Κβαντικοί Υπολογιστές και Αλγόριθμοι

Διάλεξη 1η

Θωμάς Καμαλάκης

Χαροκόπειο Πανεπιστήμιο Αθηνών

2026

Περιεχόμενα

1 Πληροφορίες για το μάθημα

2 Εφαρμογές

3 Qubit εναντίον bit

4 Εσωτερικό γινόμενο

5 Επίδραση σε ένα qubit

Αντικείμενο του μαθήματος

- Το μάθημα πραγματεύεται όσα γνωρίζουμε για την κβαντική υπολογιστική.
- Θα ασχοληθούμε α) με το κβαντικό υλικό (quantum hardware) και β) με τους κβαντικούς αλγορίθμους (quantum algorithms).
- Πρόκειται για ένα αντικείμενο που έχει ιδιαίτερο “hype” τα τελευταία χρόνια.
- Όμως προσοχή! Κανένας (από όσο ξέρουμε τουλάχιστον) δεν έχει φτιάξει ένα *χρήσιμο* κβαντικό υπολογιστή.

Συγγράμματα - Ελληνικά

- Αρχές Κβαντικής Υπολογιστικής, Ιωάννης Μαρμόκος, διαθέσιμο online εδώ.
- Κβαντική Υπολογιστική, Ιωάννης Καραφυλλίδης διαθέσιμο online εδώ.
- Κβαντική Υπολογιστική, Σάββας Ηλίας, Σαμπάνη Μαρία, πληροφορίες μπορείτε να βρείτε εδώ.

Συγγράμματα - Ξενόγλωσσα

- Quantum Computation and Quantum Information, 10th Anniversary Edition, Michael A. Nielsen and Isaac L. Chuang, Cambridge University Press.
- Introduction to Classical and Quantum Computing - Thomas Wong, Rooted Grove
- Quantum Computer Science - N. David Mermin, Cambridge University Press.
- Quantum Computing Since Democritus - Scott Aaronson, Cambridge University Press

Frameworks

- `Qiskit`, IBM (2017) - προσφέρει τη δυνατότητα προσομοίωσης κβαντικών κυκλωμάτων (ακόμα και στο κβαντικό cloud της IBM). Συνδυάζεται με `Python`.
- `Q#`, Microsoft (2017). Συνδυάζεται με το VisualStudio και χρησιμοποιεί την δική του σύνταξη (δεν βασίζεται π.χ. στην `Python`.
- `Cirq`, Google (2018). Συνδυάζεται με `Python` και εστιάζει στην προσομοίωση και βελτιστοποίηση κυκλωμάτων.

Εφαρμογές

- Αποκρυπτογράφηση κλασικών συστημάτων: Ο αλγόριθμος Shor μπορεί να διασπάσει τους αλγόριθμους RSA, ECC, κ.ά., οι οποίοι βασίζονται στην παραγοντοποίηση μεγάλων αριθμών ή στο πρόβλημα του διακριτού λογαρίθμου.
- Κβαντική κρυπτογραφία (π.χ. QKD - Quantum Key Distribution): Παρότι δεν απαιτεί κβαντικούς υπολογιστές για την υλοποίηση, η ασφάλειά της βασίζεται σε κβαντικές αρχές.
- Ο αλγόριθμος Grover επιταχύνει την εύρεση λύσεων σε μη δομημένα προβλήματα αναζήτησης (π.χ. εύρεση στοιχείου σε μια μη ταξινομημένη λίστα).
- Βελτιστοποίηση σε logistics, χρηματοοικονομικά και βιομηχανική παραγωγή μέσω κβαντικής ενίσχυσης και κβαντικής προσομοίωσης annealing.

Εφαρμογές

- Οι κβαντικοί υπολογιστές μπορούν να προσομοιώσουν συστήματα μοριακής χημείας, κβαντικής φυσικής και υλικών, κάτι που είναι πρακτικά αδύνατο για κλασικούς υπολογιστές.
- Quantum Machine Learning (QML): Εξερευνώνται αλγόριθμοι που θα μπορούσαν να επιταχύνουν την εκπαίδευση μοντέλων ή να διαχειριστούν μεγάλες ποσότητες δεδομένων πιο αποδοτικά.
- Ανάλυση κινδύνου, μοντελοποίηση χαρτοφυλακίων και προσομοιώσεις Monte Carlo μπορούν να επωφεληθούν από την ταχύτητα των κβαντικών υπολογιστών.

Bit εναντίον qubit

- Το *bit* είναι η βασική μονάδα πληροφορίας: μπορεί να είναι 0 ή 1.
- Στο υλικό τα 0 και 1 αντιστοιχούν σε διαστήματα τάσης, π.χ. στην τεχνολογία CMOS $0 - 0.3\,\mathrm{V}$ και $0.7 - 1\,\mathrm{V}$.
- Το *qubit* αποτυπώνει την πληροφορία στον *κβαντικό* κόσμο, τον κόσμο των μικρών διαστάσεων.
- Οι νόμοι του κβαντικού κόσμου διαφέρουν πολύ από όσα έχουμε συνηθίσει, άρα και τα qubit έχουν ενδιαφέρουσες ιδιότητες που δεν έχουν τα bit.
- Ποιο φυσικό σύστημα μπορεί να είναι ένα qubit; Πώς το αποθηκεύουμε και το επεξεργαζόμαστε;

Τι είναι η στροφορμή;

- Η *στροφορμή* μετράει "πόση περιστροφή" έχει ένα σώμα, όπως η ορμή μετράει "πόση κίνηση" έχει.
- Για σωματίδιο μάζας m που κινείται σε κύκλο ακτίνας r με ταχύτητα v: $L = m\,v\,r$.
- Μονάδες: $\mathrm{Kg\,m^2/s} = \mathrm{Js}$, ίδιες με της σταθεράς $\hbar$.
- Το *spin* είναι ένα είδος στροφορμής που έχει το σωματίδιο από μόνο του, ανεξάρτητα από την κίνησή του στο χώρο.
- Δεν σημαίνει ότι το ηλεκτρόνιο γυρίζει γύρω από τον εαυτό του: είναι εγγενής κβαντική ιδιότητα, με τιμές πολλαπλάσια του $\hbar/2$.

Η σταθερά του Planck

- Η σταθερά του Planck h είναι η θεμελιώδης σταθερά της κβαντικής μηχανικής:

$$h \approx 6.626 \times 10^{-34}\,\mathrm{Js}$$

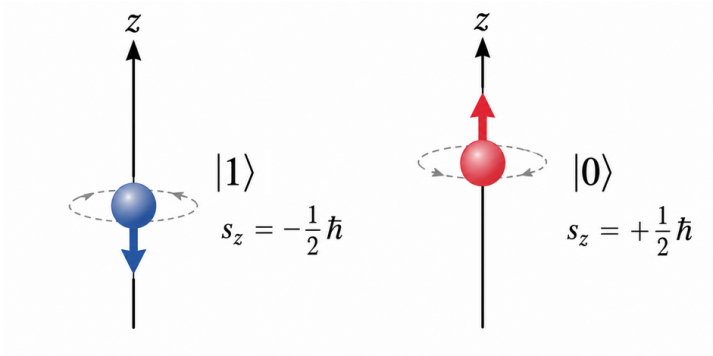
- Συνδέει την ενέργεια ενός φωτονίου με τη συχνότητά του: $E = hf$.
- Η *ανηγμένη σταθερά του Planck* είναι:

$$\hbar = \frac{h}{2\pi} \approx 1.055 \times 10^{-34}\,\mathrm{Js}$$

- Έχει μονάδες ενέργειας $\times$ χρόνου, ίδιες με της στροφορμής, και γι' αυτό εμφανίζεται στο spin: $s = \pm\hbar/2$.
- Είναι εξαιρετικά μικρή: γι' αυτό τα κβαντικά φαινόμενα δεν φαίνονται στην καθημερινή μας εμπειρία.

Το spin του ηλεκτρονίου ως qubit

- Λόγω του spin το ηλεκτρόνιο συμπεριφέρεται σαν μικρός μαγνήτης.
- Μετρώντας το spin κατά τον άξονα z βρίσκουμε μόνο $s = \pm\hbar/2$.
- Κωδικοποιούμε:
  - $|0\rangle \leftrightarrow s_z = +\hbar/2$
  - $|1\rangle \leftrightarrow s_z = -\hbar/2$
- Ένα ηλεκτρόνιο αρκεί για ένα bit, αλλά υπακούει στην κβαντική μηχανική.



Πώς μετράμε το spin;

- Στέλνουμε το ηλεκτρόνιο σε μαγνητικό πεδίο B που μεταβάλλεται κατά τον άξονα z. Η δύναμη που δέχεται είναι:

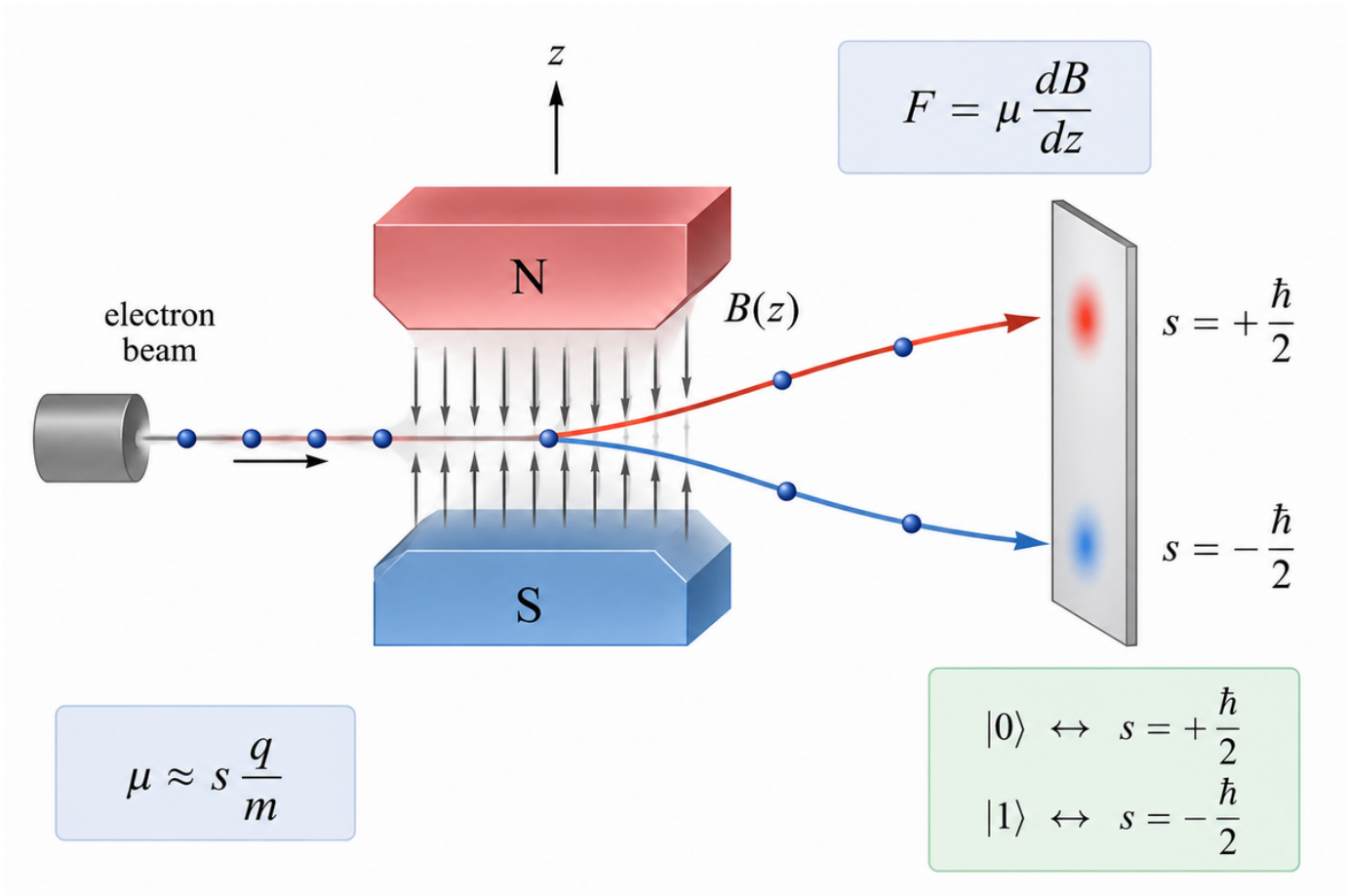
$$F = \mu \frac{dB}{dz}$$

- Η μαγνητική ροπή μ του σωματιδίου δίνεται (προσεγγιστικά) από:

$$\mu \approx s \frac{q}{m}$$

- Για $s > 0$ η δύναμη είναι θετική και για $s < 0$ αρνητική.
- Από το πού θα εκτραπεί το ηλεκτρόνιο καταλαβαίνουμε το πρόσημο του spin: $s = +\hbar/2$ ή $s = -\hbar/2$.

Το πείραμα Stern-Gerlach



Η κυματοσυνάρτηση

- Η *κυματοσυνάρτηση* περιέχει όλη την πληροφορία που μπορεί να είναι γνωστή για ένα κβαντικό σύστημα.
- Από αυτήν υπολογίζουμε τις πιθανότητες των αποτελεσμάτων κάθε δυνατής μέτρησης.
- Η εξέλιξή της στον χρόνο καθορίζεται από την εξίσωση του Schrödinger, όπως ο δεύτερος νόμος του Newton καθορίζει την κίνηση στην κλασική φυσική.
- Στην κλασική φυσική το σύστημα *προϋπάρχει* στην κατάσταση που μετράμε. Στην κβαντική μηχανική το αποτέλεσμα της μέτρησης δεν καθορίζει πλήρως την κατάσταση *πριν* τη μέτρηση.
- Συμβολίζουμε τις δύο καταστάσεις του spin ως $|0\rangle$ ($s = +\hbar/2$) και $|1\rangle$ ($s = -\hbar/2$) (συμβολισμός Dirac).

Υπέρθεση καταστάσεων

- Πριν τη μέτρηση το qubit μπορεί να βρίσκεται σε *υπέρθεση*:

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

- Οι συντελεστές a και b είναι μιγαδικοί αριθμοί.
- Μετά τη μέτρηση βρίσκουμε $|0\rangle$ με πιθανότητα $|a|^2$ και $|1\rangle$ με πιθανότητα $|b|^2$.
- Οι πιθανότητες αθροίζουν στο 1:

$$|a|^2 + |b|^2 = 1$$

- Παράδειγμα: για $a = b = \frac{1}{\sqrt{2}}$ έχουμε 50% πιθανότητα για $|0\rangle$ και 50% για $|1\rangle$.

Ket

- Η κατάσταση $|\psi\rangle$ διαβάζεται "*ket του* ψ" (συμβολισμός Dirac).
- Τα a και b της $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ είναι οι συντεταγμένες ενός διανύσματος (a, b), που το γράφουμε ως πίνακα στήλη (2×1):

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

- Ειδικότερα:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Bra

- Ο *ανάστροφος ενός πίνακα προκύπτει αν κάνουμε τις στήλες γραμμές και πάρουμε τα μιγαδικά συζυγή.*
- Ο ανάστροφος του $|\psi\rangle$ συμβολίζεται $\langle\psi|$ και διαβάζεται "*bra του* ψ":

$$\langle\psi| = \begin{bmatrix} a^* & b^* \end{bmatrix}$$

Παράδειγμα

Για $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{j}{\sqrt{2}}|1\rangle$:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ j \end{bmatrix}, \qquad \langle\psi| = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -j \end{bmatrix}$$

Εσωτερικό γινόμενο

- Για $|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$ και $|\phi\rangle = \begin{bmatrix} c \\ d \end{bmatrix}$ το $\langle\phi|$ είναι 1×2 και το $|\psi\rangle$ είναι 2×1, άρα το γινόμενό τους είναι ένας αριθμός:

$$\langle\phi|\psi\rangle = \begin{bmatrix} c^* & d^* \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = ac^* + bd^*$$

- Το $\langle\phi|\psi\rangle$ διαβάζεται "*braket του ϕ με το ψ*".

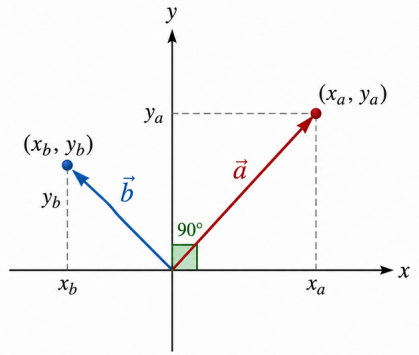
Παράδειγμα

Για $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{j}{\sqrt{2}}|1\rangle$ και $|\phi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$:

$$\langle\phi|\psi\rangle = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}} + \frac{j}{\sqrt{2}}\frac{1}{\sqrt{2}} = \frac{1+j}{2}$$

Ορθοκανονική βάση

- Στο επίπεδο, δύο διανύσματα $\vec{a}, \vec{b}$ είναι κάθετα όταν $\vec{a} \cdot \vec{b} = 0$ και το μέτρο τους είναι $|\vec{a}|^2 = \vec{a} \cdot \vec{a}$.
- Τα $\hat{x} = (1, 0)$ και $\hat{y} = (0, 1)$ είναι κάθετα, έχουν μέτρο 1 και κάθε διάνυσμα είναι γραμμικός συνδυασμός τους: $\vec{a} = x_a \hat{x} + y_a \hat{y}$.
- Ένα τέτοιο σύνολο λέγεται *ορθοκανονική βάση*.
- Τα $|0\rangle$ και $|1\rangle$ παίζουν τον ίδιο ρόλο: κάθε $|\psi\rangle$ γράφεται ως $a|0\rangle + b|1\rangle$.



Εσωτερικό γινόμενο

$$\vec{a} \cdot \vec{b} = x_a x_b + y_a y_b$$

Κάθετα διανύσματα

$$\vec{a} \cdot \vec{b} = 0$$

Μέτρο διανύσματος

$$|\vec{a}| = \sqrt{x_a^2 + y_a^2}$$

Ιδιότητες και ορθοκανονικότητα

- Συζυγής συμμετρία: $\langle\psi|\phi\rangle = \langle\phi|\psi\rangle^*$
- Γραμμικότητα: $\langle\phi|(\psi+\omega)\rangle = \langle\phi|\psi\rangle + \langle\phi|\omega\rangle$ και $\langle\phi|(\lambda\psi)\rangle = \lambda\langle\phi|\psi\rangle$
- Θετικότητα: $\langle\psi|\psi\rangle = |a|^2 + |b|^2 \geq 0$, και ισούται με 0 μόνο για $|\psi\rangle = 0$.
- Για qubit πρέπει $\langle\psi|\psi\rangle = 1$.
- Τα $|0\rangle$ και $|1\rangle$ *είναι ορθοκανονική βάση*:

$$\langle 0|0\rangle = \langle 1|1\rangle = 1, \qquad \langle 0|1\rangle = \langle 1|0\rangle = 0$$

Κυματοσυνάρτηση σε μεγαλύτερες διαστάσεις

- Για περισσότερα qubit το $|\psi\rangle$ έχει περισσότερες διαστάσεις, π.χ.

$$|\psi\rangle = \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}, \qquad |a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$$

- Το $\langle\psi|$ είναι πάλι ο ανάστροφος (με συζυγή):

$$\langle\psi| = \begin{bmatrix} a^* & b^* & c^* & d^* \end{bmatrix}$$

- Το εσωτερικό γινόμενο γενικεύεται: για $|\phi\rangle = \begin{bmatrix} e & f & g & h \end{bmatrix}^{\mathrm{T}}$,

$$\langle\psi|\phi\rangle = e^*a + f^*b + g^*c + h^*d$$

- Και πάλι $\langle\psi|\psi\rangle = \langle\phi|\phi\rangle = 1$.

Βάση για δύο qubit

- Δύο qubit έχουν 4 δυνατά αποτελέσματα: 00, 01, 10, 11. Η *υπολογιστική βάση* είναι:

$$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \; |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, \; |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \; |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

- Είναι ορθοκανονική και κάθε κατάσταση είναι υπέρθεσή της:

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

με πιθανότητα μέτρησης του 10 ίση με $|c|^2$.

Πώς επηρεάζουμε ένα qubit;

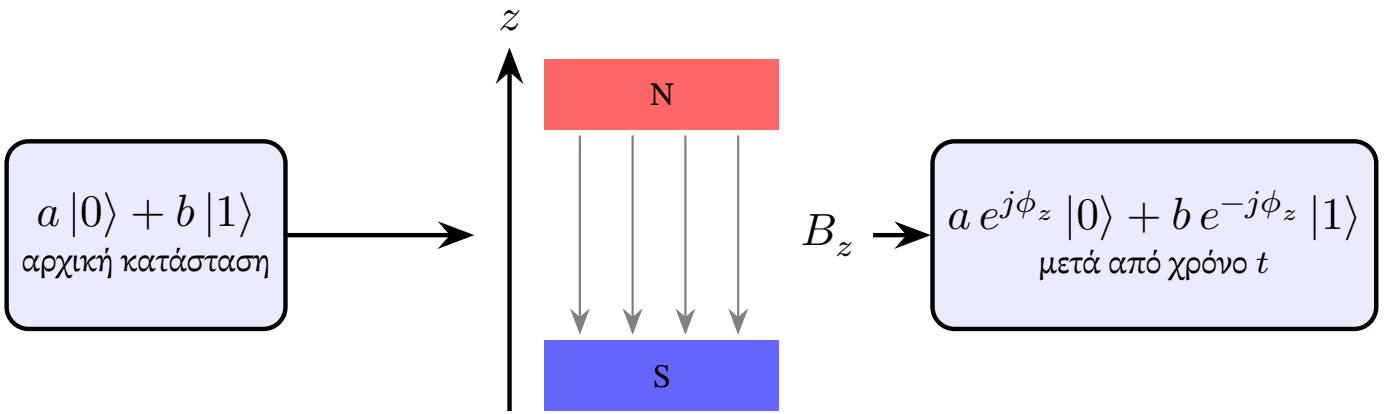
- *Μέτρηση*: το $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ μετατρέπεται σε $|0\rangle$ με πιθανότητα $|a|^2$ ή σε $|1\rangle$ με πιθανότητα $|b|^2$ (*κατάρρευση* της κυματοσυνάρτησης).
- *Μαγνητικό πεδίο* $\mathbf{B} = (B_x, B_y, B_z)$: η εξέλιξη του $|\psi\rangle$ στον χρόνο περιγράφεται από την εξίσωση του Schrödinger:

$$j\frac{d}{dt}\,|\psi\rangle = -\frac{q}{2m}\left(\mathbf{X}B_x + \mathbf{Y}B_y + \mathbf{Z}B_z\right)|\psi\rangle$$

- Οι $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$ είναι οι *πίνακες Pauli*:

$$\mathbf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \mathbf{Y} = \begin{bmatrix} 0 & -j \\ j & 0 \end{bmatrix}, \quad \mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Πεδίο κατά τον άξονα z



- Τα πλάτη παίρνουν φάση με αντίθετο πρόσημο, $\phi_z = \frac{qB_z}{2m}t$.
- Οι πιθανότητες δεν αλλάζουν: $|a(t)|^2 = |a(0)|^2$, $|b(t)|^2 = |b(0)|^2$.

Πεδίο κατά τον άξονα x

- Για $\mathbf{B} = (B_x, 0, 0)$ η εξίσωση του Schrödinger ανακατεύει τα πλάτη a και b. Με $\theta_x = -\frac{qB_x}{2m}$ η λύση είναι:

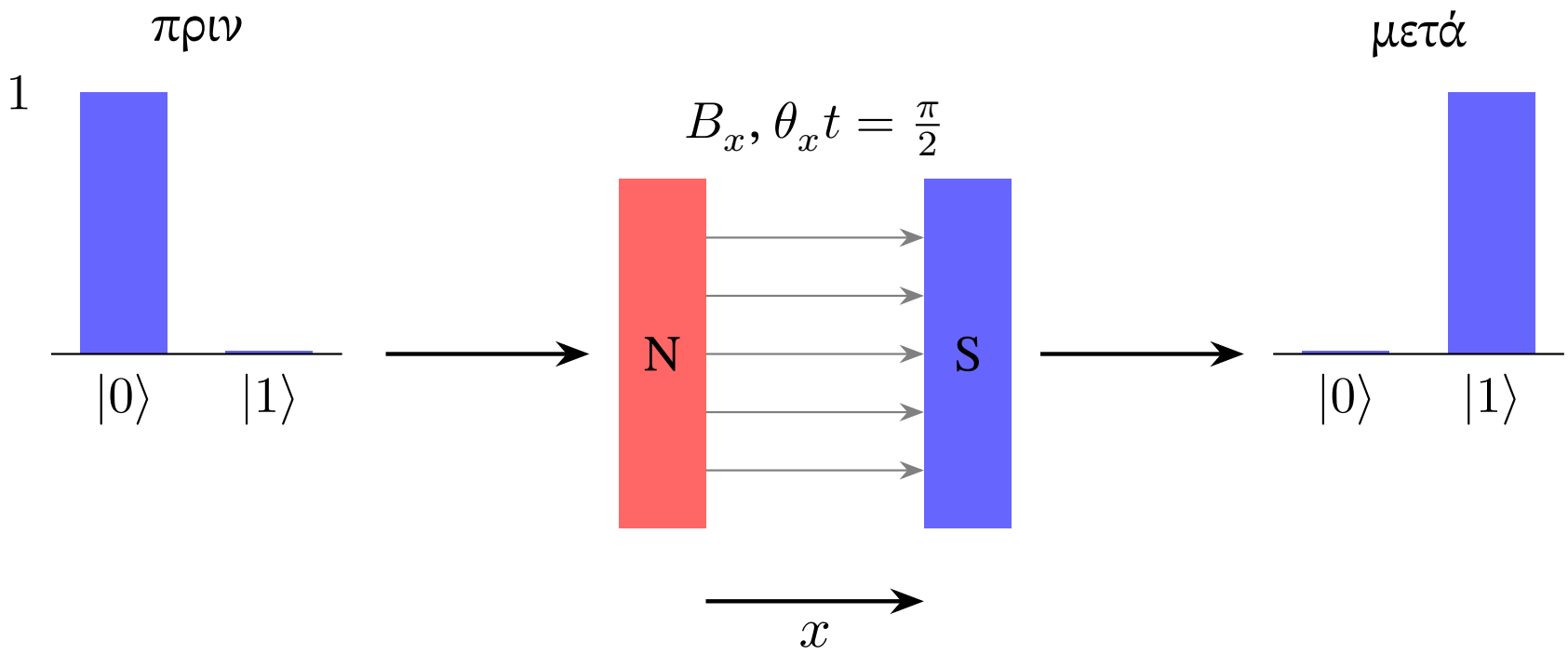
$$\begin{bmatrix} a(t) \\ b(t) \end{bmatrix} = \begin{bmatrix} \cos(\theta_x t) & j\sin(\theta_x t) \\ j\sin(\theta_x t) & \cos(\theta_x t) \end{bmatrix} \begin{bmatrix} a(0) \\ b(0) \end{bmatrix}$$

- Κάθε κβαντικό κύκλωμα περιγράφεται από έναν πίνακα $\mathbf{U}$ που συνδέει τα αρχικά με τα τελικά πλάτη.
- Αν το πεδίο δράσει για χρόνο τέτοιο ώστε $\theta_x t = \pi/2$:

$$\mathbf{U} = \begin{bmatrix} 0 & j \\ j & 0 \end{bmatrix}, \qquad a(0)\,|0\rangle + b(0)\,|1\rangle \;\mapsto\; j\,(b(0)\,|0\rangle + a(0)\,|1\rangle)$$

- Οι πιθανότητες των $|0\rangle$ και $|1\rangle$ *αντιστρέφονται*: είναι ένας κβαντικός αντιστροφέας.

Ο κβαντικός αντιστροφέας



- Για $|\psi(0)\rangle = |0\rangle$ παίρνουμε $|\psi(t)\rangle = j\,|1\rangle$: οι πιθανότητες μέτρησης αντιστρέφονται.

Πεδίο κατά τον άξονα y

- Για $\mathbf{B} = (0, B_y, 0)$ η εξίσωση του Schrödinger δίνει, με $\theta_y = \frac{qB_y}{2m}$:

$$\frac{da}{dt} = \theta_y\, b, \qquad \frac{db}{dt} = -\theta_y\, a$$

- Η λύση, με $\phi_y = \theta_y t$, είναι:

$$\begin{bmatrix} a(t) \\ b(t) \end{bmatrix} = \begin{bmatrix} \cos\phi_y & \sin\phi_y \\ -\sin\phi_y & \cos\phi_y \end{bmatrix} \begin{bmatrix} a(0) \\ b(0) \end{bmatrix}$$

Πώς φτιάχνουμε μια υπέρθεση;

- Πεδίο κατά τον y: η δράση του περιγράφεται από τον πίνακα (πραγματικός και μοναδιαίος)

$$\mathbf{U}_y(\phi) = \begin{bmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{bmatrix}, \qquad \phi = \frac{qB_y}{2m}t$$

- Διαλέγουμε διάρκεια και πλάτος του πεδίου ώστε $\phi = -\pi/4$ και ξεκινάμε από το $|0\rangle$:

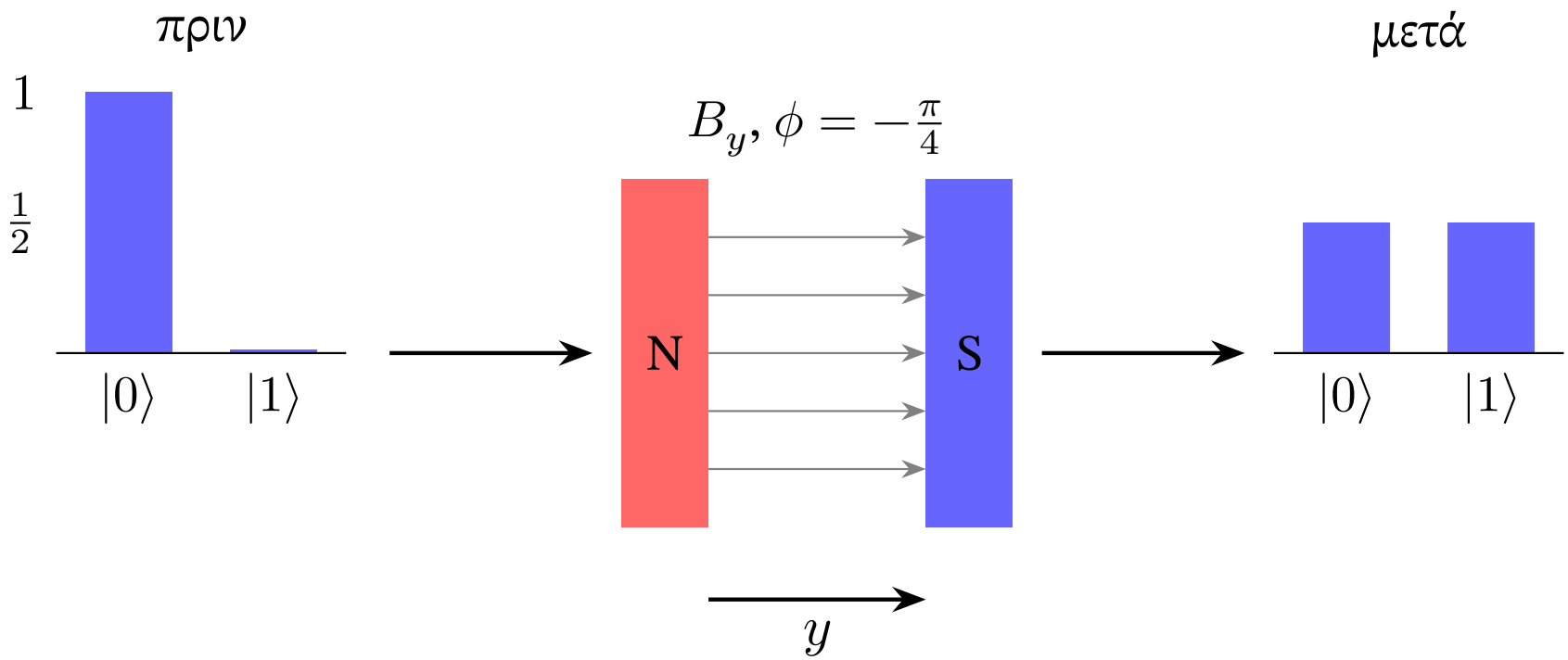
$$\mathbf{U}_y(-\tfrac{\pi}{4})\,|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

- Δηλαδή παίρνουμε την ισοπίθανη υπέρθεση:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$$

- Μετρώντας, βρίσκουμε $|0\rangle$ ή $|1\rangle$ με πιθανότητα 50% το καθένα.

Από το $|0\rangle$ στην υπέρθεση



- Ένα μαγνητικό πεδίο κατά y φτιάχνει την ισοπίθανη υπέρθεση.