Κβαντικοί Υπολογιστές και Αλγόριθμοι

Διάλεξη 7η

Θωμάς Καμαλάκης

Χαροκόπειο Πανεπιστήμιο Αθηνών

2026

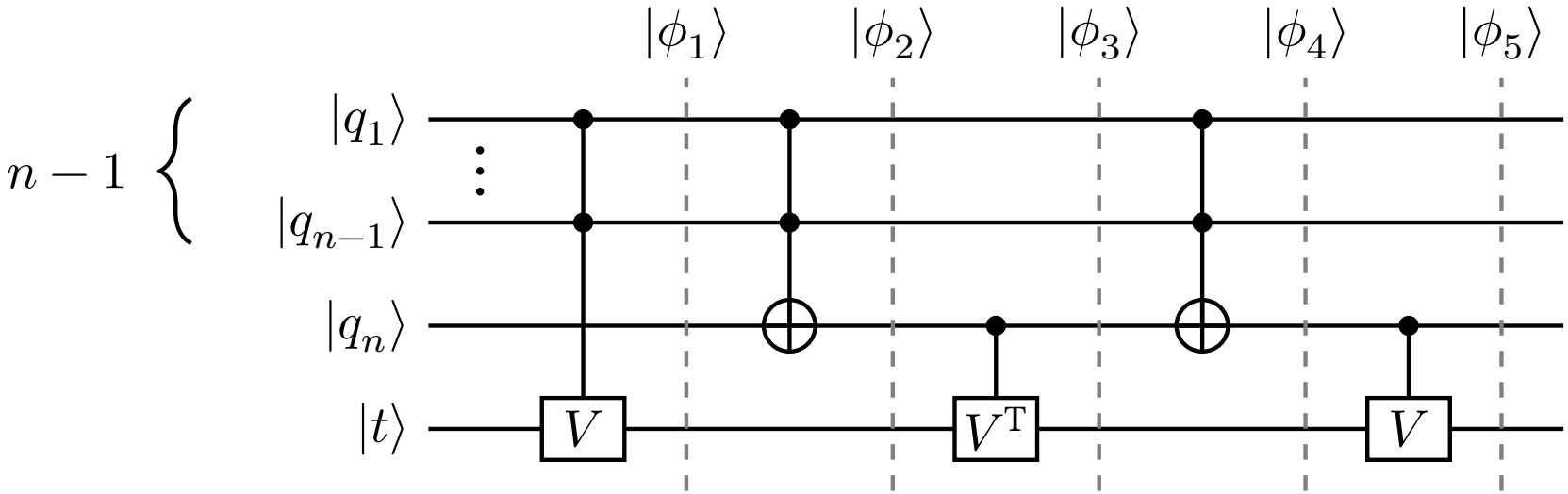
Περιεχόμενα

1. Πύλες με n ελέγχους
2. Διεπίπεδοι πίνακες
3. Κυκλώματα
4. Σύνοψη

Από δύο σε n qubit ελέγχου

- Θεωρούμε την $\hat{C}_n^1(\hat{U})$ με $n > 2$ qubit ελέγχου $q_1, \ldots, q_n$ και ένα qubit στόχο t. Ο πίνακάς της είναι $2^{n+1} \times 2^{n+1}$
- Ιδέα: επαγωγή. Με $\mathbf{V}^2 = \mathbf{U}$, η $C_n^1(U)$ προκύπτει από πύλες με $n-1$ ελέγχους ($C_{n-1}^1(V)$, $C_{n-1}^1(X)$) και πύλες με έναν έλεγχο
- Είναι το ίδιο κύκλωμα με της $C_2^1(U)$, όπου το q_1 αντικαθίσταται από τα $n-1$ qubit $q_1, \ldots, q_{n-1}$

Το κύκλωμα της $C_n^1(U)$



- Οι πύλες με $n-1$ ελέγχους είναι οι $C_{n-1}^1(V)$ και οι δύο $C_{n-1}^1(X)$

Συμβολισμός και πρώτες καταστάσεις

- Είσοδος $|q_1\rangle \cdots |q_n\rangle |t\rangle$ με bit q_i, t. Θέτουμε $Q = q_1 q_2 \cdots q_{n-1}$, δηλαδή το AND των πρώτων $n-1$ bit: $Q = 1$ μόνο όταν όλα είναι 1
- Πύλη ελεγχόμενη από τα $q_1, \ldots, q_{n-1}$ ενεργοποιείται ακριβώς όταν $Q = 1$. Η $C^1_{n-1}(V)$ εφαρμόζει τον $\mathbf{V}^Q$:

$$|\phi_1\rangle = |q_1\rangle \cdots |q_n\rangle \otimes \mathbf{V}^Q |t\rangle$$

- Η $C^1_{n-1}(X)$ αντιστρέφει το q_n όταν $Q = 1$, δηλαδή το κάνει $q_n \oplus Q$:

$$|\phi_2\rangle = |q_1\rangle \cdots |q_{n-1}\rangle |q_n \oplus Q\rangle \otimes \mathbf{V}^Q |t\rangle$$

Ενδιάμεσες καταστάσεις

- $C_1^1(V^{\mathrm{T}})$ με έλεγχο το q_n, που είναι τώρα $q_n \oplus Q$:

$$|\phi_3\rangle = |q_1\rangle \cdots |q_{n-1}\rangle \, |q_n \oplus Q\rangle \otimes (\mathbf{V}^{\mathrm{T}})^{q_n \oplus Q} \mathbf{V}^Q \, |t\rangle$$

- Δεύτερη $C_{n-1}^1(X)$: αφού $(q_n \oplus Q) \oplus Q = q_n$, το q_n επανέρχεται

$$|\phi_4\rangle = |q_1\rangle \cdots |q_n\rangle \otimes (\mathbf{V}^{\mathrm{T}})^{q_n \oplus Q} \mathbf{V}^Q \, |t\rangle$$

- Τελευταία $C_1^1(V)$ με έλεγχο το q_n:

$$|\phi_5\rangle = |q_1\rangle \cdots |q_n\rangle \otimes \mathbf{V}^{q_n} (\mathbf{V}^{\mathrm{T}})^{q_n \oplus Q} \mathbf{V}^Q \, |t\rangle$$

- Με $\mathbf{V}^{\mathrm{T}} = \mathbf{V}^{-1}$ ο πίνακας στο στόχο είναι $\mathbf{V}^m$ με

$$m = Q + q_n - (Q \oplus q_n)$$

Το αποτέλεσμα του κυκλώματος

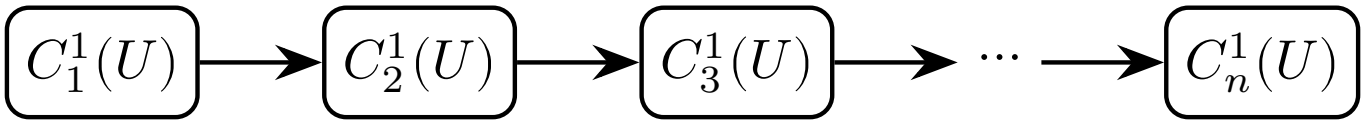
- Ίδιος πίνακας με την $C_2^1(U)$, με Q στη θέση του q_1 και q_n στη θέση του q_2: $m = 2$ μόνο όταν $Q = q_n = 1$, αλλιώς $m = 0$
- Αλλά $Q = q_n = 1$ σημαίνει ότι *όλα* τα n qubit ελέγχου είναι 1. Με $\mathbf{V}^2 = \mathbf{U}$ και $\mathbf{V}^0 = \mathbf{I}_2$:

$$|\phi_5\rangle = \begin{cases} |q_1 \cdots q_n\rangle \otimes \hat{U} |t\rangle , & q_1 = \cdots = q_n = 1 \\ |q_1 \cdots q_n\rangle |t\rangle , & \text{αλλιώς} \end{cases}$$

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

Κατασκευή κάθε $C_n^1(U)$

- Αποτέλεσμα: κάθε $C_n^1(U)$, για κάθε $n \geq 1$ και κάθε πύλη ενός qubit U, κατασκευάζεται μόνο από CNOT και πύλες ενός qubit.
  Βήμα-βήμα:
  - $C_1^1(U)$: από δύο CNOT και πύλες ενός qubit
  - $C_2^1(U)$: από CNOT και πύλες C_1^1
  - $C_3^1(U)$: από πύλες C_2^1 και C_1^1
  - $C_n^1(U)$: από πύλες C_{n-1}^1 και C_1^1

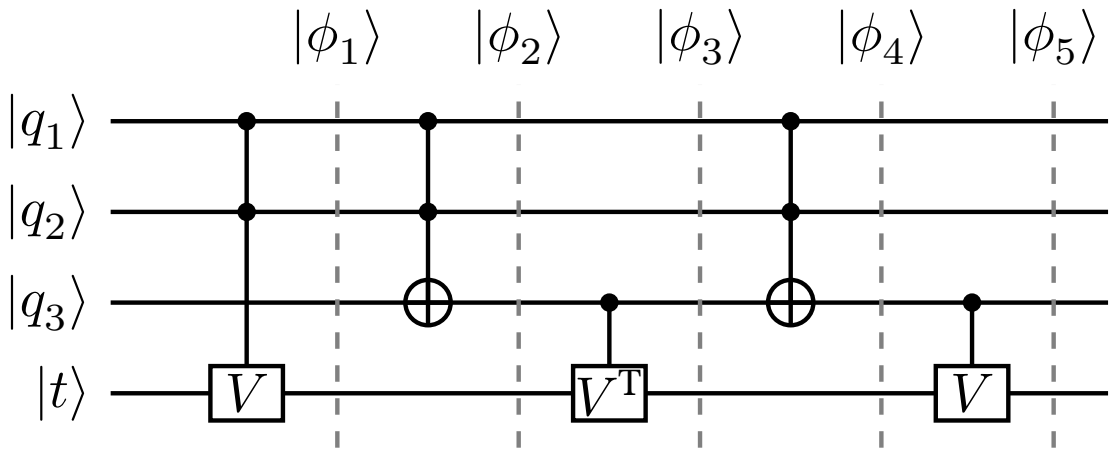


- Κάθε βήμα χρειάζεται νέα τετραγωνική ρίζα: για την $C_{n-1}^1(V)$ ένα $\mathbf{W}$ με $\mathbf{W}^2 = \mathbf{V}$, κ.ο.κ.

Παράδειγμα: $C_3^1(H)$ (1/5)

- Δύο εφαρμογές της κατασκευής: από τρεις σε δύο ελέγχους και μετά από δύο σε έναν. Πρώτο επίπεδο, $\mathbf{V}^2 = \mathbf{H}$ (από την $C_2^1(H)$):

$$\mathbf{V} = \frac{1+j}{2}\left(\mathbf{I}_2 - j\mathbf{H}\right)$$



- Η $C_2^1(V)$ και οι δύο Toffoli έχουν ελέγχους q_1, q_2. Οι $C_1^1(V^{\mathrm{T}})$, $C_1^1(V)$ έχουν έλεγχο το q_3

Παράδειγμα: $C_3^1(H)$ (2/5)

- Οι καταστάσεις, με $Q = q_1 q_2$:

$$|\phi_1\rangle = |q_1 q_2 q_3\rangle \otimes \mathbf{V}^{q_1 q_2} |t\rangle, \quad |\phi_2\rangle = |q_1 q_2\rangle |q_3 \oplus q_1 q_2\rangle \otimes \mathbf{V}^{q_1 q_2} |t\rangle$$

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

- Είσοδος $|111\rangle |t\rangle$: η $C_2^1(V)$ εφαρμόζει $\mathbf{V}$, η Toffoli κάνει $q_3 = 0$ και η V^{T} δεν ενεργοποιείται, η δεύτερη Toffoli επαναφέρει $q_3 = 1$ και η τελευταία V δρα ξανά:

$$|\phi_5\rangle = |111\rangle \otimes \mathbf{V}\mathbf{V} |t\rangle = |111\rangle \otimes \mathbf{H} |t\rangle$$

- Είσοδος $|110\rangle |t\rangle$: μετά τη V η Toffoli κάνει $q_3 = 1$, η V^{T} ακυρώνει τη V και η τελευταία V δεν ενεργοποιείται:

$$|\phi_5\rangle = |110\rangle \otimes \mathbf{V}^{\mathrm{T}}\mathbf{V} |t\rangle = |110\rangle |t\rangle$$

Παράδειγμα: $C_3^1(H)$ (3/5)

- Οι Toffoli και οι πύλες C_1^1 είναι γνωστές. Μένει η $C_2^1(V)$: ίδια κατασκευή, με $\mathbf{W}^2 = \mathbf{V}$
- Ο $\mathbf{V} = \mathrm{e}^{j\pi/4}\mathbf{R_n}(\frac{\pi}{2})$ έχει φάση $\frac{\pi}{4}$ και γωνία $\frac{\pi}{2}$. Παίρνουμε τα μισά:

$$\mathbf{W} = \mathrm{e}^{j\pi/8}\mathbf{R_n}(\tfrac{\pi}{4}) = \mathrm{e}^{j\pi/8}\left(c\,\mathbf{I}_2 - js\,\mathbf{H}\right)$$

με $c = \cos\frac{\pi}{8}$, $s = \sin\frac{\pi}{8}$

Παράδειγμα: $C_3^1(H)$ (4/5)

- Έλεγχος ότι $\mathbf{W}^2 = \mathbf{V}$: η φάση δίνει $(\mathrm{e}^{j\pi/8})^2 = \mathrm{e}^{j\pi/4}$. Με $\mathbf{H}^2 = \mathbf{I}_2$:

$$(c\,\mathbf{I}_2 - js\,\mathbf{H})^2 = (c^2 - s^2)\mathbf{I}_2 - 2jcs\,\mathbf{H}$$

- Από τις ταυτότητες διπλάσιας γωνίας:

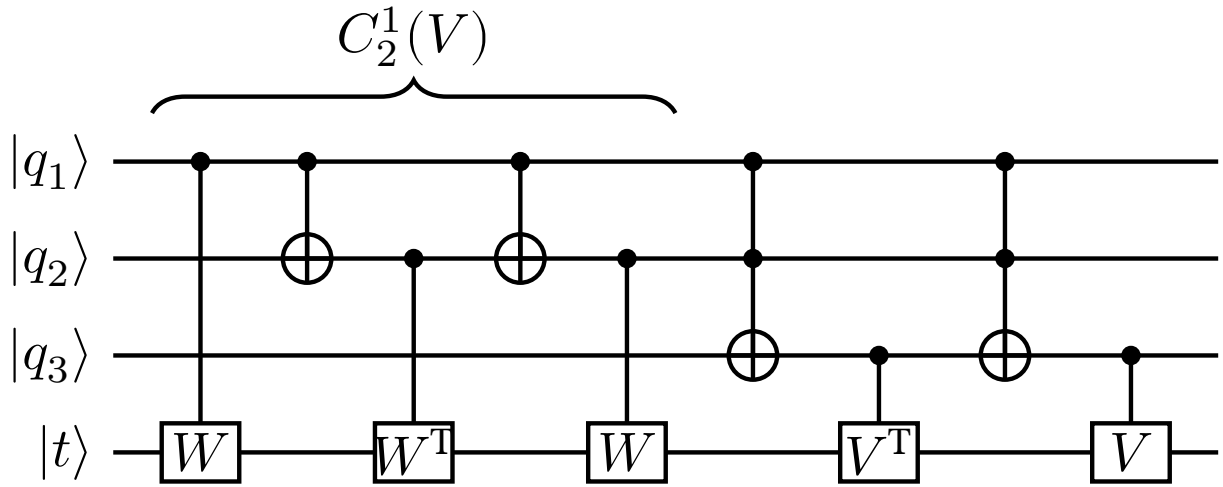
$$c^2 - s^2 = \cos\tfrac{\pi}{4} = \tfrac{1}{\sqrt{2}}, \qquad 2cs = \sin\tfrac{\pi}{4} = \tfrac{1}{\sqrt{2}}$$

- Επομένως

$$\mathbf{W}^2 = \mathrm{e}^{j\pi/4}\tfrac{1}{\sqrt{2}}\,(\mathbf{I}_2 - j\mathbf{H}) = \mathrm{e}^{j\pi/4}\mathbf{R}_{\mathbf{n}}\left(\tfrac{\pi}{2}\right) = \mathbf{V}$$

Παράδειγμα: $C_3^1(H)$ (5/5)

- Η $C_2^1(V)$ με ελέγχους q_1, q_2 (το q_3 δεν συμμετέχει). Αντικαθιστώντας την στο κύκλωμα, παίρνουμε την $C_3^1(H)$:



- 9 πύλες: 2 CNOT, 2 Toffoli και 5 ελεγχόμενες πύλες με έναν έλεγχο ($W, W^{\mathrm{T}}, W, V^{\mathrm{T}}, V$), που με τη σειρά τους κατασκευάζονται από CNOT και πύλες ενός qubit

Διεπίπεδοι μοναδιαίοι πίνακες

- Σύστημα n qubit, $N = 2^n$ καταστάσεις βάσης $|\psi_1\rangle, \ldots, |\psi_N\rangle$. Ο $\hat{U}$ έχει πίνακα $N \times N$ με $u_{pq} = \langle \psi_p | \hat{U} | \psi_q \rangle$
- Στόχος: κάθε μοναδιαίος $\mathbf{U}$ να γραφτεί ως γινόμενο απλών πινάκων
- Διεπίπεδος (two-level) λέγεται ο μοναδιαίος πίνακας που δρα μη τετριμμένα μόνο στις $|\psi_r\rangle, |\psi_s\rangle$: $\mathbf{U}|\psi_p\rangle = |\psi_p\rangle$ για $p \neq r, s$
- Παράδειγμα $N = 4, r = 2, s = 4$:

$$\mathbf{U} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & c & 0 & d \end{bmatrix}, \qquad \tilde{\mathbf{U}} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

- Διαφέρει από τον $\mathbf{I}_4$ μόνο στις γραμμές και στήλες $2, 4$, όπου βρίσκεται ο 2×2 πίνακας $\tilde{\mathbf{U}}$

Πότε είναι μοναδιαίος ένας διεπίπεδος πίνακας

- Ισχυρισμός: ο $\mathbf{U}$ είναι μοναδιαίος ακριβώς όταν ο $\tilde{\mathbf{U}}$ είναι μοναδιαίος
- Για το παράδειγμα με $r = 2, s = 4$:

$$\mathbf{U}^{\mathrm{T}}\mathbf{U} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & |a|^2 + |c|^2 & 0 & a^*b + c^*d \\ 0 & 0 & 1 & 0 \\ 0 & b^*a + d^*c & 0 & |b|^2 + |d|^2 \end{bmatrix}$$

- Τα στοιχεία στις γραμμές και στήλες $2, 4$ είναι ακριβώς τα στοιχεία του

$$\tilde{\mathbf{U}}^{\mathrm{T}}\tilde{\mathbf{U}} = \begin{bmatrix} |a|^2 + |c|^2 & a^*b + c^*d \\ b^*a + d^*c & |b|^2 + |d|^2 \end{bmatrix}$$

- Τα υπόλοιπα είναι όπως στον $\mathbf{I}_4$. Άρα $\mathbf{U}^{\mathrm{T}}\mathbf{U} = \mathbf{I}_4$ ακριβώς όταν $\tilde{\mathbf{U}}^{\mathrm{T}}\tilde{\mathbf{U}} = \mathbf{I}_2$, δηλαδή

$$|a|^2 + |c|^2 = 1, \quad |b|^2 + |d|^2 = 1, \quad a^*b + c^*d = 0$$

- Το ίδιο ισχύει για κάθε N (το στοιχείο (p, q) του $\mathbf{U}^{\mathrm{T}}\mathbf{U}$ είναι το εσωτερικό γινόμενο των στηλών p, q)

Ο συζυγής ανάστροφος διεπίπεδου πίνακα

- Αν ο $\mathbf{U}$ είναι διεπίπεδος με $\tilde{\mathbf{U}}$, ο $\mathbf{U}^{\mathrm{T}}$ είναι διεπίπεδος ως προς τις ίδιες καταστάσεις, με $\tilde{\mathbf{U}}^{\mathrm{T}}$ στη θέση του $\tilde{\mathbf{U}}$, αφού $(\mathbf{U}^{\mathrm{T}})_{pq} = u^*_{qp}$
- Παράδειγμα, $N = 4, r = 1, s = 3$:

$$\mathbf{U} = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{j}{\sqrt{2}} & 0 \\ 0 & 1 & 0 & 0 \\ \frac{j}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \mathbf{U}^{\mathrm{T}} = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & -\frac{j}{\sqrt{2}} & 0 \\ 0 & 1 & 0 & 0 \\ -\frac{j}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

- Έλεγχος: $\tilde{\mathbf{U}}^{\mathrm{T}}\tilde{\mathbf{U}} = \frac{1}{2}\begin{bmatrix} 1 & -j \\ -j & 1 \end{bmatrix}\begin{bmatrix} 1 & j \\ j & 1 \end{bmatrix} = \mathbf{I}_2$

Ανάλυση σε διεπίπεδους πίνακες

- Αποτέλεσμα: κάθε $N \times N$ μοναδιαίος πίνακας γράφεται

$$\mathbf{U} = \mathbf{U}_1 \mathbf{U}_2 \cdots \mathbf{U}_d$$

με κάθε $\mathbf{U}_i$ διεπίπεδο μοναδιαίο και

$$d \leq \frac{N(N-1)}{2}$$

- Ιδέα: πολλαπλασιάζουμε από αριστερά με διεπίπεδους $\mathbf{A}_1, \mathbf{A}_2, \ldots$ που μηδενίζουν ένα-ένα τα στοιχεία εκτός διαγωνίου, μέχρι ο πίνακας να γίνει διεπίπεδος:

$$\mathbf{A}_k \cdots \mathbf{A}_2 \mathbf{A}_1 \mathbf{U} = \Gamma$$

- Πολλαπλασιάζοντας με $\mathbf{A}_k^{\mathrm{T}}, \ldots, \mathbf{A}_1^{\mathrm{T}}$ (αφού $\mathbf{A}_i^{\mathrm{T}} \mathbf{A}_i = \mathbf{I}$):

$$\mathbf{U} = \mathbf{A}_1^{\mathrm{T}} \mathbf{A}_2^{\mathrm{T}} \cdots \mathbf{A}_k^{\mathrm{T}} \Gamma$$

- Οι $\mathbf{A}_i^{\mathrm{T}}$ είναι διεπίπεδοι, άρα $\mathbf{U}_i = \mathbf{A}_i^{\mathrm{T}}$ και $\mathbf{U}_{k+1} = \Gamma$

Μηδενισμός ενός στοιχείου (1/2)

- Σε μια στήλη t ενός πίνακα $\mathbf{M}$ έχουμε στις γραμμές r, s τα στοιχεία $a = m_{rt}$ και $b = m_{st}$. Θέλουμε να μηδενίσουμε το b
- Ορίζουμε

$$x = \frac{a}{\sqrt{|a|^2 + |b|^2}}, \qquad y = \frac{b}{\sqrt{|a|^2 + |b|^2}}$$

και τον διεπίπεδο $\mathbf{A}$ με 2×2 πίνακα στις γραμμές και στήλες r, s

$$\tilde{\mathbf{A}} = \begin{bmatrix} x^* & y^* \\ -y & x \end{bmatrix}$$

- Είναι μοναδιαίος, αφού $|x|^2 + |y|^2 = 1$:

$$\tilde{\mathbf{A}}\tilde{\mathbf{A}}^{\mathrm{T}} = \begin{bmatrix} |x|^2 + |y|^2 & -x^*y^* + y^*x^* \\ -yx + xy & |y|^2 + |x|^2 \end{bmatrix} = \mathbf{I}_2$$

Μηδενισμός ενός στοιχείου (2/2)

- Ο **AM** αλλάζει μόνο τις γραμμές r, s του **M**:

$$(\mathbf{AM})_{rk} = x^* m_{rk} + y^* m_{sk}, \qquad (\mathbf{AM})_{sk} = -y\, m_{rk} + x\, m_{sk}$$

- Στη στήλη t ($k = t$):

$$(\mathbf{AM})_{rt} = x^* a + y^* b = \frac{|a|^2 + |b|^2}{\sqrt{|a|^2 + |b|^2}} = \sqrt{|a|^2 + |b|^2} = \rho$$

$$(\mathbf{AM})_{st} = -ya + xb = \frac{-ba + ab}{\sqrt{|a|^2 + |b|^2}} = 0$$

- Το b μηδενίστηκε και το μέτρο των a, b πήγε στη γραμμή r ως θετικός πραγματικός ρ
- Οι άλλες γραμμές δεν αλλάζουν, άρα τα μηδενικά που έχουμε ήδη φτιάξει δεν χαλάνε. Αν $b = 0$ δεν κάνουμε τίποτα. Αν ο **M** είναι μοναδιαίος, είναι και ο **AM**

Ο αλγόριθμος: πρώτη στήλη

- Μηδενίζουμε διαδοχικά τα $u_{21}, u_{31}, \dots, u_{N1}$ με γραμμή αναφοράς την 1. Ο $\mathbf{A}_i$ δρα στις γραμμές και στήλες $1, i+1$, με a την τρέχουσα τιμή της γραμμής 1 και b το στοιχείο της γραμμής $i+1$:

$$\mathbf{A}_1\mathbf{U} = \begin{bmatrix} \rho_1 & * & \cdots & * \\ 0 & * & \cdots & * \\ u_{31} & u_{32} & \cdots & u_{3N} \\ \vdots & \vdots & \ddots & \vdots \end{bmatrix}, \quad \rho_1 = \sqrt{|u_{11}|^2 + |u_{21}|^2}$$

- Το βήμα i δεν αγγίζει τις γραμμές $2, \dots, i$, και δίνει $\rho_i = \sqrt{|u_{11}|^2 + \cdots + |u_{i+1,1}|^2}$
- Μετά τα $N-1$ βήματα η πρώτη στήλη του $\Gamma = \mathbf{A}_{N-1} \cdots \mathbf{A}_1 \mathbf{U}$ έχει μόνο το $\gamma_{11} = \rho_{N-1} > 0$

Στήλες και γραμμές μοναδιαίου πίνακα

- Σε μοναδιαίο πίνακα κάθε στήλη και κάθε γραμμή έχει μέτρο 1:

$$\sum_k |u_{kq}|^2 = (\mathbf{U}^{\mathrm{T}}\mathbf{U})_{qq} = 1, \qquad \sum_k |u_{pk}|^2 = (\mathbf{U}\mathbf{U}^{\mathrm{T}})_{pp} = 1$$

- Π.χ. για τη δεύτερη στήλη του $\mathcal{M} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & j & -1 & -j \\ 1 & -1 & 1 & -1 \\ 1 & -j & -1 & j \end{bmatrix}$ είναι $\frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1$
- Για τον Γ (μοναδιαίος): $|\gamma_{11}|^2 = 1$, άρα $\gamma_{11} = 1$. Η πρώτη γραμμή δίνει $|\gamma_{12}|^2 + \cdots + |\gamma_{1N}|^2 = 0$, άρα όλα μηδέν

Ο αλγόριθμος: μέτρηση των πινάκων

- Η πρώτη γραμμή του Γ μηδενίστηκε χωρίς πρόσθετο κόπο:

$$\Gamma = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \mathbf{V} & \\ 0 & & & \end{bmatrix}$$

  με τον $(N-1)\times(N-1)$ πίνακα $\mathbf{V}$ μοναδιαίο

- Επαναλαμβάνουμε στη δεύτερη στήλη με γραμμή αναφοράς την 2, χωρίς να αγγίξουμε την πρώτη γραμμή και στήλη: $N-2$ πίνακες. Και ούτω καθεξής μέχρι τη στήλη $N-2$ (2 πίνακες)
- Μαζί με τον τελικό διεπίπεδο Γ, το πλήθος είναι το πολύ

$$(N-1)+(N-2)+\cdots+2+1=\frac{N(N-1)}{2}$$

- «Το πολύ», γιατί παραλείπουμε τα βήματα όπου το στοιχείο είναι ήδη μηδέν

Παράδειγμα: ο πίνακας QFT δύο qubit (1/6)

- Αναλύουμε τον 4×4 μοναδιαίο (ο κβαντικός μετασχηματισμός Fourier δύο qubit), με το πολύ $4 \cdot 3/2 = 6$ παράγοντες:

$$\mathcal{M} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & j & -1 & -j \\ 1 & -1 & 1 & -1 \\ 1 & -j & -1 & j \end{bmatrix}$$

- Βήμα 1, μηδενισμός της γραμμής 2 της πρώτης στήλης: $a = b = \frac{1}{2}$, $\rho = \frac{1}{\sqrt{2}}$, $x = y = \frac{1}{\sqrt{2}}$

$$\mathbf{A}_1 = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

- Νέα γραμμή 1: $(\text{γρ.}1 + \text{γρ.}2)/\sqrt{2}$, νέα γραμμή 2: $(\text{γρ.}2 - \text{γρ.}1)/\sqrt{2}$

Παράδειγμα: ο πίνακας QFT δύο qubit (2/6)

- Αποτέλεσμα του βήματος 1:

$$\Gamma_1 = \mathbf{A}_1 \mathcal{M} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1+j}{2\sqrt{2}} & 0 & \frac{1-j}{2\sqrt{2}} \\ 0 & -\frac{1-j}{2\sqrt{2}} & -\frac{1}{\sqrt{2}} & -\frac{1+j}{2\sqrt{2}} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{j}{2} & -\frac{1}{2} & \frac{j}{2} \end{bmatrix}$$

- Βήμα 2 (γραμμές $1, 3$): $a = \frac{1}{\sqrt{2}}$ (τρέχουσα γραμμή 1), $b = \frac{1}{2}$, $\rho = \frac{\sqrt{3}}{2}$, $x = \frac{\sqrt{6}}{3}$, $y = \frac{\sqrt{3}}{3}$

$$\mathbf{A}_2 = \begin{bmatrix} \frac{\sqrt{6}}{3} & 0 & \frac{\sqrt{3}}{3} & 0 \\ 0 & 1 & 0 & 0 \\ -\frac{\sqrt{3}}{3} & 0 & \frac{\sqrt{6}}{3} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

- Αλλάζουν μόνο οι γραμμές 1 και 3 του Γ_1

Παράδειγμα: ο πίνακας QFT δύο qubit (3/6)

- Βήμα 3 (γραμμές $1, 4$): $a = \frac{\sqrt{3}}{2}, b = \frac{1}{2}, \rho = 1, x = \frac{\sqrt{3}}{2}, y = \frac{1}{2}$

$$\mathbf{A}_3 = \begin{bmatrix} \frac{\sqrt{3}}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -\frac{1}{2} & 0 & 0 & \frac{\sqrt{3}}{2} \end{bmatrix}$$

- Μετά το βήμα 3 η πρώτη γραμμή γίνεται $(1, 0, 0, 0)$, όπως προβλέπει η θεωρία:

$$\Gamma_3 = \mathbf{A}_3\mathbf{A}_2\Gamma_1 = \left[\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline 0 & -\frac{1-j}{2\sqrt{2}} & -\frac{1}{\sqrt{2}} & -\frac{1+j}{2\sqrt{2}} \\ 0 & -\frac{\sqrt{6}(3+j)}{12} & \frac{\sqrt{6}}{6} & -\frac{\sqrt{6}(3-j)}{12} \\ 0 & -\frac{j\sqrt{3}}{3} & -\frac{\sqrt{3}}{3} & \frac{j\sqrt{3}}{3} \end{array}\right]$$

Παράδειγμα: ο πίνακας QFT δύο qubit (4/6)

- Βήμα 4, δεύτερη στήλη, γραμμές $2, 3$: $a = -\frac{1-j}{2\sqrt{2}}$, $b = -\frac{\sqrt{6}(3+j)}{12}$, με $|a|^2 = \frac{1}{4}$, $|b|^2 = \frac{5}{12}$, άρα $\rho = \frac{\sqrt{6}}{3}$, $x = -\frac{\sqrt{3}(1-j)}{4}$, $y = -\frac{3+j}{4}$

$$\mathbf{A}_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -\frac{\sqrt{3}(1+j)}{4} & -\frac{3-j}{4} & 0 \\ 0 & \frac{3+j}{4} & -\frac{\sqrt{3}(1-j)}{4} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

- Αποτέλεσμα:

$$\Gamma_4 = \mathbf{A}_4 \Gamma_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{\sqrt{6}}{3} & \frac{j\sqrt{6}}{6} & \frac{\sqrt{6}}{6} \\ 0 & 0 & -\frac{1}{\sqrt{2}} & -\frac{j}{\sqrt{2}} \\ 0 & -\frac{j\sqrt{3}}{3} & -\frac{\sqrt{3}}{3} & \frac{j\sqrt{3}}{3} \end{bmatrix}$$

Παράδειγμα: ο πίνακας QFT δύο qubit (5/6)

- Βήμα 5 (γραμμές 2, 4): $a = \frac{\sqrt{6}}{3}, b = -\frac{j\sqrt{3}}{3}, |a|^2 + |b|^2 = 1$, άρα $x = \frac{\sqrt{6}}{3}, y = -\frac{j\sqrt{3}}{3}$

$$\mathbf{A}_5 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{\sqrt{6}}{3} & 0 & \frac{j\sqrt{3}}{3} \\ 0 & 0 & 1 & 0 \\ 0 & \frac{j\sqrt{3}}{3} & 0 & \frac{\sqrt{6}}{3} \end{bmatrix}$$

- Όπως και στην πρώτη στήλη, μηδενίζεται ολόκληρη η δεύτερη γραμμή:

$$\Gamma_5 = \mathbf{A}_5 \Gamma_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -\frac{1}{\sqrt{2}} & -\frac{j}{\sqrt{2}} \\ 0 & 0 & -\frac{1}{\sqrt{2}} & \frac{j}{\sqrt{2}} \end{bmatrix}$$

Παράδειγμα: ο πίνακας QFT δύο qubit (6/6)

- Ο Γ_5 είναι ήδη διεπίπεδος (γραμμές και στήλες $3, 4$), άρα σταματάμε: $\mathbf{A}_5\mathbf{A}_4\mathbf{A}_3\mathbf{A}_2\mathbf{A}_1\mathcal{M} = \Gamma_5$
- Πολλαπλασιάζοντας με τους συζυγείς ανάστροφους:

$$\mathcal{M} = \mathbf{U}_1\mathbf{U}_2\mathbf{U}_3\mathbf{U}_4\mathbf{U}_5\mathbf{U}_6, \qquad \mathbf{U}_i = \mathbf{A}_i^{\mathrm{T}}\ (i \leq 5), \quad \mathbf{U}_6 = \Gamma_5$$

- Δηλαδή

$$\mathbf{U}_1 = \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \mathbf{U}_2 = \begin{bmatrix} \frac{\sqrt{6}}{3} & 0 & -\frac{\sqrt{3}}{3} & 0 \\ 0 & 1 & 0 & 0 \\ \frac{\sqrt{3}}{3} & 0 & \frac{\sqrt{6}}{3} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\mathbf{U}_3 = \begin{bmatrix} \frac{\sqrt{3}}{2} & 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{\sqrt{3}}{2} \end{bmatrix}, \quad \mathbf{U}_5 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{\sqrt{6}}{3} & 0 & -\frac{j\sqrt{3}}{3} \\ 0 & 0 & 1 & 0 \\ 0 & -\frac{j\sqrt{3}}{3} & 0 & \frac{\sqrt{6}}{3} \end{bmatrix}$$

- Οι $\mathbf{U}_4$ και $\mathbf{U}_6 = \Gamma_5$ είναι διεπίπεδοι στις γραμμές $2, 3$ και $3, 4$. Έξι διεπίπεδοι παράγοντες, όσοι ακριβώς το άνω όριο

Από διεπίπεδους πίνακες σε κυκλώματα

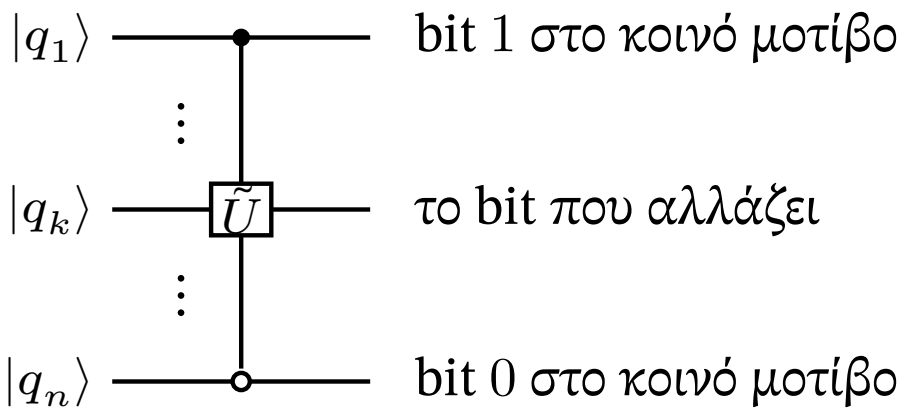
- Αν $\mathbf{U} = \mathbf{U}_1 \cdots \mathbf{U}_d$ και ξέρουμε κύκλωμα για κάθε $\mathbf{U}_i$, βάζουμε τα κυκλώματα το ένα μετά το άλλο. Πρώτος δρα ο $\mathbf{U}_d$ (δεξιότερα στο γινόμενο), άρα το κύκλωμά του μπαίνει πρώτο
- Ο $\mathbf{U}_i$ δρα στις $|\psi_r\rangle, |\psi_s\rangle$ με τον 2×2 πίνακα $\tilde{\mathbf{U}} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$:

$$\mathbf{U}|\psi_r\rangle = a|\psi_r\rangle + c|\psi_s\rangle, \qquad \mathbf{U}|\psi_s\rangle = b|\psi_r\rangle + d|\psi_s\rangle$$

- Κάθε βασική κατάσταση είναι ακολουθία n bit, π.χ. $|\psi_6\rangle = |101\rangle$ για $n = 3$
- Το κύκλωμα εξαρτάται από το σε πόσα bit διαφέρουν οι δύο ακολουθίες. Πρώτα η απλή περίπτωση: διαφέρουν σε *ένα* bit, του q_k. Τα υπόλοιπα $n - 1$ bit είναι το κοινό μοτίβο

Καταστάσεις που διαφέρουν σε ένα bit

- Εφαρμόζουμε τον $\tilde{\mathbf{U}}$ στο q_k, ελεγχόμενο από όλα τα άλλα qubit: μαύρο κυκλάκι όπου το κοινό μοτίβο έχει 1, άσπρο όπου έχει 0

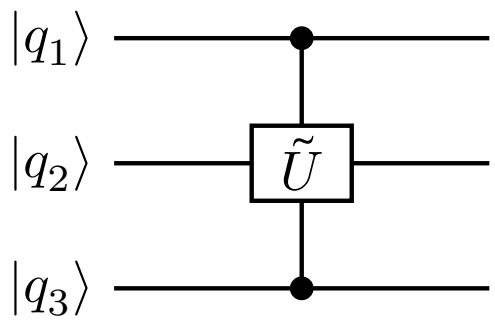


- Προσοχή: η πρώτη γραμμή και στήλη του $\tilde{\mathbf{U}}$ αντιστοιχεί στην $|\psi_r\rangle$, ενώ σε πύλη ενός qubit στην $|0\rangle$. Αν το bit του q_k είναι 1 στην $|\psi_r\rangle$, χρησιμοποιούμε τον

$$\tilde{\mathbf{U}}' = \begin{bmatrix} d & c \\ b & a \end{bmatrix}$$

Παράδειγμα: $|101\rangle$ και $|111\rangle$

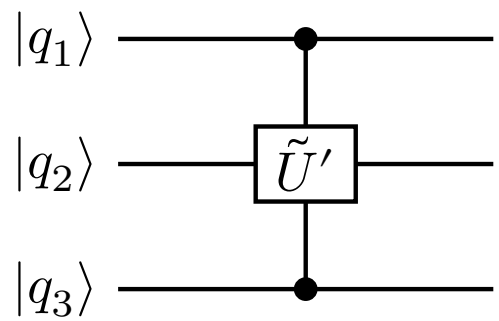
- Οι $|\psi_6\rangle = |101\rangle$, $|\psi_8\rangle = |111\rangle$ διαφέρουν στο q_2. Κοινό μοτίβο $q_1 = q_3 = 1$, και το bit του q_2 είναι 0 στην $|\psi_6\rangle$: χρησιμοποιούμε τον $\tilde{\mathbf{U}}$



- Είσοδος $|101\rangle$: η πύλη ενεργοποιείται και $\tilde{U}|0\rangle = a|0\rangle + c|1\rangle$, άρα έξοδος $a|101\rangle + c|111\rangle = a|\psi_6\rangle + c|\psi_8\rangle$
- Είσοδος $|111\rangle$: $\tilde{U}|1\rangle = b|0\rangle + d|1\rangle$, άρα $b|\psi_6\rangle + d|\psi_8\rangle$
- Σε κάθε άλλη κατάσταση ένα από τα q_1, q_3 είναι 0 και η πύλη δεν ενεργοποιείται

Παράδειγμα με ανταλλαγμένους ρόλους

- Τώρα $|\psi_r\rangle = |111\rangle$, $|\psi_s\rangle = |101\rangle$, δηλαδή
  $\hat{U}\,|111\rangle = a\,|111\rangle + c\,|101\rangle$, $\hat{U}\,|101\rangle = b\,|111\rangle + d\,|101\rangle$
- Το bit του q_2 είναι 1 στην $|\psi_r\rangle$, άρα χρησιμοποιούμε τον $\tilde{\mathbf{U}}'$:



- Είσοδος $|111\rangle$: $\tilde{U}'\,|1\rangle = c\,|0\rangle + a\,|1\rangle$, άρα
  $c\,|101\rangle + a\,|111\rangle = a\,|\psi_r\rangle + c\,|\psi_s\rangle$?.
- Είσοδος $|101\rangle$: $\tilde{U}'\,|0\rangle = d\,|0\rangle + b\,|1\rangle$, άρα $b\,|\psi_r\rangle + d\,|\psi_s\rangle$?.
- Με τον $\tilde{\mathbf{U}}$ χωρίς ανταλλαγή θα παίρναμε $b\,|101\rangle + d\,|111\rangle$, λάθος

Κώδικας Gray

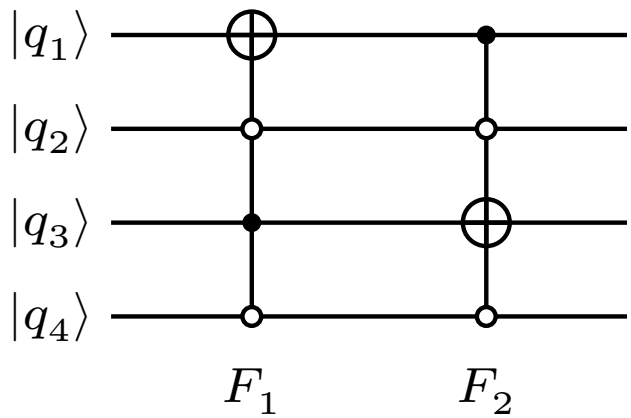
- Αν οι ακολουθίες διαφέρουν σε περισσότερα bit, μετακινούμε πρώτα την $|\psi_r\rangle$ σε κατάσταση που διαφέρει από την $|\psi_s\rangle$ σε ένα bit, εφαρμόζουμε εκεί τον $\tilde{\mathbf{U}}$ και επαναφέρουμε
- Κώδικας Gray: λίστα ακολουθιών bit όπου οι διαδοχικές διαφέρουν σε ακριβώς ένα bit. Π.χ. $00, 01, 11, 10$ (όχι η $00, 01, 10, 11$)
- Θέλουμε $g_0, g_1, \ldots, g_m$ με g_0 τη $|\psi_r\rangle$ και g_m την $|\psi_s\rangle$: αλλάζουμε ένα-ένα τα bit στα οποία διαφέρουν
- Παράδειγμα: $|0010\rangle \to |1001\rangle$ διαφέρουν στα q_1, q_3, q_4:

$$g_0 = 0010, \quad g_1 = 1010, \quad g_2 = 1000, \quad g_3 = 1001$$

- Το m είναι η απόσταση Hamming (εδώ $m = 3$)

Οι πύλες F_k

- Η F_k ανταλλάσσει τις $|g_{k-1}\rangle$ και $|g_k\rangle$ και αφήνει τις άλλες αμετάβλητες. Είναι διεπίπεδος με $\tilde{\mathbf{U}} = \mathbf{X}$ σε καταστάσεις που διαφέρουν σε ένα bit: μία X στο qubit που αλλάζει, ελεγχόμενη από όλα τα άλλα
- F_1: $0010 \leftrightarrow 1010$, X στο q_1, με $q_2 q_3 q_4 = 010$. F_2: $1010 \leftrightarrow 1000$, X στο q_3, με $q_1 q_2 q_4 = 100$



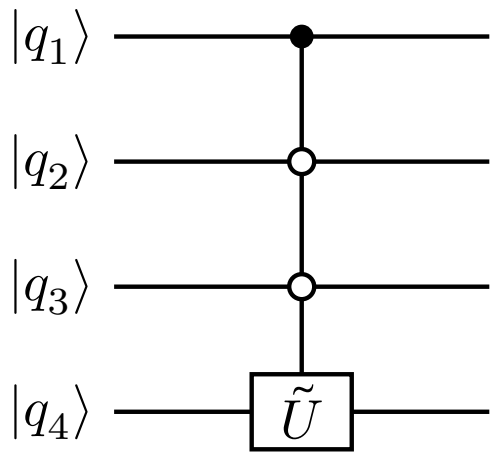
- Μαύρο: το qubit πρέπει να είναι $|1\rangle$. Άσπρο: $|0\rangle$

Η πύλη W και το πλήρες κύκλωμα

- Μετά τις $F_1, \ldots, F_{m-1}$, η $|\psi_r\rangle$ έχει πάει στην $|g_{m-1}\rangle$, που διαφέρει από την $|g_m\rangle = |\psi_s\rangle$ σε ένα bit. Η W κάνει σε αυτές ό,τι ο **U** στις $|\psi_r\rangle, |\psi_s\rangle$:

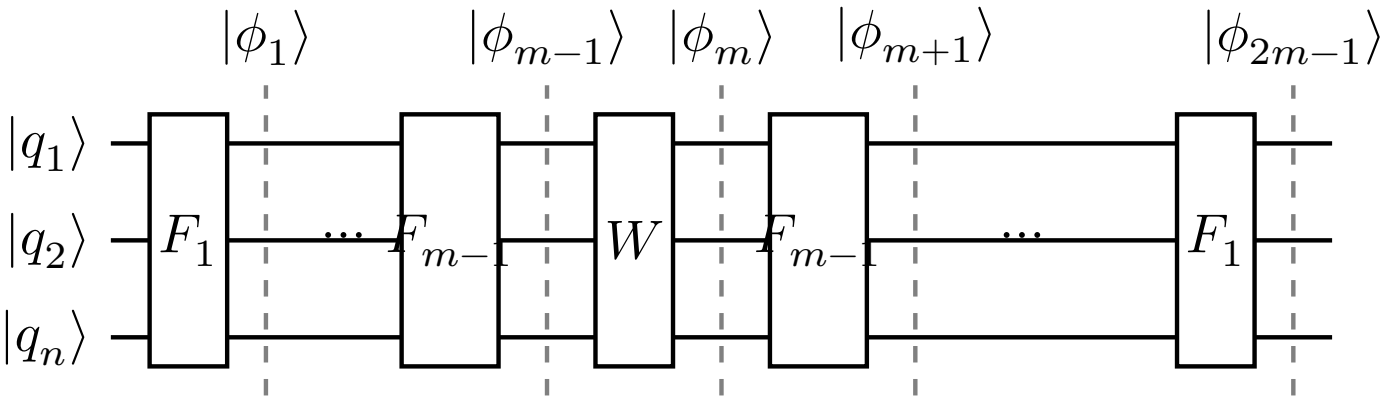
$$\hat{W}|g_{m-1}\rangle = a|g_{m-1}\rangle + c|g_m\rangle, \quad \hat{W}|g_m\rangle = b|g_{m-1}\rangle + d|g_m\rangle$$

- Στο παράδειγμα: W στις $|1000\rangle, |1001\rangle$, δηλαδή $\tilde{U}$ στο q_4 όταν $q_1q_2q_3 = 100$:



Το κύκλωμα για διεπίπεδο πίνακα

- Πρώτα οι $F_1, \ldots, F_{m-1}$, μετά η W, και τέλος οι $F_{m-1}, \ldots, F_1$ ($2m-1$ πύλες, καθεμία με $n-1$ ελέγχους):



- Κάθε ελεγχόμενη πύλη με $n-1$ ελέγχους κατασκευάζεται από CNOT και πύλες ενός qubit (§4.5), χωρίς πρόσθετα qubit

Γιατί υλοποιεί τον U (1/2)

- Είσοδος $\alpha |g_0\rangle + \beta |g_m\rangle +$ (όροι με τις άλλες βασικές καταστάσεις)
- Μετά την F_k το α είναι στην $|g_k\rangle$, ενώ η $|g_m\rangle$ δεν αλλάζει:

$$|\phi_k\rangle = \alpha |g_k\rangle + \beta |g_m\rangle + (...), \qquad k = 1, ..., m-1$$

- Η W αναμιγνύει τις $|g_{m-1}\rangle, |g_m\rangle$:

$$|\phi_m\rangle = (a\alpha + b\beta) |g_{m-1}\rangle + (c\alpha + d\beta) |g_m\rangle + (...)$$

- Οι δεύτερες $F_{m-1}, ..., F_1$ φέρνουν το πρώτο πλάτος πίσω στην $|g_0\rangle$:

$$|\phi_{2m-1}\rangle = (a\alpha + b\beta) |g_0\rangle + (c\alpha + d\beta) |g_m\rangle + (...)$$

- Με $|g_0\rangle = |\psi_r\rangle$, $|g_m\rangle = |\psi_s\rangle$, αυτή είναι η δράση του U

Γιατί υλοποιεί τον $\mathbf{U}$ (2/2)

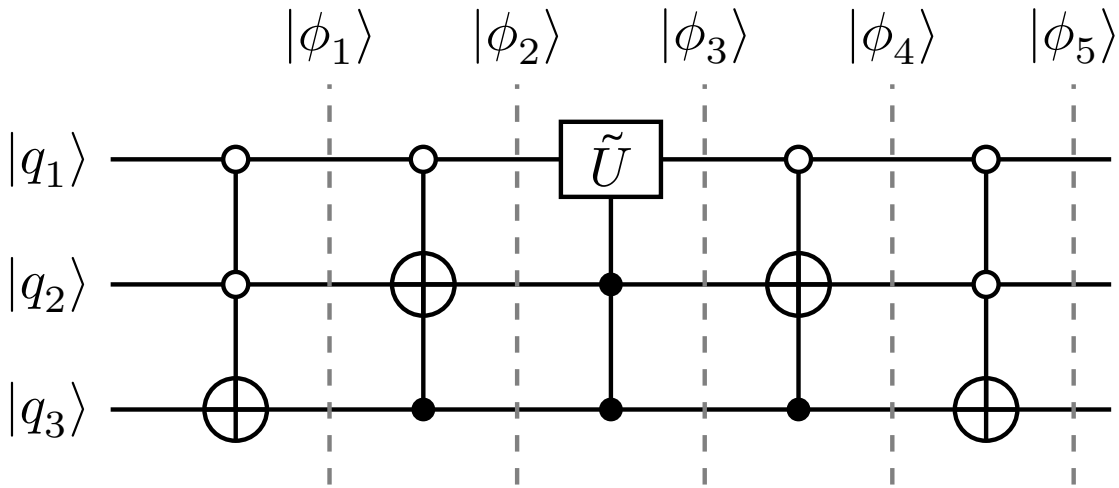
- Οι υπόλοιπες βασικές καταστάσεις: οι $F_1, \ldots, F_{m-1}$ μαζί δίνουν μια αντιστοιχία P βασικών καταστάσεων (μία-προς-μία), με $P|g_0\rangle = |g_{m-1}\rangle$ και $P|g_m\rangle = |g_m\rangle$
- Κάθε άλλη κατάσταση πάει σε κατάσταση διαφορετική από τις $|g_{m-1}\rangle, |g_m\rangle$, όπου η W δεν ενεργοποιείται
- Οι δεύτερες $F_{m-1}, \ldots, F_1$ εφαρμόζουν την αντίστροφη P^{-1}, άρα η κατάσταση επανέρχεται αμετάβλητη
- Συνολικά το κύκλωμα είναι $P^{-1}WP$ και ισούται με τον $\mathbf{U}$

Παράδειγμα: διεπίπεδος στις $|000\rangle, |111\rangle$ (1/2)

- Οι $|\psi_1\rangle = |000\rangle, |\psi_8\rangle = |111\rangle$ διαφέρουν και στα τρία bit, $m = 3$. Κώδικας Gray με αλλαγή πρώτα του q_3, μετά του q_2, μετά του q_1:

$$g_0 = 000, \quad g_1 = 001, \quad g_2 = 011, \quad g_3 = 111$$

- F_1: $|000\rangle \leftrightarrow |001\rangle$, X στο q_3 με $q_1 = q_2 = 0$ (δύο άσπρα). F_2: $|001\rangle \leftrightarrow |011\rangle$, X στο q_2 με $q_1 = 0, q_3 = 1$. W: $\tilde{U}$ στο q_1 με $q_2 = q_3 = 1$ ($|011\rangle, |111\rangle$, bit 0 στην g_2, άρα όπως είναι)



Παράδειγμα: διεπίπεδος στις $|000\rangle, |111\rangle$ (2/2)

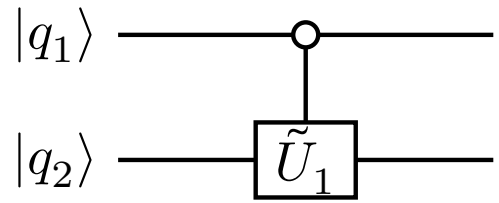
- Πλάτη κάθε βασικής κατάστασης σε κάθε στάδιο για είσοδο $\sum a_i |\psi_i\rangle$, με $b_1 = a\, a_1 + b\, a_8$, $b_8 = c\, a_1 + d\, a_8$:

	είσοδος	$\|\phi_1\rangle$	$\|\phi_2\rangle$	$\|\phi_3\rangle$	$\|\phi_4\rangle$	$\|\phi_5\rangle$
$\|000\rangle$	a_1	a_2	a_2	a_2	a_2	b_1
$\|001\rangle$	a_2	a_1	a_4	a_4	b_1	a_2
$\|010\rangle$	a_3	a_3	a_3	a_3	a_3	a_3
$\|011\rangle$	a_4	a_4	a_1	b_1	a_4	a_4
$\|100\rangle$	a_5	a_5	a_5	a_5	a_5	a_5
$\|101\rangle$	a_6	a_6	a_6	a_6	a_6	a_6
$\|110\rangle$	a_7	a_7	a_7	a_7	a_7	a_7
$\|111\rangle$	a_8	a_8	a_8	b_8	b_8	b_8

- Το a_1 μεταφέρεται δίπλα στο a_8 ($|011\rangle$), η W τα αναμιγνύει, και μετά οι F_2, F_1 επαναφέρουν. Στην έξοδο αλλάζουν μόνο τα πλάτη των $|000\rangle, |111\rangle$

Παράδειγμα: κυκλώματα για παράγοντες της QFT (1/2)

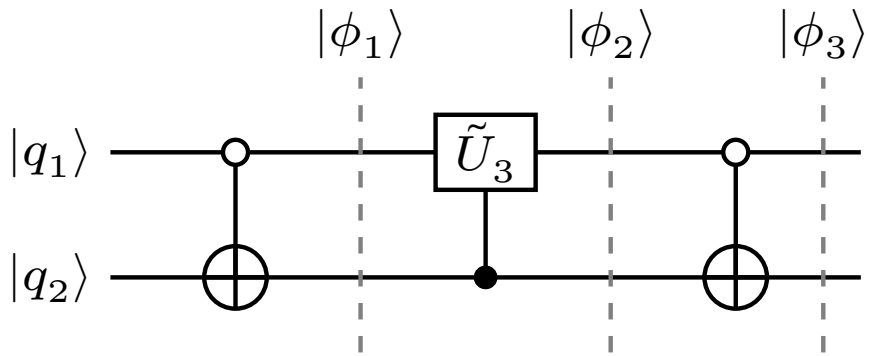
- Ο $\mathbf{U}_1$ της QFT δύο qubit δρα στις $|00\rangle, |01\rangle$ με $\tilde{\mathbf{U}}_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$
- Διαφέρουν σε ένα bit (q_2), με κοινό μοτίβο $q_1 = 0$ (άσπρο κυκλάκι). Το bit του q_2 είναι 0 στην $|00\rangle$, άρα χρησιμοποιούμε τον $\tilde{\mathbf{U}}_1$ όπως είναι:



- Ο $\mathbf{U}_3$ δρα στις $|00\rangle, |11\rangle$ με $\tilde{\mathbf{U}}_3 = \begin{bmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix}$. Διαφέρουν σε δύο bit, $m = 2$, και $g_0 = 00, g_1 = 01, g_2 = 11$

Παράδειγμα: κυκλώματα για παράγοντες της QFT (2/2)

- F_1: CNOT με άσπρο έλεγχο (X στο q_2 όταν $q_1 = 0$). W: $\tilde{\mathbf{U}}_3$ στο q_1 όταν $q_2 = 1$ (το bit του q_1 είναι 0 στην g_1, άρα όπως είναι)

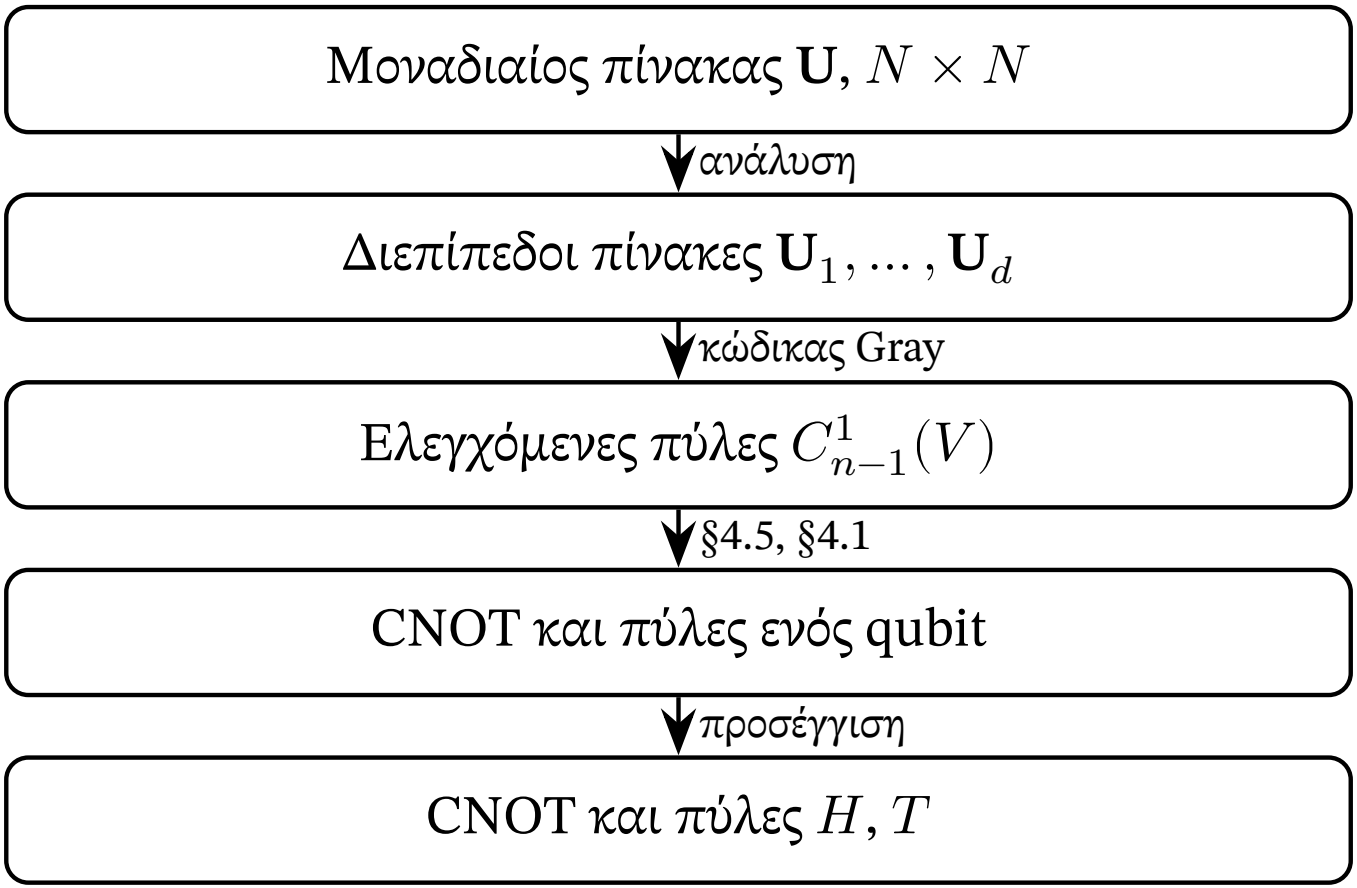


- Είσοδος $|00\rangle$: $|\phi_1\rangle = |01\rangle$, $|\phi_2\rangle = \frac{\sqrt{3}}{2}|01\rangle + \frac{1}{2}|11\rangle$, $|\phi_3\rangle = \frac{\sqrt{3}}{2}|00\rangle + \frac{1}{2}|11\rangle$ (πρώτη στήλη του $\tilde{\mathbf{U}}_3$)
- Είσοδος $|11\rangle$: η πρώτη F_1 δεν ενεργοποιείται, η W δίνει $-\frac{1}{2}|01\rangle + \frac{\sqrt{3}}{2}|11\rangle$ και η δεύτερη F_1 το κάνει $-\frac{1}{2}|00\rangle + \frac{\sqrt{3}}{2}|11\rangle$
- Η $|01\rangle$ πάει στη $|00\rangle$, η W δεν δρα και επιστρέφει στην $|01\rangle$ (αμετάβλητη)

Τα βήματα της κατασκευής

- Έστω μοναδιαίος $\mathbf{U}$, $N \times N$ με $N = 2^n$ (π.χ. ολόκληρου αλγορίθμου)
- 1. Ανάλυση σε διεπίπεδους: $\mathbf{U} = \mathbf{U}_1 \cdots \mathbf{U}_d$ με $d \leq N(N-1)/2$
- 2. Κύκλωμα για κάθε $\mathbf{U}_i$: αν οι καταστάσεις διαφέρουν σε m bit, $2m-1$ ελεγχόμενες πύλες $C^1_{n-1}(V)$ ($V = \mathbf{X}$ για τις F_k, $\tilde{\mathbf{U}}_i$ ή $\tilde{\mathbf{U}}'_i$ για τη W)
- 3. Τα κυκλώματα βάζονται το ένα μετά το άλλο: πρώτο του $\mathbf{U}_d$, τελευταίο του $\mathbf{U}_1$
- 4. Κάθε $C^1_{n-1}(V)$ αναλύεται σε CNOT και ελεγχόμενες πύλες ενός ελέγχου (§4.5), και αυτές σε δύο CNOT και πύλες ενός qubit (§4.1)
- 5. Κάθε πύλη ενός qubit προσεγγίζεται όσο θέλουμε με H, T

Η αλυσίδα της κατασκευής



Παράδειγμα: από την QFT δύο qubit σε ελεγχόμενες πύλες

- $\mathcal{M} = \mathbf{U}_1 \cdots \mathbf{U}_6$. Για κάθε $\mathbf{U}_i$: οι καταστάσεις και το πλήθος των bit που διαφέρουν

πίνακας	καταστάσεις	bit που διαφέρουν	πύλες
$\mathbf{U}_1$	$\|00\rangle, \|01\rangle$	1	1
$\mathbf{U}_2$	$\|00\rangle, \|10\rangle$	1	1
$\mathbf{U}_3$	$\|00\rangle, \|11\rangle$	2	3
$\mathbf{U}_4$	$\|01\rangle, \|10\rangle$	2	3
$\mathbf{U}_5$	$\|01\rangle, \|11\rangle$	1	1
$\mathbf{U}_6$	$\|10\rangle, \|11\rangle$	1	1

- Συνολικά $1+1+3+3+1+1 = 10$ πύλες $C_1^1(V)$, καθεμία από δύο CNOT και πύλες ενός qubit. Πρώτο μπαίνει το κύκλωμα του $\mathbf{U}_6$, τελευταίο του $\mathbf{U}_1$
- Δεν είναι το μικρότερο κύκλωμα για την QFT, αλλά δουλεύει για οποιονδήποτε μοναδιαίο

Σχόλια και αποτέλεσμα

- Μόνο το τελευταίο βήμα (πύλες ενός qubit από H, T) είναι προσεγγιστικό. Η ανάλυση σε διεπίπεδους, ο κώδικας Gray και η ανάλυση σε CNOT είναι *ακριβή*
- Η κατασκευή δεν είναι αποδοτική: το πλήθος των διεπίπεδων φτάνει τα $N(N-1)/2 \approx 4^n/2$, εκθετικό στο n. Για $n = 10$ περίπου μισό εκατομμύριο
- Δείχνει ότι κάθε μοναδιαίος *μπορεί* να υλοποιηθεί, όχι ότι είναι πρακτική μέθοδος σχεδίασης
- Αποτέλεσμα: κάθε μοναδιαίος τελεστής σε οποιοδήποτε πλήθος qubit υλοποιείται, με όσο μικρό σφάλμα θέλουμε, μόνο με τις πύλες H, T και CNOT. Το σύνολο $\{H, T, \text{CNOT}\}$ λέγεται *καθολικό*