Κβαντικοί Υπολογιστές και Αλγόριθμοι

Διάλεξη 1η

Θωμάς Καμαλάκης

Χαροκόπειο Πανεπιστήμιο Αθηνών

2025

Περιεχόμενα

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.

Ο κλασικός κόσμος

- Ο κόσμος που ζούμε περιγράφεται από την *κλασική* φυσική.
- Η κλασική φυσική, σε μία πρώτη προσέγγιση, περιγράφεται εν μέρει από τους νόμους του Νεύτωνα.
- Αν πετάξουμε μία μπάλα τότε χρησιμοποιώντας τους νόμους του Νεύτωνα και τον νόμο της βαρύτητας (πάλι του Νεύτωνα) μπορούμε να προβλέψουμε *ακριβώς* την κίνηση της μπάλας.
- Για παράδειγμα μπορούμε να υπολογίσουμε *ακριβώς* σε ποιό σημείο θα πέσει η μπάλα.
- Στο σχολείο είχαμε δει πολλά παραδείγματα.

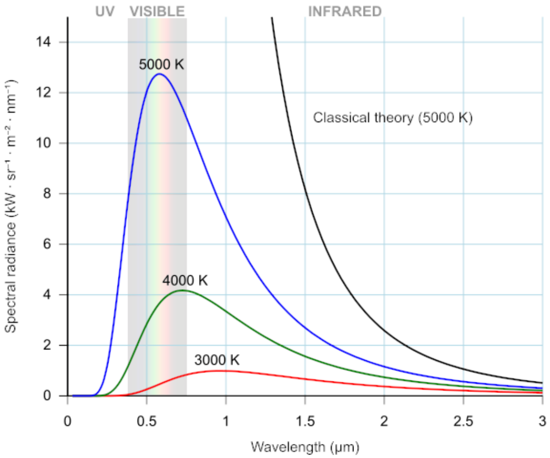
Ο νεαρός Planck

- Η κβαντική ιστορία ξεκινάει με τον Max Planck (1858-1947).
- Ο Planck εγγράφηκε στο Πανεπιστήμιο του Μονάχου και αποφάσισε να ασχοληθεί με την θεωρητική φυσική.
- Ο καθηγητής του, τον αποθάρρυνε.
- Του είπε πως δεν έχει ενδιαφέρον καθώς πρόκειται για μία“*άκρως ανεπτυγμένη, σχεδόν πλήρως ώριμη επιστήμη, η οποία, μέσω του αποκορύφωμά της την ανακάλυψη της αρχής διατήρησης της ενέργειας, θα λάβει πιθανότατα σύντομα την τελική και σταθερή της μορφή.*”

Η ακτινοβολία του μέλανος σώματος

- Υπήρχε όμως ένα πρόβλημα που δεν μπορούσε να λυθεί με την κλασική φυσική.
- Πρόκειται για την ακτινοβολία ενός σώματος που απορροφά όλα τα μήκη κύματος (χρώματα).
- Τέτοια αντικείμενα ονομάζονται "μέλανα" σώματα.
- Προσοχή: δεν είναι μαύρο ένα μελάν σώμα. Εκπέμπει φως ανάλογα με τη θερμοκρασία!
- Η κλασική φυσική προβλέπει έναν "απειρισμό" για μικρά μήκη κύματος.

Η ακτινοβολία του μέλανος σώματος



Η ιδέα του Planck

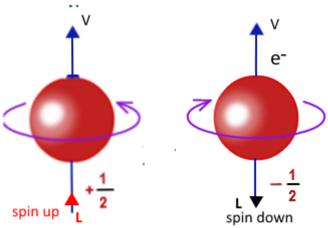
- Ο Planck σκέφτηκε να δοκιμάσει μία νέα ιδέα για να διώξει τον απειρισμό.
- Θεώρησε ότι η ακτινοβολία εκπέμπεται και απορροφάται μόνο στοιχειώδη "πακέτα", τα κβάντα (quanta).
- Δηλαδή η ενέργεια E απορρόφησης ή εκπομπής θα είναι πάντα $E = nhf$ όπου h η σταθερά του Planck, f η συχνότητα του κύματος και n ο (ακέραιος) αριθμός των κβάντων.
- Γιατί γίνεται αυτό; ο Planck δεν ήξερε. Αλλά έτσι ξεκίνησε μία επανάσταση στη φυσική.

Κβαντική Μηχανική

- Περιγράφει τον τρόπο με τον οποίο συμπεριφέρεται ο μικρόκοσμος.
- Αποτελεί την πλέον πειραματικά επαληθευμένη θεωρία: οι προβλέψεις της ισχύουν με εκπληκτική ακρίβεια.
- Ωστόσο πολλοί πιστεύουν ότι *δεν είναι πλήρης* καθώς ορισμένες προβλέψεις της φαίνεται να αψηφούν την "κοινή λογική".
- Ωστόσο τι σημαίνει η κοινή λογική; Μήπως προσπαθούμε να ερμηνεύσουμε τον μικρόκοσμο έτσι όπως αντιλαμβανόμαστε τον μακρόκοσμο;
- Μήπως τα ηλεκτρόνια δεν μπορούν να περιγραφούν ως μικροσκοπικές μπάλες;

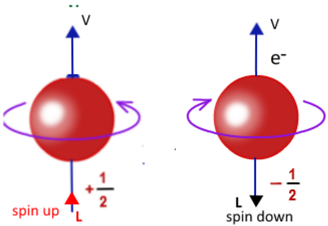
Qubits

- Κάθε κβαντικό σύστημα έχει έναν αριθμό καταστάσεων στις οποίες μπορεί να βρίσκεται.
- Για παράδειγμα τα ηλεκτρόνια έχουν μία ιδιότητα που ονομάζεται *spin*.
- Ένας πρώτος τρόπος να καταλάβουμε τι είναι το spin είναι να θεωρήσουμε ότι περιγράφει την περιστροφή του ηλεκτρονίου γύρω από έναν άξονα.



Qubits

- Το spin του ηλεκτρονίου εμφανίζεται *κβαντισμένο* και έχει δύο τιμές $+\frac{1}{2}$ και $-\frac{1}{2}$.
- Είναι κάτι μετρήσιμο: ανάλογα με το μαγνητικό πεδίο που υπάρχει επηρεάζει την κίνηση του ηλεκτρονίου.
- Ας αντιστοιχήσουμε το $+\frac{1}{2}$ στο λογικό 0 και το $-\frac{1}{2}$ στο λογικό 1.



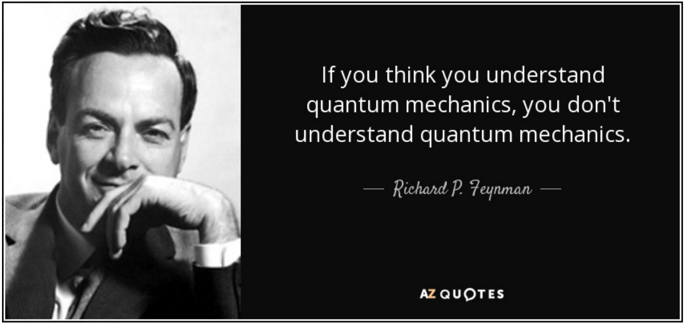
Qubits: Συμβολισμός Dirac

- Όταν ασχολούμαστε με την κβαντική υπολογιστική χρησιμοποιούμε τον συμβολισμό Dirac, $|\psi\rangle$.
- Έτσι συμβολίζουμε το λογικό 0 με $|0\rangle$ και το λογικό 1 με $|1\rangle$.
- Υπάρχει όμως μία πολύ βασική διαφορά με τα κλασικά bits που μάθαμε και αγαπήσαμε μέχρι τώρα.
- Ένα κλασικό bit θα είναι είτε 0, είτε 1.
- Ένα qubit μπορεί να είναι σε μία υπέρθεση καταστάσεων, $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$.
- Δηλαδή να είναι *ταυτόχρονα* και 0 και 1!

Qubits: Υπέρθεση

- Πως γίνεται να ισχύει αυτό; και όμως ισχύει!
- Μπορεί μία μπάλα να περιστρέφεται ταυτόχρονα δεξιόστροφα και αριστερόστροφα; Όχι βέβαια.
- Ωστόσο τα ηλεκτρόνια δεν είναι οι μπάλες που βλέπουμε στον μακρόκοσμο.
- Είναι σωματίδια στο μικρόκοσμο.
- Η φυσική τους διαφέρει από την φυσική που χρησιμοποιούμε για τις μπάλες.
- Η κβαντική μηχανική προβλέπει και υπέρθεση καταστάσεων: ένα qubit μπορεί να είναι και 0 και 1!

Qubits: Τι δεν καταλαβαίνετε;



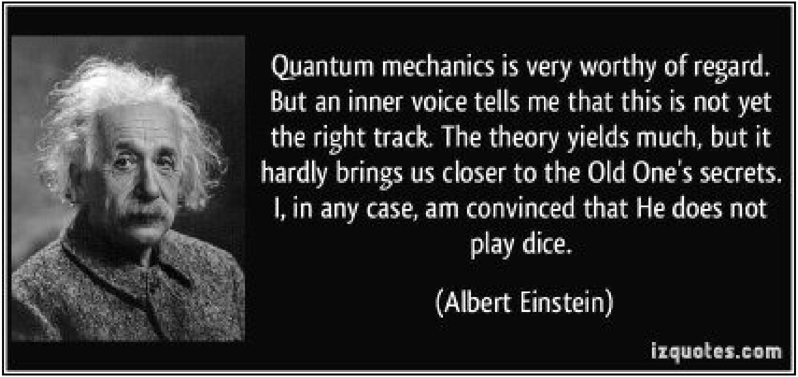
Qubits: Τι είναι τα a και b;

- Είναι μιγαδικοί αριθμοί!
- Θυμηθείτε ένας μιγαδικός αριθμός z έχει πραγματικό και φανταστικό μέρος, $z = p + jq$ όπου p και q το πραγματικό και φανταστικό μέρος αντίστοιχα.
- Το μέτρο του φανταστικού αριθμού $|z|$ είναι $\sqrt{p^2 + q^2}$.
- Εάν $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$, τότε η κβαντική μηχανική λέει ότι $|a|^2 + |b|^2 = 1$.
- Εάν μετρήσουμε το $|\psi\rangle$ για να δούμε εάν είναι 0 ή 1 τότε η θεωρία λέει ότι θα είναι 0 με πιθανότητα $|a|^2$ και 1 με πιθανότητα $|b|^2$.

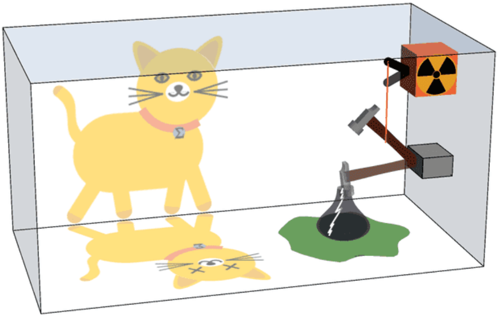
Qubits: Τι είναι τα a και b;

- Για παράδειγμα έστω ότι το qubit βρίσκεται στην κατάσταση $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$.
- Τότε εάν μετρήσουμε το $|\psi\rangle$ για να δούμε εάν είναι 0 ή 1, θα πάρουμε με πιθανότητα $\frac{1}{2}$ ότι είναι 0 και με πιθανότητα πάλι $\frac{1}{2}$ ότι είναι ίσο με 1.
- Μετά την μέτρηση το qubit θα είναι στην κατάσταση $|0\rangle$ εάν μετρήσαμε 0 ή στην κατάσταση $|1\rangle$ εάν μετρήσαμε 1.
- Η μέτρηση παρήγαγε ένα τυχαίο αποτέλεσμα και προκάλεσε κατάρρευση της υπέρθεσης.
- από $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ πήγαμε τυχαία στο $|0\rangle$ ή στο $|1\rangle$.

Ο Θεός παίζει ζάρια;



Η γάτα του Schrödinger



- Μία περιγραφή από το Big Bang Theory εδώ.

Η γάτα του Schrödinger

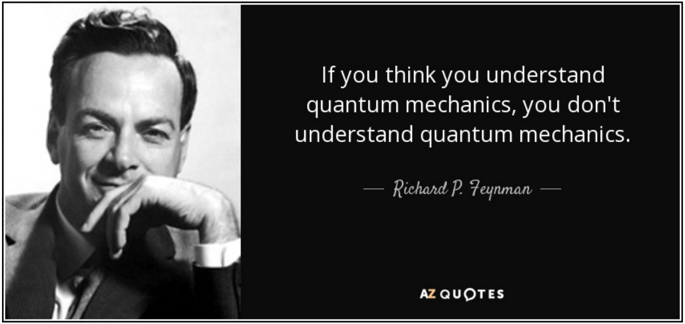
- Παίρνουμε ένα κουτί το οποίο έχει τέλεια ηχομόνωση και βάζουμε μέσα μία γάτα.
- Ο ελεγκτής ελέγχεται από ένα qubit $|\psi\rangle$.
- Εάν το qubit $|\psi\rangle$ είναι $|0\rangle$ δεν συμβαίνει τίποτα.
- Εάν το qubit $|\psi\rangle$ είναι $|1\rangle$ τότε ελευθερώνει ένα αέριο και κοιμίζει την γάτα.
- Τι συμβαίνει όταν $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$;

Η γάτα του Schrödinger

- Αν ανοίξουμε το κουτί είναι σαν να κάνουμε μία μέτρηση.
- Με πιθανότητα $\frac{1}{2}$ θα βρούμε το qubit να είναι $|0\rangle$ οπότε και την γάτα ξύπνια.
- Με πιθανότητα $\frac{1}{2}$ θα βρούμε το qubit να είναι $|1\rangle$ οπότε και την γάτα να κοιμάται.
- Τι συμβαίνει πριν να ανοίξουμε το κουτί και να κάνουμε την μέτρηση;
- Η κβαντική θεωρία λέει ότι η γάτα υπάρχει σε μία υπέρθεση καταστάσεων.
- Το σύστημα περιγράφεται από την κατάσταση

$$|\Psi\rangle = \frac{1}{\sqrt{2}} |\text{ξύπνια}\rangle |0\rangle + \frac{1}{\sqrt{2}} |\text{κοιμάται}\rangle |1\rangle \tag{1}$$

Qubits: Τι δεν καταλαβαίνετε;



Τα qubit ως διανύσματα

- Εφόσον $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ μπορούμε να αντιστοιχήσουμε κάθε qubit με ένα διάνυσμα 2×1:

$$|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \tag{2}$$

- Επίσης είναι χρήσιμο να ορίσουμε ένα διάνυσμα που προκύπτει από το $|\psi\rangle$, το $\langle\psi|$, ως το εξής διάνυσμα 1×2:

$$\langle\psi| = \left[a^*, b^*\right] \tag{3}$$

- όπου με z^* έχουμε συμβολίσει το μιγαδικό συζυγές του z.
- Αν $z = p + jq$, τότε $z^* = p - jq$.

Παραδείγματα

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

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

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$|\phi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{j}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ j \end{bmatrix}$$

Εσωτερικό γινόμενο

- Στην κβαντική υπολογιστική η έννοια του εσωτερικού γινομένου είναι πάρα πολύ χρήσιμη.
- Έστω δύο qubit $|\psi\rangle$ και $|\phi\rangle$ που περιγράφονται από δύο καταστάσεις:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \tag{4}$$

$$|\phi\rangle = c\,|0\rangle + d\,|1\rangle = \begin{bmatrix} c \\ d \end{bmatrix} \tag{5}$$

- Τότε το εσωτερικό γινόμενο $\langle\phi|\psi\rangle$ δίνεται από την σχέση:

$$\langle\phi|\psi\rangle = c^* a + d^* b \tag{6}$$

Η ομορφιά του συμβολισμού Dirac

- Γιατί συμβολίζουμε το εσωτερικό γινόμενο με $\langle\phi|\psi\rangle$;
- Το $\langle\phi|$ και το $|\psi\rangle$ είναι 1×2 και 2×1 πίνακες αντίστοιχα με στοιχεία:

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

- Θυμηθείτε πως πολλαπλασιάζουμε δύο πίνακες A και B που έχουν διαστάσεις $m \times n$ και $n \times p$ αντίστοιχα.
- Για κάθε γραμμή του A παίρνουμε ένα ένα τα στοιχεία της και τα πολλαπλασιάζουμε με κάθε στήλη του B και τα αθροίζουμε.
- Με τον τρόπο αυτό φτιάχνουμε έναν πίνακα που έχει $m \times p$ στοιχεία που είναι το γινόμενο των πινάκων, $A \cdot B$.

Η ομορφιά του συμβολισμού Dirac

- Ας εφαρμόσουμε αυτή την διαδικασία τώρα στους πίνακες $\langle\phi|$ και $|\psi\rangle$.

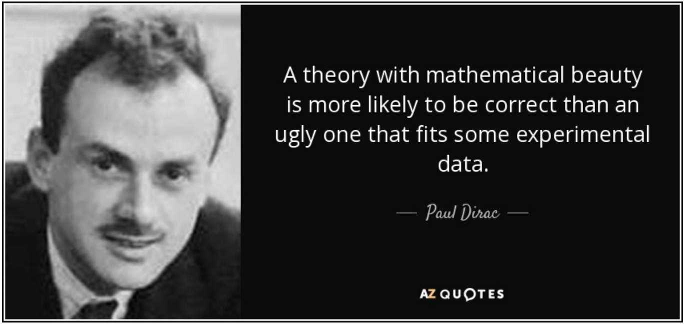
$$\langle\phi| = \left[c^*, d^*\right] \;,\; |\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$$

- Το αποτέλεσμα του γινομένου των πινάκων 1×2 και 2×1 θα είναι 1×1 δηλαδή ένα απλό νούμερο!

$$\langle\phi|\psi\rangle = \langle\phi| \cdot |\psi\rangle = c^* a + d^* b$$

- Δηλαδή ο συμβολισμός Dirac βοηθάει να εκφράσουμε με κομψό τρόπο το εσωτερικό γινόμενο.

Η ομορφιά του συμβολισμού Dirac



Ιδιότητες εσωτερικού γινομένου

- Συζυγία:

$$\langle\psi|\phi\rangle^* = (ca^* + db^*)^* = c^*a + d^*b = \langle\phi|\psi\rangle$$

- Γραμμικότητα:

$$\langle\phi|c_1\psi_1 + c_2\psi_2\rangle = c_1\langle\phi|\psi_1\rangle + c_2\langle\phi|\psi_2\rangle$$

- Μέτρο:

$$\|\psi\|^2 = \langle\psi|\psi\rangle = |a|^2 + |b|^2 = 1$$

Ιδιότητες εσωτερικού γινομένου

- Είναι εύκολο να δούμε ότι

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

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

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

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

Εσωτερικό γινόμενο και πιθανότητες

- Μπορούμε να υπολογίσουμε τις πιθανότητες να έχουμε $|0\rangle$ ή $|1\rangle$ μετά μία μέτρηση, χρησιμοποιώντας το εσωτερικό γινόμενο.
- Έστω $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$.
- Τότε η πιθανότητα να έχουμε $|0\rangle$ ή $|1\rangle$ είναι $P_0 = |a|^2$ ή $P_1 = |b|^2$ αντίστοιχα.
- Βλέπουμε ότι:

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

- Επομένως μπορούμε να εκφράσουμε τις πιθανότητες με την βοήθεια του εσωτερικού γινομένου ως:

$$P_0 = |\,\langle\psi|0\rangle\,|^2\,,\, P_1 = |\,\langle\psi|1\rangle\,|^2$$