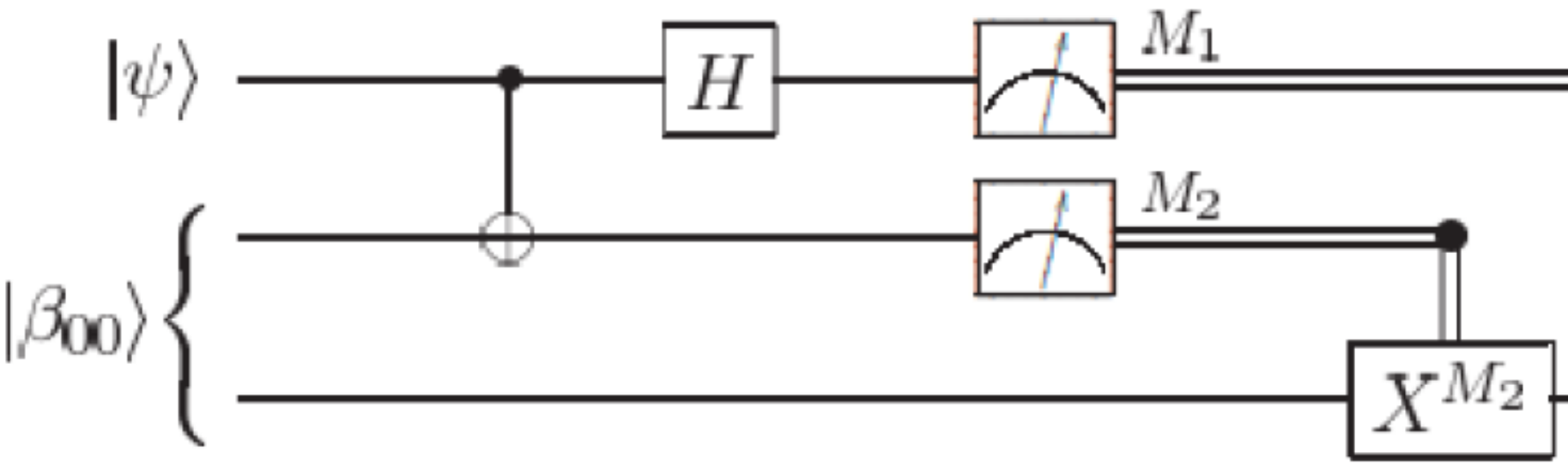
- Ας μεταφράσουμε όσα είδαμε σε μια πιο γνώριμη γλώσσα: την γλώσσα των κυκλωμάτων!
- Ένα κβαντικό κύκλωμα μοιάζει με τα κλασικά κυκλώματα, έχει όμως και κάποιες διαφοροποιήσεις.
- Κάθε καλώδιο του κυκλώματος αντιπροσωπεύει ένα qubit που μεταβάλλεται με τον χρόνο με την εφαρμογή κβαντικών πυλών (quantum gates).
- Ο χρόνος στο κβαντικό κύκλωμα "κυλάει" από αριστερά προς δεξιά.
- Άρα, αριστερά του κυκλώματος είναι η είσοδος, και δεξιά η έξοδος.

Μοντέλο Κβαντικών Κυκλωμάτων

Υπάρχουν τρεις σημαντικές διαφορές με τα κλασικά κυκλώματα:

- Τα κβαντικά κυκλώματα είναι ακυκλικά (acyclic). Δηλαδή, η έξοδος ενός μέρους του κυκλώματος δεν μπορεί να είναι είσοδος σε ένα άλλο μέρος του.
- Δεν υπάρχει η πράξη **FANIN**.
- Δεν υπάρχει η πράξη **FANOUT**. Αυτό, είναι αποτέλεσμα του θεωρήματος της μη-κλωνοποίσης κβαντικών καταστάσεων (no-cloning theorem), το οποίο είναι θεμελιώδες θεώρημα της κβαντικής μηχανικής.

Παράδειγμα



1-qubit Gates

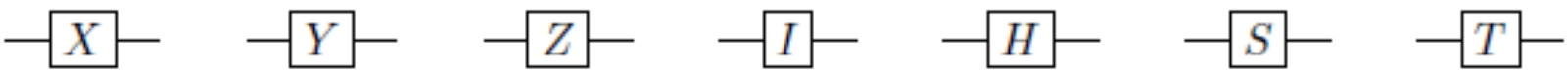
Οι πιο συνηθισμένες πύλες που δρουν σε ένα qubit είναι οι:

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Αυτές οι πύλες λέγονται πύλες Πάολι (Pauli gates). Εξίσου σημαντικές είναι η πύλη Χάνταμαρντ (Hadamard), η πύλη φάσης (phase gate), και η πύλη $\pi/8$.:

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad S \equiv \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \quad T \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

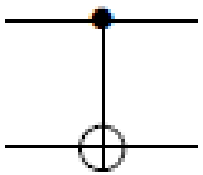
Εντός κβαντικού κυκλώματος συμβολίζονται ως εξής:



2-qubit gates

- Η πιο συνηθισμένη πύλη που δρα σε δύο qubits είναι η πύλη Controlled NOT (CNOT).
- Η CNOT αποτελείται από ένα qubit ελέγχου (control qubit) και ένα qubit στόχου (target qubit).
- Στο qubit στόχου εκτελείται η πράξη NOT, αν το qubit ελέγχου έχει τιμή 1.
- Αναπαράσταση σε μορφή πίνακα και κβαντικού κυκλώματος:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



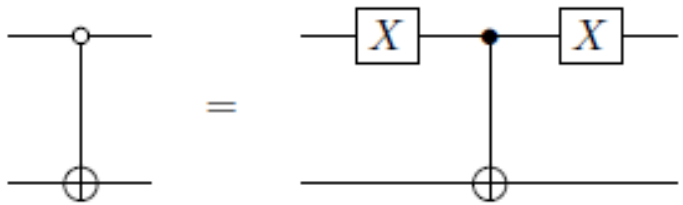
Πύλες πολλαπλών qubits

- Οποιαδήποτε κβαντική πύλη μπορεί να κατασκευαστεί από 1-qubit πύλες και την πύλη CNOT.
- Το σύνολο των 1-qubit πυλών και της πύλης CNOT συνιστούν Universal Set.

Μοντέλο Κβαντικών Κυκλωμάτων

Παράδειγμα 1

- Η "αντίστροφη" πύλη CNOT μπορεί να κατασκευαστεί με τον εξής τρόπο:

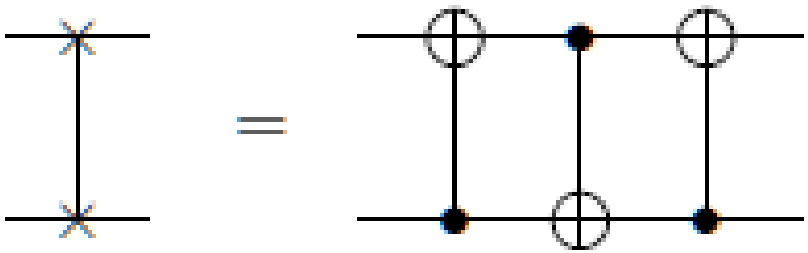


- Η πράξη NOT εκτελείται στο qubit στόχου, αν το qubit ελέγχου έχει τιμή 0.

Μοντέλο Κβαντικών Κυκλωμάτων

Παράδειγμα 2

- Η πύλη αντιστροφής (Swap gate) μπορεί να κατασκευαστεί με τον εξής τρόπο:

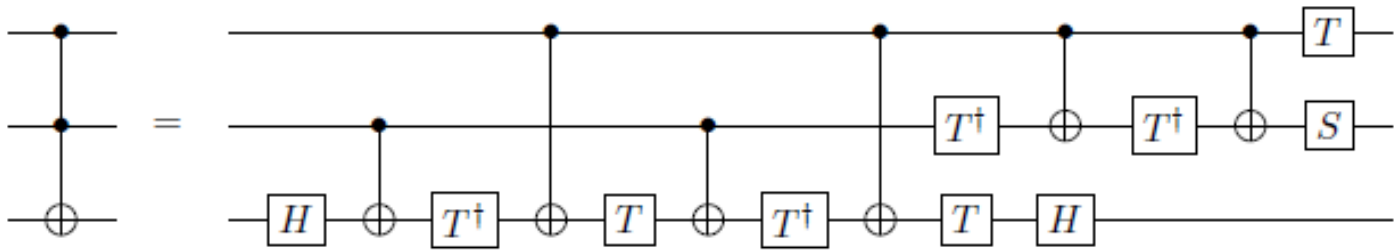


- Η πύλη αντιστροφής, αντιστρέφει τις τιμές των δύο qubits.

Μοντέλο Κβαντικών Κυκλωμάτων

Παράδειγμα 3

- Η πύλη controlled-controlled-NOT ή αλλιώς πύλη Toffoli κατασκευάζεται ως εξής:



- Η πύλη Toffoli εκτελεί την πράξη NOT στο qubit στόχου, αν και τα δύο qubit ελέγχου έχουν τιμή 1.

Κβαντικοί Αλγόριθμοι

- Γιατί να προτιμήσω έναν κβαντικό υπολογιστή;
- Υπάρχουν ενδείξεις ότι ένας κβαντικός υπολογιστής έχει μεγαλύτερη υπολογιστική ισχύ σε σχέση με τους κλασικούς.
- Δηλαδή, μπορεί να επιλύσει προβλήματα πιο *αποδοτικά* από έναν κλασικό.
- Δεν έχει αποδειχτεί ακόμα ότι ένας κβαντικός υπολογιστής είναι *γενικά* πιο ισχυρός από έναν κλασικό. Έχουν βρεθεί όμως αλγόριθμοι που επιλύουν συγκεκριμένα προβλήματα πιο αποδοτικά.

Κβαντικοί Αλγόριθμοι

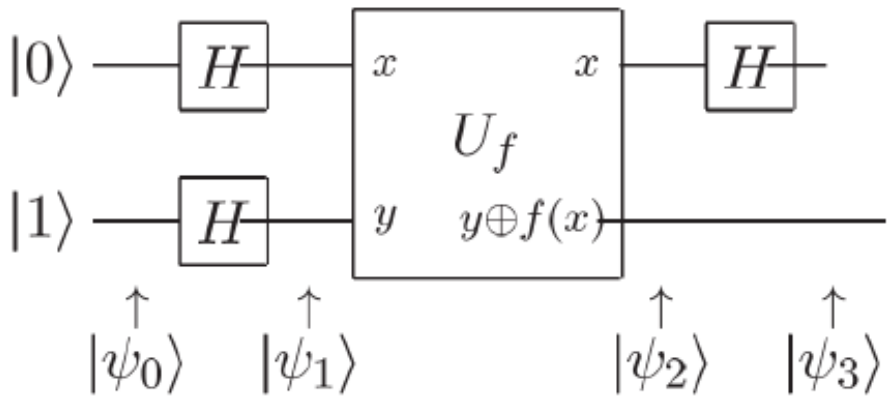
Γνωστοί αλγόριθμοι

- Αλγόριθμος Deutch
- Αναζήτηση στοιχείου σε σε μη ταξινομημένη λίστα (αλγόριθμος Grover)
- Παραγοντοποίηση αριθμού σε πρώτους αριθμούς (αλγόριθμος Shor)

Αλγόριθμος Deutch

- Ο αλγόριθμος Deutch είναι πολύ απλός και ίσως χωρίς κάποια πρακτική εφαρμογή, δείχνει όμως την υπεροχή των κβαντικών υπολογιστών έναντι των κλασικών.
- Το πρόβλημα που λύνει είναι το εξής: Έστω μια δυαδική συνάρτηση $f(x) : \{0, 1\} \mapsto \{0, 1\}$. Να υπολογίστεί αν η συνάρτηση είναι σταθερη ή όχι. Δηλαδή αν $f(0) = f(1)$ ή $f(0) \neq f(1)$.
- Ένας κλασικός υπολογιστής χρειάζεται προφανώς δύο υπολογισμούς της συνάρτησης. Μία για $f(0)$ και μία για $f(1)$.
- Με τον αλγόριθμο Deutch ένας κβαντικός υπολογιστής χρειάζεται μόνο έναν!

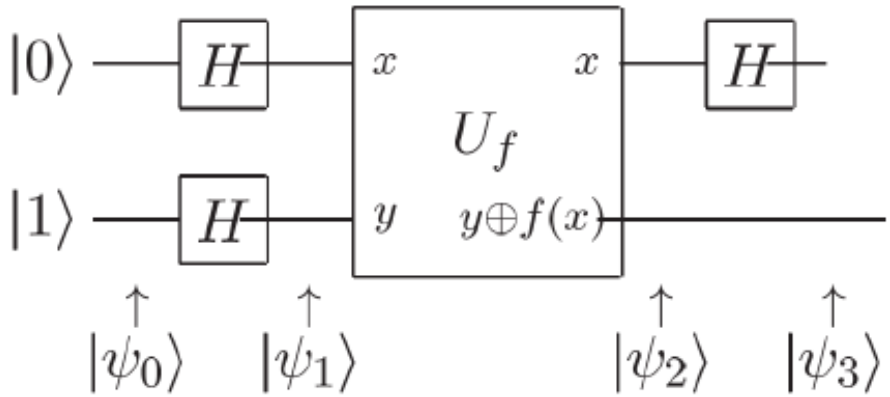
Αλγόριθμος Deutch



- Η κατάσταση εισόδου $|\psi_0\rangle = |01\rangle$ μετασχηματίζεται από τις πύλες Hadamard σε

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

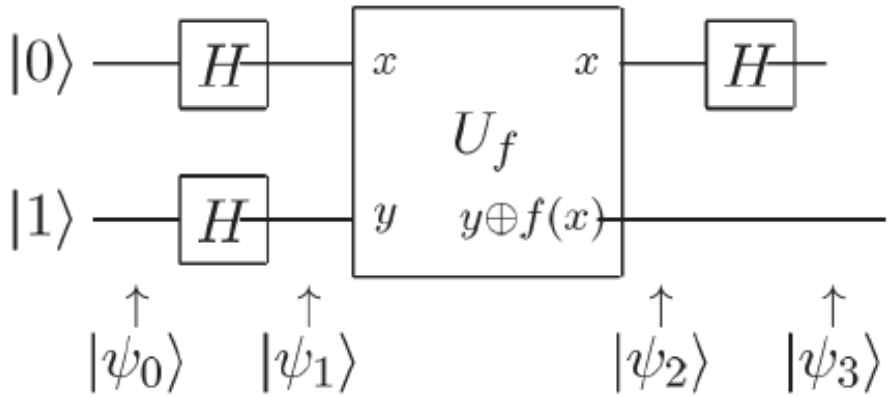
Αλγόριθμος Deutch



- Αν εκτελέσουμε την πύλη U_f τότε θα λάβουμε την κατάσταση $(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$. Δηλαδή, η εκτέλεση της U_f στην κατάσταση $|\psi_1\rangle$ αφήνει το κύκλωμα μας σε δύο πιθανές καταστάσεις:

$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{αν } f(0) = f(1) \\ \pm\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{αν } f(0) \neq f(1) \end{cases}$$

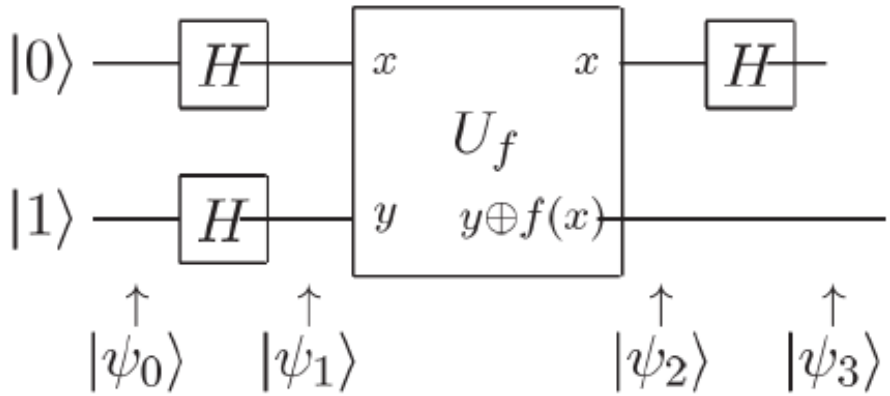
Αλγόριθμος Deutch



- Αν εκτελέσουμε την πύλη U_f τότε θα λάβουμε την κατάσταση $(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$. Δηλαδή, η εκτέλεση της U_f στην κατάσταση $|\psi_1\rangle$ αφήνει το κύκλωμα μας σε δύο πιθανές καταστάσεις:

$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{αν } f(0) = f(1) \\ \pm\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{αν } f(0) \neq f(1) \end{cases}$$

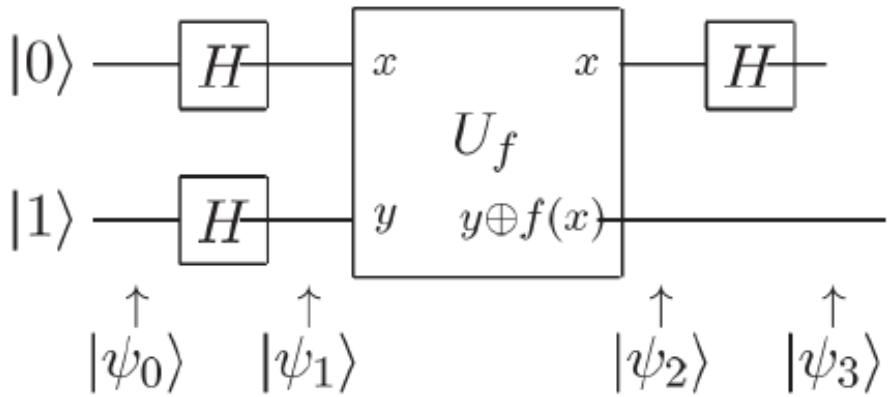
Αλγόριθμος Deutch



- Η τελευταία πύλη Hadamard αφήνει το κύκλωμα στην κατάσταση

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{αν } f(0) = f(1) \\ \pm|1\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{αν } f(0) \neq f(1) \end{cases} \quad (1)$$

Αλγόριθμος Deutch



- Αν λάβουμε υπόψη πως $f(0) \oplus f(1)$ ισούται με 0 αν $f(0) = f(1)$ ή 1 αν $f(0) \neq f(1)$, μπορούμε να γράψουμε το τελευταίο αποτέλεσμα ως

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

και άρα μετρώντας το πρώτο qubit να μάθουμε αν $f(0) \oplus f(1)$.

Κβαντική Παραλληλότητα

- Η δύναμη του αλγορίθμου Deutch έγκειται στις πύλες Hadamard που εκτελούνται στην αρχή.
- Αυτές οι πύλες φέρνουν το σύστημα σε κατάσταση πλήρους υπέρθεσης. Ο μετασχηματισμός αυτός ονομάζεται μετασχηματισμός Γουαλς-Χανταμαρντ (Walsh-Hadamard transform) και η ιδιότητα που προσδίδει *κβαντική παραλληλότητα* (quantum parallelism).
- Όπως και ο κβαντικός εναγκαλισμός, η κβαντική παραλληλότητα είναι μια μοναδική ιδιότητα των κβαντικών υπολογιστών και χρησιμοποιείται κατά κόρον στους κβαντικούς αλγορίθμους.

Αλγόριθμος Grover

- Ο αλγόριθμος Grover χρησιμοποιεί μια τεχνική που ονομάζεται *περιστροφή περί το μέσο* (inversion around average).
- Επιτυγχάνει την αναζήτηση ενός στοιχείου σε μια μη-ταξινομημένη λίστα μεγέθους n σε χρόνο $O(\sqrt{n})$.
- Σε έναν κλασικό υπολογιστή χρειαζόμαστε $O(n)$!

Αλγόριθμος Shor

- Ο αλγόριθμος Shor είναι ίσως ο πιο σημαντικός κβαντικός αλγόριθμος που έχει κατασκευαστεί μέχρι σήμερα.
- Επιτυγχάνει την παραγοντοποίηση αριθμού σε πρώτους αριθμούς, ένα πρόβλημα που θεωρείται $NP - complete$ και ο καλύτερος κλασικός αλγόριθμος χρειάζεται $e^{\Theta(n^{1/3}\log^{2/3}n)}$ για την παραγοντοποίηση ενός n-bit ακεραίου.
- Ο αλγόριθμος Shor λύνει το ίδιο πρόβλημα σε $O(n^2 \log n \log\log n)$!
- Εσωτερικά, χρησιμοποιεί διάφορες τεχνικές όπως ο κβαντικός μετασχηματισμός Fourier, εκτίμηση φάσης, κβαντική ύψωση σε εκθέτη modulo N, μερικές από τις οποίες υλοποιούνται πιο αποδοτικά σε κβαντικό υπολογιστή.

Κβαντικοί Αλγόριθμοι

- Γιατί δεν υπάρχουν πολλοί κβαντικοί αλγόριθμοι;
- Υπάρχουν δύο εμπόδια:
  1. Η φύση της κβαντικής μηχανικής κάνει την εύρεση αλγορίθμων δύσκολη για κάποιον που έχει "συνηθήσει" να σκέφτεται βάση της κλασικής μηχανικής.
  2. Δεν αρκεί να βρεθεί ένας αλγόριθμος. Πρέπει να είναι και πιο αποδοτικός απο τον αντίστοιχο κλασικό.

CoveX

- Το Cove Extended ή αλλιώς CoveX, είναι ένας εξομοιωτής κβαντικών κυκλωμάτων.
- Φιλοδοξεί να γίνει το πρώτο online εργαλείο για την μελέτη κβαντικών κυκλωμάτων.
- Χρησιμοποιεί το Cove Framework, μια βιβλιοθήκη γραμμένη σε C# από τον Matthew Purkeypile.
- Έχει υλοποιηθεί με την μηχανή ανάπτυξης παιχνιδιών Unity3d.

I think I can safely say that nobody understands quantum mechanics.

(Richard Feynman)

Ερωτήσεις

- Ερωτήσεις;