Κβαντικοί Υπολογιστές και Αλγόριθμοι

Διάλεξη 4η

Θωμάς Καμαλάκης

Χαροκόπειο Πανεπιστήμιο Αθηνών

2025

Περιεχόμενα

1. Θεμελίωση της Κβαντικής Φυσικής
2. Πύλες πολλαπλών qubits

Τρίτο Αξίωμα: Μετρήσεις

- Είδαμε στα προηγούμενα ότι το πρώτο αξίωμα καθορίζει πως περιγράφουμε ένα σύστημα με ένα διάνυσμα κατάστασης $|\psi\rangle$ σε ένα χώρο Hilbert.
- Το δεύτερο αξίωμα καθορίζει πως μπορεί να μεταβάλλεται το $|\psi\rangle$.
- Μόνο μοναδιαία εξέλιξη επιτρέπεται: Ξεκινώντας από το $|\psi\rangle$ για το οποίο ισχύει $\langle\psi|\psi\rangle = 1$, η μετασχηματισμένη κατάσταση $|\psi'\rangle$ πρέπει και αυτή να υπακούει $\langle\psi'|\psi'\rangle = 1$.
- Το τρίτο αξίωμα καθορίζει πως κάνουμε μετρήσεις στο σύστημα μας.
- Αν και σχετικά απλό, εντούτοις έχει κατά καιρούς πυροδοτήσει πολλή συζήτηση στην ερευνητική κοινότητα.

Τρίτο Αξίωμα: Μετρήσεις

- Σύμφωνα με το 3ο αξίωμα της κβαντικής φυσικής, η μέτρηση σε ένα σύστημα είναι μία διαδικασία η οποία *περιέχει μία τυχαιότητα*. Ας πάρουμε την απλή περίπτωση ένος qubit που περιγράφεται από την κατάσταση $|\psi\rangle$:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

- Είχαμε πει στην αρχή των διαλέξεων ότι από την παραπάνω κατάσταση προκύπτει ότι η πιθανότητα P_0 και P_1 να έχουμε το $|0\rangle$ και το $|1\rangle$ αντίστοιχα είναι:

$$p_0 = |a|^2 \qquad\qquad p_1 = |b|^2$$

- Είχαμε επίσης δει ότι οι πιθανότητες μπορούν να γραφούν με την βοήθεια του εσωτερικού γινομένου:

$$p_0 = |\,\langle 0|\psi\rangle\,|^2 \qquad\qquad p_1 = |\,\langle 1|\psi\rangle\,|^2$$

Τρίτο Αξίωμα: Μετρήσεις

- Η παραπάνω διαδικασία μπορεί να εκφραστεί και με την βοήθεια των τελεστών προβολής:

$$P_0 = |0\rangle\langle 0|$$

$$P_1 = |1\rangle\langle 1|$$

- Έχουμε:

$$p_0 = |\langle 0|\psi\rangle|^2 = \langle 0|\psi\rangle^* \langle 0|\psi\rangle = \langle\psi|0\rangle\langle 0|\psi\rangle = \langle\psi|P_0|\psi\rangle$$

$$p_1 = |\langle 1|\psi\rangle|^2 = \langle 1|\psi\rangle^* \langle 1|\psi\rangle = \langle\psi|1\rangle\langle 1|\psi\rangle = \langle\psi|P_1|\psi\rangle$$

- Επομένως οι πιθανότητες εμφάνισης p_i εκφράζονται σε απλή μορφή βάση των τελεστών προβολής P_i ως $p_i = \langle\psi|P_i|\psi\rangle$.
- Παρατηρείστε ότι

$$P_0 + P_1 = |0\rangle\langle 0| + |1\rangle\langle 1| = I$$

Τρίτο Αξίωμα: Μετρήσεις

- Θα μπορούσαμε επίσης να εκφράσουμε τις πιθανές τελικές καταστάσεις $|0\rangle$ και $|1\rangle$ βάσει των τελεστών μέτρησης P_0 και P_1:

$$\langle 0|\psi\rangle\,|0\rangle = |0\rangle\,\langle 0|\psi\rangle = a\,|0\rangle = P_0\,|\psi\rangle \rightarrow |0\rangle = \tfrac{1}{a}P_0\,|\psi\rangle$$

- Ας θυμηθούμε ότι η αρχική φάση σε μία κατάσταση $|\phi\rangle$ δεν παίζει κάποιο ρόλο. Οπότε η κατάσταση $|\phi\rangle$ είναι ίδια με την $\mathrm{e}^{jv}\,|\phi\rangle$ όπου το v είναι πραγματικός αριθμός.
- Επομένως αντί του $1/a$ στην παραπάνω εξίσωση μπορούμε να χρησιμοποιήσουμε το $1/|a|$.
- Η κατάσταση $|0\rangle$ είναι ισοδύναμη με την κατάσταση

$$\frac{1}{|a|}P_0\,|\psi\rangle = \frac{P_0\,|\psi\rangle}{\sqrt{\langle\psi|P_0|\psi\rangle}}$$

Τρίτο Αξίωμα: Μετρήσεις

- Δείξαμε ότι η πιθανότητα εμφάνισης p_i των πιθανών καταστάσεων $|i\rangle$ με $i = 0$ ή $i = 1$ σε ένα qubit είναι:

$$p_i = |\langle i|\psi\rangle|^2 = \langle\psi|P_i|\psi\rangle$$

- Το αντίστοιχο αποτέλεσμα $|i\rangle$ μετά την μέτρηση ισοδύναμα γράφεται:

$$\frac{P_i|\psi\rangle}{\sqrt{\langle\psi|P_i|\psi\rangle}}$$

- Αυτό ισχύει *αξιωματικά* και στην γενική περίπτωση.
- Δηλαδή για κάθε μέτρηση που κάνουμε υπάρχουν τελεστές προβολής $P_i = |i\rangle\langle i|$ έλεσμα $|i\rangle$ για τους οποίους ισχύει:

$$\sum_i P_i = \sum_i |i\rangle\langle i| = I$$

Τρίτο Αξίωμα: Μετρήσεις

- Το τρίτο αξίωμα της κβαντικής φυσικής λέει ότι για κάθε μέτρηση που μπορούμε να σκεφτούμε σε ένα κβαντικό σύστημα (π.χ. μία ομάδα από qubits) μπορούμε να βρούμε ένα τελεστή $\mathcal{M}$ ο οποίος είναι ερμιτιανός.
- Ο $\mathcal{M}$ περιγράφει ένα μέγεθος που θέλουμε να μετρήσουμε (π.χ. θέση, ορμή, spin κτλ)
- Εφόσον πρόκειται για ερμιτιανό τελεστή, έπεται ότι θα μπορούμε να τον διαγωνιοποιήσουμε ως εξής:

$$\mathcal{M} = \sum_i \lambda_i \left|i\right\rangle \left\langle i\right| = \sum_i \lambda_i P_i$$

- όπου $\left|i\right\rangle$ τα ιδιοδιανύσματα του $\mathcal{M}$, λ_i οι αντίστοιχες ιδιοτιμές και P_i οι αντίστοιχοι τελεστής προβολής, $P_i = \left|i\right\rangle \left\langle i\right|$.

Τρίτο Αξίωμα: Μετρήσεις

- Το αποτέλεσμα της μέτρησης θα είναι ίσο με λ_m με πιθανότητα $p_m = |\langle m|\mathcal{M}|m\rangle|^2$
- Εάν το αποτέλεσμα της μέτρησης είναι το λ_m τότε η κατάσταση του συστήματος γίνεται:

$$\frac{P_m|\psi\rangle}{\sqrt{\langle\psi|P_m|\psi\rangle}}$$

- Είναι ενδιαφέρον να δούμε ότι η μέση τιμή του αποτελέσματος $\langle\mathcal{M}\rangle$ μπορεί να υπολογιστεί ως εξής:

$$\langle\mathcal{M}\rangle = \sum_m \lambda_m p_m = \sum_m \lambda_m \langle\psi|P_m|\psi\rangle = \langle\psi|\sum_m \lambda_m P_m|\psi\rangle = \langle\psi|\mathcal{M}|\psi\rangle$$

Παράδειγμα

- Ας γυρίσουμε στην απλή περίπτωση του qubit $|\psi\rangle = a|0\rangle + b|1\rangle$.
- Αν κάνουμε μία μέτρηση για να δούμε εάν το qubit είναι $|0\rangle$ ή $|1\rangle$ τότε έχουμε δύο πιθανά αποτελέσματα:
- $\lambda_0 = 0$, οπότε διαπιστώνουμε ότι το qubit είναι $|0\rangle$ και
- $\lambda_1 = 1$, οπότε διαπιστώνουμε ότι το qubit είναι $|1\rangle$.
- Ο τελεστής $\mathcal{M}$ σε αυτή την περίπτωση είναι

$$\mathcal{M} = \lambda_0 |0\rangle\langle 0| + \lambda_1 |1\rangle\langle 1| = |1\rangle\langle 1|$$

- Επομένως η μέση τιμή στην περίπτωση αυτή είναι:

$$\langle \mathcal{M} \rangle = \langle \psi | \mathcal{M} | \psi \rangle = \langle \psi | 1 \rangle \langle 1 | \psi \rangle = aa^* = |a|^2$$

- Έτσι εάν $a = b = 1/\sqrt{2}$, τότε 50% των φορών θα βρίσκουμε 0 και 50% θα βρίσκουμε 1. Επομένως η μέση τιμή είναι $|a|^2 = 0 \times \frac{1}{2} + 1 \times \frac{1}{2} = \frac{1}{2}$.

Το πρόβλημα της κβαντικής μέτρησης

- Το κβαντικό σύστημα εξελίσσεται μοναδιαία με καθορισμένο τρόπο μέχρι που κάποιος κάνει μία μέτρηση.
- Η κατάσταση του συστήματος πηγαίνει από $|\psi(t)\rangle$ εξελίσσεται όπως είδαμε ως $|\psi(t)\rangle = U|\psi(0)\rangle$.
- Όταν όμως γίνεται μία μέτρηση η $|\psi\rangle$ που περιγράφει το σύστημα πλέον περιγράφεται από την κατάσταση $|m\rangle$ που περιγράφει το σύστημα όταν διαβάσουμε την μέτρηση λ_m.
- Το αποτέλεσμα της μέτρησης είναι *τυχαίο* και έρχεται σε αντίθεση με την αυστηρά καθορισμένη εξέλιξη του συστήματος όταν δεν μετράμε.
- Πως συμβιβάζονται αυτά τα δύο; Εφόσον η μέτρηση είναι μία φυσική διαδικασία δεν θα έπρεπε και αυτή να περιγράφεται από κάποιον μοναδιαίο τελεστή;

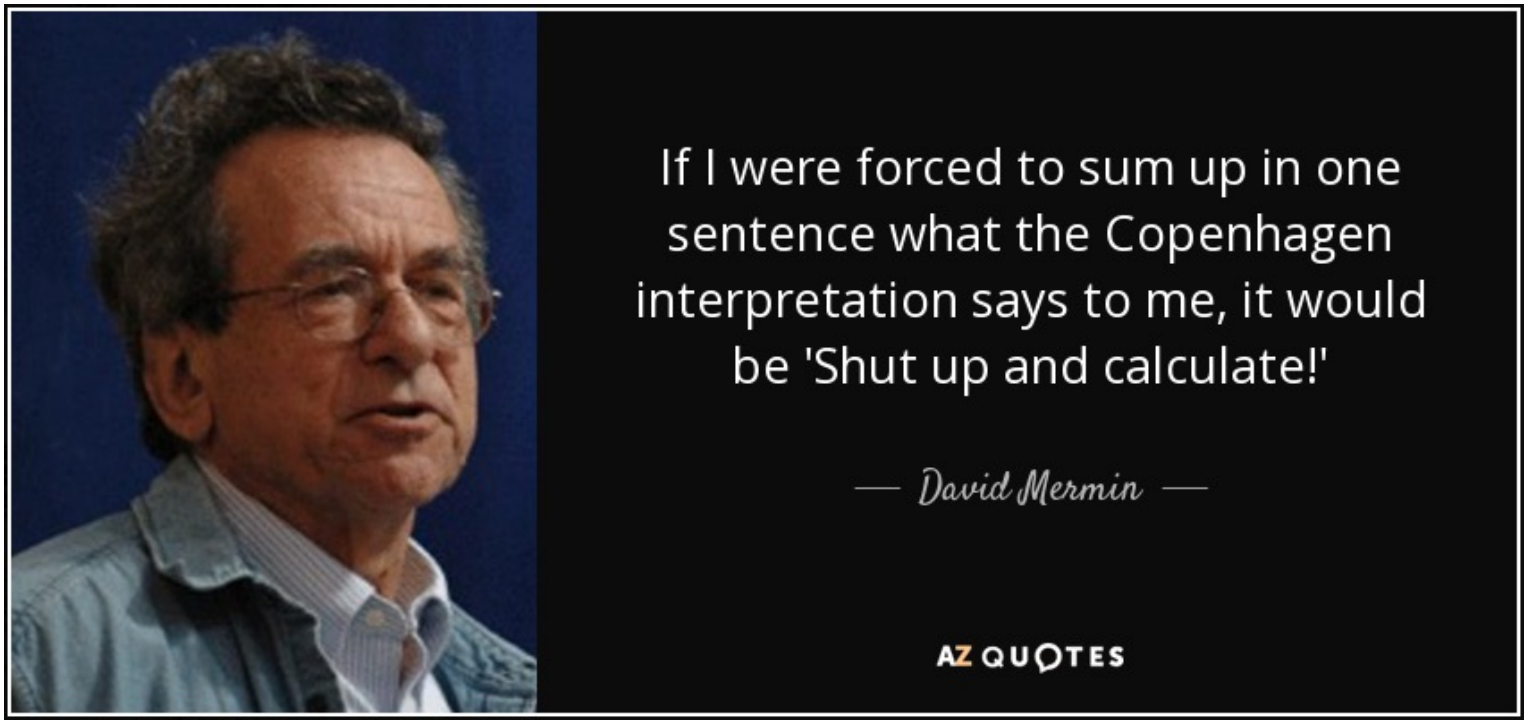
Το πρόβλημα της κβαντικής μέτρησης

- Στην περίπτωση του απλού qubit, $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$, όταν μετράμε να δούμε σε ποιά κατάσταση είναι το qubit θα πάρουμε $|0\rangle$ ή $|1\rangle$ με πιθανότητα $|a|^2$ και $|b|^2$ αντίστοιχα.
- Ποιά όμως είναι η *φυσική διαδικασία* που αναγκάζει το $|\psi\rangle$ να γίνει είτε $|0\rangle$ ή $|1\rangle$;
- Στην κβαντική φυσική αυτό ονομάζεται *κατάρρευση της κυματοσυνάστησης*. Δηλαδή λέμε ότι η $|\psi\rangle$ καταρρέει στην $|0\rangle$ ή στην $|1\rangle$ όταν γίνεται η μέτρηση.
- Υπάρχουν διάφορες ερμηνείες για το ζήτημα αυτό, κατά την ταπεινή μου άποψη μου, καμία δεν είναι ικανοποιητική.

Η ερμηνεία της Κοπεγχάγης

- Η ερμηνεία της Κοπεγχάγης είναι ίσως η πιο διαδεδομένη ερμηνεία της κβαντικής μέτρησης στην φυσική.
- Έχει προταθεί από τον Nils Bohr και τον Werner Heisenberg οι οποίοι την υποστήριξαν στα μέσα της δεκαετίας του 1920 στο ινστιτούτο του Bohr στην Κοπεγχάγη.
- Η ερμηνεία παίρνει πολύ στα σοβαρά τα τρία αξιώματα της κβαντικής φυσικής.
- Η κυμοτοσυνάρτηση και η κατάρρευση της κυματοσυνάρτησης είναι *πραγματικές* και *θεμελιώδεις*.
- Έτσι λειτουργεί η φύση ίσως στην πιο βασική της μορφή. Δεν έχει νόημα να διερωτόμαστε το "γιατί".
- Το σύμπαν είναι τυχαίο *από την φύση* του και επομένως όταν ένας παρατηρητής μετράει θα λάβει τυχαία αποτελέσματα.

Shut up and calculate



Η ερμηνεία της Κοπεγχάγης

- Θα υιοθετήσουμε την προσέγγιση του Mermin αλλά πριν το κάνουμε ας θέσουμε μερικά ερωτήματα.
- Είναι η κβαντική φυσική, η τελική θεωρία που περιγράφει τα πάντα στο κόσμο; Μέχρι στιγμής δεν έχουμε κατορθώσει να την συμβιβάσουμε με την βαρύτητα άρα μπορεί και να μην είναι.
- Τι είναι ο παρατηρητής; Είναι ο άνθρωπος που διαβάζει τα αποτελέσματα; είναι η συσκευή μέτρησης; Γιατί αυτός μπορεί να προκαλεί την κατάρρευση ενώ τα άλλα συστήματα εξελίσσονται μοναδίαια;
- Μπορούμε όντως να δεχτούμε ότι το σύμπαν είναι τυχαίο; Βέβαια και όταν ο Νεύτωνας έλεγε ότι τίποτα δεν είναι τυχαίο πάλι δεν μας άρεσε.

Η ερμηνεία των πολλαπλών κόσμων

- Όμως δεν είναι η ερμηνεία της Κοπεγχάγης η μόνη δυνατή ερμηνεία.
- Η ερμηνεία των πολλαπλών κόσμων προτείνει μία εναλλακτική που προτιμάται από πολλούς.
- Στην ερμηνεία αυτή, υπό μία έννοια δεν υπάρχει η κατάρρευση της κυματοσυνάρτησης.
- Όταν μετρήσουμε ένα qubit $\psi = a\,|0\rangle + b\,|1\rangle$ τότε και τα δύο ενδεχόμενα συνηπάρχουν.
- Δηλαδή το αποτέλεσμα της μέτρησης είναι:

$$|\psi'\rangle = a\,|0\rangle\,|\lambda_0\rangle + b\,|1\rangle\,|\lambda_1\rangle$$

- οπου με $|\lambda_i\rangle$ έχουμε συμβολίσει την κατάσταση όπου ο παρατηρητής έχει μετρήσει το $\lambda_0 = 0$ ή το $\lambda_1 = 1$.

Η ερμηνεία των πολλαπλών κόσμων

- Σύμφωνα με αυτή την ερμηνεία, το σύμπαν διακλαδίζεται όταν γίνεται μία μέτρηση.
- Στον ένα κλάδο ο παρατηρητής έχει μετρήσει $|0\rangle$ στο άλλο έχει μετρήσει $|1\rangle$.
- Οι δύο κλάδοι αντιστοιχούν σε δύο ξεχωριστούς κόσμους: στον ένα κόσμο μετρήσαμε $|0\rangle$ στον άλλο $|1\rangle$.
- Και οι δύο υπάρχουν παράλληλα και ανεξάρτητα ο ένας με τον άλλο. Δεν μπορούμε πλέον να πάμε από τον ένα κόσμο στον άλλο.
- Διακλαδίζεται και ο παρατηρητής. Στον ένα κόσμο είναι στην κατάσταση $|\lambda_0\rangle$ στην άλλη στο $|\lambda_1\rangle$.

Η ερμηνεία των πολλαπλών κόσμων

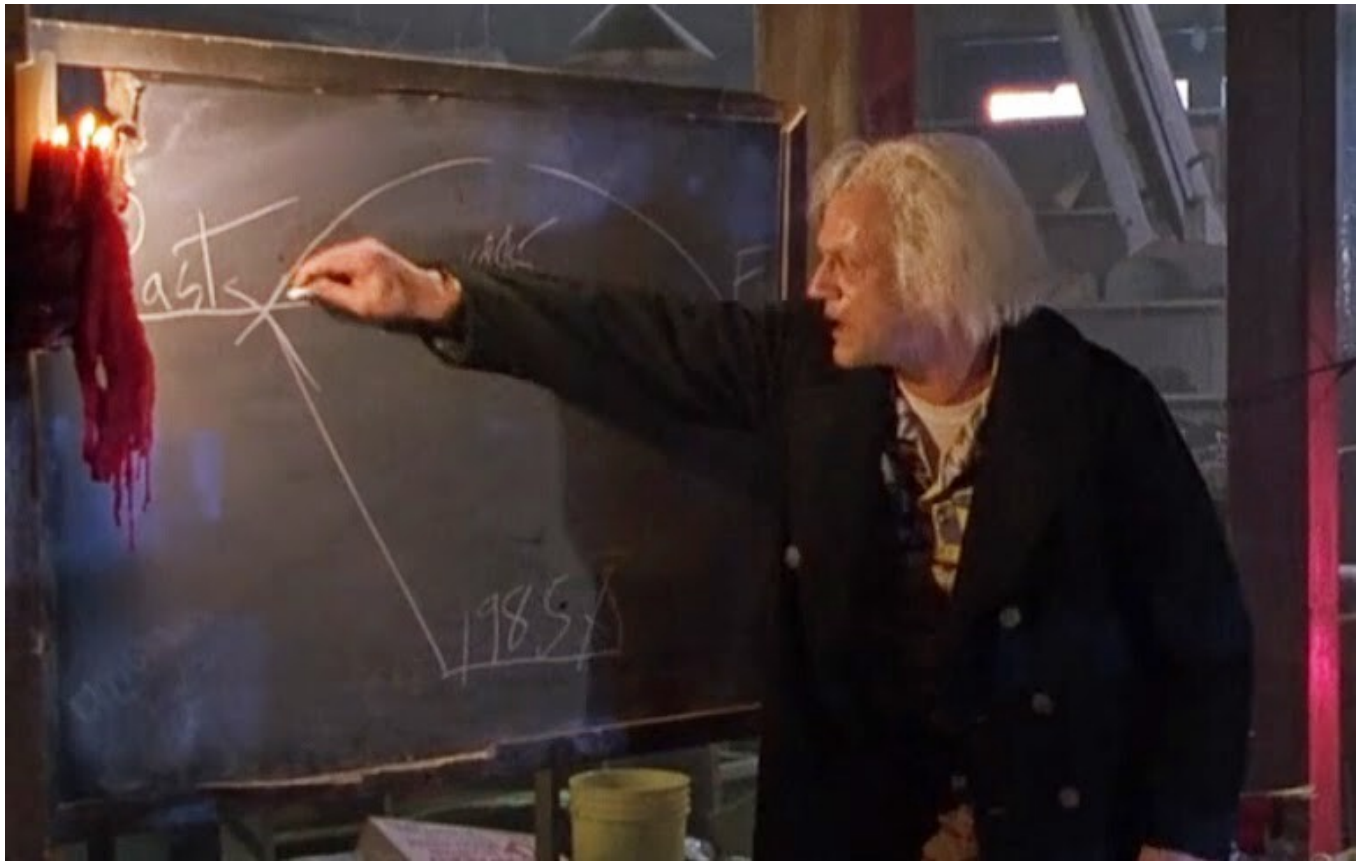
- Οπότε η ερμηνεία αυτή μας λέει ότι όταν μετράτε ένα qubit ή ένα άλλο κβαντικό σύστημα, δημιουργούνται δύο ή περισσότερα αντίγραφα του εαυτού σας και κάθε αντίγραφο παίρνει διαφορετικό αποτέλεσμα για την μέτρηση.
- Δεν μπορείτε να έχετε κάποια επαφή όμως με τον εαυτό σας που μέτρησε το άλλο αποτέλεσμα.
- Οι φιλοσοφικές επιπτώσεις φαίνονται ριζοσπαστικές.
- Κάθε φορά που κάπου γίνεται μία μέτρηση το σύμπαν διακλαδίζεται. Επομένως έχουμε έναν τεράστιο αριθμό παράλληλων κόσμων οι οποίοι συνεχώς διακλαδίζονται.
- Προσοχή όμως γιατί μερικές φορές παρασυρόμαστε σε περιέργες ερμηνείες που είναι μάλλον επιστημονική φαντασία.

Back to the future II

Back to the future II

- Στην ταινία Back to the future II, ο Biff γυρνάει στο 1955 και δίνει στον νεαρό εαυτό του ένα περιοδικό που έχει όλα τα μελλοντικά αποτελέσματα των αγώνων.
- Με τον τρόπο αυτό (σύμφωνα με το σενάριο!) το μέλλον αλλάζει και ο Biff γίνεται μεγιστάνας.
- Ο Dr. Brown και ο Marty πρέπει και αυτοί να ταξιδέψουν στο 1955 για να αποτρέψουν τον Biff να δώσει στον εαυτό του το περιοδικό.
- Ο Dr. Brown εξηγεί ότι το σύμπαν έχει διακλαδιστεί και πρέπει να γυρίσουν πίσω *πριν γίνει η διακλάδωση*.
- Ακόμα και αν καταφέρνανε οι ήρωες να γυρίσουν στο παρελθόν πως θα καταφέρουν να σίγουρα να επιλέξουν τον ίδιο κλάδο που επέλεξε ο Biff;

Back to the future II



Χειρότερα και από επιστημονική φαντασία

Google says it accessed parallel universes with its new supercomputer

- **READ MORE:** Scientist says human consciousness comes from other dimension

By MATTHEW PHELAN SENIOR SCIENCE REPORTER FOR DAILYMAIL.COM
PUBLISHED: 17:49 BST, 15 December 2024 | **UPDATED:** 17:56 BST, 15 December 2024

Share 499 shares 503 View comments

Google's quantum computing breakthrough on Monday has left the physicist who heads the project a believer in 'the idea that we live in a multiverse.'

'Willow,' the tech giant's new quantum chip, succeeded in solving a computational problem so complex it would have taken today's best super-computers an estimated 10 septillion years to solve it — vastly more than the age of our entire universe.

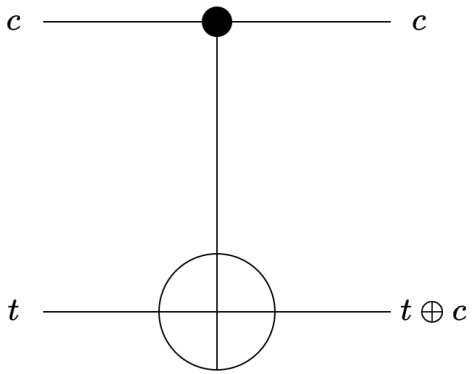
But **Google** said its new quantum computer solved the puzzle 'in under five minutes.'

Πύλες πολλών qubits

- Σε προηγούμενη διάλεξη είχαμε δει μερικές βασικές κβαντικές πύλες ενός qubit.
- Παράδειγμα αποτελούν οι πύλες X (κβαντικό NOT), Y και Z.
- Οι κβαντικοί υπολογισμοί φυσικά δεν περιορίζονται σε πύλες του ενός qubit.
- Τα πράγματα γίνονται ιδιαίτερα ενδιαφέροντα όταν συνδυάζουμε πολλά qubit μαζί.
- Για παράδειγμα ας υποθέσουμε ότι ένα qubit $|t\rangle$ ελέγχεται από ένα άλλο qubit $|c\rangle$.
- Το qubit $|c\rangle$ εμφανίζεται στην έξοδο ατόφιο χωρίς κάποια αλλαγή.
- Στο qubit $|t\rangle$ εφαρμόζουμε την πύλη NOT εάν $|c\rangle = |1\rangle$ ή παραμένει αμετάβλητο εάνε $|c\rangle = |0\rangle$.

Η πύλη CNOT

- Η πύλη αυτή υπάρχει και στα κλασικά ψηφιακά κυκλώματα αν και δεν χρησιμοποιείται τόσο συχνά.
- Η παραδοσιακή έκδοση της πύλης όπου τα c και t είναι απλά bits φαίνεται παρακάτω.



Η πύλη CNOT

- Πως θα γενικεύσουμε την CNOT στην κβαντική περίπτωση;
- Περιγράφουμε αρχικά την δράση της πύλης στην υπολογιστική βάση.
- Επειδή έχουμε δύο qubit θα έχουμε τέσσερις καταστάσεις βάσης $|ct\rangle$ όπου το c και το t θα είναι 0 ή 1: $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$
- Επομένως σε ότι αφορά τις καταστάσεις βάσεις ανάλογα με το εάν το πρώτο qubit (δηλαδή το $|c\rangle$) είναι μηδέν ή ένα έχουμε:

$$|00\rangle \rightarrow |00\rangle$$

$$|01\rangle \rightarrow |01\rangle$$

$$|10\rangle \rightarrow |11\rangle$$

$$|11\rangle \rightarrow |10\rangle$$

Η πύλη CNOT

- Εφόσον ξέρουμε πως η CNOT δρα πάνω στις καταστάσεις βάσης, μπορούμε να καταλάβουμε την δράση της σε μία υπέρθεση καταστάσεων:

$$|\psi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$$

- Θυμηθείτε ότι οτιδήποτε γίνεται σε επίπεδο επεξεργασίας στην κβαντική υπολογιστική αντιστοιχεί σε μοναδιαίο τελεστή.
- Οι τελεστές αυτοί είναι γραμμικοί αφού περιγράφονται και απο πίνακες. Έστω U_{C} ο τελεστής που αντιστοιχεί στην CNOT, τότε θα έχουμε:

$$U_{\mathrm{C}}\,|00\rangle = |00\rangle$$

$$U_{\mathrm{C}}\,|01\rangle = |01\rangle$$

$$U_{\mathrm{C}}\,|10\rangle = |11\rangle$$

$$U_{\mathrm{C}}\,|11\rangle = |10\rangle$$

Η πύλη CNOT

- Χρησιμοποιώντας την γραμμικότητα του U_{C} γράφουμε:

$$\begin{aligned}|\phi\rangle = U_{\mathrm{C}}|\psi\rangle = U_{\mathrm{C}}\left(a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle\right) = \\ aU_{\mathrm{C}}|00\rangle + bU_{\mathrm{C}}|01\rangle + cU_{\mathrm{C}}|10\rangle + dU_{\mathrm{C}}|11\rangle = \\ = a|00\rangle + b|01\rangle + c|11\rangle + d|10\rangle\end{aligned}$$

- Επομένως σε μία υπέρθεση καταστάσεων η πύλη CNOT στην ουσία ανταλλάσει τους συντελεστές των καταστάσεων $|10\rangle$ και $|11\rangle$.

Η πύλη CNOT

- Μπορούμε να βρούμε τον πίνακα που περιγράφει την πύλη CNOT.
- Έχουμε δύο qubits και $2^2 = 4$ διαφορετικές καταστάσεις βάσης $|ct\rangle$.
- Ο πίνακας U_{C} επομένως θα είναι 4×4.
- Καλό θα είναι να αριθμήσουμε τις καταστάσεις ως εξής: $|0\rangle \to |00\rangle$, $|1\rangle \to |01\rangle$, $|2\rangle \to |10\rangle$, $|3\rangle \to |11\rangle$.
- Με αυτή την αρίθμηση:

$$U_{\mathrm{C}}\,|0\rangle = |0\rangle$$

$$U_{\mathrm{C}}\,|1\rangle = |1\rangle$$

$$U_{\mathrm{C}}\,|2\rangle = |3\rangle$$

$$U_{\mathrm{C}}\,|3\rangle = |2\rangle$$

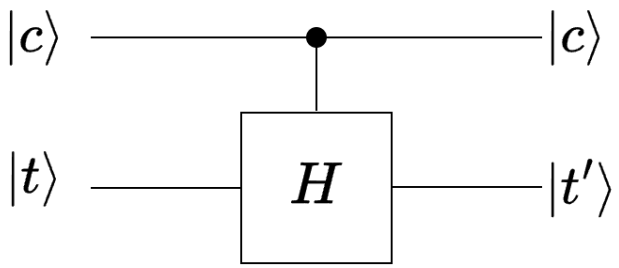
Η πύλη CNOT

- Ο πίνακας που περιγράφει τον τελεστή CNOT θα έχει στοιχεία $u_{\mu\nu} = \langle \nu | U_{\mathrm{C}} | \mu \rangle$.
- Επομένως βρίσκουμε εύκολα ότι ο πίνακας θα έχει όλα τα στοιχεία ίσα με μηδέν εκτός από τα $u_{00} = 1, u_{11} = 1, u_{23} = 1$ και $u_{32} = 1$.
- Ο πίνακας που περιγράφει την πύλη γράφεται:

$$U_{\mathrm{C}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Ελεγχόμενη πύλη Hadamard

- Ας δούμε τώρα ένα λίγο πιο σύνθετο παράδειγμα.
- Ας θεωρήσουμε την ελεγχόμενη πύλη Hadamard,
- Παρακάτω δείχνουμε το σύμβολο της:



- Όπως και πριν, η πύλη εφαρμόζεται στο qubit $|t\rangle$ όταν το $|c\rangle = |1\rangle$ ή ισοδύναμα $c = 1$.
- Ένας τρόπος να γράψουμε την δράση της πύλης είναι:

$$|c\rangle\,|t\rangle \rightarrow |c\rangle\,H^c\,|t\rangle$$

Ελεγχόμενη πύλη Hadamard

- Ας δούμε τώρα πως δρα η πύλη στις συναρτήσεις βάσης.

$$|00\rangle \to |00\rangle \qquad |0\rangle \to |0\rangle$$

$$|01\rangle \to |01\rangle \qquad |1\rangle \to |1\rangle$$

$$|10\rangle \to \frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle \qquad |2\rangle \to \frac{1}{\sqrt{2}}|2\rangle + \frac{1}{\sqrt{2}}|3\rangle$$

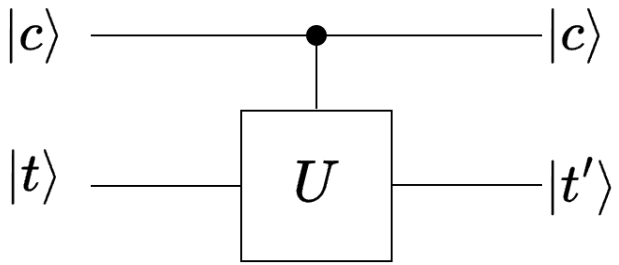
$$|11\rangle \to \frac{1}{\sqrt{2}}|10\rangle - \frac{1}{\sqrt{2}}|11\rangle \qquad |3\rangle \to \frac{1}{\sqrt{2}}|2\rangle - \frac{1}{\sqrt{2}}|3\rangle$$

- Ο πίνακας που περιγράφει την πύλη θα είναι

$$\mathcal{C}_H = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

Πως να φτιάχνετε ελεγχόμενες πύλες

- Είναι ενδιαφέρον να δούμε ότι μία οποιαδήποτε ελεγχόμενη πύλη δύο εισόδων όπου η μία είσοδος είναι η είσοδος ελέγχου και η άλλη η είσοδος υπολογισμού μπορεί να υλοποιηθεί χρησιμοποιώντας μόνο α) πύλες CNOT και β) απλές πύλες ενός qubit.



- Εν γένει συμβολίζουμε την ελεγχόμενη πύλη που πραγματοποιεί τον μοναδιαίο μετασχηματισμό και έχει ένα qubit ελέγχου ως $C^1(U)$.
- Η πύλη μπορεί να περιγραφεί και ως:

$$|c\rangle\,|t\rangle \rightarrow |c\rangle\,U^c\,|t\rangle$$

Πως να φτιάχνετε ελεγχόμενες πύλες

- Αν υποθέσουμε ότι ο πίνακας U έχει στοιχεία:

$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

- Τότε η δράση του πίνακα περιγράφεται ως εξής:

$$|00\rangle \to |00\rangle \qquad |0\rangle \to |0\rangle$$

$$|01\rangle \to |01\rangle \qquad |1\rangle \to |1\rangle$$

$$|10\rangle \to u_{00}\,|10\rangle + u_{01}\,|11\rangle \qquad |2\rangle \to u_{00}\,|2\rangle + u_{01}\,|3\rangle$$

$$|11\rangle \to u_{10}\,|10\rangle + u_{11}\,|11\rangle \qquad |3\rangle \to u_{10}\,|2\rangle + u_{11}\,|3\rangle$$

Πως να φτιάχνετε ελεγχόμενες πύλες

- Οπότε ο πινακας που περιγράφει την πύλη δίνεται από την σχέση:

$$C^1(U) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$$

- Μπορούμε να υλοποιήσουμε την πύλη $C^1(U)$ χρησιμοποιώντας μόνο πύλες CNOT και απλές πύλες ενός qubit.
- Για να δούμε γιατί ισχύει αυτό ας σκεφτούμε καταρχήν την μορφή του πίνακα U στην γενική περίπτωση:

$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

Μία γενική έκφραση για το U

- Εφόσον ο U είναι μοναδιαίος θα έχουμε:

$$UU^{\mathrm{T}} = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix} \begin{bmatrix} u_{00}^* & u_{10}^* \\ u_{01}^* & u_{11}^* \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

- Επομένως θα πρέπει:

$$|u_{00}|^2 + |u_{01}|^2 = 1$$
$$u_{00}u_{10}^* + u_{01}u_{11}^* = 0$$
$$u_{10}u_{00}^* + u_{11}u_{01}^* = 0$$
$$|u_{10}|^2 + |u_{11}|^2 = 1$$

- Για να κάνουμε λίγο πιο εύκολη τη ζωή μας, μπορούμε να θέσουμε:

$$u_{00} = x, u_{01} = y, u_{10} = z, u_{11} = w$$

Μία γενική έκφραση για το U

- Με την πιο απλή αυτή μορφή οι εξισώσεις γράφονται ως εξής:

$$|x|^2 + |y|^2 = 1$$

$$xz^* + yw^* = 0$$

$$x^*z + y^*w = 0$$

$$|z|^2 + |w|^2 = 1$$

- Παρατηρείστε ότι η 2η και η 3η εξίσωση είναι στην ουσία ίδιες αφού η μία προκύπτει από την άλλη αν πάρουμε μιγαδικά συζυγή.
- Μπορούμε να θέσουμε $|x| = \cos\phi$, $|y| = \sin\phi$ ώστε να πληρείται η πρώτη εξίσωση, $|z| = \sin\theta$, $|w| = \cos\theta$, όπου $0 \leq \phi, \theta \leq \frac{\pi}{2}$.
- Από την δεύτερη εξίσωση προκύπτει:

$$|x||z| = |y||w| \rightarrow \cos\phi\sin\theta - \sin\phi\cos\theta = \sin(\theta - \phi) = 0$$

Μία γενική έκφραση για το U

- Εφόσον $0 \leq \phi, \theta \leq \frac{\pi}{2}$ και $\sin(\theta - \phi) = 0$ έπεται ότι $\theta = \phi$.
- Γράφουμε τώρα τους μιγαδικούς αριθμούς ως εξής:

$$x = \cos\theta e^{j\phi_x} \qquad z = -\sin\theta e^{j\phi_z}$$

$$y = \sin\theta e^{j\phi_y} \qquad w = \cos\theta e^{j\phi_w}$$

- Οπότε από τα παραπάνω προκύπτει ότι:

$$xz^* + yw^* = \cos\theta\sin\theta e^{j\phi_x - j\phi_z} - \cos\theta\sin\theta e^{j\phi_y - j\phi_w} = 0$$

- και επομένως εάν $\theta \neq 0, \frac{\pi}{2}$ θα έχουμε:

$$e^{j\phi_x - j\phi_z} = e^{j\phi_y - j\phi_w} \rightarrow \phi_x + \phi_w = \phi_y + \phi_z$$

Μία γενική έκφραση για το U

- Ας θέσουμε:

$$2\alpha = \phi_x + \phi_w = \phi_y + \phi_z$$
$$\phi_z - \phi_x = \beta$$
$$\phi_y - \phi_x = \delta$$

- Τότε βρίσκουμε:

$$\phi_z = \phi_x + \beta \qquad \phi_w = 2\alpha - \phi_x$$
$$\phi_y = \phi_x + \delta \qquad 2\alpha = \phi_y + \phi_z = 2\phi_x + \beta + \delta$$

- Λύνοντας τις εξισώσεις:

$$\phi_x = \alpha - \frac{\beta}{2} - \frac{\delta}{2} \qquad \phi_z = \alpha + \frac{\beta}{2} - \frac{\delta}{2}$$
$$\phi_y = \alpha - \frac{\beta}{2} + \frac{\delta}{2} \qquad \phi_w = \alpha + \frac{\beta}{2} + \frac{\delta}{2}$$

Μία γενική έκφραση για το U

- Τελικά αν θέσουμε και $\theta = \frac{\gamma}{2}$ θα έχουμε την εξής γενική μορφή για οποιοδήποτε μοναδιαίο πίνακα:

$$U = \begin{bmatrix} \cos\frac{\gamma}{2} e^{j(\alpha-\beta/2-\delta/2)} & -\sin\frac{\gamma}{2} e^{j(\alpha-\beta/2+\delta/2)} \\ \sin\frac{\gamma}{2} e^{j(\alpha+\beta/2-\delta/2)} & \cos\frac{\gamma}{2} e^{j(\alpha+\beta/2+\delta/2)} \end{bmatrix}$$

- Θα δείξουμε τώρα ότι το U μπορεί να γραφεί ως γινόμενο των τελεστών περιστροφής $\mathcal{R}_z$ και $\mathcal{R}_y$ που είδαμε ότι δίνονται από τις σχέσεις:

$$\mathcal{R}_y(\gamma) = \begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix}$$

$$\mathcal{R}_z(\omega) = \begin{bmatrix} \mathrm{e}^{-j\omega/2} & 0 \\ 0 & \mathrm{e}^{j\omega/2} \end{bmatrix}$$

Μία γενική έκφραση για το U

- Για να δούμε πως θα γράψουμε το U ως γινόμενο των $\mathcal{R}_z$ και $\mathcal{R}_y$, ας σκεφτούμε τι συμβαίνει όταν πολλαπλασιάζουμε έναν πίνακα A με στοιχεία a_{pq} με έναν διαγώνιο πίνακα D με στοιχεία $d_{pq} = 0$ όταν $p \neq q$.
- Αν υπολογίσουμε το $\Gamma = DA$ τότε βλέπουμε ότι τα στοιχεία γ_{pq} του πίνακα Γ δίνονται από την σχέση:

$$\gamma_{pq} = \sum_m d_{pm}\gamma_{mq} = d_{pp}a_{pq}$$

- Οπότε όταν πολλαπλασιάζουμε *αριστερά* με τον D κάθε *γραμμή* του A πολλαπλασιάζεται με το αντίστοιχο διαγώνιο στοιχείο του D.
- Αντίστοιχα όταν πολλαπλασιάζουμε *δεξιά* με τον D τότε ο πίνακας $E = AD$ έχει στοιχεία $e_{pq} = a_{pq}d_{qq}$.
- Οπότε όταν πολλαπλασιάζουμε *δεξιά* με τον D κάθε *στήλη* του A πολλαπλασιάζεται με το αντίστοιχο διαγώνιο στοιχείο του D.

Μία γενική έκφραση για το U

- Μπορούμε να γράψουμε το U ως εξής:

$$U = e^{j\alpha} \begin{bmatrix} \cos\frac{\gamma}{2} e^{-j\beta/2} e^{-j\delta/2} & -\sin\frac{\gamma}{2} e^{-j\beta/2} e^{j\delta/2} \\ \sin\frac{\gamma}{2} e^{j\beta/2} e^{-j\delta/2} & \cos\frac{\gamma}{2} e^{j\beta/2} e^{j\delta/2} \end{bmatrix}$$

- Τα στοιχεία του πίνακα επομένως προκύπτουν από τα στοιχεία του πίνακα $\mathcal{R}_y$

$$\mathcal{R}_y(\gamma) = \begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix}$$

- αν πολλαπλασιάσουμε την πρώτη και την δεύτερη γραμμή του με το $e^{-j\beta/2}$ και το $e^{j\beta/2}$ αντίστοιχα και την πρώτη και την δεύτερη στήλη του με $e^{-j\delta/2}$ και το $e^{j\delta/2}$ αντίστοιχα.
- Οπότε:

$$U = e^{j\alpha} \mathcal{R}_z(\beta) \mathcal{R}_y(\gamma) \mathcal{R}_z(\delta)$$

Μία γενική έκφραση για το U

- Αν θεωρήσουμε τους παρακάτω πίνακες:

$$A = \mathcal{R}_z(\beta)\mathcal{R}_y(\gamma/2)$$

$$B = \mathcal{R}_y(-\gamma/2)\mathcal{R}_z(-(\beta+\delta)/2)$$

$$C = \mathcal{R}_z((\delta-\beta)/2)$$

- Τότε μπορούμε να δείξουμε ότι:

$$ABC = \mathcal{R}_z(\beta)\mathcal{R}_y(\gamma/2)\mathcal{R}_y(-\gamma/2)\mathcal{R}_z(-(\beta+\delta)/2)\mathcal{R}_z((\delta-\beta)/2) = \mathcal{R}_z(\beta)\mathcal{R}_z(-(\beta+\delta)/2)\mathcal{R}_z((\delta-\beta)/2) = \mathcal{R}_z(\beta-\beta/2-\delta/2+\delta/2-\beta/2) = \mathcal{R}_z(0) = I$$

Μία γενική έκφραση για το U

- Επίσης:

$$X\mathcal{R}_y(\omega)X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \cos\frac{\omega}{2} & -\sin\frac{\omega}{2} \\ \sin\frac{\omega}{2} & \cos\frac{\omega}{2} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} =$$

$$\begin{bmatrix} \sin\frac{\omega}{2} & \cos\frac{\omega}{2} \\ \cos\frac{\omega}{2} & -\sin\frac{\omega}{2} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \cos\frac{\omega}{2} & \sin\frac{\omega}{2} \\ -\sin\frac{\omega}{2} & \cos\frac{\omega}{2} \end{bmatrix} = \mathcal{R}_y(-\omega)$$

$$X\mathcal{R}_z(\omega)X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} e^{-j\omega/2} & 0 \\ 0 & e^{j\omega/2} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} =$$

$$\begin{bmatrix} e^{-j\omega/2} & 0 \\ 0 & e^{-j\omega/2} \end{bmatrix} = \mathcal{R}_z(-\omega)$$

- Οπότε εφόσον και $XX = I$ θα έχουμε

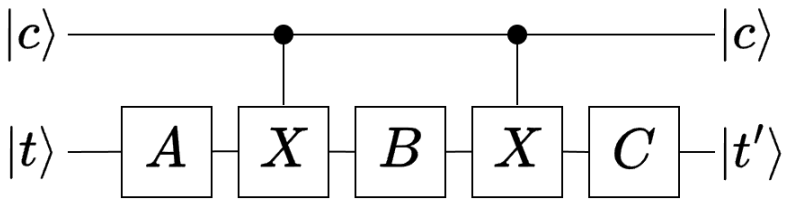
$$XBX = X\mathcal{R}_y(-\tfrac{\gamma}{2})XX\mathcal{R}_z(-\tfrac{\beta+\delta}{2})X = \mathcal{R}_y(\tfrac{\gamma}{2})\mathcal{R}_z(\tfrac{\beta+\delta}{2})$$

Πως να φτιάχνετε ελεγχόμενες πύλες

- Επομένως αν υπολογίσουμε το $AXBXC$ θα έχουμε:

$$AXBXC = \mathcal{R}_z(\beta)\mathcal{R}_y(\tfrac{\gamma}{2})\mathcal{R}_y(\tfrac{\gamma}{2})\mathcal{R}_z(\tfrac{\beta+\delta}{2})\mathcal{R}_z(\tfrac{\delta-\beta}{2}) = \mathcal{R}_z(\beta)\mathcal{R}_y(\gamma)\mathcal{R}_z(\delta)$$

- Η παραπάνω εξίσωση σημαίνει ότι $U = e^{j\alpha}AXBXC$ και μας δίνει ένα τρόπο να υλοποιούμε μια $C^1(U)$ χρησιμοποιώντας ελεγχόμενες NOT.



- Όταν το $|c\rangle$ είναι $|0\rangle$ τότε οι ελεγχόμενες NOT δεν επιδρούν στο κάτω bit και έχουμε $|t'\rangle = ABC|t\rangle = |t\rangle$.
- Για $|c\rangle = |1\rangle$ έχουμε: $|t'\rangle = AXBXC|t\rangle = e^{-j\alpha}U|t\rangle$.

Ολίσθηση φάσης

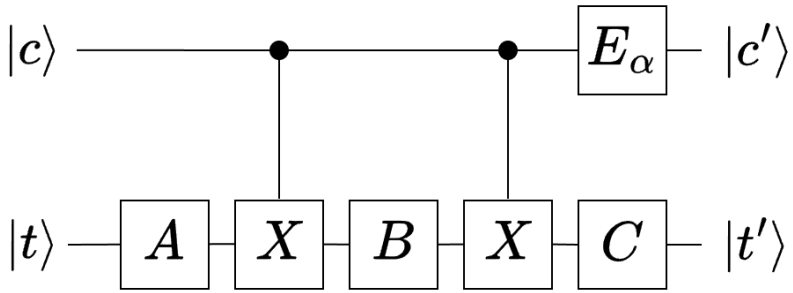
- Το μόνο που πρέπει να σκεφτούμε είναι πως θα αφαιρέσουμε το $e^{-j\alpha}$ στην περίπτωση όπου $|c\rangle = |1\rangle$.
- Ας θεωρήσουμε μία πύλη ενός qubit E_α η οποία αντιστοιχεί σε έναν πίνακα:

$$E_\alpha = \begin{bmatrix} 1 & 0 \\ 0 & e^{j\alpha} \end{bmatrix}$$

- Τι κάνει αυτή η πύλη; όταν στην είσοδο έχουμε $|0\rangle$ στην έξοδο έχουμε $|0\rangle$ ενώ όταν στην είσοδο έχουμε $|1\rangle$ στην έξοδο παίρνουμε $e^{j\alpha}|1\rangle$.
- Άρα αν εφαρμόσουμε την E_α στο $|c\rangle$, θα προστίθεται μία φάση $e^{j\alpha}$ όταν $|c\rangle = |1\rangle$.

Ολίσθηση φάσης

- Στο παρακάτω κύκλωμα:



$$|0\rangle\,|t\rangle \to |0\rangle\,|t\rangle$$

$$|1\rangle\,|t\rangle \to |1\rangle\, e^{j\alpha} AXBXC\,|t\rangle = |1\rangle\, U\,|t\rangle$$

- Δηλαδή ενώ εφαρμόζουμε και μία πύλη στο $|c\rangle$ επειδή είναι μαζί με το $|t\rangle$ τελικά το πλάτος του $|c'\rangle$ στην έξοδο συνδυάζεται με το πλάτος του $|t'\rangle$ για να δώσουν την σωστή κβαντική κατάσταση:

$$|c\rangle\,|t\rangle = |c\rangle\, U^c\,|t\rangle\, 5$$

Παράδειγμα: Ελεγχόμενη Hadamard

- Πως θα υλοποιούσαμε μία ελεγχόμενη Hadamard με αυτό τον τρόπο, δηλαδή χρησιμοποιώντας ελεγχόμενες NOT και απλές πύλες ενός qubit;
- Ο πίνακας της πύλης Hadamard είναι:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

- Ας θυμηθούμε την γενική μορφή οποιοδήποτε μοναδιαίου 2×2 πίνακα:

$$U = \begin{bmatrix} x & y \\ z & w \end{bmatrix} = e^{j\alpha} \begin{bmatrix} \cos\frac{\gamma}{2} e^{-j\beta/2} e^{-j\delta/2} & -\sin\frac{\gamma}{2} e^{-j\beta/2} e^{j\delta/2} \\ \sin\frac{\gamma}{2} e^{j\beta/2} e^{-j\delta/2} & \cos\frac{\gamma}{2} e^{j\beta/2} e^{j\delta/2} \end{bmatrix}$$

Παράδειγμα: Ελεγχόμενη Hadamard

- Είχαμε δει ότι εάν ϕ_x, ϕ_y, ϕ_z και ϕ_w σχετίζονται με τα ορίσματα των μιγαδικών αριθμών x, y, z και w:

$$x = \cos\frac{\gamma}{2}e^{j\phi_x} \qquad z = \sin\frac{\gamma}{2}e^{j\phi_z}$$

$$y = -\sin\frac{\gamma}{2}e^{j\phi_y} \qquad w = \cos\frac{\gamma}{2}e^{j\phi_w}$$

- Έχουμε $\phi_x = \phi_z = 0$ και $\phi_y = \phi_w = \pi$

$$2\alpha = \phi_x + \phi_w = \pi \rightarrow \alpha = \frac{\pi}{2}$$

$$\beta = \phi_z - \phi_x = 0$$

$$\delta = \phi_y - \phi_x = \pi$$

- Επίσης $|x| = \cos\frac{\gamma}{2} = \frac{1}{\sqrt{2}}$ οπότε $\gamma = \frac{\pi}{2}$.

Παράδειγμα: Ελεγχόμενη Hadamard

- Θα έχουμε:

$$A = \mathcal{R}_z(0)\mathcal{R}_y(\tfrac{\pi}{4})$$
$$B = \mathcal{R}_y(-\tfrac{\pi}{4})\mathcal{R}_z(-\tfrac{\pi}{2})$$
$$C = \mathcal{R}_z(\tfrac{\pi}{2})$$

- Είναι εύκολο να δούμε ότι:

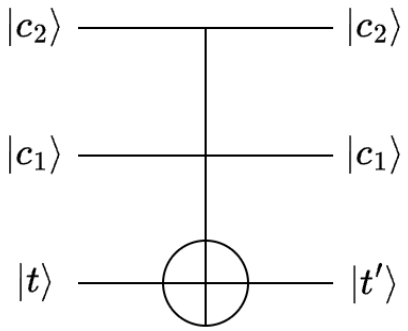
$$ABC = I$$

- Επίσης, εφόσον $XX = I$,

$$e^{j\alpha}AXBXC = \mathcal{R}_y(\tfrac{\pi}{4})X\mathcal{R}_y(-\tfrac{\pi}{4})XX\mathcal{R}_z(-\tfrac{\pi}{2})X\mathcal{R}_z(\tfrac{\pi}{2}) =$$
$$j\mathcal{R}_y(\tfrac{\pi}{4})\mathcal{R}_y(\tfrac{\pi}{4})\mathcal{R}_z(\tfrac{\pi}{2})\mathcal{R}_z(\tfrac{\pi}{2}) = j\mathcal{R}_y(\tfrac{\pi}{2})\mathcal{R}_z(\pi) = \frac{j}{\sqrt{2}}\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix}\begin{bmatrix}-j & 0\\ 0 & j\end{bmatrix} =$$
$$= \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} = H$$

Η πύλη Toffoli

- Η πύλη Toffoli έχει τρεις εισόδους: δύο ελέγχου και μία επεξεργασίας.
- Ονομάζεται CCNOT γιατί στην ουσία πρόκειται για μία NOT που ελέγχεται από δύο εισόδους.



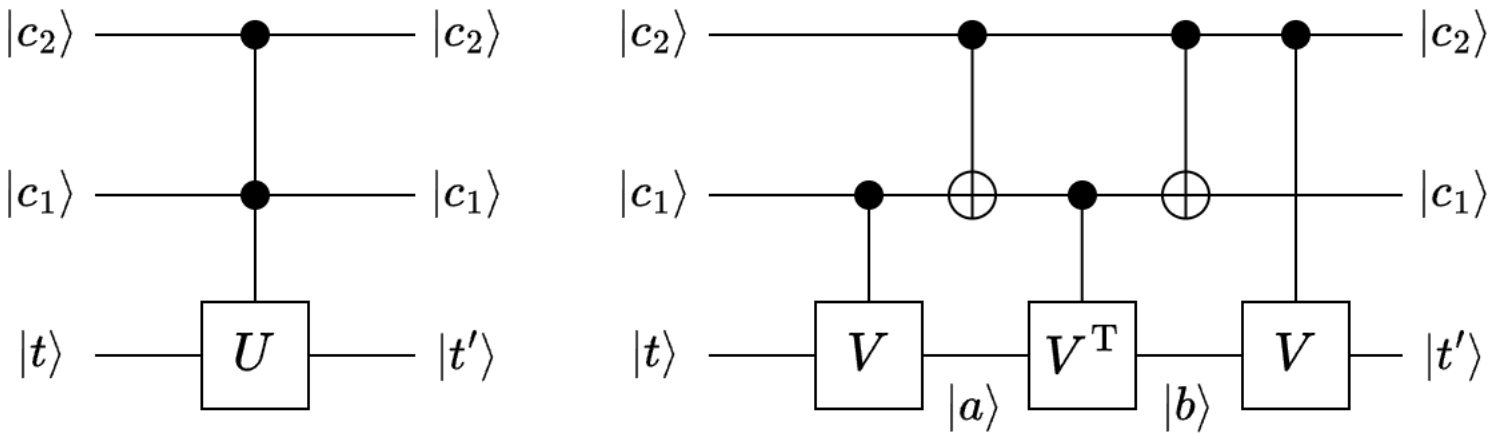
- Εάν $|c_1\rangle = |0\rangle$ ή $|c_2\rangle = |0\rangle$, τότε έχουμε $|t'\rangle = |t\rangle$
- Εάν $|c_1\rangle = |c_2\rangle = |1\rangle$, τότε έχουμε $|t'\rangle = X|t\rangle$.
- Οπότε $|t'\rangle = X^{c_1 c_2}|t\rangle$

- Η πύλη CCNOT συμβολίζεται και με $C^2(X)$.
- Είναι χρήσιμο να γράψουμε την δράση της πύλης και ως εξής:

$$|t'\rangle = |c_1 c_2 \oplus t\rangle$$

Υλοποίηση μίας ελεγχόμενης πύλης με δύο εισόδους ελέγχου

- Γενικότερα οι πύλες που ελέγχονται από δύο εισόδους συμβολίζονται με $C^2(U)$ όπου U είναι ένας οποιοσδήποτε μοναδιαίος πίνακας.
- Η πύλη περιγράφεται από την σχέση $|t'\rangle = U^{c_1 c_2} |t\rangle$.
- Είναι ενδιαφέρον να δούμε ότι μπορούμε να υλοποιήσουμε οποιαδήποτε πύλη $C^2(U)$ με πύλες $C^1(X)$ και πύλες ενός qubit.



- Στα παραπάνω έχουμε επιλέξει $V^2 = U$, δηλαδή το V να είναι η τετραγωνική ρίζα του U.

Ο πίνακας V

- Ο πίνακας V είναι και αυτός μοναδιαίος πίνακας όπως θα δείξουμε παρακάτω, δηλαδή ισχύει $VV^{\mathrm{T}} = V^{\mathrm{T}}V = I$.
- Δεδομένου ότι ο πίνακας U είναι μοναδιαίος, θα διαγωνιοποιείται (θυμηθείτε κάθε μοναδίαιος πίνακας είναι και κανονικός εφόσον $UU^{\mathrm{T}} = U^{\mathrm{T}}U$).
- Αν $|i\rangle$ τα ιδιοδιανύσματα του U που συνθέτουν μία κανονική βάση και λ_i οι αντίστοιχες ιδιοτιμές τους, τότε:

$$U = \sum_i \lambda_i \, |i\rangle \langle i|$$

$$U^{\mathrm{T}} = \sum_i \lambda_i^* \, |i\rangle \langle i|$$

- Θα έχουμε:

$$I = UU^{\mathrm{T}} = \sum_p \lambda_p \, |p\rangle \langle p| \sum_q \lambda_q^* \, |q\rangle \langle q| = \sum_p |\lambda_p|^2 \, |p\rangle \langle p|$$

Ο πίνακας V

- Αν πάρουμε τα διαγώνια στοιχεία του UU^{T}, αυτά θα πρέπει να ισούται με 1:

$$1 = \langle p|UU^{\mathrm{T}}|p\rangle = |\lambda_p|^2$$

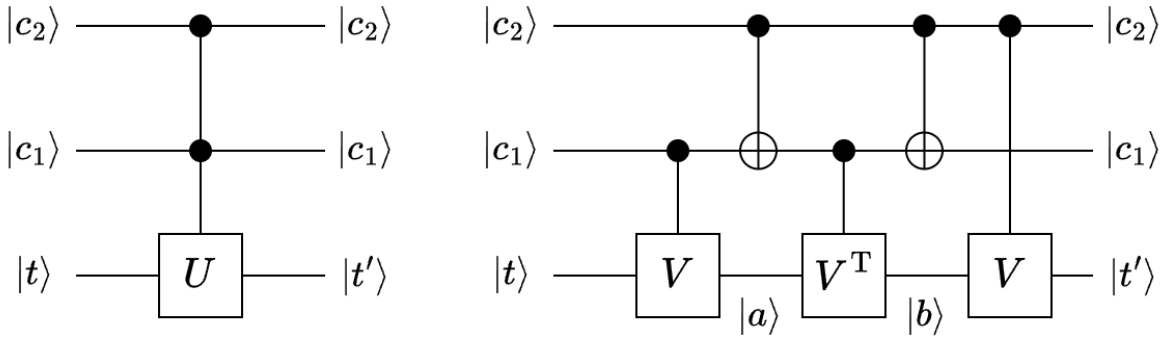
- Οπότε ένας μοναδιαίος πίνακας έχει πάντα ιδιοτιμές που έχουν μέτρο 1.
- Εύκολα μπορούμε να δείξουμε και το ανάποδο: Δηλαδή εάν ένας πίνακας διαγωνιοποιείται και οι ιδιοτιμές του λ_p έχουν μέτρο 1 τότε είναι μοναδιαίος.
- Ο πίνακας $V = \sqrt{U}$ γράφεται ως εξής:

$$V = \sqrt{U} = \sum_p \sqrt{\lambda_p}\,|p\rangle\,\langle p|$$

- Επειδή $|\sqrt{\lambda_p}|^2 = |\lambda_p| = 1$, έπεται ότι και ο V είναι μοναδιαίος.
- Επομένως ισχύει $VV^{\mathrm{T}} = V^{\mathrm{T}}V = I$.

Ελεγχόμενες πύλες δύο εισόδων

- Ας ξαναδούμε το σχήμα υλοποίησης μίας πύλης $C^2(U)$:



$$|a\rangle = V^{c_1}\,|t\rangle$$

$$|b\rangle = (V^{\mathrm{T}})^{c_2\oplus c_1}\,|a\rangle = (V^{-1})^{c_2\oplus c_1}V^{c_1}\,|t\rangle = V^{c_1-(c_2\oplus c_1)}\,|t\rangle$$

$$|t'\rangle = V^{c_2}\,|b\rangle = V^{c_2+c_1-c_2\oplus c_1}\,|t\rangle$$

Ελεγχόμενες πύλες δύο εισόδων

- Στην σχέση:
$$|t'\rangle = V^{c_2}|b\rangle = V^{c_2+c_1-c_2\oplus c_1}|t\rangle$$
- ο εκθέτης $c_2 + c_1 - c_2 \oplus c_1$ έχει ιδιαίτερο ενδιαφέρον.
- Το πρώτο $+$ δηλώνει μία κλασική πρόσθεση και όχι λογικό OR. Αυτό γιατί έχει προκύψει από πολλαπλασιασμούς πινάκων και όχι κάποια λογική πράξη.
- Το $\oplus$ όμως είναι XOR επειδή έχει προκύψει από την πρώτη πύλη CNOT, $|c_1\rangle|c_2\rangle \to |c_1\rangle|c_1 \oplus c_2\rangle$.

$$c_2 + c_1 - c_2 \oplus c_1 = \begin{cases} 2, & \text{εάν } c_1 = c_2 = 1 \\ 0, & \text{εάν } c_1 \neq c_2 \\ 0, & \text{εάν } c_1 = c_2 = 0 \end{cases} = 2c_1c_2$$

- Επομένως $|t'\rangle = V^{2c_1c_2}|t\rangle = U^{c_1c_2}|t\rangle$

Παράδειγμα: η πύλη $C_2(\mathrm{X})$

- Ας δούμε για παράδειγμα πως μπορούμε να υλοποιήσουμε την $C_2(\mathrm{X})$
- Θα πρέπει να βρούμε έναν πίνακα V τέτοιο ώστε $V^2 = X$.
- Οι ιδιοτιμές του πίνακα X υπολογίζονται ως εξής:

$$0 = \det(X - \lambda I) = \begin{vmatrix} \lambda & 1 \\ 1 & \lambda \end{vmatrix} = \lambda^2 - 1 \rightarrow \lambda = \pm 1$$

- Το ιδιοδιάνυσμα $|v\rangle$ για την ιδιοτιμή $\lambda = 1$ υπολογίζεται από την σχέση:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$$

- Από την παραπάνω σχέση προκύπτει $v_1 = v_2$, οπότε επιλέγουμε $v_1 = v_2 = \frac{1}{\sqrt{2}}$ για να έχει μέτρο 1 το ιδιοδιάνυσμα $|v\rangle$,

$$|v\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

Παράδειγμα: η πύλη $C_2(\mathrm{X})$

- Με τον ίδιο τρόπο καταλήγουμε ότι το ιδιοδιάνυσμα που αντιστοιχεί στην ιδιοτιμή $\lambda = -1$ είναι:

$$|w\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

- Ο πίνακας X διαγωνιοποιείται ως εξής:

$$X = U^{\mathrm{T}} D U$$

- όπου ο πίνακας U έχει στήλες τα ιδιοδιανύσματα του X ενώ ο D είναι διαγώνιος και τα στοιχεία της διαγωνίου είναι οι ιδιοτιμές του X,

$$U = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad D = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad U^{\mathrm{T}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Παράδειγμα: η πύλη $C_2(\mathrm{X})$

- Η ρίζα V του U έχει τα ίδια ιδιοδιανύσματα αλλά οι ιδιοτιμές είναι οι ρίζες των αρχικών, ± 1 επομένως είναι οι 1 και j.
- Επομένως ο V γράφεται:

$$V = U^{\mathrm{T}} D_V U$$

- Θα έχουμε:

$$V = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & j \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & j \\ 1 & -j \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} =$$

$$= \frac{1}{2}\begin{bmatrix} 1+j & 1-j \\ 1-j & 1+j \end{bmatrix} = \frac{1+j}{2} I + \frac{1-j}{2} X$$

- Εφόσον έχουμε βρει τον πίνακα V μπορούμε να υλοποιήσουμε την $C_2(X)$ με τον τρόπο που συζητήσαμε προηγουμένως.

Κβαντικό AND

- Το κβαντικό AND είναι χρήσιμο καθώς μπορεί να χρησιμοποιηθεί για την υλοποίηση διάφορων κυκλωμάτων.
- Η πρώτη σκέψη ίσως είναι να υλοποιήσουμε ένα κβαντικό κύκλωμα $|x\rangle\,|y\rangle \to |xy\rangle$.
- Ωστόσο *δεν υπάρχει* τέτοιο κβαντικό κύκλωμα!
- Θυμηθείτε ότι οτιδήποτε φτιάχνουμε πρέπει να περιγράφεται από μοναδίαιο τελεστή και πίνακα.
- Επομένως για δύο εισόδους θέλουμε δύο εξόδους και όχι μία!
- Μία δεύτερη σκέψη θα ήταν να δοκιμάσουμε κάτι της μορφής: $|x\rangle\,|y\rangle \to |x\rangle\,|xy\rangle$
- Οπότε $|00\rangle \to |00\rangle, |01\rangle \to |00\rangle, |10\rangle \to |10\rangle, |11\rangle \to |11\rangle$

Κβαντικό AND

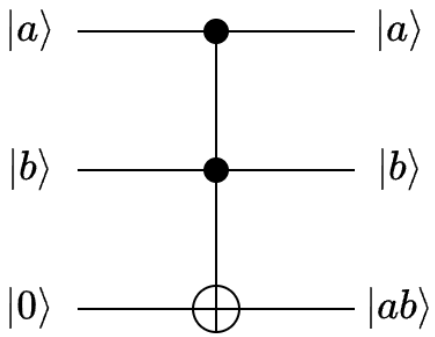
- Ας αντιστοιχίσουμε πάλι διανύσματα βάσης στις καταστάσεις ως εξής: $|0\rangle \to |00\rangle, |1\rangle \to |01\rangle, |2\rangle \to |10\rangle, |3\rangle \to |11\rangle$.
- Ο πίνακας που αντιστοιχεί είναι

$$\mathcal{M} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

- Μπορούμε να δούμε ότι $\det\{\mathcal{M}\} = 0$ οπότε ο πίνακας δεν είναι αντιστρέψιμος!
- Άρα δεν είναι και μοναδιαίος! Αφού αν ήταν, θα έπρεπε $\mathcal{M}\mathcal{M}^{\mathrm{T}} = I$ οπότε θα ήταν και αντίστρεψιμος!

Κβαντικό AND

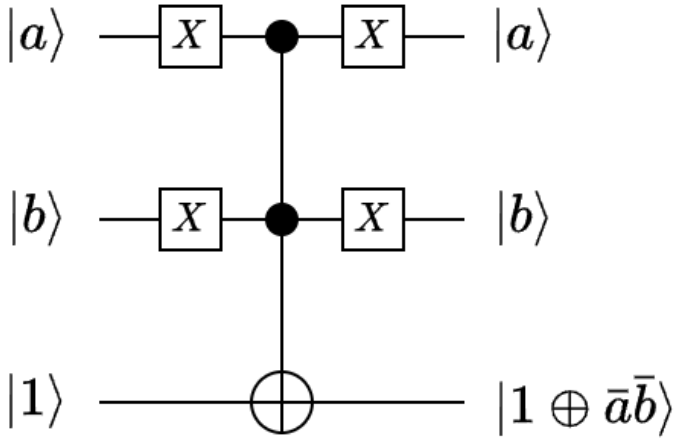
- Ας δοκιμάσουμε με περισσότερα qubits.
- Η πύλη $C^2(X)$ μπορεί να χρησιμοποιηθεί για να φτιάξουμε την κβαντική έκδοση του AND ως εξής:



- Στην ουσία χρησιμοποιούμε ένα βοηθητικό qubit το οποίο έχουμε αρχικοποιήσει στην κατάσταση $|0\rangle$.
- Οπότε η έξοδος είναι $|t'\rangle = X^{ab}|0\rangle$ δηλαδή $|1\rangle$ μόνο όταν $a = b = 1$ αλλιώς $|0\rangle$ που στην ουσία είναι το κβαντικό AND!

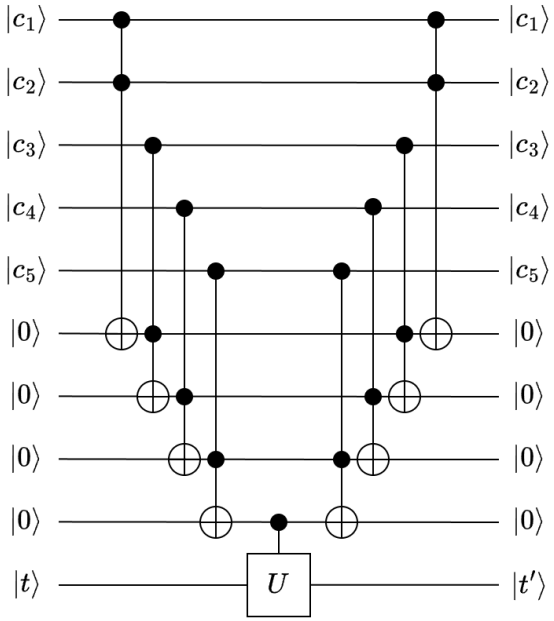
Κβαντικό OR

- Το κβαντικό OR μπορεί και αυτό να υλοποιηθεί με μία πύλη $C^2(X)$ και μερικές NOT.
- Ας θυμηθούμε από την (κλασική) Λογική Σχεδίαση ότι $a + b = 0$ μόνο εάν $a = b = 0$ αλλιώς $a + b = 1$.
- Οπότε μπορούμε να γράψουμε $a + b = 1 \oplus \bar{a}\bar{b}$ όπου με $\bar{x}$ συμβολίζουμε το αντίστροφο του x.
- Εφόσον έχουμε πλέον ένα XOR μπορούμε εύκολα να το υλοποιήσουμε την πύλη.



Υλοποίηση $C^n(U)$

- Παρακάτω φαίνεται μία υλοποίηση μίας πύλης $C^5(U)$ που εύκολα γενικεύεται και για μεγαλύτερες τιμές του n.



- Στην ουσία υπολογίζουμε διαδοχικά τα AND των qubit ελέγχου πύλες Toffoli και βοηθητικά qubit.
- Στην αριστερότερη πύλη υπολογίζεται το $|c_1c_2\rangle$, στην αμέσως μετά το $|c_1c_2c_3\rangle$ κ.ο.κ.
- Το qubit που ελέγχει την μεσαία πύλη $C_1(U)$ είναι ίσο με $|c_1c_2c_3c_4c_5\rangle$.