

3. Τελεστές και κβαντικές πύλες

Σύνοψη

Στο κεφάλαιο αυτό παρουσιάζονται οι κβαντικές πύλες ως τελεστές του χώρου Hilbert. Περιγράφονται οι κβαντικές πύλες που δρουν σε ένα qubit. Παρουσιάζονται επίσης οι κβαντικές πύλες που δρουν σε κβαντικούς καταχωρητές των δύο και των τριών qubits. Δίνεται η απόδειξη του θεωρήματος αδυναμίας αντιγραφής κβαντικής κατάστασης.

Προαπαιτούμενη γνώση

Γραμμική άλγεβρα, το πρώτο και το δεύτερο κεφάλαιο του βιβλίου αυτού.

3. 1 Οι κβαντικές πύλες ως τελεστές του χώρου Hilbert

Οι επεξεργαστές των κλασικών υπολογιστών αποτελούνται από αγωγούς και λογικές πύλες οι οποίες συγκροτούν κυκλώματα. Οι αγωγοί μεταφέρουν την πληροφορία με τη μορφή τάσης ή ρεύματος από πύλη σε πύλη. Οι λογικές πύλες επεξεργάζονται και μετατρέπουν την πληροφορία που έρχεται στην είσοδό τους, σύμφωνα με τον πίνακα αληθείας τους. Οι λογικές πύλες στους κλασικούς υπολογιστές είναι φυσικά συστήματα κατασκευασμένα από πυρίτιο και, σε όλους σχεδόν τους κλασικούς υπολογιστές, αποτελούνται από τρανζίστορες που ονομάζονται MOSFETs. Δηλαδή, οι πύλες των κλασικών υπολογιστών είναι φυσικά συστήματα και η πληροφορία διέρχεται από μέσα τους.

Αντίθετα, στους κβαντικούς υπολογιστές οι κβαντικές πύλες δεν είναι συνήθως φυσικά συστήματα, αλλά αντιπροσωπεύουν δράσεις που ασκούνται σε qubits ή σε κβαντικούς καταχωρητές. Οι δράσεις στα κβαντικά συστήματα αντιπροσωπεύονται από τελεστές του χώρου Hilbert που, όπως είδαμε, περιγράφονται από πίνακες (Kaye, Lafflamme & Mosca, 2007). Η δράση του Quant στο κβαντικό παιχνίδι που είδαμε στο πρώτο κεφάλαιο, είναι μία κβαντική πύλη και συγκεκριμένα η πύλη Hadamard, την οποία θα περιγράψουμε στο κεφάλαιο αυτό.

Μία άλλη σημαντική διαφορά είναι ότι η πληροφορία δεν διέρχεται μέσα από τις κβαντικές πύλες. Η πληροφορία βρίσκεται αποθηκευμένη σε qubits ή σε κβαντικούς καταχωρητές και παραμένει εκεί. Αυτό συμβαίνει σε όλες τις υλοποιήσεις στερεάς κατάστασης των κβαντικών κυκλωμάτων, όπως με παγίδες ιόντων ή με NMR. Τα qubits είναι σωματίδια που παραμένουν σταθερά στις θέσεις τους, όσο βέβαια τους το επιτρέπει η αρχή της απροσδιοριστίας. Όπως θα δούμε στο επόμενο κεφάλαιο, οι κβαντικές πύλες δρουν η μία μετά την άλλη στα qubits ή στους κβαντικούς καταχωρητές αλλάζοντας την κατάστασή τους. Οι κβαντικές πύλες είναι δηλαδή, δράσεις πάνω στα σωματίδια με μαγνητικά πεδία ή παλμούς laser. Θυμηθείτε ότι στο κβαντικό μας παιχνίδι το κβαντικό κέρμα που αντιπροσωπεύει το qubit ή τον κβαντικό καταχωρητή παραμένει στην ίδια θέση ενώ οι δύο παίκτες δρουν σε αυτό ο ένας μετά τον άλλο. Όπως θα δούμε, το παιχνίδι αυτό είναι ένας κβαντικός υπολογισμός, όπου το κβαντικό κέρμα αντιπροσωπεύει το qubit ή τον κβαντικό καταχωρητή και ο Quant τις κβαντικές πύλες.

Τώρα μπορούμε να ορίσουμε τις κβαντικές πύλες. Οι καταστάσεις των qubits και των κβαντικών καταχωρητών είναι διανύσματα στον χώρο Hilbert. Οι κβαντικές πύλες είναι τελεστές του χώρου Hilbert που δρουν σε qubits και σε κβαντικούς καταχωρητές αλλάζοντας την κατάστασή τους. Δηλαδή οι κβαντικές πύλες περιστρέφουν τα διανύσματα κατάστασής των qubits και των κβαντικών καταχωρητών χωρίς να αλλάζουν το μήκος τους, το οποίο είναι πάντα ίσο με τη μονάδα (Keyl 2002).

Όλοι οι τελεστές του χώρου Hilbert μπορούν να είναι κβαντικές πύλες; Όχι. Οι κβαντικές πύλες πρέπει να μην μεταβάλλουν το μήκος του διανύσματος κατάστασης και να μην μεταβάλουν τις τιμές των εσωτερικών γινομένων μεταξύ δύο διανυσμάτων κατάστασης. Για τον λόγο αυτό αντιπροσωπεύονται από ορθομοναδιαίους τελεστές και πίνακες. Έστω ότι έχουμε δύο διανύσματα κατάστασης, τα $|q_{R1}\rangle$ και $|q_{R2}\rangle$. Το εσωτερικό τους γινόμενο διατηρείται, όταν δρα σε αυτά ένας ορθομοναδιαίος τελεστής \hat{G} :

$$\langle q_{R2} | q_{R1} \rangle = \langle q_{R2} | G^\dagger G | q_{R1} \rangle = \langle q_{R2} | G^{-1} G | q_{R1} \rangle = \langle q_{R2} | q_{R1} \rangle \quad (3.1)$$

Παρακάτω θα περιγράψουμε τις κβαντικές πύλες και θα δούμε τα αποτελέσματα των δράσεών τους.

3. 2 Κβαντικές πύλες που δρουν σε ένα qubit

Εδώ θα ασχοληθούμε με κβαντικές πύλες που δρουν σε ένα μόνο qubit. Οι πύλες αυτές περιστρέφουν το διάνυσμα κατάστασης ενός qubit μέσα στη σφαίρα Bloch, δηλαδή μεταβάλλουν τις γωνίες θ και φ . Υπάρχουν άπειρες τέτοιες περιστροφές και επομένως, υπάρχουν άπειρες κβαντικές πύλες που δρουν σε ένα qubit. Δηλαδή, κάθε ορθομοναδιαίος τελεστής μπορεί να θεωρηθεί ως μία κβαντική πύλη που δρα σε ένα qubit. Υπάρχουν λοιπόν άπειρες κβαντικές πύλες που δρουν σε ένα qubit, όμως δεν χρησιμοποιούνται όλες. Χρησιμοποιούνται κυρίως τρεις πύλες οι οποίες έχουν ονομαστεί και θα τις δούμε αμέσως παρακάτω.

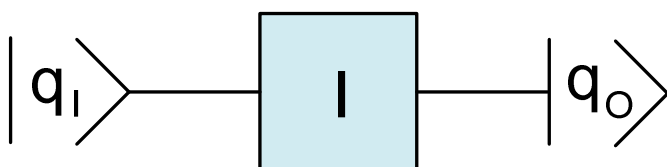
3.2.1 Η κβαντική πύλη αδρανείας

Η πύλη αδρανείας και συμβολίζεται με I και περιγράφεται από έναν τελεστή που ονομάζεται τελεστής αδρανείας. Ο πίνακας που αντιστοιχεί στον τελεστή της πύλης αυτής είναι:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (3.2)$$

Η κβαντική πύλη αδρανείας, αφήνει αμετάβλητη την κατάσταση του qubit:

$$I |q\rangle = |q\rangle \quad (3.3)$$



Σχήμα 3-1. Το σύμβολο της κβαντικής πύλης αδρανείας, I .

Στο Σχήμα 3-1 φαίνεται το σύμβολο της πύλης αδρανείας. Ο Πίνακας 3-1 δείχνει τη δράση της πύλης αυτής στις καταστάσεις ενός qubit:

$ q_i\rangle$	$ q_o\rangle$
$ 0\rangle$	$ 0\rangle$
$ 1\rangle$	$ 1\rangle$
$ q\rangle$	$ q\rangle$

Πίνακας 3-1. Η δράση της κβαντικής πύλης αδρανείας στις καταστάσεις ενός qubit.

Στην πρώτη στήλη του πίνακα φαίνονται οι καταστάσεις των qubits πριν τη δράση της πύλης και στη δεύτερη οι καταστάσεις μετά τη δράση της πύλης. Προσοχή στον συμβολισμό. Στο Σχήμα 3-1 η πληροφορία δεν διέρχεται μέσα από την πύλη, αλλά συμβολίζουμε με $|q_i\rangle$ την κατάσταση του qubit πριν τη δράση της πύλης και με $|q_o\rangle$ την κατάστασή του μετά τη δράση της πύλης.

3.2.2 Η Κβαντική πύλη μετατόπισης φάσης

Η κβαντική πύλη μετατόπισης φάσης περιγράφεται από έναν τελεστή που ονομάζεται Φ . Ο πίνακας που αντιστοιχεί στον τελεστή της πύλης αυτής είναι (Barenco, 1995):

$$\Phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix} \quad (3.4)$$

Ας δούμε τώρα το αποτέλεσμα της δράσης αυτής της πύλης σε ένα qubit. Έστω ένα qubit $|q_I\rangle$ του οποίου η κατάσταση δίνεται από:

$$|q_I\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \quad (3.5)$$

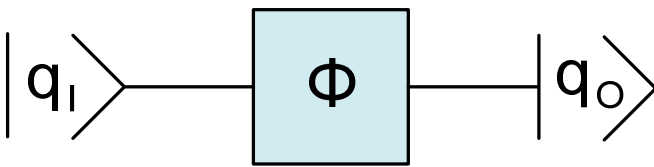
Η κβαντική πύλη μετατόπισης φάσης δρα σ' αυτό και αλλάζει την κατάστασή του σε $|q_O\rangle$. Ας υπολογίσουμε τη νέα αυτή κατάσταση:

$$|q_O\rangle = \Phi |q_I\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ e^{i\varphi} b \end{bmatrix} \quad (3.6)$$

Η νέα κατάσταση του qubit είναι:

$$|q_O\rangle = a|0\rangle + e^{i\varphi}b|1\rangle \quad (3.7)$$

Δηλαδή, η δράση της πύλης αυτής άλλαξε μόνο τη γωνία φάσης του qubit.



Σχήμα 3-2. Το σύμβολο της κβαντικής πύλης μετατόπισης φάσης, Φ .

Στο Σχήμα 3-2 φαίνεται το σύμβολο της πύλης Φ και στον Πίνακα 3-2 οι ιδιότητές της. Στην πρώτη στήλη του πίνακα φαίνονται οι καταστάσεις των qubits πριν τη δράση της πύλης ($|q_I\rangle$) και στη δεύτερη οι καταστάσεις μετά τη δράση της πύλης ($|q_O\rangle$).

$ q_I\rangle$	$ q_O\rangle$
$ 0\rangle$	$ 0\rangle$
$ 1\rangle$	$e^{i\varphi} 1\rangle$
$a 0\rangle + b 1\rangle$	$a 0\rangle + e^{i\varphi}b 1\rangle$

Πίνακας 3-2. Η δράση της κβαντικής πύλης μετατόπισης φάσης στις καταστάσεις ενός qubit.

3.2.3 Η κβαντική πύλη Hadamard

Η κβαντική πύλη Hadamard περιγράφεται από έναν τελεστή που ονομάζεται H . Ο πίνακας που αντιστοιχεί στον τελεστή της πύλης αυτής είναι:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (3.8)$$

Ας δούμε το αποτέλεσμα της δράσης αυτής της πύλης σε ένα qubit που βρίσκεται στη βασική κατάσταση $|0\rangle$:

$$H|0\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (3.9)$$

Ας δούμε και το αποτέλεσμα της δράσης αυτής της πύλης σε ένα qubit που βρίσκεται στη βασική κατάσταση $|1\rangle$:

$$H|1\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (3.10)$$

Δηλαδή, όταν η πύλη Hadamard δρα σε qubits που βρίσκονται σε μία από τις δύο βασικές καταστάσεις, τα θέτει σε μία κατάσταση που είναι υπέρθεση των βασικών καταστάσεων. Όταν ένα qubit βρίσκεται είτε στην κατάσταση που δίνεται από την (3.9) είτε στην κατάσταση που δίνεται από την (3.10), η πιθανότητα να μετρήσουμε και να το βρούμε στην βασική κατάσταση $|0\rangle$ είναι ίση με την πιθανότητα να το βρούμε στην βασική κατάσταση $|1\rangle$. Φυσικά και οι δύο πιθανότητες είναι ίσες με 0,5.

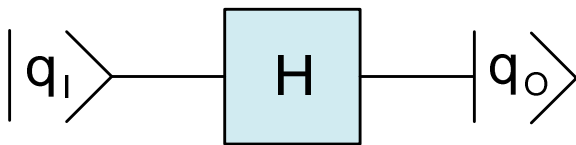
Ας δούμε τώρα τι αποτέλεσμα θα έχουμε αν η πύλη Hadamard δράσει σε ένα qubit που βρίσκεται στην υπέρθεση καταστάσεων που δίνεται από την (3.9):

$$H \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \quad (3.11)$$

Ας δούμε τη δράση της πύλης και στο qubit που βρίσκεται στην υπέρθεση καταστάσεων που δίνεται από την (3.10):

$$H \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle \quad (3.12)$$

Δηλαδή η πύλη Hadamard επιστρέφει τα qubits στις βασικές τους καταστάσεις.



Σχήμα 3-3. Το σύμβολο της κβαντικής πύλης Hadamard, H .

$ q_I\rangle$	$ q_O\rangle$
$ 0\rangle$	$\frac{1}{\sqrt{2}} (0\rangle + 1\rangle)$
$ 1\rangle$	$\frac{1}{\sqrt{2}} (0\rangle - 1\rangle)$
$\frac{1}{\sqrt{2}} (0\rangle + 1\rangle)$	$ 0\rangle$
$\frac{1}{\sqrt{2}} (0\rangle - 1\rangle)$	$ 1\rangle$

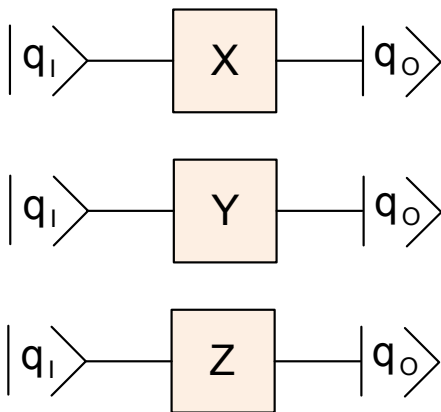
Πίνακας 3-3. Η δράση της κβαντικής Hadamard στις καταστάσεις ενός qubit.

Στο Σχήμα 3-3 φαίνεται το σύμβολο της πύλης H και στον Πίνακα 3-3 οι ιδιότητές της. Στην πρώτη στήλη του πίνακα φαίνονται οι καταστάσεις των qubits πριν τη δράση της πύλης ($|q_I\rangle$) και στη δεύτερη οι καταστάσεις μετά τη δράση της πύλης ($|q_O\rangle$).

Η πύλη Hadamard είναι πολύ σημαντική διότι μπορεί να μεταφέρει τα qubits από τις βασικές τους καταστάσεις (οι οποίες γίνονται αντιληπτές από εμάς), σε υπέρθεση καταστάσεων, που είναι χαρακτηριστικό μόνο των κβαντικών συστημάτων. Επίσης, μεταφέρει τα qubits από υπέρθεση καταστάσεων στις βασικές τους καταστάσεις. Αναμένεται ότι οι πύλες Hadamard θα αποτελέσουν το κύριο στοιχείο για τη διασύνδεση κλασικών και κβαντικών υπολογιστών.

3. 3 Κβαντικές πύλες Pauli

Μία πολύ σημαντική ομάδα κβαντικών πυλών που δρουν σε ένα qubit είναι οι κβαντικές πύλες Pauli. Αυτές οι κβαντικές πύλες είναι σημαντικές διότι κάθε δυνατή κβαντική πύλη του ενός qubit μπορεί να συντεθεί από έναν γραμμικό συνδυασμό των πυλών Pauli και της πύλης αδρανείας (Cybenko, 2001). Δηλαδή, με τις πύλες αυτές μπορούμε να εκτελέσουμε όλες τις περιστροφές του διανύσματος κατάστασης ενός qubit στη σφαίρα Bloch.



Σχήμα 3-4. Τα σύμβολα των κβαντικών πυλών Pauli.

	$ q_I\rangle$	$ q_O\rangle$
X	$a 0\rangle + b 1\rangle$	$b 0\rangle + a 1\rangle$
Y	$a 0\rangle + b 1\rangle$	$-ib 0\rangle + ia 1\rangle$
Z	$a 0\rangle + b 1\rangle$	$a 0\rangle - b 1\rangle$

Πίνακας 3-4. Οι δράσεις των κβαντικών πυλών Pauli στις καταστάσεις ενός qubit.

Οι κβαντικές πύλες Pauli συμβολίζονται με τα γράμματα X, Y και Z. Τα σύμβολα των πυλών αυτών φαίνονται στο Σχήμα 3-4. Οι πύλες Pauli περιγράφονται αντίστοιχα από τους τελεστές X, Y και Z στους οποίους αντιστοιχούν οι παρακάτω πίνακες:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (3.13)$$

Η δράση της πύλης X σε ένα qubit είναι:

$$X|q_I\rangle = X(a|0\rangle + b|1\rangle) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix} = b|0\rangle + a|1\rangle = |q_O\rangle \quad (3.14)$$

Η δράση της πύλης Y σε ένα qubit είναι:

$$Y|q_I\rangle = Y(a|0\rangle + b|1\rangle) = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} -ib \\ ia \end{bmatrix} = -ib|0\rangle + ia|1\rangle = |q_O\rangle \quad (3.15)$$

Η δράση της πύλης Z σε ένα qubit είναι:

$$Z|q_I\rangle = Z(a|0\rangle + b|1\rangle) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ -b \end{bmatrix} = a|0\rangle - b|1\rangle = |q_O\rangle \quad (3.16)$$

Οι ιδιότητες των κβαντικών πυλών Pauli φαίνονται συνοπτικά στον Πίνακα 3-4.

3. 4 Κβαντικές πύλες που δρουν σε δύο qubits

Εδώ θα περιγραφούν δύο κβαντικές πύλες που δρουν σε δύο qubits, η κβαντική πύλη ελεγχόμενου ΟΧΙ και η κβαντική πύλη ελεγχόμενης μετατόπισης φάσης. Μπορεί επίσης να θεωρηθεί ότι οι πύλες αυτές δρουν σε κβαντικούς καταχωρητές των δύο qubits.

3.4.1 Η κβαντική πύλη ελεγχόμενου ΟΧΙ

Η πύλη ελεγχόμενου ΟΧΙ δρα σε δύο qubits. Ο Αγγλικός όρος για την πύλη αυτή είναι Controlled-NOT και ο τελεστής που την περιγράφει συμβολίζεται με $CNOT$, από το αρχικό της λέξης controlled και το NOT.

Όπως είπαμε, η πύλη αυτή δρα σε δύο qubits, το ένα ονομάζεται qubit ελέγχου και συμβολίζεται με c και το άλλο qubit στόχος και συμβολίζεται με t . Οι καταστάσεις των δύο qubits πριν τη δράση της πύλης είναι $|c_i\rangle$ και $|t_i\rangle$. Οι καταστάσεις των qubits μετά τη δράση της πύλης είναι $|c_o\rangle$ και $|t_o\rangle$. Η πύλη $CNOT$ αλλάζει την κατάσταση του qubit στόχου, όταν η κατάσταση του qubit ελέγχου είναι $|1\rangle$, ενώ αφήνει την κατάσταση του qubit στόχου αναλλοίωτη, όταν η κατάσταση του qubit ελέγχου είναι $|0\rangle$. Η κατάσταση του qubit ελέγχου $|c_i\rangle$ δεν μεταβάλλεται, δηλαδή ισχύει πάντα $|c_i\rangle = |c_o\rangle$. Η πύλη $CNOT$ περιγράφεται από τον παρακάτω πίνακα:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad (3.17)$$

Ας δούμε τη δράση της πύλης αυτής σε έναν κβαντικό καταχωρητή που αποτελείται από δύο qubits. Η γενική περιγραφή της δράσης της πύλης είναι:

$$CNOT |c_i t_i\rangle = |c_o t_o\rangle \quad (3.18)$$

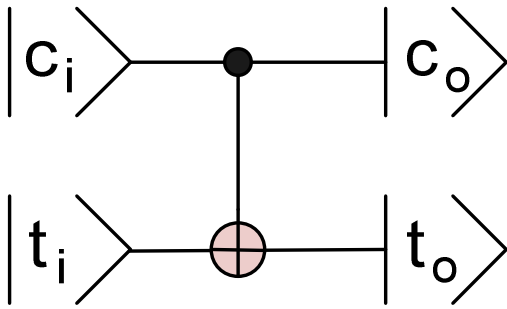
Έστω ότι η κατάσταση του κβαντικού καταχωρητή πριν τη δράση της πύλης είναι $|10\rangle$, τότε:

$$CNOT|10\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |11\rangle \quad (3.19)$$

Δηλαδή, η κατάσταση του qubit στόχου άλλαξε από $|0\rangle$ σε $|1\rangle$ διότι η κατάσταση του qubit ελέγχου είναι $|1\rangle$. Ας δούμε και την περίπτωση $|01\rangle$:

$$CNOT|01\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle \quad (3.20)$$

Αφού η κατάσταση του qubit ελέγχου είναι $|0\rangle$, η κατάσταση του qubit στόχου δεν αλλάζει. Με τον ίδιο τρόπο μπορούμε να δούμε και τις υπόλοιπες δύο περιπτώσεις.



Σχήμα 3-5. Το σύμβολο της κβαντικής πύλης ελεγχόμενου ΟΧΙ, $CNOT$.

$ c_i t_i\rangle$	$ c_o t_o\rangle$
$ 00\rangle$	$ 00\rangle$
$ 01\rangle$	$ 01\rangle$
$ 10\rangle$	$ 11\rangle$
$ 11\rangle$	$ 10\rangle$

Πίνακας 3-5. Η δράση της κβαντικής πύλης $CNOT$ στα qubits ελέγχου και στόχου.

Στο Σχήμα 3-5 φαίνονται το σύμβολο της πύλης $CNOT$ και στον Πίνακα 3-5 οι ιδιότητές της. Στην πρώτη στήλη του πίνακα φαίνονται οι καταστάσεις των δύο qubits πριν τη δράση της πύλης ($|c_i t_i\rangle$) και στη δεύτερη οι καταστάσεις τους μετά τη δράση της πύλης ($|c_o t_o\rangle$).

Κάτι πολύ σημαντικό: η πύλη $CNOT$ η πύλη H και η πύλη Φ αποτελούν ένα γενικευμένο σύνολο κβαντικών πυλών. Δηλαδή, μπορούμε να εκτελέσουμε οποιοδήποτε κβαντικό υπολογισμό χρησιμοποιώντας μόνο αυτές τις πύλες.

3.4.2 Η κβαντική πύλη ελεγχόμενης μετατόπισης φάσης

Η πύλη αυτή δρα σε δύο qubits. Στη βιβλιογραφία ο τελεστής της πύλης αυτής συμβολίζεται με διάφορους τρόπους, αλλά οι πιο συνηθισμένοι είναι οι S , CP και $C\Phi$. Εδώ θα χρησιμοποιήσουμε το $C\Phi$. Όπως και στην πύλη $CNOT$ το ένα qubit ονομάζεται qubit ελέγχου και συμβολίζεται με c και το άλλο qubit στόχος και συμβολίζεται με t . Με $|c_i\rangle$ και $|t_i\rangle$ συμβολίζονται οι καταστάσεις των δύο qubits πριν τη δράση της πύλης, και με $|c_o\rangle$ και $|t_o\rangle$ οι καταστάσεις των qubits μετά τη δράση της πύλης. Η πύλη $C\Phi$ πολλαπλασιάζει την κατάσταση του qubit στόχου με τον παράγοντα φάσης $e^{i\phi}$ μόνο όταν και η κατάσταση του qubit ελέγχου και η κατάσταση του qubit στόχου είναι $|1\rangle$. Σε όλες τις άλλες περιπτώσεις δεν μεταβάλλει τις καταστάσεις των qubits. Η πύλη $C\Phi$ περιγράφεται από τον παρακάτω πίνακα:

$$C\Phi = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{bmatrix} \quad (3.21)$$

Η γενική περιγραφή της δράσης της πύλης είναι:

$$C\Phi |c_i t_i\rangle = |c_o t_o\rangle \quad (3.22)$$

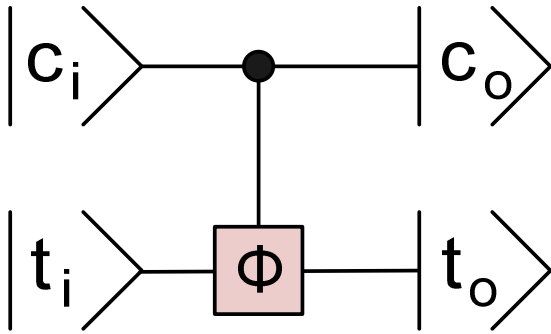
Ας δούμε τη δράση της πύλης στην κατάσταση ενός κβαντικού καταχωρητή που αποτελείται από δύο qubits. Έστω ότι η κατάσταση του κβαντικού καταχωρητή πριν τη δράση της πύλης είναι $|10\rangle$, τότε:

$$C\Phi |10\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle \quad (3.23)$$

Ας δούμε και την περίπτωση $|11\rangle$:

$$C\Phi |11\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ e^{i\phi} \end{bmatrix} = e^{i\phi} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = e^{i\phi} |11\rangle \quad (3.24)$$

Δηλαδή, αλλάζει η γωνία φάσης της κατάστασης $|11\rangle$. Με τον ίδιο τρόπο μπορούμε να υπολογίσουμε και τις άλλες δύο περιπτώσεις.



Σχήμα 3-6. Το σύμβολο της κβαντικής πύλης ελεγχόμενης μετατόπισης φάσης, $C\Phi$.

$ c_i t_i\rangle$	$ c_o t_o\rangle$
$ 00\rangle$	$ 00\rangle$
$ 01\rangle$	$ 01\rangle$
$ 10\rangle$	$ 10\rangle$
$ 11\rangle$	$e^{i\varphi} 11\rangle$

Πίνακας 3-6. Η δράση της κβαντικής πύλης $C\Phi$ στα qubits ελέγχου και στόχου.

Στο Σχήμα 3-6 φαίνεται το σύμβολο της πύλης $C\Phi$ και στον Πίνακα 3-6 οι ιδιότητές της. Στην πρώτη στήλη του πίνακα φαίνονται οι καταστάσεις των δύο qubits πριν τη δράση της πύλης ($|c_i t_i\rangle$) και στη δεύτερη οι καταστάσεις τους μετά τη δράση της πύλης ($|c_o t_o\rangle$).

3. 5 Κβαντικές πύλες που δρουν σε τρία qubits

Παρακάτω θα περιγραφούν δύο κβαντικές πύλες που δρουν σε τρία qubits, η κβαντική πύλη διπλά ελεγχόμενου OXI και η κβαντική πύλη Fredkin. Μπορεί επίσης να θεωρηθεί ότι οι πύλες αυτές δρουν σε κβαντικούς καταχωρητές των τριών qubits.

3.5.1 Η κβαντική πύλη διπλά ελεγχόμενου OXI

Ο Αγγλικός όρος για την πύλη αυτή είναι Controlled-Controlled-NOT και ο τελεστής που την περιγράφει συμβολίζεται με $CCNOT$. Η πύλη αυτή δρα σε τρία qubits. Τα δύο qubits ονομάζονται qubits ελέγχου, και συμβολίζονται με c_1 και c_2 και το άλλο qubit στόχος και συμβολίζεται με t . Οι καταστάσεις των τριών qubits πριν τη δράση της πύλης είναι $|c_{1i}\rangle$, $|c_{2i}\rangle$ και $|t_i\rangle$, ενώ οι καταστάσεις των qubits μετά τη δράση της πύλης είναι $|c_{1o}\rangle$, $|c_{2o}\rangle$ και $|t_o\rangle$. Η πύλη $CCNOT$ αλλάζει την κατάσταση του qubit στόχου, όταν και τα δύο qubits ελέγχου βρίσκονται στην κατάσταση $|1\rangle$, ενώ δεν αλλάζει την κατάσταση του qubit στόχου σε κάθε

άλλη περίπτωση. Οι καταστάσεις των qubits ελέγχου $|c_{1i}\rangle$ και $|c_{2i}\rangle$ δεν μεταβάλλονται, δηλαδή ισχύει πάντα $|c_{1i}\rangle = |c_{1o}\rangle$ και $|c_{2i}\rangle = |c_{2o}\rangle$.

Η πύλη $CCNOT$ περιγράφεται από τον παρακάτω πίνακα:

$$CCNOT = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad (3.25)$$

Η γενική περιγραφή της δράσης της πύλης είναι:

$$CCNOT |c_{2i} c_{1i} t_i\rangle = |c_{2o} c_{1o} t_o\rangle \quad (3.26)$$

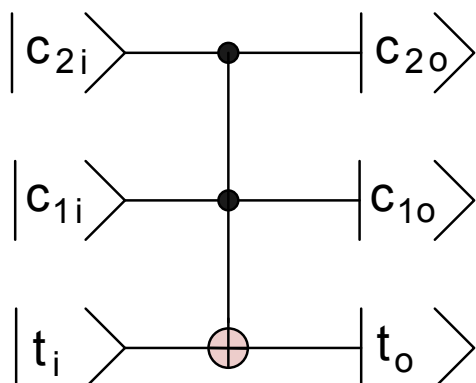
Ας δούμε τη δράση αυτής της πύλης σε έναν καταχωρητή που αποτελείται από τρία qubits. Έστω ότι η κατάσταση του κβαντικού καταχωρητή πριν τη δράση της πύλης είναι $|101\rangle$, τότε:

$$CCNOT |101\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |101\rangle \quad (3.27)$$

Ας δούμε και την περίπτωση που η κατάσταση του κβαντικού καταχωρητή πριν τη δράση της πύλης είναι $|111\rangle$:

$$CCNOT |111\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |110\rangle \quad (3.28)$$

Δηλαδή, η κατάσταση του qubit στόχου αλλάζει μόνο όταν και τα δύο qubits ελέγχου βρίσκονται στην κατάσταση $|1\rangle$. Με τον ίδιο τρόπο υπολογίζουμε και τις άλλες περιπτώσεις.



Σχήμα 3-7. Το σύμβολο και οι ιδιότητες της κβαντικής πύλης διπλά ελεγχόμενου OXI, CCNOT.

$ c_i t_{2i} t_{1i}\rangle$	$ c_o t_{2o} t_{1o}\rangle$
$ 000\rangle$	$ 000\rangle$
$ 001\rangle$	$ 001\rangle$
$ 010\rangle$	$ 010\rangle$
$ 011\rangle$	$ 011\rangle$
$ 100\rangle$	$ 100\rangle$
$ 101\rangle$	$ 110\rangle$
$ 110\rangle$	$ 101\rangle$
$ 111\rangle$	$ 111\rangle$

Πίνακας 3-7. Η δράση της κβαντικής πύλης CCNOT στα qubits ελέγχου και στόχου.

Στο Σχήμα 3-7 φαίνεται το σύμβολο της πύλης CCNOT και στον Πίνακα 3-7 οι ιδιότητές της. Στην πρώτη στήλη του πίνακα φαίνονται οι καταστάσεις των τριών qubits πριν τη δράση της πύλης ($|c_{2i} c_{1i} t_i\rangle$) και στη δεύτερη οι καταστάσεις τους μετά τη δράση της πύλης ($|c_{2o} c_{1o} t_o\rangle$).

3.5.2 Η κβαντική πύλη Fredkin

Η κβαντική πύλη Fredkin δρα σε τρία qubits και ο τελεστής της συμβολίζεται με F . Το ένα qubit ονομάζεται qubit ελέγχου, και συμβολίζεται με c , και τα άλλα δύο qubits ονομάζονται qubits στόχοι και συμβολίζονται με t_1 και t_2 . Οι καταστάσεις των τριών qubits πριν τη δράση της πύλης είναι $|c_i\rangle$, $|t_{1i}\rangle$ και $|t_{2i}\rangle$, ενώ οι καταστάσεις των qubits μετά τη δράση της πύλης είναι $|c_o\rangle$, $|t_{1o}\rangle$ και $|t_{2o}\rangle$. Η πύλη F εναλλάσσει τις καταστάσεις των qubits στόχων, όταν το qubit ελέγχου βρίσκεται στην κατάσταση $|1\rangle$. Όταν το qubit ελέγχου

βρίσκεται στην κατάσταση $|0\rangle$, οι καταστάσεις των qubits στόχων δεν αλλάζουν. Η κατάσταση του qubit ελέγχου $|c_i\rangle$ δεν μεταβάλλεται, δηλαδή ισχύει πάντα $|c_i\rangle = |c_o\rangle$.

Η πύλη F περιγράφεται από τον παρακάτω πίνακα:

$$F = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (3.29)$$

Η γενική περιγραφή της δράσης της πύλης είναι:

$$F |c_i t_{2i} t_{1i}\rangle = |c_o t_{2o} t_{1o}\rangle \quad (3.30)$$

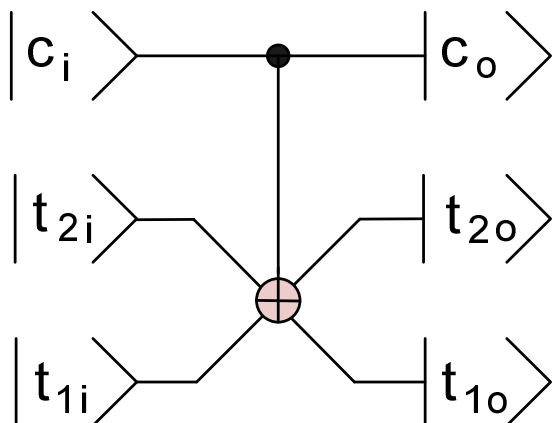
Ας δούμε τη δράση αυτής της πύλης F σε έναν καταχωρητή που αποτελείται από τρία qubits. Έστω ότι η κατάσταση του κβαντικού καταχωρητή πριν τη δράση της πύλης είναι $|001\rangle$, τότε:

$$F |001\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |001\rangle \quad (3.31)$$

Ας δούμε και την περίπτωση όπου η κατάσταση του κβαντικού καταχωρητή πριν τη δράση της πύλης είναι $|101\rangle$, τότε:

$$F |101\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |110\rangle \quad (3.32)$$

Δηλαδή οι καταστάσεις των qubits στόχων εναλλάχθηκαν διότι το qubit ελέγχου βρισκόταν στην κατάσταση $|1\rangle$. Με τον ίδιο τρόπο υπολογίζουμε και τις άλλες περιπτώσεις.



Σχήμα 3-8. Το σύμβολο και οι ιδιότητες της κβαντικής πύλης Fredkin, F .

$ c_i t_{2i} t_{1i}\rangle$	$ c_o t_{2o} t_{1o}\rangle$
$ 000\rangle$	$ 000\rangle$
$ 001\rangle$	$ 001\rangle$
$ 010\rangle$	$ 010\rangle$
$ 011\rangle$	$ 011\rangle$
$ 100\rangle$	$ 100\rangle$
$ 101\rangle$	$ 110\rangle$
$ 110\rangle$	$ 101\rangle$
$ 111\rangle$	$ 111\rangle$

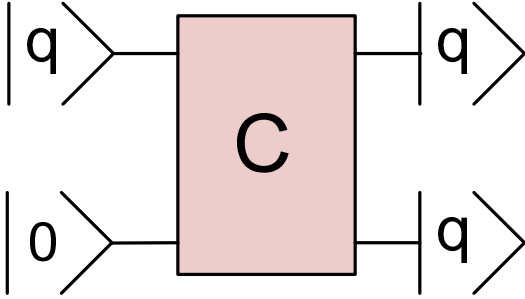
Πίνακας 3-8. Η δράση της κβαντικής πύλης Fredkin στα qubits ελέγχου και στόχου.

Στο Σχήμα 3-8 φαίνεται το σύμβολο της πύλης F και στον Πίνακα 3-8 οι ιδιότητές της. Στην πρώτη στήλη του πίνακα φαίνονται οι καταστάσεις των τριών qubits πριν τη δράση της πύλης ($|c_i t_{2i} t_{1i}\rangle$) και στη δεύτερη οι καταστάσεις τους μετά τη δράση της πύλης ($|c_o t_{2o} t_{1o}\rangle$).

3. 6 Η αδυναμία αντιγραφής της κατάστασης ενός qubit

Εδώ θα αναφερθούμε σε μία πύλη που δεν υπάρχει. Η διακλάδωση (cloning) ενός bit σε δύο ανεξάρτητα bits, δηλαδή η αντιγραφή ενός bit, είναι πάρα πολύ εύκολη στους κλασικούς υπολογιστές. Κάτι τέτοιο όμως

είναι αδύνατον στους κβαντικούς υπολογιστές, δηλαδή δεν μπορούμε να αντιγράψουμε την άγνωστη κατάσταση ενός qubit (Hirvensalo, 2001). Ας δούμε καλύτερα αυτή την αδυναμία.



Σχήμα 3-9. Η κατάσταση του άγνωστου qubit $|q\rangle$ διακλαδίζεται (αντιγράφεται) με τη δράση της κβαντικής πύλης C . Μια τέτοια πύλη είναι αδύνατον να υπάρξει.

Στο Σχήμα 3-9 φαίνεται μία κβαντική πύλη που τον τελεστή της τον ονομάσαμε C . Η πύλη αυτή δρα σε δύο qubits. Το ένα βρίσκεται στην κατάσταση $|0\rangle$ και το άλλο σε μία άγνωστη κατάσταση $|q\rangle$. Η κβαντική αυτή πύλη αλλάζει την κατάσταση του qubit που βρίσκεται στην κατάσταση $|0\rangle$, ώστε να γίνει ίδια με την κατάσταση $|q\rangle$. Μετά τη δράση της πύλης και τα δύο qubits βρίσκονται στην ίδια κατάσταση, δηλαδή η κατάσταση του $|q\rangle$ αντιγράφηκε στο qubit που είχε αρχικά την κατάσταση $|0\rangle$. Έχει αποδειχθεί ότι μια τέτοια πύλη είναι αδύνατον να υπάρξει. Αυτή η απόδειξη είναι γνωστή ως το θεώρημα αδυναμίας διακλάδωσης (στα Αγγλικά no-cloning theorem). Παρακάτω θα διατυπώσουμε και θα αποδείξουμε το θεώρημα αυτό.

Θεώρημα της αδυναμίας διακλάδωσης: Δεν μπορεί να υπάρξει μια κβαντική πύλη C τέτοια ώστε:

$$C |q 0\rangle = |q q\rangle \quad (3.33)$$

όπου $|q\rangle$ είναι ένα qubit με άγνωστη κατάσταση.

Απόδειξη: Υποθέτουμε ότι υπάρχει μία τέτοια κβαντική πύλη. Αυτή η κβαντική πύλη αντιπροσωπεύεται από τον ορθομοναδιαίο τελεστή \hat{C} . Βάζουμε την πύλη να δράσει σε δύο qubits το $|q\rangle$ και το $|b\rangle$ που είναι ορθογώνια μεταξύ τους και να τα αντιγράψει:

$$\hat{C} |q 0\rangle = |q q\rangle \quad (3.34)$$

$$\hat{C} |b 0\rangle = |b b\rangle$$

Θεωρούμε ένα άλλο qubit, το $|c\rangle$, η κατάσταση του οποίου είναι η υπέρθεση των καταστάσεων των δύο ορθογώνιων qubits $|q\rangle$ και $|b\rangle$:

Θεωρούμε τη γραμμική υπέρθεση των δύο qubits:

$$|c\rangle = \frac{1}{\sqrt{2}}(|q\rangle + |b\rangle) \quad (3.35)$$

Δρούμε τώρα με την κβαντική πύλη C στο qubit $|c\rangle$ αντιγράφοντας την κατάσταση του:

$$\begin{aligned} \hat{C}|c0\rangle &= \frac{1}{\sqrt{2}} \hat{C}(|q\rangle + |b\rangle)|0\rangle = \frac{1}{\sqrt{2}} \hat{C}(|q0\rangle + |b0\rangle) = \frac{1}{\sqrt{2}} \left(\hat{C}|q0\rangle + \hat{C}|b0\rangle \right) \\ &= \frac{1}{\sqrt{2}} (|qq\rangle + |bb\rangle) \end{aligned} \quad (3.36)$$

Αλλά πρέπει να ισχύει και:

$$\hat{C}|c0\rangle = |cc\rangle = |c\rangle|c\rangle = \frac{1}{\sqrt{2}}(|q\rangle + |b\rangle) \frac{1}{\sqrt{2}}(|q\rangle + |b\rangle) = \frac{1}{2}(|qq\rangle + |qb\rangle + |bq\rangle + |bb\rangle) \quad (3.37)$$

Οι εξισώσεις (3.36) και (3.37) έχουν τα αριστερά τους μέλη ίσα μεταξύ τους, όμως τα δεξιά τους μέλη είναι διαφορετικά, επομένως η κβαντική πύλη C δεν είναι δυνατόν να υπάρχει. ♦

Η αδυναμία διακλάδωσης, δηλαδή η αδυναμία αντιγραφής των qubits αποτελεί τη βάση της κβαντικής κρυπτογραφίας. Ας υποθέσουμε ότι η Αλίκη θέλει να στείλει στον Βασίλη ένα μήνυμα και το κωδικοποιεί σε qubits. Η Εύα θέλει να υποκλέψει το μήνυμα. Ακόμα και αν το μήνυμα βρεθεί στα χέρια της, δεν μπορεί να το αντιγράψει και να το αποκωδικοποιήσει. Αν το κρατήσει, τότε, για να το διαβάσει πρέπει να καταστρέψει την υπέρθεση των καταστάσεων των qubits. Δεν μπορεί δηλαδή να το διαβάσει και μετά να το στείλει στον Βασίλη. Ο Βασίλης δεν θα λάβει το μήνυμα και θα είναι σίγουρος ότι έχει υποκλαπεί και ότι η Εύα γνωρίζει το περιεχόμενό του, οπότε θα αλλάξει την τακτική ή τη στρατηγική του.

Ας συνοψίσουμε:

- Οι καταστάσεις των qubits και των κβαντικών καταχωρητών είναι διανύσματα στον χώρο Hilbert. Οι κβαντικές πύλες είναι ορθομοναδιαίοι τελεστές του χώρου Hilbert που δρουν σε qubits και σε κβαντικούς καταχωρητές αλλάζοντας την κατάσταση τους. Δηλαδή, οι κβαντικές πύλες περιστρέφουν τα διανύσματα κατάστασης των qubits και των κβαντικών καταχωρητών χωρίς να αλλάζουν το μήκος τους, το οποίο είναι πάντα ίσο με τη μονάδα.
- Οι κβαντικές πύλες που δρουν σε ένα qubit είναι η πύλη αδρανείας, I , η πύλη μετατόπισης φάσης, Φ και η πύλη Hadamard, H .
- Με τις κβαντικές πύλες Pauli μπορούμε να εκτελέσουμε όλες τις περιστροφές του διανύσματος κατάστασης ενός qubit στη σφαίρα Bloch.
- Οι κβαντικές πύλες που δρουν σε δύο qubits είναι η πύλη ελεγχόμενου OXI, $CNOT$ και η πύλη ελεγχόμενης μετατόπισης φάσης, $C\Phi$.
- Οι κβαντικές πύλες που δρουν σε τρία qubits είναι η πύλη διπλά ελεγχόμενου OXI, $CCNOT$ και η πύλη Fredkin, F .
- Η πύλη $CNOT$ η πύλη H και η πύλη Φ αποτελούν ένα γενικευμένο σύνολο κβαντικών πυλών. Δηλαδή μπορούμε να εκτελέσουμε οποιονδήποτε κβαντικό υπολογισμό χρησιμοποιώντας μόνο αυτές τις πύλες.
- Δεν μπορούμε να αντιγράψουμε την άγνωστη κατάσταση ενός qubit.

Βιβλιογραφία

- Barenco A., Bennett Ch. H., Cleve, R. et al., Elementary Gates for Quantum Computation, *Physical Review A*, vol. 52, pp. 3457-3467, 1995.
- Cybenko G., Reducing Quantum Computations to Elementary Unitary Operations, *IEEE Computers*, March/April issue, pp. 27-32, 2001.
- Hirvensalo M., *Quantum computing*, Springer-Verlag, 2001.
- Kaye P., Laflamme R., & Mosca M., *An introduction to quantum computing*, Oxford University Press, 2007.
- Keyl M., Fundamentals of Quantum Information Theory, *Physics Reports*, vol. 369, pp. 431-548, 2002.

Ασκήσεις

Άσκηση 3.1

Μία κβαντική πύλη που δρα σε ένα qubit, αλλά χρησιμοποιείται ελάχιστα είναι η πύλη \sqrt{NOT} . Η πύλη συμβολίζεται με $U_{\sqrt{NOT}}$ και περιγράφεται από τον πίνακα:

$$U_{\sqrt{NOT}} = \begin{bmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{bmatrix}$$

Να δείξετε ότι ο πίνακας αυτός είναι ορθομοναδιαίος.

Άσκηση 3.2

Να εφαρμόσετε την κβαντική πύλη $U_{\sqrt{NOT}}$ δύο φορές σε ένα qubit που βρίσκεται:

- α. Στη βασική κατάσταση $|0\rangle$
- β. Στη βασική κατάσταση $|1\rangle$

Άσκηση 3.3

Οι πίνακες:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

ονομάζονται πίνακες Pauli και είναι πολύ χρήσιμοι, γιατί μπορούμε με αυτούς να συνθέσουμε κβαντικές πύλες. (Να τους συγκρίνετε με τις κβαντικές πύλες Pauli). Να γράψετε την κβαντική πύλη H ως συνάρτηση των πινάκων Pauli πολλαπλασιασμένη επί έναν πραγματικό αριθμό.

Άσκηση 3.4

Υποθέστε ότι οι πίνακες Pauli περιγράφουν κβαντικές πύλες. Να υπολογίσετε τις δράσεις τους στις βασικές καταστάσεις του qubit. Δηλαδή να υπολογίσετε τα:

α. $\sigma_x |0\rangle$, β. $\sigma_x |1\rangle$

γ. $\sigma_y |0\rangle$, δ. $\sigma_y |1\rangle$

ε. $\sigma_z |0\rangle$, στ. $\sigma_z |1\rangle$

Άσκηση 3.5

Να υπολογίσετε τη δράση της κβαντικής πύλης $CNOT$ στις παρακάτω βασικές καταστάσεις:

α. $|00\rangle$

β. $|11\rangle$

Άσκηση 3.6

Να υπολογίσετε τη δράση της κβαντικής πύλης $C\Phi$ στη βασική κατάσταση $|01\rangle$:

Άσκηση 3.7

Να υπολογίσετε τη δράση της κβαντικής πύλης $CCNOT$ στις παρακάτω βασικές καταστάσεις:

α. $|011\rangle$

β. $|110\rangle$

Άσκηση 3.8

Να υπολογίσετε τη δράση της κβαντικής πύλης F στις παρακάτω βασικές καταστάσεις:

α. $|000\rangle$

β. $|110\rangle$

Άσκηση 3.9

Να υπολογίσετε τη δράση της κβαντικής πύλης H στο παρακάτω qubit που βρίσκεται σε υπέρθεση βασικών καταστάσεων:

$$|q\rangle = a|0\rangle + b|1\rangle$$

Άσκηση 3.10

Να υπολογίσετε τη δράση της κβαντικής πύλης $CNOT$ στο παρακάτω qubit που βρίσκεται σε υπέρθεση βασικών καταστάσεων:

$$|q\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle$$

Άσκηση 3.11

Να υπολογίσετε τη δράση της κβαντικής πύλης $C\Phi$ στο παρακάτω qubit που βρίσκεται σε υπέρθεση βασικών καταστάσεων:

$$|q\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle$$

Άσκηση 3.12

Να υπολογίσετε τη δράση της κβαντικής πύλης $CCNOT$ στο παρακάτω qubit που βρίσκεται σε υπέρθεση βασικών καταστάσεων:

$$|q\rangle = c_0|000\rangle + c_1|001\rangle + c_2|010\rangle + c_3|011\rangle + c_4|100\rangle + c_5|101\rangle + c_6|110\rangle + c_7|111\rangle$$

Άσκηση 3.13

Να υπολογίσετε τη δράση της κβαντικής πύλης F στο παρακάτω qubit που βρίσκεται σε υπέρθεση βασικών καταστάσεων:

$$|q\rangle = c_0|000\rangle + c_1|001\rangle + c_2|010\rangle + c_3|011\rangle + c_4|100\rangle + c_5|101\rangle + c_6|110\rangle + c_7|111\rangle$$