Κβαντικοί Υπολογιστές και Αλγόριθμοι

Διάλεξη 6η

Θωμάς Καμαλάκης

Χαροκόπειο Πανεπιστήμιο Αθηνών

2026

Περιεχόμενα

1 Ελεγχόμενες πύλες δύο qubit

2 Το θεώρημα μη κλωνοποίησης

3 Πύλες τριών qubit

Ελεγχόμενες πύλες

- Σε μια *ελεγχόμενη πύλη* ένα ή περισσότερα qubit παίζουν τον ρόλο του *ελέγχου* και άλλα τον ρόλο του *στόχου*
- Ανάλογα με την κατάσταση των qubit ελέγχου εφαρμόζεται ή όχι μια πύλη U στα qubit στόχου
- Π.χ. η U εφαρμόζεται μόνο όταν *όλα* τα n qubit ελέγχου είναι ταυτόχρονα $|1\rangle$, αλλιώς όλα τα qubit μένουν αμετάβλητα
- Συμβολισμός: $C_n^k(U)$ για την πύλη, $\hat{C}_n^k(\hat{U})$ για τον τελεστή και $\mathbf{C}_n^k(\mathbf{U})$ για τον πίνακα
- Η $\mathbf{C}_n^k(\mathbf{U})$ δρα σε $n+k$ qubit, άρα είναι $2^{n+k} \times 2^{n+k}$, ενώ η $\mathbf{U}$ δρα σε k qubit και είναι $2^k \times 2^k$
- Εδώ μελετάμε την απλούστερη περίπτωση $\hat{C}_1^1(\hat{U})$: ένα qubit ελέγχου και ένα στόχου

Παράδειγμα: η πύλη CNOT

- Η CNOT, $C_1^1(X)$: όταν το πρώτο qubit (έλεγχος) είναι $|1\rangle$, εφαρμόζεται η X στο δεύτερο

$$|00\rangle \to |00\rangle\,, \quad |01\rangle \to |01\rangle\,, \quad |10\rangle \to |11\rangle\,, \quad |11\rangle \to |10\rangle$$

- Με βάση $|\psi_1\rangle = |00\rangle$, $|\psi_2\rangle = |01\rangle$, $|\psi_3\rangle = |10\rangle$, $|\psi_4\rangle = |11\rangle$ τα στοιχεία είναι $c_{pq} = \left\langle \psi_p | \hat{C}_1^1(\hat{X}) | \psi_q \right\rangle$. Π.χ.

$$c_{34} = \langle \psi_3 | \psi_3 \rangle = 1$$

- Οι στήλες του πίνακα είναι οι συντεταγμένες των $\hat{C}\,|\psi_q\rangle$:

$$\mathbf{C}_1^1(\mathbf{X}) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

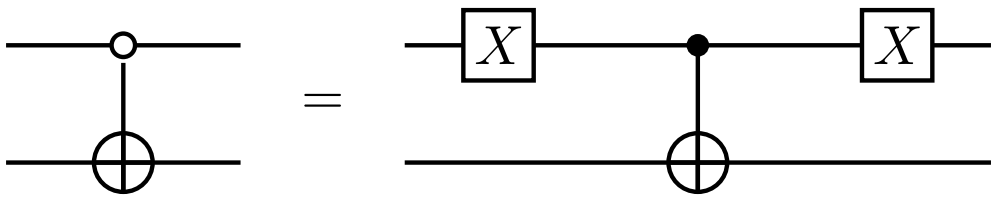
Σύμβολα στα κυκλώματα

- Η $\hat{C}_1^1(\hat{U})$: κουκκίδα • στο qubit ελέγχου, ενωμένη με κουτί U στο qubit στόχου
- Για την CNOT χρησιμοποιείται το σύμβολο $\oplus$, γιατί κάνει πρόσθεση modulo 2 (XOR) στο στόχο



Αντι-ελεγχόμενες πύλες

- Το άσπρο κυκλάκι ∘ σημαίνει ότι η πύλη ενεργοποιείται όταν ο έλεγχος είναι $|0\rangle$ (αντιστρόφως ελεγχόμενη πύλη), ενώ το μαύρο όταν είναι $|1\rangle$
- Ισοδύναμη με συνηθισμένη ελεγχόμενη πύλη, αν αντιστρέψουμε τον έλεγχο με X πριν και μετά:



- Αν ο έλεγχος είναι $|0\rangle$, η πρώτη X τον κάνει $|1\rangle$ και ενεργοποιεί την πύλη, και η δεύτερη τον επαναφέρει. Αν είναι $|1\rangle$, οι δύο X τον στέλνουν στο $|0\rangle$ και πίσω, χωρίς να ενεργοποιηθεί η πύλη

Παράδειγμα: η ελεγχόμενη Hadamard

- $\hat{C}_1^1(\hat{H})$: όταν $q_1 = 1$ εφαρμόζεται η H στο δεύτερο qubit
- Για $q_1 = 0$ δεν αλλάζει τίποτα: $\hat{C}\,|\psi_1\rangle = |\psi_1\rangle$, $\hat{C}\,|\psi_2\rangle = |\psi_2\rangle$
- Για $q_1 = 1$:

$$\hat{C}\,|\psi_3\rangle = |1\rangle \otimes \hat{H}\,|0\rangle = \frac{|\psi_3\rangle + |\psi_4\rangle}{\sqrt{2}}$$

$$\hat{C}\,|\psi_4\rangle = |1\rangle \otimes \hat{H}\,|1\rangle = \frac{|\psi_3\rangle - |\psi_4\rangle}{\sqrt{2}}$$

- Οι στήλες του πίνακα είναι οι συντεταγμένες αυτών των καταστάσεων:

$$\mathbf{C}_1^1(\mathbf{H}) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

Ο πίνακας κάθε ελεγχόμενης πύλης

- Στο τέλος του προηγούμενου παραδείγματος: πάνω αριστερά ο $\mathbf{I}_2$ (για $q_1 = 0$ δεν συμβαίνει τίποτα) και κάτω δεξιά ο $\mathbf{H}$
- Αυτό ισχύει για κάθε ελεγχόμενη πύλη. Αποτέλεσμα: για οποιαδήποτε πύλη ενός qubit με πίνακα $\mathbf{V}$,

$$\mathbf{C}_1^1(\mathbf{V}) = \begin{bmatrix} \mathbf{I}_2 & \mathbf{0} \\ \mathbf{0} & \mathbf{V} \end{bmatrix}$$

  όπου κάθε στοιχείο είναι 2×2 πίνακας
- Το qubit στόχος μένει αμετάβλητο όταν $q_1 = 0$ (πρώτη γραμμή τεταρτημορίων) και υφίσταται την $\mathbf{V}$ όταν $q_1 = 1$ (δεύτερη)

Παράδειγμα: ελεγχόμενη καθολική φάση

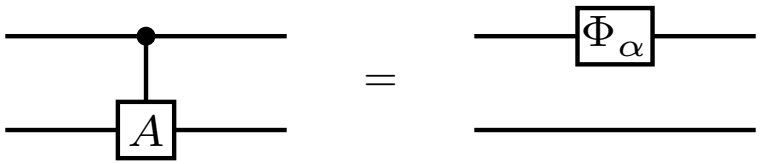
- Η $\mathbf{A} = \mathrm{e}^{j\alpha}\mathbf{I}_2$ δεν έχει από μόνη της φυσική συνέπεια. Η ελεγχόμενη εκδοχή της:

$$\mathbf{C}_1^1(\mathbf{A}) = \begin{bmatrix} \mathbf{I}_2 & \mathbf{0} \\ \mathbf{0} & \mathrm{e}^{j\alpha}\mathbf{I}_2 \end{bmatrix}$$

- Με $\Phi_\alpha = \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{e}^{j\alpha} \end{bmatrix}$ μόνο στο πρώτο qubit:

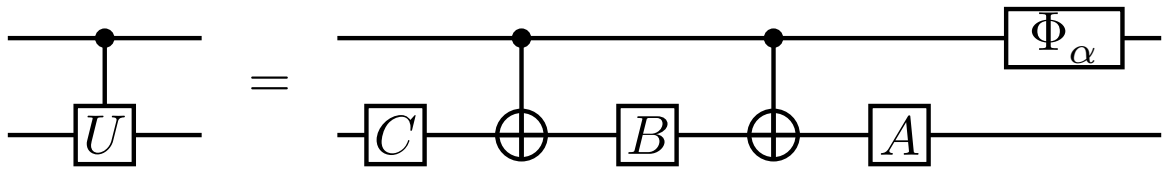
$$\Phi_\alpha \otimes \mathbf{I}_2 = \begin{bmatrix} \mathbf{I}_2 & \mathbf{0} \\ \mathbf{0} & \mathrm{e}^{j\alpha}\mathbf{I}_2 \end{bmatrix}$$

- Άρα ισοδυναμία κυκλωμάτων (ελεγχόμενη, η καθολική φάση γίνεται σχετική φάση του qubit ελέγχου):



Ελεγχόμενη πύλη οποιασδήποτε U με CNOT (1/2)

- Από την $\mathbf{U} = \mathrm{e}^{j\alpha}\mathbf{AXBXC}$ και την ελεγχόμενη φάση, η $\hat{C}_1^1(\hat{U})$ οποιασδήποτε πύλης ενός qubit κατασκευάζεται μόνο με CNOT και πύλες ενός qubit A, B, C, Φ_α:



- Έλεγχος $|0\rangle$: καμία CNOT δεν ενεργοποιείται, το στόχος δίνει $\mathbf{ABC}\,|\psi\rangle = |\psi\rangle$ και $\hat{\Phi}_\alpha\,|0\rangle = |0\rangle$: όπως η $\hat{C}_1^1(\hat{U})$ για $q_1 = 0$

Ελεγχόμενη πύλη οποιασδήποτε U με CNOT (2/2)

- Έλεγχος $|1\rangle$: ενεργοποιούνται και οι δύο CNOT, άρα

$$|\phi\rangle = \mathbf{AXBXC}\,|\psi\rangle = \mathrm{e}^{-j\alpha}\mathbf{U}\,|\psi\rangle$$

  δηλαδή η **U** με «λανθασμένη» καθολική φάση $\mathrm{e}^{-j\alpha}$

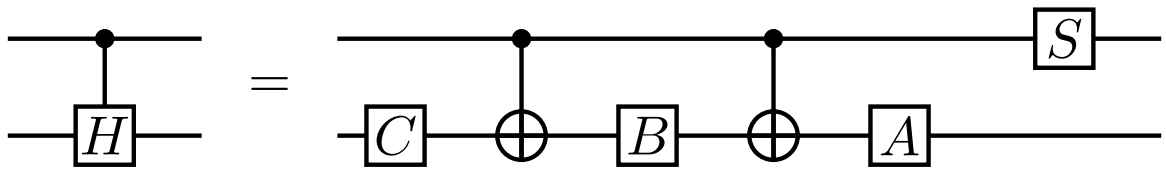
- Η Φ_α δίνει στον έλεγχο την ελλείπουσα φάση, αφού $\hat{\Phi}_\alpha\,|1\rangle = \mathrm{e}^{j\alpha}\,|1\rangle$. Για την ολική κατάσταση:

$$|1\rangle\,|\psi\rangle \xrightarrow{AXBXC} |1\rangle \otimes \left(\mathrm{e}^{-j\alpha}\mathbf{U}\,|\psi\rangle\right) \xrightarrow{\Phi_\alpha} \mathbf{U}\,|\psi\rangle \text{ με } |1\rangle$$

- Δύο CNOT και οι τέσσερις πύλες ενός qubit A, B, C, Φ_α αρκούν για την $C_1^1(U)$ οποιασδήποτε πύλης U ενός qubit

Παράδειγμα: η ελεγχόμενη Hadamard μέσω CNOT

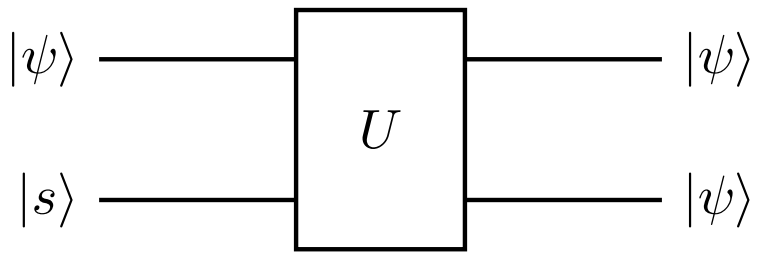
- Για $U = H$: $\alpha = \frac{\pi}{2}$ και οι πίνακες $\mathbf{A} = -\mathbf{R}_y(\frac{\pi}{4})$, $\mathbf{B} = \mathbf{R}_y(-\frac{\pi}{4})\mathbf{R}_z(-\frac{\pi}{2})$, $\mathbf{C} = -\mathbf{R}_z(\frac{\pi}{2})$ από το παράδειγμα της διάλεξης 5
- Η φάση: $\Phi_{\pi/2} = \begin{bmatrix} 1 & 0 \\ 0 & j \end{bmatrix} = \mathbf{S}$
- Κύκλωμα:



- Δύο CNOT, οι A, B, C στο στόχο και μια S στον έλεγχο

Αντιγραφή πληροφορίας

- Στα κλασικά κυκλώματα αντιγράφουμε εύκολα ένα bit: αν το δεύτερο bit είναι αρχικά 0,
$$b_1, 0 \xrightarrow{\text{COPY}} b_1, b_1$$
- Υλοποιείται με μια πύλη XOR: $b_1 \oplus 0 = b_1$
- Στα κβαντικά κυκλώματα δεν υπάρχει αντίστοιχο: δεν μπορούμε να αντιγράψουμε (κλωνοποιήσει) ένα qubit σε γενική κατάσταση $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$
- Αυτό είναι το *θεώρημα μη κλωνοποίησης*



Απόδειξη με απαγωγή σε άτοπο (1/4)

- Υποθέτουμε μοναδιαίο τελεστή $\hat{U}$ σε δύο qubit που αντιγράφει κάθε κατάσταση, με το δεύτερο qubit να ξεκινά πάντα από την ίδια κατάσταση $|s\rangle$:
$$\hat{U}(|\psi\rangle\,|s\rangle) = |\psi\rangle\,|\psi\rangle$$
- Ο ίδιος $\hat{U}$ πρέπει να δουλεύει για όλα τα $|\psi\rangle$, χωρίς να ξέρουμε ποιο είναι. Αν ξέραμε ότι είναι μία από δύο γνωστές καταστάσεις, θα μπορούσαμε απλά να το μετρήσουμε
- Για δύο διαφορετικές καταστάσεις $|\psi_1\rangle \neq |\psi_2\rangle$:
$$\hat{U}(|\psi_1\rangle\,|s\rangle) = |\psi_1\rangle\,|\psi_1\rangle\,, \qquad \hat{U}(|\psi_2\rangle\,|s\rangle) = |\psi_2\rangle\,|\psi_2\rangle$$

Απόδειξη με απαγωγή σε άτοπο (2/4)

- Εσωτερικό γινόμενο των αριστερών μελών, με $\hat{U}^{\mathrm{T}}\hat{U} = \hat{I}$ και $\langle s|s\rangle = 1$:

$$(\langle\psi_1|\langle s|)\hat{U}^{\mathrm{T}}\hat{U}(|\psi_2\rangle|s\rangle) = \langle\psi_1|\psi_2\rangle$$

- Το ίδιο, υπολογισμένο μέσω των δεξιών μελών:

$$(\langle\psi_1|\langle\psi_1|)(|\psi_2\rangle|\psi_2\rangle) = \langle\psi_1|\psi_2\rangle^2$$

- Εξισώνοντας: $\langle\psi_1|\psi_2\rangle = \langle\psi_1|\psi_2\rangle^2$
- Με $x = \langle\psi_1|\psi_2\rangle$ γράφεται $x(x-1) = 0$, άρα $x = 0$ ή $x = 1$

Απόδειξη με απαγωγή σε άτοπο (3/4)

- Το $x = 1$ αποκλείεται όταν $|\psi_1\rangle \neq |\psi_2\rangle$. Γράφουμε $|\psi_1\rangle = \sum_i a_i |\phi_i\rangle$, $|\psi_2\rangle = \sum_i b_i |\phi_i\rangle$
- Από $|a_i - b_i|^2 = |a_i|^2 + |b_i|^2 - a_i b_i^* - a_i^* b_i$:

$$\sum_i |a_i - b_i|^2 = \langle\psi_1|\psi_1\rangle + \langle\psi_2|\psi_2\rangle$$

$$- \langle\psi_1|\psi_2\rangle - \langle\psi_2|\psi_1\rangle$$

- Με κανονικοποιημένες καταστάσεις και $\langle\psi_1|\psi_2\rangle = 1$:

$$\sum_i |a_i - b_i|^2 = 1 + 1 - 1 - 1 = 0$$

- Άρα $a_i = b_i$ και $|\psi_1\rangle = |\psi_2\rangle$, άτοπο

Απόδειξη με απαγωγή σε άτοπο (4/4)

- Μένει $\langle\psi_1|\psi_2\rangle = 0$: ο $\hat{U}$ αντιγράφει δύο διαφορετικές καταστάσεις *μόνο αν* είναι κάθετες
- Αυτό δεν μπορεί να ισχύει για *κάθε* ζευγάρι καταστάσεων, όπως απαιτεί η υπόθεση. Π.χ. οι $|0\rangle$ και $|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ είναι διαφορετικές αλλά όχι κάθετες:

$$\langle 0| + x\rangle = \frac{1}{\sqrt{2}} \neq 0$$

- Καταλήγουμε σε άτοπο: δεν υπάρχει μοναδιαίος τελεστής $\hat{U}$ που να αντιγράφει κάθε δυνατή κατάσταση qubit

Παράδειγμα: η CNOT δεν αντιγράφει την $|+x\rangle$

- Η CNOT αντιγράφει σωστά τις $|0\rangle, |1\rangle$: $|00\rangle \to |00\rangle, |10\rangle \to |11\rangle$
- Για την $|+x\rangle$:
$$|+x\rangle |0\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |01\rangle$$
- Εφαρμόζοντας την CNOT σε κάθε όρο ($|00\rangle \to |00\rangle, |01\rangle \to |11\rangle$):
$$\hat{C}_1(\hat{X}) |+x\rangle |0\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$$
- Αν αντέγραφε σωστά, θα έπρεπε να πάρουμε
$$|+x\rangle |+x\rangle = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$
- Δεν ταυτίζονται: η έξοδος δεν γράφεται καν ως γινόμενο δύο μονο-qubit καταστάσεων

Θεώρημα μη κλωνοποίησης

- Δεν υπάρχει μοναδιαίος τελεστής $\hat{U}$ σε δύο qubit που να ικανοποιεί

$$\hat{U}(|\psi\rangle\,|s\rangle) = |\psi\rangle\,|\psi\rangle$$

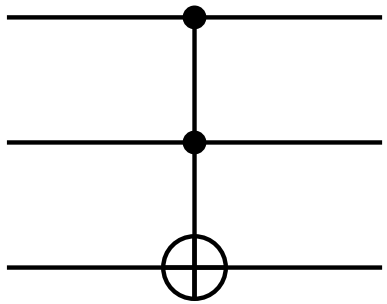
για κάθε δυνατή κατάσταση $|\psi\rangle$ ενός qubit, όπου $|s\rangle$ σταθερή αρχική κατάσταση

- Καμία φυσική διεργασία δεν μπορεί να αντιγράψει μια αυθαίρετη άγνωστη κβαντική κατάσταση

Η πύλη Toffoli

- Δύο qubit ελέγχου q_1, q_2 και ένα qubit στόχος q_3, που αντιστρέφεται μόνο όταν $q_1 = q_2 = 1$. Λέγεται και CCNOT, συμβολίζεται $\hat{C}_2^1(\hat{X})$:

$$\hat{C}_2^1(\hat{X})\,|q_1 q_2 q_3\rangle = \begin{cases} |q_1 q_2 q_3\rangle\,, & q_1 q_2 \neq 1 \\ |q_1 q_2 \bar{q}_3\rangle\,, & q_1 q_2 = 1 \end{cases}$$



Παράδειγμα: ο πίνακας της Toffoli

- Βάση $|\psi_1\rangle = |000\rangle, \ldots, |\psi_8\rangle = |111\rangle$. Στις πρώτες έξι ένας τουλάχιστον έλεγχος είναι $|0\rangle$, άρα $\hat{C}|\psi_p\rangle = |\psi_p\rangle$
- Στις $|110\rangle, |111\rangle$ και οι δύο έλεγχοι είναι $|1\rangle$:

$$\hat{C}|\psi_7\rangle = |\psi_8\rangle, \qquad \hat{C}|\psi_8\rangle = |\psi_7\rangle$$

- Οι στήλες του πίνακα είναι οι συντεταγμένες αυτών των καταστάσεων:

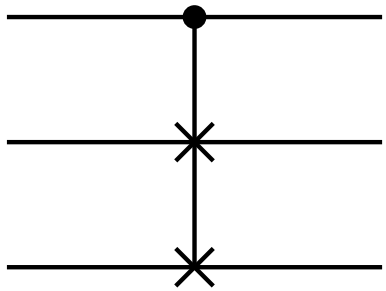
$$\mathbf{C}_2^1(\mathbf{X}) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

- Ταυτοτικός, εκτός από το κάτω δεξιά τεταρτημόριο 2×2 που είναι ο $\mathbf{X}$, όπως στο αποτέλεσμα για $\mathbf{C}_1^1(\mathbf{V})$

Η πύλη Fredkin

- Ελεγχόμενη SWAP, $\hat{C}_1^2(\hat{S}_W)$: ένα qubit ελέγχου και δύο στόχοι, που ανταλλάσσουν καταστάσεις *μόνο* όταν $q_1 = 1$ (με SWAP $|ab\rangle = |ba\rangle$):

$$\hat{C}_1^2(\hat{S}_W)\,|q_1 q_2 q_3\rangle = \begin{cases} |q_1 q_2 q_3\rangle\,, & q_1 = 0 \\ |q_1 q_3 q_2\rangle\,, & q_1 = 1 \end{cases}$$



Παράδειγμα: ο πίνακας της Fredkin

- Για $q_1 = 0$ ($|\psi_1\rangle, \ldots, |\psi_4\rangle$) δεν αλλάζει τίποτα. Για $q_1 = 1$ ανταλλάσσονται τα δύο τελευταία qubit: οι $|100\rangle$, $|111\rangle$ μένουν ίδιες, ενώ

$$\hat{C}\,|\psi_6\rangle = |\psi_7\rangle\,, \qquad \hat{C}\,|\psi_7\rangle = |\psi_6\rangle$$

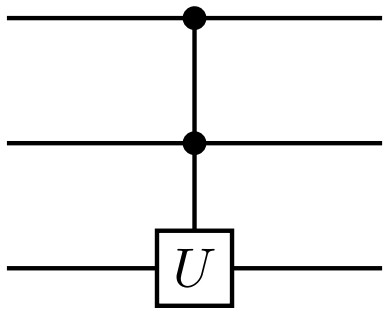
- Ο πίνακας 8×8 είναι ο $\mathbf{C}_1^2(\mathbf{S}_W) = \begin{bmatrix} \mathbf{I}_4 & \mathbf{0} \\ \mathbf{0} & \mathbf{S}_W \end{bmatrix}$, όπου η $\mathbf{S}_W$ είναι ο πίνακας της SWAP:

$$\mathbf{S}_W = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Η ελεγχόμενη πύλη με δύο ελέγχους $C_2^1(U)$

- Εφαρμόζει μια πύλη U ενός qubit στο q_3 μόνο όταν $q_1 = q_2 = 1$:

$$\hat{C}_2^1(\hat{U})\,|q_1 q_2 q_3\rangle = \begin{cases} |q_1 q_2 q_3\rangle\,, & q_1 q_2 \neq 1 \\ |q_1 q_2\rangle \otimes \hat{U}\,|q_3\rangle\,, & q_1 q_2 = 1 \end{cases}$$



- Η Toffoli είναι η ειδική περίπτωση $\mathbf{U = X}$
- Θα την κατασκευάσουμε μόνο από CNOT και ελεγχόμενες πύλες με έναν έλεγχο

Κατασκευή της $C_2^1(U)$: η τετραγωνική ρίζα V

- Πρώτο βήμα: ένας πίνακας $\mathbf{V}$ με $\mathbf{V}^2 = \mathbf{U}$
- Γράφουμε $\mathbf{U} = \mathrm{e}^{j\alpha}\mathbf{R_n}(\theta)$ και επιλέγουμε

$$\mathbf{V} = \mathrm{e}^{j\alpha/2}\mathbf{R_n}\left(\tfrac{\theta}{2}\right)$$

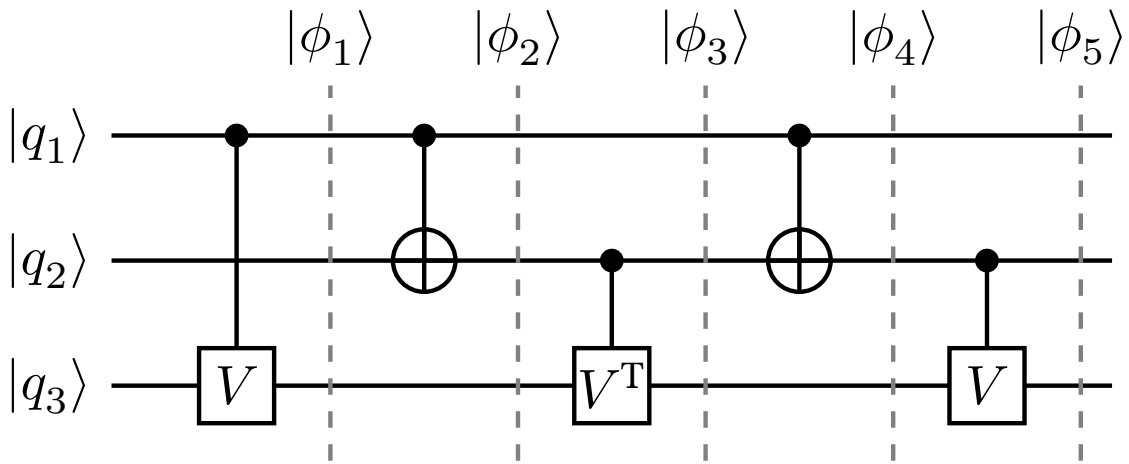
- Αφού $\mathbf{R_n}(\theta_1)\mathbf{R_n}(\theta_2) = \mathbf{R_n}(\theta_1 + \theta_2)$:

$$\mathbf{V}^2 = \mathrm{e}^{j\alpha}\mathbf{R_n}(\theta) = \mathbf{U}$$

- Ο $\mathbf{V}$ είναι μοναδιαίος, άρα $\mathbf{V}^{\mathrm{T}} = \mathbf{V}^{-1}$

Το κύκλωμα της $C_2^1(U)$

- Πέντε πύλες, με πέντε σημεία παρακολούθησης $|\phi_1\rangle \ldots |\phi_5\rangle$ (ακριβώς μετά από κάθε πύλη):



- Είσοδος $|q_1\rangle\,|q_2\rangle\,|q_3\rangle$ με $q_i \in \{0,1\}$. Γράφουμε $\mathbf{V}^q$ για τον $\mathbf{V}$ $(q=1)$ ή τον $\mathbf{I}_2$ $(q=0)$
- Η CNOT δίνει στο στόχο $|q_1 \oplus q_2\rangle$, με $\oplus$ το XOR

Ενδιάμεσες καταστάσεις (1/2)

- Πρώτη πύλη, $C_1^1(V)$ με έλεγχο το q_1:

$$|\phi_1\rangle = |q_1\rangle\,|q_2\rangle \otimes \mathbf{V}^{q_1}\,|q_3\rangle$$

- Δεύτερη, CNOT από το πρώτο στο δεύτερο:

$$|\phi_2\rangle = |q_1\rangle\,|q_1 \oplus q_2\rangle \otimes \mathbf{V}^{q_1}\,|q_3\rangle$$

- Τρίτη, $C_1^1(V^{\mathrm{T}})$ με έλεγχο το δεύτερο qubit, που είναι τώρα $|q_1 \oplus q_2\rangle$:

$$|\phi_3\rangle = |q_1\rangle\,|q_1 \oplus q_2\rangle \otimes (\mathbf{V}^{\mathrm{T}})^{q_1 \oplus q_2}\mathbf{V}^{q_1}\,|q_3\rangle$$

Ενδιάμεσες καταστάσεις (2/2)

- Τέταρτη, η ίδια CNOT. Αφού $q_1 \oplus (q_1 \oplus q_2) = q_2$, το δεύτερο qubit επανέρχεται:

$$|\phi_4\rangle = |q_1\rangle\,|q_2\rangle \otimes (\mathbf{V}^{\mathrm{T}})^{q_1 \oplus q_2}\mathbf{V}^{q_1}\,|q_3\rangle$$

- Πέμπτη, $C_1^1(V)$ με έλεγχο το q_2:

$$|\phi_5\rangle = |q_1\rangle\,|q_2\rangle \otimes \mathbf{V}^{q_2}(\mathbf{V}^{\mathrm{T}})^{q_1 \oplus q_2}\mathbf{V}^{q_1}\,|q_3\rangle$$

- Με $\mathbf{V}^{\mathrm{T}} = \mathbf{V}^{-1}$ οι εκθέτες προστίθενται:

$$\mathbf{V}^{q_2}\mathbf{V}^{-(q_1 \oplus q_2)}\mathbf{V}^{q_1} = \mathbf{V}^{m}, \qquad m = q_1 + q_2 - (q_1 \oplus q_2)$$

Το αποτέλεσμα του κυκλώματος

- Ο εκθέτης m για όλους τους συνδυασμούς:

q_1	q_2	$q_1 \oplus q_2$	m
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	2

- $m = 0$ εκτός από $q_1 = q_2 = 1$ όπου $m = 2$, και $\mathbf{V}^0 = \mathbf{I}_2$, $\mathbf{V}^2 = \mathbf{U}$:

$$|\phi_5\rangle = \begin{cases} |q_1 q_2 q_3\rangle\,, & q_1 q_2 \neq 1 \\ |q_1 q_2\rangle \otimes \hat{U}\,|q_3\rangle\,, & q_1 q_2 = 1 \end{cases}$$

- Αυτό είναι ακριβώς η $\hat{C}_2^1(\hat{U})$

Παράδειγμα: η Toffoli από πύλες με έναν έλεγχο (1/3)

- Για $\mathbf{U} = \mathbf{X}$ χρειαζόμαστε $\mathbf{V}^2 = \mathbf{X}$. Από $\mathbf{R}_x(\pi) = -j\mathbf{X}$:

$$\mathbf{X} = \mathrm{e}^{j\pi/2}\mathbf{R}_x(\pi) \quad \Rightarrow \quad \mathbf{V} = \mathrm{e}^{j\pi/4}\mathbf{R}_x\left(\tfrac{\pi}{2}\right)$$

- Με $\mathbf{R}_x(\frac{\pi}{2}) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -j \\ -j & 1 \end{bmatrix}$ και $\mathrm{e}^{j\pi/4} = \frac{1+j}{\sqrt{2}}$:

$$\mathbf{V} = \frac{1}{2}\begin{bmatrix} 1+j & 1-j \\ 1-j & 1+j \end{bmatrix}, \qquad \mathbf{V}^{\mathrm{T}} = \frac{1}{2}\begin{bmatrix} 1-j & 1+j \\ 1+j & 1-j \end{bmatrix}$$

Παράδειγμα: η Toffoli από πύλες με έναν έλεγχο (2/3)

- Έλεγχος ότι $\mathbf{V}^2 = \mathbf{X}$, με $(1+j)^2 = 2j$, $(1-j)^2 = -2j$, $(1+j)(1-j) = 2$:

$$\mathbf{V}^2 = \frac{1}{4}\begin{bmatrix} (1+j)^2 + (1-j)^2 & 2(1+j)(1-j) \\ 2(1+j)(1-j) & (1-j)^2 + (1+j)^2 \end{bmatrix}$$

$$= \frac{1}{4}\begin{bmatrix} 0 & 4 \\ 4 & 0 \end{bmatrix} = \mathbf{X}$$

- Ο $\mathbf{V}$ λέγεται και τετραγωνική ρίζα της NOT
- Η δράση του στην $|0\rangle$ (πρώτη στήλη):

$$\mathbf{V}|0\rangle = \tfrac{1}{2}\left((1+j)|0\rangle + (1-j)|1\rangle\right)$$

Παράδειγμα: η Toffoli από πύλες με έναν έλεγχο (3/3)

- Είσοδος $|110\rangle$ (*πρέπει να γίνει* $|111\rangle$): η CNOT *κάνει το δεύτερο qubit* $|0\rangle$, η V^{T} *δεν ενεργοποιείται*

$$|\phi_1\rangle = |11\rangle \otimes \mathbf{V}|0\rangle\,, \quad |\phi_2\rangle = |\phi_3\rangle = |10\rangle \otimes \mathbf{V}|0\rangle\,, \quad |\phi_4\rangle = |11\rangle \otimes \mathbf{V}|0\rangle$$

$$|\phi_5\rangle = |11\rangle \otimes \mathbf{V}\mathbf{V}|0\rangle = |11\rangle \otimes \mathbf{X}|0\rangle = |111\rangle$$

- Είσοδος $|100\rangle$ (*πρέπει να μείνει ίδια*): η CNOT *κάνει το δεύτερο qubit* $|1\rangle$, η V^{T} *ακυρώνει την πρώτη* V

$$|\phi_1\rangle = |10\rangle \otimes \mathbf{V}|0\rangle\,, \quad |\phi_2\rangle = |11\rangle \otimes \mathbf{V}|0\rangle\,, \quad |\phi_3\rangle = |11\rangle \otimes \mathbf{V}^{\mathrm{T}}\mathbf{V}|0\rangle = |110\rangle$$

$$|\phi_4\rangle = |100\rangle\,, \qquad |\phi_5\rangle = |100\rangle$$

- Η *τελευταία* V *δεν ενεργοποιείται, αφού το δεύτερο qubit επανήλθε στο* $|0\rangle$

Παράδειγμα: η $C_2^1(H)$

- Για $\mathbf{U} = \mathbf{H} = \mathrm{e}^{j\pi/2}\mathbf{R_n}(\pi)$ με $\mathbf{n} = \frac{1}{\sqrt{2}}(1,0,1)$ (αφού $\mathbf{A} = \mathbf{H}$):

$$\mathbf{V} = \mathrm{e}^{j\pi/4}\mathbf{R_n}\left(\tfrac{\pi}{2}\right) = \frac{1+j}{2}\left(\mathbf{I}_2 - j\mathbf{H}\right)$$

- Έλεγχος με $\mathbf{H}^2 = \mathbf{I}_2$, χωρίς στοιχεία πινάκων:

$$\left(\tfrac{1+j}{2}\right)^2 = \tfrac{j}{2}, \quad (\mathbf{I}_2 - j\mathbf{H})^2 = \mathbf{I}_2 - 2j\mathbf{H} - \mathbf{I}_2 = -2j\mathbf{H}$$

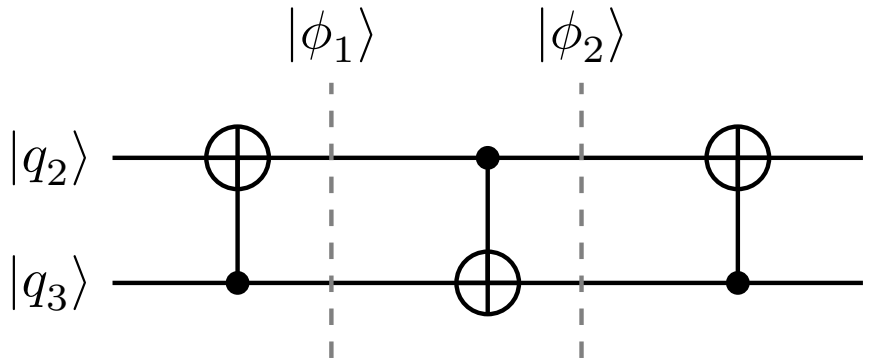
$$\mathbf{V}^2 = \tfrac{j}{2}\cdot(-2j\mathbf{H}) = \mathbf{H}$$

- Ο $\mathbf{V}^\mathrm{T} = \frac{1-j}{2}(\mathbf{I}_2 + j\mathbf{H})$ και το ίδιο κύκλωμα με την Toffoli δίνει για είσοδο $|110\rangle$:

$$|\phi_5\rangle = |11\rangle \otimes \mathbf{V}^2\,|0\rangle = |11\rangle \otimes \mathbf{H}\,|0\rangle = |11\rangle\,|+x\rangle$$

Παράδειγμα: η SWAP από τρεις CNOT

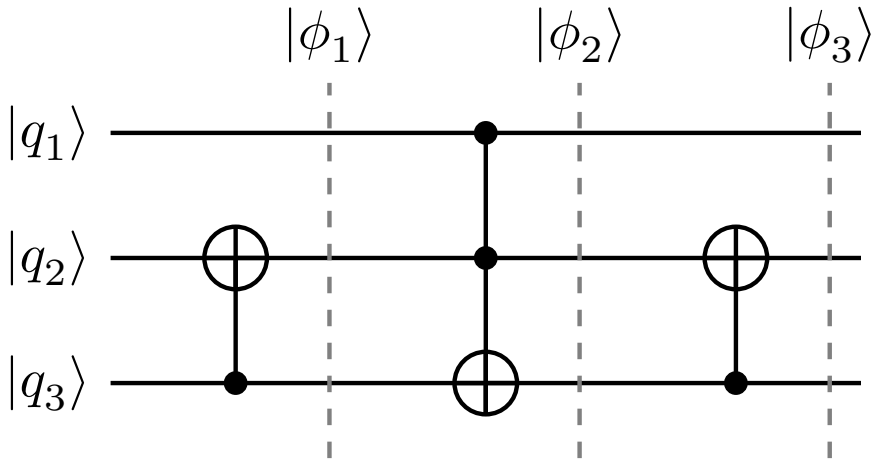
- Δύο qubit $|q_2\rangle\,|q_3\rangle$, με CNOT εναλλάξ προς τις δύο κατευθύνσεις και $\oplus$ το XOR ($x \oplus 0 = x$, $x \oplus x = 0$):



- $|\phi_1\rangle = |q_2 \oplus q_3\rangle\,|q_3\rangle$,
  $|\phi_2\rangle = |q_2 \oplus q_3\rangle\,|q_3 \oplus (q_2 \oplus q_3)\rangle = |q_2 \oplus q_3\rangle\,|q_2\rangle$
- Τρίτη CNOT: $|(q_2 \oplus q_3) \oplus q_2\rangle = |q_3\rangle$. Έξοδος $|q_3\rangle\,|q_2\rangle$

Παράδειγμα: η Fredkin από δύο CNOT και μία Toffoli

- Η μεσαία CNOT της SWAP γίνεται Toffoli με πρόσθετο έλεγχο το q_1:



- Η Toffoli δίνει $|t\rangle \to |t \oplus c_1 c_2\rangle$. Το q_1 δεν αλλάζει:

$$|\phi_1\rangle = |q_1\rangle\,|q_2 \oplus q_3\rangle\,|q_3\rangle$$

$$|\phi_2\rangle = |q_1\rangle\,|q_2 \oplus q_3\rangle\,|q_3 \oplus q_1(q_2 \oplus q_3)\rangle$$

Fredkin από Toffoli: οι δύο περιπτώσεις

- $q_1 = 0$: το γινόμενο $q_1(q_2 \oplus q_3)$ είναι 0, η Toffoli δεν κάνει τίποτα και οι δύο CNOT αναιρούνται:

$$|\phi_3\rangle = |0\rangle\,|(q_2 \oplus q_3) \oplus q_3\rangle\,|q_3\rangle = |0\rangle\,|q_2\rangle\,|q_3\rangle$$

- $q_1 = 1$: το γινόμενο είναι $q_2 \oplus q_3$, η Toffoli δρα σαν τη μεσαία CNOT της SWAP:

$$|\phi_2\rangle = |1\rangle\,|q_2 \oplus q_3\rangle\,|q_2\rangle\,, \qquad |\phi_3\rangle = |1\rangle\,|q_3\rangle\,|q_2\rangle$$

- Άρα η έξοδος είναι ακριβώς ο ορισμός της Fredkin
- Έλεγχος για $|101\rangle$ (πρέπει να δώσει $|110\rangle$):

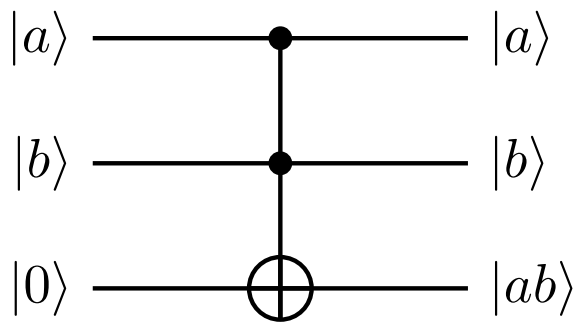
$$|\phi_1\rangle = |111\rangle\,, \quad |\phi_2\rangle = |1\rangle\,|1\rangle\,|1 \oplus 1 \cdot 1\rangle = |110\rangle\,, \quad |\phi_3\rangle = |110\rangle$$

Παράδειγμα: το κβαντικό AND (1/2)

- Θέλουμε το ab από δύο qubit $|a\rangle, |b\rangle$. Κύκλωμα δύο qubit εισόδου και ενός εξόδου είναι αδύνατο: ο $\hat{U}$ είναι τετραγωνικός πίνακας
- Η αντικατάσταση $|a\rangle |b\rangle \to |a\rangle |ab\rangle$ δεν είναι αντιστρέψιμη:

$$|0\rangle |0\rangle \to |0\rangle |0\rangle, \qquad |0\rangle |1\rangle \to |0\rangle |0\rangle$$

  ενώ ο μοναδιαίος τελεστής είναι πάντα αντιστρέψιμος
- Λύση: τρίτο, βοηθητικό (ancilla) qubit στην $|0\rangle$, ως στόχος Toffoli:



Παράδειγμα: το κβαντικό AND (2/2)

- Η Toffoli στέλνει $|t\rangle \to |t \oplus c_1 c_2\rangle$, άρα με $t = 0$:

$$|a\rangle\,|b\rangle\,|0\rangle \to |a\rangle\,|b\rangle\,|0 \oplus ab\rangle = |a\rangle\,|b\rangle\,|ab\rangle$$

a	b	είσοδος	έξοδος
0	0	$\|000\rangle$	$\|000\rangle$
0	1	$\|010\rangle$	$\|010\rangle$
1	0	$\|100\rangle$	$\|100\rangle$
1	1	$\|110\rangle$	$\|111\rangle$

- Το τρίτο qubit είναι $|1\rangle$ μόνο όταν $a = b = 1$. Τα $|a\rangle\,, |b\rangle$ διατηρούνται, γι' αυτό το κύκλωμα είναι αντιστρέψιμο

Παράδειγμα: το κβαντικό OR (1/2)

- Το OR $a + b$ $(1 + 1 = 1)$ από τον νόμο De Morgan:

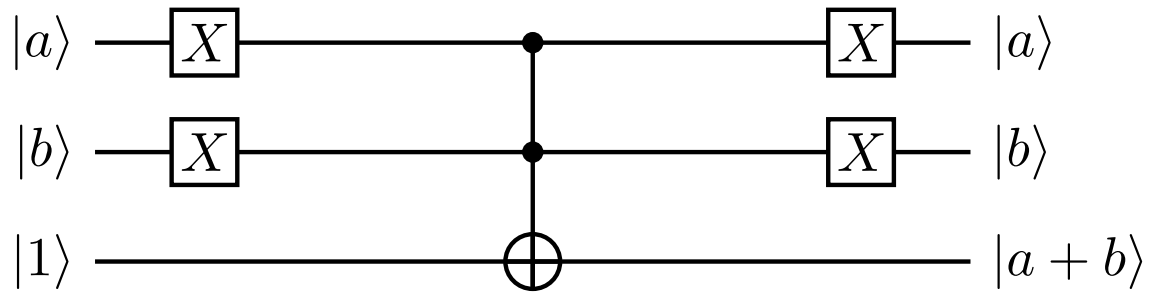
$$a + b = \overline{\overline{a}\,\overline{b}}$$

δηλαδή AND των $\overline{a}, \overline{b}$ και αντιστροφή. Πίνακας αλήθειας:

a	b	$\overline{a}$	$\overline{b}$	$\overline{a}\,\overline{b}$	$\overline{\overline{a}\,\overline{b}}$
0	0	1	1	1	0
0	1	1	0	0	1
1	0	0	1	0	1
1	1	0	0	0	1

Παράδειγμα: το κβαντικό OR (2/2)

- Βοηθητικό qubit στην $|1\rangle$. Δύο X, Toffoli, και πάλι δύο X:



- Μετά τις πρώτες X: $|\phi_1\rangle = |\overline{a}\rangle\,|\overline{b}\rangle\,|1\rangle$. Η Toffoli, με $1 \oplus x = \overline{x}$ και De Morgan:

$$|\phi_2\rangle = |\overline{a}\rangle\,|\overline{b}\rangle\,|1 \oplus \overline{a}\,\overline{b}\rangle = |\overline{a}\rangle\,|\overline{b}\rangle\,|a+b\rangle$$

- Οι τελευταίες X επαναφέρουν τα δύο πρώτα: $|\phi_3\rangle = |a\rangle\,|b\rangle\,|a+b\rangle$

Παράδειγμα: έλεγχος του OR

- $a = b = 0$ (πρέπει $a + b = 0$):

$$|\phi_1\rangle = |111\rangle\,, \quad |\phi_2\rangle = |11\rangle\,|1 \oplus 1 \cdot 1\rangle = |110\rangle\,, \quad |\phi_3\rangle = |000\rangle$$

- $a = 1, b = 0$ (πρέπει $a + b = 1$):

$$|\phi_1\rangle = |011\rangle\,, \quad |\phi_2\rangle = |01\rangle\,|1 \oplus 0 \cdot 1\rangle = |011\rangle\,, \quad |\phi_3\rangle = |101\rangle$$

- Και στις δύο περιπτώσεις το τρίτο qubit δίνει το σωστό αποτέλεσμα και τα δύο πρώτα qubit επανέρχονται