κ ε φ ά λ α ι ο

15

ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ

ΜΙΑ ΣΤΟΙΧΕΙΩΔΗΣ ΕΙΣΑΓΩΓΗ

Εισαγωγή: Η αναγκαιότητα του κβαντικού υπολογιστή

Με τούτο το κεφάλαιο εισερχόμαστε πλέον στην περιοχή του αγνώστου. Εκεί όπου όλα μπορούν να συμβούν: από μια μεγάλη τεχνολογική και επιστημονική επανάσταση έως. . . τίποτα: ή σχεδόν. Διότι στην επιστήμη ακόμα και η αρνητική έκβαση ενός μεγάλου εγχειρήματος είναι πάντα πλούσια σε ανακαλύψεις αν και όχι πάντα εκείνες που επιδιώκαμε. Το θέμα μας είναι οι *κβαντικοί υπολογιστές*: Οι υπολογιστές στους οποίους η βασική μονάδα εγγραφής και επεξεργασίας της πληροφορίας στο δυαδικό σύστημα –με τα γνωστά δύο ψηφία 0 και 1– δεν είναι πλέον ένα κλασικό αντικείμενο, π.χ. μια μαγνητική ψηφίδα μνήμης, αλλά ένα *κβαντικό σύστημα*. Παραδείγματος χάριν ένα άτομο υδρογόνου στη θεμελιώδη του κατάσταση, όπου το *μηδέν* αντιπροσωπεύεται από την ηλεκτρονιακή κατάσταση με *σπιν πάνω* και το *ένα* από την κατάσταση με *σπιν κάτω*. Για προφανείς λόγους θα συμβολίζουμε την πρώτη κατάσταση (*σπιν πάνω*) με το διάνυσμα ket $|0\rangle$ και τη δεύτερη (*σπιν κάτω*) με το διάνυσμα $|1\rangle$. Όμως ακριβώς επειδή το άτομο –και ειδικότερα το ηλεκτρόνιό του– είναι ένα κβαντικό σύστημα, εκτός από τις παραπάνω δύο καταστάσεις, $|0\rangle$ και $|1\rangle$, θα είναι επίσης μια πραγματοποιήσιμη κατάσταση και κάθε γραμμικός τους συνδυασμός της μορφής

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

με $|\alpha|^2 + |\beta|^2 = 1$ για τους γνωστούς λόγους. Και είναι φανερό ότι εδώ ακριβώς βρίσκεται η πηγή της θεμελιώδους διαφοράς μεταξύ ενός κλασικού και ενός κβαντικού υπολογιστή. Ότι στη δεύτερη περίπτωση η βασική μονάδα μνήμης μπορεί

να βρίσκεται όχι μόνο στις καταστάσεις 0 και 1 αλλά και σε κάθε δυνατή επαλληλία τους. Το τι εκπληκτικές νέες δυνατότητες ενυπάρχουν σε αυτό το βασικό γεγονός θα το δούμε σύντομα. Προς το παρόν –στο πλαίσιο τούτης της σύντομης εισαγωγής– θα εξετάσουμε απλώς τους κύριους λόγους που κάνουν τον ερχομό του κβαντικού υπολογιστή, κατά πολλούς, *αναπόφευκτο*. Ο ένας λόγος είναι πολύ πρακτικός: Έχει να κάνει με τον λεγόμενο *νόμο του Moore*: Την εμπειρική διαπίστωση ότι περίπου κάθε δύο χρόνια η χωρητικότητα της μνήμης των κλασικών υπολογιστών διπλασιάζεται. Έτσι, με έναν τέτοιο ρυθμό σμίκρυνσης της βασικής μονάδας μνήμης, είναι θέμα χρόνου –το πολύ δύο δεκαετίες λένε οι ειδικοί– που η μονάδα αυτή θα αποκτήσει ατομικές διαστάσεις. Οπότε, βεβαίως, η εφαρμογή των κβαντικών νόμων –για το καλό ή για το κακό(!)– θα είναι αναγκαστική.

Έναν πιο θεμελιώδη λόγο για την αναγκαιότητα των κβαντικών υπολογιστών παρουσίασε ο Richard Feynman το 1982.(*) Το επιχείρημα του Feynman είναι πράγματι πολύ θεμελιώδες. Η βασική του ιδέα είναι η εξής: Ότι η υπολογιστική πολυπλοκότητα των κβαντικών συστημάτων –μετρημένη σε αριθμό αναγκαίων πράξεων για την επίλυσή τους– είναι τόσο πολύ μεγαλύτερη (στην πραγματικότητα *εκθετικά μεγαλύτερη*) από τα αντίστοιχα κλασικά συστήματα, ώστε μπορεί να αντιμετωπιστεί μόνο με έναν υπολογιστή που θα είναι κι αυτός ένα κβαντικό σύστημα. Δηλαδή έναν *κβαντικό υπολογιστή*. Η δικαιολόγηση αυτού του ισχυρισμού είναι πολύ απλή. Ο υπολογισμός ενός κλασικού συστήματος συνίσταται στην επίλυση ενός (μη γραμμικού εν γένει) συστήματος διαφορικών εξισώσεων δευτέρας τάξεως πλήθους $3N$, όπου N ο αριθμός των σωματιδίων του συστήματος, ενώ, βέβαια, το 3 αντιστοιχεί στον αριθμό των συντεταγμένων x, y και z που απαιτούνται για τον προσδιορισμό της θέσης του καθενός. Η υπολογιστική πολυπλοκότητα του συστήματος –για τη δεδομένη ακρίβεια που επιδιώκουμε– θα αυξάνεται λοιπόν ανάλογα με το *μέγεθός* του, δηλαδή τον αριθμό των σωματιδίων του. (Αν και η μη γραμμικότητα των εξισώσεων –και η αναμενόμενη εμφάνιση χαοτικής συμπεριφοράς– αυξάνουν σημαντικά αυτή την εκτίμηση.)

Κοιτάξτε τώρα πόσο διαφορετική είναι η κατάσταση σε ένα κβαντικό σύστημα με τον ίδιο αριθμό σωματιδίων· δηλαδή N. Κατ' αρχάς, έστω και με ένα μόνο σωματίδιο, το πρόβλημα που έχουμε να λύσουμε –παραδείγματος χάριν ο υπολογισμός των ενεργειακών ιδιοτιμών του σωματιδίου μέσα στο δεδομένο δυναμικό– είναι πολύ απαιτητικό σε υπολογιστικό χρόνο, παρότι γραμμικό. Θα πρέπει να διαγωνιοποιήσουμε μια μήτρα –ας πούμε τη χαμιλτονιανή μήτρα H– που είναι θεωρητικά *απειροδιάστατη*, αφού τόση είναι και η διάσταση του σχετικού *χώρου Hilbert*. Στην πράξη γινόμαστε, βεβαίως, πιο «ολιγαρκείς» και προσεγγίζουμε τον απειροδιάστατο αυτό χώρο με έναν πεπερασμένης διάστασης, ας πούμε ίσης με

(*) R.P. Feynman, Simulating Physics with computers, *Int. J. Theor. Phys.*, 21:467, 1982.

d, όπου το d –δηλαδή ο αριθμός των βασικών διανυσμάτων– μπορεί να αυξηθεί όσο θέλουμε (ή όσο μπορούμε!) ανάλογα με την επιδιωκόμενη ακρίβεια. Αν τώρα έχουμε δυο σωματίδια –ας τα πούμε 1 και 2– τότε ο χώρος Hilbert των δυνατών καταστάσεών τους θα είναι (δείτε Κεφ. 4, § 4) το *τανυστικό γινόμενο* $\mathcal{H}_1 \otimes \mathcal{H}_2$ των χώρων Hilbert του καθενός και η διάστασή του θα είναι ίση με d^2 αν κάνουμε την ίδια προσέγγιση και στους δύο επιμέρους χώρους: Τους θεωρήσουμε δηλαδή και τους δύο ως χώρους πεπερασμένης διάστασης ίσης με d. Και η γενίκευση για N σωματίδια είναι προφανής. Τώρα ο σχετικός χώρος Hilbert $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_N$ έχει διάσταση $D = d^N$ και αντίστοιχα για τις κβαντομηχανικές μήτρες –όπως η χαμιλτονιανή– που αντιπροσωπεύουν τα φυσικά μεγέθη του συστήματος. Η διάστασή τους θα είναι $D \times D = d^N \times d^N$. Ένα απλό παράδειγμα θα μας βοηθήσει να καταλάβουμε σε τι περιπέτεια έχουμε... μπλέξει. Έστω ότι $d = 10$ και $N = 100$. Ότι δηλαδή έχουμε ένα σύστημα *εκατό σωματιδίων* –περίπου ο αριθμός ηλεκτρονίων ενός μικρού μορίου από ελαφρά στοιχεία– και ότι έχουμε προσεγγίσει τον χώρο Hilbert του καθενός με έναν χώρο μόνο *δέκα διαστάσεων*. (Μια πολύ χονδροειδής προσέγγιση βεβαίως.) Και όμως, αν θέλαμε να υπολογίσουμε τις ενεργειακές ιδιοτιμές αυτού του συστήματος *από πρώτες αρχές* –δηλαδή χωρίς τις συνήθεις προσεγγίσεις της μοριακής φυσικής– θα έπρεπε να διαγωνιοποιήσουμε μια χαμιλτονιανή μήτρα διαστάσεων $10^{100} \times 10^{100}$! Όταν ο αριθμός των σωματιδίων όλου του ορατού σύμπαντος είναι «μόνο» 10^{80}! Το συμπέρασμα είναι προφανές. Επειδή η υπολογιστική πολυπλοκότητα των κβαντικών συστημάτων αυξάνεται *εκθετικά* συναρτήσει του αριθμού των σωματιδίων τους –έναντι μόνο μιας *γραμμικής* αύξησης για τα κλασικά συστήματα (d^N έναντι $3N$)– η επίλυσή τους από πρώτες αρχές (πλην ελαχίστων εξαιρέσεων) είναι ένα *ανέφικτο πρόβλημα*. Απλούστατα *δεν γίνεται*. Δεν γίνεται σε έναν κλασικό υπολογιστή είναι, βέβαια, η σωστή διατύπωση. Αλλά γιατί να γίνεται σε έναν κβαντικό υπολογιστή, οτιδήποτε κι αν σημαίνει αυτό; Για έναν λόγο πολύ απλό όσο και θεμελιώδη. Αφού ο κβαντικός κόσμος υπάρχει, σημαίνει ότι μάλλον τα... καταφέρνει να λύνει τις εξισώσεις του! Πώς τις λύνει; Απλώς υπάρχοντας! Κατά κάποιον τρόπο η ίδια η ύπαρξη ενός κβαντικού συστήματος –όπως, βέβαια, και ενός κλασικού– είναι μια *έμπρακτη επίλυση* των σχετικών εξισώσεων. Απλώς έχουμε κάποια δυσκολία να «διαβάσουμε» τη λύση επειδή το «πράγμα» δεν φτιάχτηκε γι' αυτόν ακριβώς το σκοπό. (Αν και... ποιος ξέρει!) Αν όμως εμείς –συνεχίζει ο συλλογισμός– κατασκευάσουμε ένα τεχνητό κβαντικό σύστημα, που να μπορούμε να το «προγραμματίζουμε» απ' έξω αλλά και να το «διαβάζουμε», τότε αυτό θα λύνει το πρόβλημά μας απλώς... υπάρχοντας. Δηλαδή, απλώς δουλεύοντας με βάση τους κβαντικούς νόμους. Τόσο απλό! Τόσο απλό που ίσως και να... μην γίνει ποτέ! Η περιπέτεια τώρα αρχίζει!

1. *Η βασική έννοια: Κβαντικά δυαδικά ψηφία*

Θα αρχίσουμε με μια μικρή δόση βασικής ορολογίας από το πεδίο των κλασικών υπολογιστών. Η βασική έννοια εδώ είναι το bit: το **bi***nary digi***t**, το **δυ***αδικό ψη***φίο**. Ελληνική σύντμηση το *δυφίο*. Bit σημαίνει όμως και το *μικρό κομμάτι*, το *κομματάκι*. Ό,τι δηλαδή και η ελληνική λέξη *ψηφίο* στην πρωτογενή της σημασία ($\equiv$ *ψηφίδα*). Έτσι το bit ως επιστημονικός όρος δηλώνει ταυτόχρονα το *δυαδικό ψηφίο* –το 0 ή το 1– αλλά και το *ελάχιστο κομμάτι μνήμης*. Εκεί που εγγράφεται και γίνεται αντικείμενο επεξεργασίας το δυαδικό ψηφίο. Επιπλέον το bit έχει συμφωνηθεί να αντιπροσωπεύει και την *μονάδα πληροφορίας*. Ένα απλό παράδειγμα: Αν γνωρίζουμε τα καταχωρημένα ψηφία, ας πούμε σε πέντε θέσεις μνήμης, η πληροφορία που κατέχουμε αξιολογείται ποσοτικά ως *πέντε bit*.(*) Όλες αυτές οι ιδιότητες του bit –δυαδικό ψηφίο, θέση μνήμης, μονάδα πληροφορίας– κληροδοτούνται, βεβαίως, στον αντίστοιχο ελληνικό όρο· το δυφίο.

Και προχωρούμε τώρα στην εισαγωγή της αντίστοιχης έννοιας για έναν κβαντικό υπολογιστή. Όπου τώρα –σύμφωνα με όσα είπαμε πριν– η θέση μνήμης (το δυφίο) αποκτά κβαντικό χαρακτήρα. Γίνεται ένα κβαντικό σύστημα με δύο μόνο βασικές καταστάσεις· τις $|0\rangle$ και $|1\rangle$. Οπότε βεβαίως θα είναι μια επιτρεπτή κατάσταση του συστήματος και κάθε γραμμικός τους συνδυασμός της μορφής

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{15.1}$$

όπου το $|\alpha|^2$ δηλώνει την πιθανότητα να βρίσκεται η συγκεκριμένη θέση μνήμης στην κατάσταση $|0\rangle$ ενώ το $|\beta|^2$ είναι η πιθανότητα να βρίσκεται στην κατάσταση $|1\rangle$. Και θα είναι, βεβαίως,

$$|\alpha|^2 + |\beta|^2 = 1.$$

Στην περίπτωση του κβαντικού υπολογιστή λοιπόν, το bit –ως φυσικό αντικείμενο– είναι ένα κβαντικό σύστημα, ένα **qu***antum* **bit**, και κατά σύντμηση *qubit*. Ελληνική απόδοση *κβαντικό δυφίο* ή, απλούστερα, *κβαντοδυφίο*.

(*) Σημειώστε σχετικά ότι η «πληροφοριακή αξία» μιας πληροφορίας ορίζεται ποσοτικά ως εξής

$$I = \log_2 N - \log_2 M = \log_2(N/M), \tag{1}$$

όπου N ο αριθμός των περιπτώσεων (που έπρεπε να ερευνηθούν) πριν δοθεί η συγκεκριμένη πληροφορία και M ο (μικρότερος πλέον) αριθμός τους μετά την παροχή της συγκεκριμένης πληροφορίας. Έτσι, παραδείγματος χάριν, αν είχαμε πέντε θέσεις μνήμης και δεν γνωρίζαμε τίποτε για τα ψηφία 0 ή 1 που έχουν εγγραφεί εκεί, ο αριθμός των δυνατών περιπτώσεων είναι, προφανώς, $N = 2^5$. Αν όμως πληροφορηθούμε ότι τα τρία πρώτα από αυτά είναι –κατά σειράν– τα 0 1 0 και δεν γνωρίζουμε τίποτα για τα άλλα δύο, τότε ο αριθμός των δυνατών περιπτώσεων (που πρέπει να ψαχτούν) έχει περιοριστεί πλέον στο $M = 2^2$. Σύμφωνα με τον ορισμό (1) θα είναι λοιπόν $I = 3 \equiv 3$ bit, ακριβώς όπως το περιμένουμε. Η πληροφορία είναι τόσα bit όσες οι θέσεις μνήμης που μάθαμε την τιμή τους.

Η μνήμη του υπολογιστή –του κβαντικού στην περίπτωσή μας– θα αποτελείται, βέβαια, όχι μόνο από ένα qubit –ένα κβαντοδυφίο– αλλά από έναν επαρκή αριθμό από αυτά, τοποθετημένα σχετικά κοντά, αλλά όχι πολύ κοντά, ώστε να είναι δυνατός ο ανεξάρτητος «έλεγχός» τους με κατάλληλα εξωτερικά πεδία. Στην απλή περίπτωση ενός κβαντικού υπολογιστή με δύο κβαντοδυφία οι δυνατές καταστάσεις του συστήματος θα είναι, προφανώς, οι

$$\begin{array}{ll} |00\rangle \equiv |0\rangle|0\rangle & |01\rangle \equiv |0\rangle|1\rangle \\ |10\rangle \equiv |1\rangle|0\rangle \end{array}, \qquad \begin{array}{l} \\ |11\rangle \equiv |1\rangle|1\rangle \end{array}$$

και θα αποτελούν μια πλήρη βάση στον τετραδιάστατο πλέον χώρο των δύο κβαντοδυφίων. Η γενική κατάσταση της μνήμης –ή του *καταχωρητή* (register) όπως επίσης λέγεται– θα περιγράφεται από την επαλληλία

$$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$$

όπου, βέβαια, η τετραγωνισμένη απόλυτη τιμή καθενός από τους παραπάνω συντελεστές θα δίνει την πιθανότητα να βρούμε τον καταχωρητή στην αντίστοιχη κβαντική κατάσταση. Και θα είναι, βεβαίως,

$$\sum_{\alpha,\beta} |c_{\alpha\beta}|^2 = 1 \qquad \alpha, \beta \in \{0, 1\},$$

όπου $\{0, 1\}$ το (διμελές) σύνολο των δύο ψηφίων 0 και 1.

Για έναν κβαντικό υπολογιστή με N θέσεις μνήμης το τυχόν στοιχείο της *υπολογιστικής βάσης* –έτσι αποκαλούνται τα βασικά διανύσματα της μορφής $|011\ldots\rangle \equiv |0\rangle|1\rangle|1\rangle\ldots$ κ.λπ.– θα γράφεται ως

$$|x\rangle = |x_1, \ldots, x_N\rangle \equiv |x_1\rangle|x_2\rangle, \ldots, |x_N\rangle,$$

όπου $x_1, x_2, \ldots, x_N$ είναι οι δυαδικές μεταβλητές για την κάθε θέση μνήμης –το κάθε κβαντοδυφίο– και το x ένας πυκνός συμβολισμός για τη νιάδα $x_1, \ldots, x_N$. Δηλαδή $x \equiv x_1, \ldots, x_N$. Η γενική κβαντική κατάσταση της μνήμης (ή του καταχωρητή) θα γράφεται λοιπόν ως

$$|\psi\rangle = \sum_x c_x|x\rangle \equiv \sum_{x_1,\ldots,x_N} c_{x_1,\ldots,x_N}|x_1, \ldots, x_N\rangle,$$

με συνθήκη κανονικοποίησης την

$$\sum_x |c_x|^2 = 1.$$

Ως προς τη διάσταση αυτού του χώρου, δηλαδή το πλήθος των βασικών του διανυσμάτων,

$$|x_1, \ldots, x_N\rangle \equiv |x_1\rangle|x_2\rangle \ldots |x_N\rangle,$$

αυτή θα ισούται, προφανώς, με

$$D = 2^N,$$

αφού τόσοι είναι οι συνδυασμοί δύο βασικών διανυσμάτων από το πρώτο κβαντοδυφίο με δύο από το δεύτερο, δύο από το τρίτο κ.ο.κ. Ακόμα και με έναν πολύ μικρό αριθμό κβαντοδυφίων (π.χ. $N = 200$) –ασήμαντο με τα μέτρα ενός κλασικού υπολογιστή– η διάσταση αυτού του χώρου είναι εξωφρενική. Δεδομένου ότι $2^n \simeq 10^{n/2,3}$ θα είναι

$$D = 2^{200} \simeq 10^{200/2,3} \simeq 10^{87},$$

που είναι ένας αριθμός μεγαλύτερος από τον αριθμό των υλικών σωματιδίων όλου του ορατού σύμπαντος! Πρόκειται, βέβαια, για τον ίδιο εκθετικό νόμο που επισημάναμε και στην εισαγωγή, αλλά με $d = 2$, αφού τώρα τα σωματίδιά μας ($\equiv$ τα κβαντοδυφία) θεωρούνται ως δικαταστασιακά συστήματα και άρα ο χώρος Hilbert του καθενός έχει διάσταση *δύο*.

Βρισκόμαστε έτσι ξανά μπροστά στις εκπληκτικές –σχεδόν αδιανόητες– δυνατότητες του κβαντικού υπολογιστή. Πάνω σε έναν υπολογιστή με διακόσιες μόνο θέσεις μνήμης μπορεί να «φορτωθεί» και να γίνει αντικείμενο επεξεργασίας πληροφορία 2^{200} bit $\equiv$ 2^{200} δυφίων. Σαφώς περισσότερη από ό,τι σε όλα τα υλικά σωματίδια του σύμπαντος, αν θεωρηθούν ως κλασικές θέσεις μνήμης· ως κλασικά δυφία. Και ο λόγος γι' αυτό αξίζει να αναλυθεί και από μια διαφορετική γωνία, που φωτίζει πολύ καλύτερα τη βασική αρχή λειτουργίας του κβαντικού υπολογιστή. Το βασικό γεγονός είναι η δυνατότητα των κβαντικών δυφίων να υπάρχουν σε καταστάσεις επαλληλίας της μορφής (15.1) και επομένως να είναι και «πάνω» και «κάτω» ταυτόχρονα. Δηλαδή να μπορούν να καταχωρούν και να διαχειρίζονται και το 0 και το 1 ταυτόχρονα. Αφού όμως η χωρητικότητα του κάθε κβαντοδυφίου είναι ίση με δύο, η χωρητικότητα των δύο κβαντοδυφίων θα είναι ίση με $2^2 = 4$ –όσοι είναι οι συνδυασμοί ενός ψηφίου (0 ή 1) από το πρώτο κβαντοδυφίο και ενός από το δεύτερο– και, βέβαια, ίση με 2^N για N κβαντοδυφία. Η προέλευση του εκθετικού νόμου είναι τώρα τελείως φανερή και πολύ αποκαλυπτική για τις δυνατότητες του κβαντικού υπολογιστή.

Όμως... μια στιγμή, θα... ψελλίσει ο εντυπωσιασμένος αλλά όχι ευκολόπιστος αναγνώστης. Πώς μπορεί ένα κβαντοδυφίο, στην κατάσταση επαλληλίας $\alpha|0\rangle + \beta|1\rangle$, να κρατάει και να διαχειρίζεται *ταυτόχρονα* και το $|0\rangle$ και το $|1\rangle$, αφού σε μια μέτρηση μόνο η μία από τις δύο καταστάσεις θα βρεθεί ότι υπάρχει; Και η

απάντηση είναι βέβαια γνωστή. Πράγματι με τη μέτρηση το κβαντοδυφίο θα καταρρεύσει στη μία ή την άλλη από τις καταστάσεις $|0\rangle$ ή $|1\rangle$. Όμως ουδεμία τέτοια μέτρηση πραγματοποιείται στη διάρκεια ενός υπολογισμού. Έτσι το κβαντοδυφίο –όλα τα κβαντοδυφία– παραμένουν συνεχώς σε διάφορες καταστάσεις επαλληλίας, οπότε το υπολογιστικό πρόγραμμα εκτελείται ταυτόχρονα –ή «παράλληλα»– και για τις δύο τιμές της δυαδικής μεταβλητής του κάθε κβαντοδυφίου. Το φαινόμενο αυτό –δηλαδή η παράλληλη εκτέλεση του προγράμματος για όλες τις ενδεχόμενες καταστάσεις των κβαντοδυφίων– είναι γνωστό ως *μαζικός κβαντικός παραλληλισμός* και αποτελεί τον θεμελιώδη μηχανισμό λειτουργίας ενός κβαντικού υπολογιστή. Και σε αυτόν τον, καθαρά κβαντικό, μηχανισμό οφείλεται βέβαια η τερατώδης υπολογιστική ικανότητα αυτής της μοναδικής μηχανής!

Υπάρχει όμως και μια άλλη απορία που πρέπει να απαντηθεί πριν ο αναγνώστης αισθανθεί ότι αρχίζει να καταλαβαίνει κάπως το πώς μπορεί να δουλεύει –και να *δίνει απαντήσεις*– ένας κβαντικός υπολογιστής. Η απορία είναι πολύ στοιχειώδης. Στον κλασικό υπολογιστή η απάντηση είναι γραμμένη στον καταχωρητή ως μια αλυσίδα 0 και 1 πάνω στα διαδοχικά δυφία του. Δηλαδή ως ένα *ψηφιακό μήνυμα* που μπορεί να είναι ένας αριθμός, ένα ψηφιοποιημένο κείμενο ή οτιδήποτε άλλο. Τι γίνεται όμως με τον κβαντικό υπολογιστή του οποίου οι θέσεις μνήμης μπορεί να βρίσκονται –και συνήθως βρίσκονται– σε καταστάσεις επαλληλίας με κάποια πιθανότητα να είναι *μηδέν* ή να είναι *ένα*; Οπότε το πλήθος των δυνατών μηνυμάτων θα είναι επίσης 2^N, όπως πριν. Τι κάνουμε τότε; Θα μετρήσουμε μια φορά όλα τα κβαντοδυφία και... ότι προκύψει; Ή θα μετράμε συνέχεια έως το... τέλος του κόσμου; Και όταν... τελειώσουμε, ποια απ' όλες τις 2^N αλυσίδες ψηφίων 0 και 1 θα θεωρήσουμε ότι αποτελεί την απάντηση στο πρόβλημά μας;

Αντιλαμβάνεστε, βεβαίως, ότι αν δεν δώσουμε μια ικανοποιητική απάντηση στο ερώτημα αυτό, τότε η όλη ιδέα του κβαντικού υπολογιστή δεν θα είναι απλώς μια χίμαιρα αλλά μια καθαρή ανοησία. Ένα υπέροχο μηχάνημα που θα μας κάνει εκθετικά γρήγορα τις πράξεις αλλά θα απαιτεί μετά εκθετικά μεγάλο χρόνο για να διαβαστεί το αποτέλεσμα· αν διαβαστεί ποτέ!

Ευτυχώς τα πράγματα δεν είναι ακριβώς έτσι. Πρώτα απ' όλα η απάντηση δεν χρειάζεται να είναι τόσο μακροσκελής όσο η μνήμη του υπολογιστή. Σε πολλά προβλήματα η απάντηση που ζητάμε μπορεί να είναι μόνο ένα ΝΑΙ ή ένα ΟΧΙ. Όπως, παραδείγματος χάριν, όταν θέλουμε απλώς να μάθουμε αν ένας δεδομένος μεγάλος αριθμός είναι πρώτος ή όχι. Το πρόβλημα αυτό είναι αφάνταστα δύσκολο –στην πραγματικότητα άλυτο με τους κλασικούς υπολογιστές– και σίγουρα θα απαιτεί όλες τις δυνατότητες της μνήμης ενός κβαντικού υπολογιστή. Όμως το αποτέλεσμα είναι ένα ΝΑΙ ή ένα ΟΧΙ που μπορεί να καταχωρηθεί μόνο στο πρώτο κβαντοδυφίο της μνήμης: Αν η απάντηση είναι ΝΑΙ το κβαντοδυφίο να

βγαίνει –ως μέρος της αλγοριθμικής διαδικασίας– στην κατάσταση $|0\rangle$ και αν είναι ΟΧΙ, στην κατάσταση $|1\rangle$. Οπότε δεν έχουμε παρά να μετρήσουμε αυτό μόνο το κβαντοδυφίο και να πάρουμε αμέσως την απάντηση που ζητάμε. Και αν δεν είμαστε βέβαιοι –λόγω συσσώρευσης σφαλμάτων– ότι το κβαντοδυφίο εξόδου ήταν πράγματι στην κατάσταση που μετρήσαμε, δεν έχουμε παρά να «ξανατρέξουμε» το πρόγραμμα όσες φορές χρειαστεί –και να επαναλάβουμε τη μέτρηση– ώστε να περιορίσουμε το ενδεχόμενο σφάλματος κάτω από ένα ανεκτό επίπεδο. Και συνειδητοποιούμε έτσι, με αυτή την ευκαιρία, κάτι που ίσως θα έπρεπε να μας είναι προφανές από την αρχή. Ότι δηλαδή *ο κβαντικός υπολογιστής δεν είναι μια ντετερμινιστική μηχανή*. Εμπεριέχει ένα στοιχείο τυχαιότητας που όμως μπορεί να τεθεί υπό έλεγχο ώστε το αποτέλεσμα να πλησιάζει την *πρακτική βεβαιότητα*.

Θα κλείσουμε τούτη την παράγραφο με μια σύντομη αναφορά στις λεγόμενες *καταστάσεις Bell* που ορίζονται μέσω των σχέσεων

$$\begin{aligned} |B_{00}\rangle &= \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) \\ |B_{01}\rangle &= \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big) \end{aligned} \qquad \begin{aligned} |B_{10}\rangle &= \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big) \\ |B_{11}\rangle &= \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big) \end{aligned} \tag{15.2}$$

από όπου είναι προφανές ότι: α) Πρόκειται για καταστάσεις δύο κβαντοδυφίων και επειδή ο χώρος αυτός είναι τετραδιάστατος μπορούν να θεωρηθούν και ως μια διαφορετική εκλογή βάσης σε αυτό τον χώρο έναντι της τετράδας $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. Επιπλέον –όπως είναι εύκολο να δείτε– οι καταστάσεις (15.2) είναι αμοιβαία ορθογώνιες (και βεβαίως κανονικοποιημένες), οπότε μπορούν να θεωρηθούν ως μια άλλη *ορθοκανονική βάση* σε αυτό τον χώρο. β) Από φυσικής πλευράς είναι επίσης φανερό ότι οι καταστάσεις (15.2) είναι *σύμπλεκτες καταστάσεις* και σ' αυτό, βέβαια, οφείλεται η ονομασία τους, αφού ο Bell είναι εκείνος που ανέδειξε τη θεμελιώδη σημασία των καταστάσεων αυτού του τύπου. Σημειώστε ειδικότερα ότι για κβαντοδυφία που πραγματώνονται μέσω των δύο καταστάσεων σπιν $|\uparrow\rangle$ και $|\downarrow\rangle$ –σπιν πάνω και σπιν κάτω αντίστοιχα– θα είναι $|0\rangle \equiv |\uparrow\rangle$, $|1\rangle \equiv |\downarrow\rangle$ οπότε η κατάσταση Bell $|B_{10}\rangle$ θα γράφεται ως

$$|B_{10}\rangle = \frac{1}{\sqrt{2}}\big(|\uparrow,\downarrow\rangle - |\downarrow,\uparrow\rangle\big) \equiv \frac{1}{\sqrt{2}}\big(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle\big)$$

και σε αυτή τη μορφή αναγνωρίζεται αμέσως ως η περίφημη *κατάσταση EPR*.

Όπως θα δούμε στη συνέχεια του κεφαλαίου η κβαντική σύμπλεξη θα αποτελέσει συστατικό στοιχείο της λειτουργίας ενός κβαντικού υπολογιστή και ειδικότερα των τηλεπικοινωνιακών εφαρμογών του και της κβαντικής κρυπτογραφίας. Και σε αυτό το πλαίσιο οι καταστάσεις Bell θα αναδειχτούν σε ένα θεμελιώδες εργαλείο.

2. *Κβαντικές πύλες και κυκλώματα*

Όπως θα έπρεπε να το περιμένουμε, η λειτουργία ενός κβαντικού υπολογιστή –δηλαδή η εκτέλεση ενός υπολογιστικού προγράμματος για έναν συγκεκριμένο σκοπό– θα γίνεται με κατάλληλους χειρισμούς πάνω στα κβαντοδυφία που συγκροτούν τη μνήμη του ή τον καταχωρητή του όπως έχει επίσης καθιερωθεί να λέγεται. Και επειδή τα κβαντοδυφία είναι, βεβαίως, κβαντικά αντικείμενα, ο χειρισμός τους –δηλαδή η πρόκληση των επιθυμητών αλλαγών στην κατάστασή τους– θα γίνεται με τις δύο μόνες διαδικασίες που προβλέπει η κβαντική θεωρία. Τη *μοναδιαία εξέλιξη μέσω της εξισώσεως Schrödinger* –που προκαλείται κυρίως με τη δράση κατάλληλων ηλεκτρομαγνητικών παλμών– καθώς και τη *διαδικασία της μέτρησης* που δεν είναι μοναδιαία όπως γνωρίζουμε, αλλά διέπεται από την αρχή της κατάρρευσης του καταστασιακού διανύσματος. Επειδή όμως, πλην ειδικών εξαιρέσεων, η μέτρηση εκτελείται στο τέλος της υπολογιστικής διαδικασίας (και αποσκοπεί κυρίως στην *ανάγνωση* του αποτελέσματος) οι δυνατοί χειρισμοί επί των κβαντοδυφίων θα πρέπει να είναι υποχρεωτικά μοναδιαίοι και σε αυτούς πράγματι θα περιορίσουμε τις επιλογές μας στη συνέχεια. Ως προς την ορολογία, ο καθιερωμένος όρος γι' αυτές τις μοναδιαίες «πράξεις» είναι *κβαντικές πύλες* ή απλώς *πύλες*, όπως και στους κλασικούς υπολογιστές. Και είναι σημαντικό να υπογραμμίσουμε από την αρχή ένα βασικό γεγονός πάνω στο οποίο βασίζεται όλο το *κυκλωματικό μοντέλο* (circuit model) των υπολογιστών, κλασικών και μη. Ότι αρκεί ένας μικρός αριθμός στοιχειωδών πυλών –δηλαδή απλών μοναδιαίων τελεστών– για να υλοποιηθεί μέσω αυτών (έστω προσεγγιστικά) κάθε δυνατός μοναδιαίος μετασχηματισμός επί του συνόλου των κβαντοδυφίων του καταχωρητή. Ακόμα πιο συγκεκριμένα: Αρκεί ένας μικρός αριθμός πυλών που δρουν μόνο πάνω σε *ένα κβαντοδυφίο*, σε συνδυασμό με *μία μόνο πύλη* που δρα σε *δύο κβαντοδυφία*. Οπότε, βεβαίως, οι πρώτες πύλες θα αναπαρίστανται από μοναδιαίες μήτρες διαστάσεως 2×2 και η δεύτερη (με τις γενικεύσεις της) από μια αντίστοιχη μήτρα διαστάσεως 4×4. Θα αρχίσουμε τη μελέτη μας με την πρώτη κατηγορία πυλών.

2.1. Πύλες που δρουν μόνο πάνω σε ένα κβαντοδυφίο

Όπως είπαμε πριν οι πύλες αυτού του τύπου δρουν πάνω στις καταστάσεις ενός μόνο κβαντοδυφίου, δηλαδή στον διδιάστατο χώρο των διανυσμάτων $\alpha|0\rangle+\beta|1\rangle$, και επομένως θα αναπαρίστανται από μοναδιαίες μήτρες της ίδιας διάστασης –δηλαδή 2×2– όπως στον κατάλογο που ακολουθεί. Όπου παρατίθεται επίσης το *όνομα* και το *κυκλωματικό σύμβολο* της κάθε πύλης.

Οι βασικές μονοδυφιακές πύλες

Μονάδα	$-\boxed{I}-$	$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Hadamard	$-\boxed{H}-$	$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Pauli X	$-\boxed{X}-$	$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauli Y	$-\boxed{Y}-$	$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauli Z	$-\boxed{Z}-$	$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Φάση S	$-\boxed{S}-$	$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

Σημειώστε κατ' αρχάς –ως πρώτη παρατήρηση πάνω στον κατάλογο αυτό– ότι οι τρεις πύλες X, Y και Z –και οι αντίστοιχες μήτρες– δεν είναι παρά οι γνωστές μας *μήτρες του Pauli* σ_x, σ_y και σ_z που είναι ταυτόχρονα ερμιτιανές και μοναδιαίες λόγω της γνωστής τους ιδιότητας να είναι $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = 1$. Ερμιτιανή και μοναδιαία είναι επίσης και η πύλη Hadamard αφού ισχύει και γι' αυτήν ότι $H^2 = 1$. Μεταξύ άλλων αυτό συνεπάγεται ότι η διπλή δράση αυτών των πυλών επαναφέρει το κβαντοδυφίο στην αρχική του κατάσταση.

Ως προς το αποτέλεσμα της «μονής» δράσης των παραπάνω πυλών είναι χρήσιμο να σημειώσουμε τα εξής:

► ***Για την πύλη Hadamard:*** Με βάση τη δεδομένη μήτρα θα έχουμε

$$H|0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \equiv |+\rangle$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big) \equiv |-\rangle,$$

από όπου είναι φανερός και ο ρόλος αυτής της πύλης: Δημιουργεί ισοβαρείς επαλληλίες των βασικών καταστάσεων $|0\rangle$ και $|1\rangle$, οι οποίες είναι αναγκαίες για την

αποτελεσματική αξιοποίηση των δυνατοτήτων ενός κβαντικού υπολογιστή, όπως θα δούμε σε λίγο.

► ***Για την πύλη*** X***:*** Εδώ θα έχουμε

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

που σημαίνει ότι η πύλη αυτή αναστρέφει την κατάσταση του κβαντοδυφίου μετατρέποντας το 0 σε 1 και το 1 σε 0. Κάνει δηλαδή ό,τι και η κλασική πύλη NOT που οφείλει το όνομά της ακριβώς στο γεγονός ότι λέει «ΟΧΙ» στην εκάστοτε κατάσταση του δυφίου μετασχηματίζοντάς την στην αντίθετή της. Ένας συμπαγής συμβολισμός γι' αυτή τη δράση είναι ο

$$X|x\rangle = |\overline{x}\rangle,$$

όπου, $x = (0,1)$ η συνήθης δυαδική μεταβλητή και $\overline{x} = (1,0)$ το ανεστραμμένο είδωλό της όπου η παύλα πάνω από το x παραπέμπει εύλογα στο καθιερωμένο σύμβολο για το αντισωματίδιο.

Ανάλογα απλή είναι και η δράση των άλλων πυλών πάνω στα κβαντοδυφία και περιοριζόμαστε στην απλή καταγραφή της:

► **Πύλη** Y

$$Y|0\rangle = i|1\rangle, \qquad Y|1\rangle = -i|0\rangle.$$

► **Πύλη** Z

$$Z|0\rangle = |0\rangle, \qquad Z|1\rangle = -|1\rangle.$$

► **Πύλη** S

$$S|0\rangle = |0\rangle, \qquad S|1\rangle = i|1\rangle$$

ενώ, βέβαια, για την τυχούσα κατάσταση υπέρθεσης θα έχουμε

$$\begin{aligned}
X\big(\alpha|0\rangle + \beta|1\rangle\big) &= \beta|0\rangle + \alpha|1\rangle \\
Y\big(\alpha|0\rangle + \beta|1\rangle\big) &= -i\beta|0\rangle + i\alpha|1\rangle \\
Z\big(\alpha|0\rangle + \beta|1\rangle\big) &= \alpha|0\rangle - \beta|1\rangle \\
S\big(\alpha|0\rangle + \beta|1\rangle\big) &= \alpha|0\rangle + i\beta|1\rangle
\end{aligned}$$

και για την πύλη Hadamard

$$H\big(\alpha|0\rangle + \beta|1\rangle\big) = \frac{1}{\sqrt{2}}\big((\alpha+\beta)|0\rangle + (\alpha-\beta)|1\rangle\big).$$

2.2. Πύλες που δρουν σε δύο κβαντοδυφία

Η βασική πύλη αυτού του είδους είναι γνωστή ως

$$\text{Controlled-NOT} \equiv \text{CNOT}$$

και η δράση της πάνω σε μια τυχούσα κατάσταση $|x, y\rangle \equiv |x\rangle|y\rangle$ περιγράφεται από τις σχέσεις

$$\text{CNOT}\ |0\rangle|y\rangle = |0\rangle|y\rangle, \qquad \text{CNOT}\ |1\rangle|y\rangle = |1\rangle|\overline{y}\rangle$$

που γράφονται επίσης ως

$$|0\rangle|y\rangle \xrightarrow{\text{CNOT}} |0\rangle|y\rangle, \qquad |1\rangle|y\rangle \xrightarrow{\text{CNOT}} |1\rangle|\overline{y}\rangle$$

και μας λένε το εξής απλό. Ότι αν το πρώτο κβαντοδυφίο είναι στην κατάσταση $|0\rangle$ η πύλη CNOT δεν κάνει τίποτε στο δεύτερο, ενώ αν το πρώτο είναι στην κατάσταση $|1\rangle$ η πύλη CNOT αναστρέφει το δεύτερο. Το πρώτο κβαντοδυφίο είναι επομένως το *κβαντοδυφίο ελέγχου* (control qubit) ενώ το δεύτερο είναι το *κβαντοδυφίο-στόχος* (target qubit) και σε αυτόν τον τρόπο δράσης οφείλεται, βεβαίως, η ονομασία αυτής της πολύ σημαντικής πύλης. Ως προς την αναπαράστασή της υπό μορφήν μήτρας, δείξτε μόνοι σας ότι θα είναι

$$W_{\text{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

όπου στην πάνω αριστερή γωνία υπάρχει η 2×2 ταυτοτική μήτρα –που αντιπροσωπεύει, βεβαίως, τη δράση της CNOT στο πρώτο κβαντοδυφίο– ενώ στην κάτω δεξιά γωνία είναι η μήτρα $X \equiv$ NOT που αντιπροσωπεύει επίσης τον τρόπο δράσης της CNOT πάνω στο δεύτερο κβαντοδυφίο.

Σημειώστε ακόμα ότι η δράση της πύλης CNOT πάνω στην τυχούσα κατάσταση $|x, y\rangle$ μπορεί να γραφεί στη συμπαγή μορφή

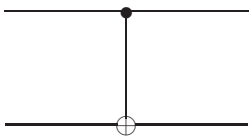
$$\text{CNOT}\ |x, y\rangle = |x, y \oplus x\rangle,$$

όπου το σύμβολο $\oplus$ δηλώνει την *πρόσθεση modulo 2*, που δεν είναι παρά η συνήθης πρόσθεση ακεραίων αλλά με «αφαίρεση» από το άθροισμα των πολλαπλασίων του *δύο*. Έτσι το αποτέλεσμα είναι πάντα 0 ή 1 και άρα πρόκειται για το είδος της

πρόσθεσης που ταιριάζει σε ένα δυαδικό σύστημα όπου μόνο τα ψηφία 0 και 1 είναι δεκτά. Τρία απλά παραδείγματα είναι τα εξής:

$$1 \oplus 1 = 0, \qquad 3 \oplus 2 = 1, \qquad 2 \oplus 2 = 0.$$

Ως προς τον κυκλωματικό συμβολισμό της, η πύλη CNOT θα διαφέρει βεβαίως από τις πύλες που εξετάσαμε προηγουμένως –που δηλώνονταν με ένα ευθύγραμμο τμήμα και το σύμβολο της πύλης στο μέσον του– εφόσον τώρα τα εμπλεκόμενα κβαντοδυφία είναι δύο και άρα θα απαιτούνται δύο ευθείες γραμμές. Πράγματι το καθιερωμένο κυκλωματικό σύμβολο για την CNOT είναι το

CNOT 

όπου η βαρειά τελεία δηλώνει το κβαντοδυφίο ελέγχου και το «σταυρωμένο» κυκλάκι το κβαντοδυφίο-στόχο.

Μια θεμελιώδης νέα δυνατότητα που μας παρέχει η πύλη CNOT είναι η σύμπλεξη καταστάσεων που ήταν ασύμπλεκτες πριν τη δράση της. Ένα απλό σχετικό παράδειγμα παρέχεται από την (εμφανώς ασύμπλεκτη) αρχική κατάσταση

$$|\psi_{\rm in}\rangle = \big(\alpha|0\rangle + \beta|1\rangle\big)|1\rangle \tag{15.3}$$

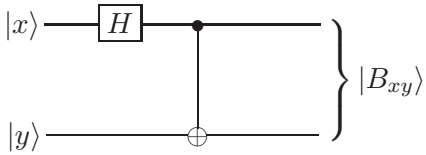
στην οποία το πρώτο κβαντοδυφίο είναι στην κατάσταση επαλληλίας $\alpha|0\rangle + \beta|1\rangle$ ενώ το δεύτερο στην κατάσταση βάσης $|1\rangle$. Δρώντας τώρα με την CNOT πάνω στην (15.3) παίρνουμε

$$\text{CNOT}\ |\psi_{\rm in}\rangle = \alpha|0\rangle|1\rangle + \beta|1\rangle|0\rangle \tag{15.4}$$

που είναι τώρα μια σύμπλεκτη κατάσταση αφού δεν μπορεί πλέον να γραφεί ως γινόμενο καταστάσεων των δύο κβαντοδυφίων αλλά μόνο ως γραμμικός συνδυασμός τέτοιων γινομένων. Ειδικότερα για $\alpha = \beta = 1/\sqrt{2}$ η (15.4) γράφεται ως

$$\frac{1}{\sqrt{2}}\big(|0\rangle|1\rangle + |1\rangle|0\rangle\big)$$

και δεν είναι παρά η κατάσταση Bell $|B_{01}\rangle$ στην οποία είχαμε αναφερθεί λίγο νωρίτερα. Σημειώστε ακόμα ότι όχι μόνο η $|B_{01}\rangle$ αλλά και οι άλλες καταστάσεις Bell $|B_{xy}\rangle$ μπορούν να δημιουργηθούν με τον ίδιο τρόπο και η σχετική «κατασκευή» φαίνεται στο κύκλωμα που ακολουθεί.



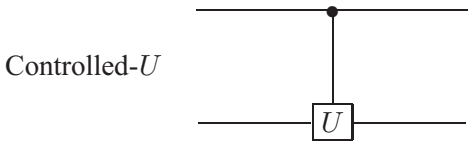
Σχημα 15.1: Κύκλωμα για τη δημιουργία των καταστάσεων Bell.

Έτσι, παραδείγματος χάριν, με κατάσταση εισόδου $|0\rangle|0\rangle \equiv |00\rangle$ προκύπτει ως έξοδος η κατάσταση Bell

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$$

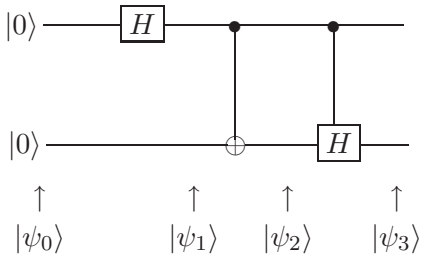
και παρόμοια για τις άλλες καταστάσεις.

Όπως θα το περίμενε κανείς η Controlled-NOT $\equiv$ CNOT είναι το αρχέτυπο μιας κατηγορίας πυλών του τύπου Controlled-U $\equiv$ C-U $\equiv$ CU, όπου τη θέση του NOT $\equiv X$ την παίρνει μια οποιαδήποτε άλλη πύλη U που δρα πάνω στο κβαντοδυφίο-στόχο. Και βέβαια το κυκλωματικό σύμβολο θα είναι



Μια απλή άσκηση για την εξοικείωση με την κυκλωματική γλώσσα του κβαντικού υπολογιστή είναι η εξής:

Ασκηση: Γράψτε την κβαντική κατάσταση $|\psi_i\rangle$, $i = 0, 1, 2, 3$ που αντιστοιχεί στα διαδοχικά στάδια λειτουργίας του ακόλουθου κβαντικού κυκλώματος



Λύση: Θα έχουμε διαδοχικά

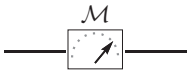
$$
\begin{aligned}
|\psi_0\rangle &= |0\rangle|0\rangle \\
|\psi_1\rangle = \big(H|0\rangle\big)|0\rangle &= \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)|0\rangle \\
|\psi_2\rangle = \text{CNOT}\,|\psi_1\rangle &= \frac{1}{\sqrt{2}}\big[\text{CNOT}\,\big(|0\rangle|0\rangle\big) + \text{CNOT}\,\big(|1\rangle|0\rangle\big)\big] \\
&= \frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle + |1\rangle|1\rangle\big) \\
|\psi_3\rangle = (C\text{-}H)|\psi_2\rangle &= \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\big(H|1\rangle\big) \\
&= \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{2}|1\rangle|0\rangle - \frac{1}{2}|1\rangle|1\rangle, \qquad (15.5)
\end{aligned}
$$

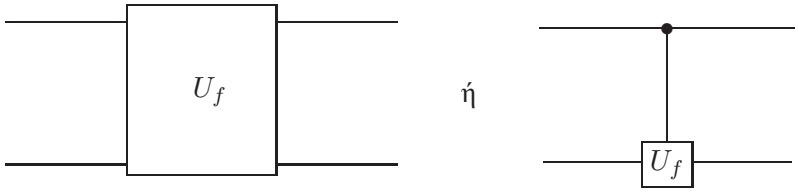
και βέβαια –όπως θα έπρεπε– το τελικό αποτέλεσμα (15.5) είναι μια κανονικοποιημένη κατάσταση, αφού $(1/\sqrt{2})^2 + (1/2)^2 + (1/2)^2 = 1$. Οι κυκλωματικοί κανόνες έγιναν, πιστεύουμε, τελείως σαφείς από το παραπάνω παράδειγμα: Κάθε οριζόντια γραμμή αντιπροσωπεύει το αντίστοιχο κβαντοδυφίο –το πρώτο η πάνω γραμμή και το δεύτερο η κάτω– ενώ οι πύλες που δρουν μόνο πάνω σε ένα κβαντοδυφίο δείχνονται με το σύμβολό τους πάνω στην αντίστοιχη γραμμή. Τέλος, η από αριστερά προς τα δεξιά κίνηση πάνω στις γραμμές του κυκλώματος αντιστοιχεί στη χρονική αλληλουχία των διαδοχικών δράσεων των πυλών του.

Και μια ερώτηση για σας: Αν στο τέλος της παραπάνω υπολογιστικής διαδικασίας μετρήσετε το κβαντοδυφίο #1 –τοποθετήσετε δηλαδή μια μετρητική συσκευή $\mathcal{M}$(*) στο τέλος της πρώτης γραμμής– ποιες είναι οι πιθανότητες να το βρείτε στην κατάσταση $|0\rangle$ ή την κατάσταση $|1\rangle$; Και ποια θα είναι η κατάσταση του καταχωρητή μετά τη μέτρηση που έδωσε το ένα ή το άλλο αποτέλεσμα;

Ως ένα ακόμη παράδειγμα κβαντικής πύλης του τύπου Controlled-U –που διαφέρει όμως ελαφρώς από τις άλλες– αναφέρουμε την πύλη U_f που συμβολίζεται ως

(*) Σημειώστε επ' ευκαιρία ότι το σχετικό κυκλωματικό σύμβολο είναι το





και δρα πάνω σε μια κατάσταση $|x\rangle|y\rangle \equiv |x, y\rangle$ ως ακολούθως

$$U_f|x\rangle|y\rangle \equiv |x\rangle|y \oplus f(x)\rangle,$$

δηλαδή όπως η CNOT αλλά με $f(x)$ όχι κατ' ανάγκην τη συνάρτηση $f(x) = x$ αλλά την πιο γενική *συνάρτηση τύπου Boole* πάνω στη δυαδική μεταβλητή x. Δηλαδή την πιο γενική συνάρτηση με πεδίο ορισμού και πεδίο τιμών το σύνολο $\{0, 1\}$. Και είναι εύκολο να δείτε αμέσως ότι υπάρχουν τέσσερις τέτοιες συναρτήσεις που χωρίζονται φυσιολογικά σε δύο ομάδες ως ακολούθως

$$f(x) = \text{σταθερά} \begin{cases} f(0) = f(1) = 0 & (1) \\ f(0) = f(1) = 1 & (2) \end{cases},$$

$$f(x) \neq \text{σταθερά} \begin{cases} f(0) = 0,\ f(1) = 1 & (3) \\ f(0) = 1,\ f(1) = 0 & (4) \end{cases}$$

εκ των οποίων η δεύτερη ομάδα $-f(x) \neq$ σταθ.– φέρει το όνομα *ισοζυγισμένη* ή απλώς *ζυγισμένη*, για τον προφανή λόγο ότι στο πεδίο τιμών της αντιπροσωπεύονται εξίσου και το *μηδέν* και το *ένα*. (Αντίθετα με την περίπτωση $f(x) =$ σταθ., όπου το πεδίο τιμών περιλαμβάνει μόνο το μηδέν ή μόνο το ένα κάθε φορά.) Η μπουλεανή συνάρτηση $f(x)$ αντιπροσωπεύει λοιπόν τέσσερις συναρτήσεις f_i $(i = 1, 2, 3, 4)$ –όπως παραπάνω– και για κάθε μία από αυτές βεβαιωθείτε μόνοι σας ότι η αντίστοιχη πύλη U_f θα παίρνει τη μορφή(*)

$$f(x) = \text{σταθερά} \begin{cases} U_{f_1} = I \otimes I \\ U_{f_2} = I \otimes X \equiv I \otimes \text{NOT} \end{cases},$$

(*) Εδώ –όπως και σε άλλες παρόμοιες περιπτώσεις λίγο αργότερα– είναι αναγκαίο να επαναφέρουμε τον συμβολισμό $A \otimes B$ του *τανυστικού γινομένου* (βλ. σελ. 210) σύμφωνα με τον οποίο ο πρώτος τελεστής δρα πάνω στο πρώτο σωματίδιο –δηλαδή, εδώ, το πρώτο κβαντοδυφίο– και ο δεύτερος πάνω στο δεύτερο.

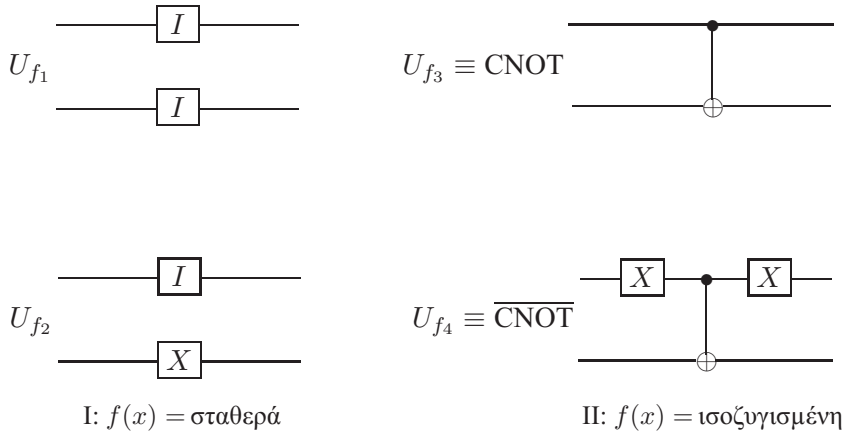
$$f(x) = \text{ισοζυγισμένη} \begin{cases} U_{f_3} = \text{CNOT} \\ U_{f_4} = \overline{\text{CNOT}} \end{cases}$$

όπου το σύμβολο $\overline{\text{CNOT}}$ εισήχθη εδώ για να δηλώσει την περίπτωση μιας πύλης που λειτουργεί ακριβώς όπως η CNOT αλλά με εναλλαγή των ρόλων των $|0\rangle$ και $|1\rangle$ στο κβαντοδυφίο ελέγχου. (Το δεύτερο κβαντοδυφίο αναστρέφεται όταν το πρώτο είναι 0 και παραμένει ως έχει αν το πρώτο είναι 1.) Το οποίο ισοδυναμεί, βεβαίως, με το να δράσει πρώτα η πύλη X πάνω στο πρώτο κβαντοδυφίο –οπότε θα εναλλαγούν οι καταστάσεις $|0\rangle$ και $|1\rangle$– να ακολουθήσει η CNOT και μετά πάλι η X για να επαναφέρει το κβαντοδυφίο ελέγχου στην αρχική του κατάσταση.

Μπορούμε επομένως να συνοψίσουμε τις τέσσερις παραπάνω περιπτώσεις στην κυκλωματική απεικόνιση του Σχήματος 15.2.

Βεβαιωθήκαμε λοιπόν παρεμπιπτόντως ότι τουλάχιστον για την πύλη U_f αληθεύει ο βασικός ισχυρισμός μας ότι κάθε άλλη πύλη μπορεί να πραγματωθεί με συνδυασμό των απλών πυλών που έχουμε ήδη εισαγάγει.

Σημειώστε τέλος ότι η πύλη U_f είναι σημαντική για τους ίδιους λόγους που είναι σημαντικές οι συναρτήσεις τύπου Boole για κάθε είδος υπολογιστή βασισμένου σε λογικές πύλες και κυκλώματα.



Σχημα 15.2: Κυκλωματική αναπαράσταση της πύλης U_f για τις δύο ομάδες συναρτήσεων Boole· I: $f(x) =$ σταθερά, II: $f(x) =$ ισοζυγισμένη.

2.3. Και μια πύλη που δεν υπάρχει: Ο κβαντικός αντιγραφέας

Θα κλείσουμε τούτη την παράγραφο με μια ακόμα πύλη που θα επιθυμούσαμε να εκτελεί μια εργασία ανάλογη με την *αντιγραφή αρχείων* σε έναν κλασικό υπολογιστή. Θέλουμε δηλαδή έναν *κβαντικό αντιγραφέα*. Και το ερώτημα είναι: Υπάρχει τέτοιου είδους πύλη; Δυστυχώς, όπως θα αποδείξουμε αμέσως, η απάντηση είναι αρνητική και ακούει στο όνομα «θεώρημα της μη αντιγραφής» ή, επί το βιολογικότερον, «θεώρημα της μη κλωνοποίησης» (no cloning theorem).

Υποθέστε όμως προς στιγμήν ότι μια τέτοια πύλη υπάρχει και αντιπροσωπεύεται από τον μοναδιαίο τελεστή U. Τι αναμένεται να κάνει αυτός ο τελεστής; Προφανώς το εξής. Να δρα πάνω σε μια κατάσταση γινομένου $|\psi\rangle|\phi\rangle$ –στην οποία η $|\psi\rangle$ ανήκει σε ένα κβαντικό σύστημα και η $|\phi\rangle$ σε ένα άλλο– και να την μετατρέπει στην $|\psi\rangle|\psi\rangle$, οπότε πράγματι η κατάσταση $|\psi\rangle$ –το *πρωτότυπο*– θα έχει «εκτυπωθεί» και στο δεύτερο κβαντικό σύστημα και έτσι θα διαθέτουμε πλέον δύο πανομοιότυπα αντίγραφά της. Θέλουμε δηλαδή να είναι

$$U|\psi\rangle|\phi\rangle = |\psi\rangle|\psi\rangle \tag{15.6}$$

για κάθε δυνατή κατάσταση $|\psi\rangle$ αλλά και για οποιαδήποτε αρχική κατάσταση $|\phi\rangle$ του δεύτερου συστήματος. Έστω ότι η (15.6) ισχύει πράγματι για δύο γραμμικά ανεξάρτητες καταστάσεις $|\psi_1\rangle$ και $|\psi_2\rangle$. Είναι δηλαδή

$$U|\psi_1\rangle|\phi\rangle = |\psi_1\rangle|\psi_1\rangle, \qquad U|\psi_2\rangle|\phi\rangle = |\psi_2\rangle|\psi_2\rangle.$$

Για να είναι όμως ο U ένας γενικός αντιγραφέας, τότε θα πρέπει να ισχύει η (15.6) και για κάθε γραμμικό συνδυασμό των $|\psi_1\rangle$ και $|\psi_2\rangle$ αφού και αυτός είναι μια δυνατή κατάσταση του αντιγραφόμενου συστήματος. Το οποίο όμως δεν αληθεύει, όπως φαίνεται αμέσως από τις πράξεις που ακολουθούν:

$$\begin{aligned} U\big(c_1|\psi_1\rangle + c_2|\psi_2\rangle\big)|\phi\rangle &= c_1\big(U|\psi_1\rangle|\phi\rangle\big) + c_2\big(U|\psi_2\rangle|\phi\rangle\big) \\ &= c_1|\psi_1\rangle|\psi_1\rangle + c_2|\psi_2\rangle|\psi_2\rangle \\ &\neq \big(c_1|\psi_1\rangle + c_2|\psi_2\rangle\big)\big(c_1|\psi_1\rangle + c_2|\psi_2\rangle\big) \end{aligned}$$

Όμως το θεώρημα της «μη αντιγραφής» χρειάζεται κάποιες διευκρινίσεις. Αυτό που αποκλείει είναι η δημιουργία πανομοιότυπων αντιγράφων μιας *άγνωστης κβαντικής κατάστασης*. Διότι αν η κατάσταση είναι γνωστή τότε μπορούμε πάντα να την θεωρήσουμε ως ιδιοκατάσταση κάποιου ερμιτιανού τελεστή και να «στήσουμε» μια μετρητική διαδικασία που θα «μετράει» αυτό το φυσικό μέγεθος(*)

(*) Στο πλαίσιο του αφηρημένου κβαντικού φορμαλισμού *κάθε* ερμιτιανός τελεστής μπορεί να θεωρηθεί ότι αντιπροσωπεύει κάποιο φυσικό μέγεθος και άρα μπορεί πάντα να επινοηθεί –έστω θεωρητικά– μια κατάλληλη συσκευή που να το μετράει.

και άρα θα μας δίνει –ως αποτέλεσμα μιας μέτρησης που «έβγαλε» τη σωστή ιδιοτιμή– την κατάσταση που επιθυμούμε. Αντιλαμβάνεστε όμως ότι η διαδικασία αυτή δεν συνιστά αντιγραφή –αφού οι καταστάσεις που εισέρχονται στη μετρητική συσκευή μπορούν να είναι οποιεσδήποτε– αλλά *κατασκευή* (μέσω μέτρησης) προαποφασισμένων κβαντικών καταστάσεων. Το θεώρημα της μη αντιγραφής αναφέρεται λοιπόν σε γνήσια αντιγραφή μιας άγνωστης κβαντικής κατάστασης και όχι στην πολλαπλή δημιουργία μιας γνωστής.

Και με αυτή την ουσιώδη διευκρίνιση το θεώρημα είναι μάλλον προφανές από φυσικής πλευράς. Διότι αν πράγματι μπορούσαμε να βγάλουμε όσα αντίγραφα θέλουμε μιας άγνωστης κβαντικής κατάστασης, τότε θα είχαμε τη δυνατότητα –εκτελώντας μετρήσεις πάνω στα αντίγραφα αυτά– να μάθουμε ό,τι θέλουμε για την κατάσταση αυτή διατηρώντας άθικτο το «πρωτότυπο». Το οποίο μάλλον καταστρατηγεί τη βασική αρχή της κβαντικής μέτρησης που αποκλείει την απόκτηση πληροφορίας για ένα κβαντικό σύστημα χωρίς καταστροφή της κατάστασής του. *Δεν υπάρχει δωρεάν πληροφορία στο κβαντικό πλαίσιο*.

3. *Κβαντικοί αλγόριθμοι*

3.1. Ένα απλό παράδειγμα: Ο αλγόριθμος του Deutsch

Μετά τις κβαντικές πύλες και τα σχετικά κυκλώματα το αναγκαίο επόμενο βήμα είναι η ανάπτυξη κατάλληλων προγραμμάτων –δηλαδή *κατάλληλων αλγορίθμων*– σχεδιασμένων να εκτελούν συγκεκριμένα καθήκοντα. Και το στοίχημα εδώ είναι πολύ σαφές. Να αποδειχτεί όχι μόνο ότι τέτοιοι αλγόριθμοι υπάρχουν, αλλά και ότι μπορεί να είναι πολύ αποτελεσματικότεροι, στη λύση ορισμένων τουλάχιστον προβλημάτων, από ό,τι οι αντίστοιχοι κλασικοί αλγόριθμοι. Έτσι, από αυτή την άποψη, ήταν μια σημαντική εξέλιξη στο θέμα όταν, το 1994, ο Peter Shor επινόησε έναν κβαντικό αλγόριθμο –βασισμένο στον περίφημο *κβαντικό μετασχηματισμό Fourier*– χάρις στον οποίο έγινε για πρώτη φορά εφικτή η επίλυση ενός από τα δυσκολότερα προβλήματα στην ιστορία των μαθηματικών και της επιστήμης των υπολογιστών: Η παραγοντοποίηση (factoring) ενός πολύ μεγάλου ακέραιου αριθμού.

Όμως στο πλαίσιο τούτης της σύντομης εισαγωγής θα περιοριστούμε στην παρουσίαση ενός πολύ στοιχειωδέστερου παραδείγματος που έχει και αυτό τη δική του ξεχωριστή θέση στη μικρή ιστορία του κλάδου. Πρόκειται για τον περίφημο *αλγόριθμο του Deutsch* (Deutsch, 1984) ο οποίος –στην πιο «παιδική» του μορφή– προορίζεται για έναν υπολογιστή με δύο μόνο κβαντοδυφία και αποσκοπεί στην επίλυση ενός εξίσου «παιδικού» προβλήματος. Να αποφανθούμε κατά πόσον μια συνάρτηση *τύπου Boole* –δηλαδή μια απεικόνιση από το $\{0,1\}$ στο $\{0,1\}$– είναι

σταθερή ή *ισοζυγισμένη* (balanced) σύμφωνα με την ορολογία που είχαμε εισαγάγει νωρίτερα (§ 2.2). Αν δηλαδή είναι $f(0) = f(1)$ ή $f(0) \neq f(1)$. Όπως είχαμε δει και νωρίτερα, υπάρχουν τέσσερις τέτοιες συναρτήσεις που ομαδοποιούνται ως ακολούθως

$$\text{I: } f(x) = \text{σταθερή} : \begin{cases} f(0) = 0,\ f(1) = 0 \\ f(0) = 1,\ f(1) = 1 \end{cases},$$

$$\text{II: } f(x) = \text{ισοζυγισμένη} : \begin{cases} f(0) = 0,\ f(1) = 1 \\ f(0) = 1,\ f(1) = 0 \end{cases}$$

Ένας κλασικός υπολογιστής μπορεί να απαντήσει το ερώτημά μας –αν η δοθείσα συνάρτηση f είναι σταθερή ή όχι– εκτελώντας *δύο πράξεις*: Υπολογίζοντας τις δύο τιμές $f(0)$ και $f(1)$. Και αν βγουν ίσες (μηδέν ή ένα αδιάφορο) τότε η δοθείσα f είναι σταθερή, αν όχι τότε δεν είναι.

Θα δείξουμε τώρα ότι με τον αλγόριθμο του Deutsch το παραπάνω πρόβλημα μπορεί να λυθεί με *μία μόνο πράξη*. Το σχετικό κβαντικό κύκλωμα δείχνεται στο Σχήμα 15.3.

Πριν προχωρήσουμε στην βήμα προς βήμα εκτέλεση του αλγορίθμου είναι χρήσιμο να δείξουμε πρώτα –ως άσκηση– ότι ισχύει η

$$U_f|x\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}} = (-1)^{f(x)}|x\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{15.7}$$

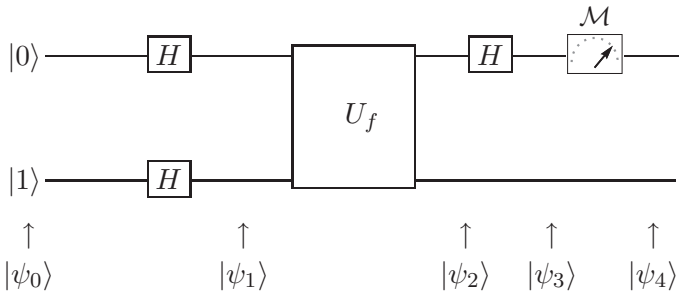
η οποία προφανώς θα μας χρειαστεί, διότι η δράση της πύλης H πάνω στο δεύτερο κβαντοδυφίο θα δώσει $(|0\rangle - |1\rangle)/\sqrt{2}$ οπότε –σε συνδυασμό με την κατάσταση $(|0\rangle + |1\rangle)/\sqrt{2}$ που θα εμφανιστεί στο πρώτο κβαντοδυφίο– θα έχουμε να υπολογίσουμε εκφράσεις του τύπου $U_f|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$ με $x = 0$ ή 1 που βεβαίως υπολογίζονται πολύ ευκολότερα βάσει της (15.7).

Απόδειξη της (15.7). Θα είναι κατ' αρχάς

$$U_f|x\rangle|0\rangle = |x\rangle|0 \oplus f(x)\rangle, \qquad U_f|x\rangle|1\rangle = |x\rangle|1 \oplus f(x)\rangle.$$

Δεδομένου όμως ότι $f(x) = 0$ ή 1 θα έχουμε

$$U_f|x\rangle|0\rangle = \begin{cases} \xrightarrow{f(x)=0} & |x\rangle|0\rangle \\ \xrightarrow{f(x)=1} & |x\rangle|1\rangle \end{cases}$$



Σχημα 15.3: *Κυκλωματική υλοποίηση του αλγορίθμου του Deutsch*. Στα δύο κβαντοδυφία του υπολογιστή –που ξεκινάνε από την αρχική κατάσταση $|0\rangle$ το πρώτο και $|1\rangle$ το δεύτερο– εφαρμόζεται η πύλη Hadamard H, αμέσως μετά η πύλη U_f : $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$, και τέλος πάλι η πύλη H πάνω στο πρώτο κβαντοδυφίο ακολουθούμενη από τη μέτρηση $\mathcal{M}$. Και αν το αποτέλεσμα αυτής της μέτρησης είναι 0, τότε η συνάρτηση f είναι *σταθερή* ($f(0) = f(1)$), ενώ αν είναι 1 η συνάρτηση f είναι *ισοζυγισμένη* ($f(0) \neq f(1)$). Έτσι ο αλγόριθμος του Deutsch απαντά το ερώτημά μας –αν η f είναι σταθερή ή όχι– με μία μόνο πράξη (έναν «γύρο») έναντι δύο του κλασικού υπολογιστή. Και είναι αυτονόητο, βεβαίως, ότι η μετρούμενη συνάρτηση f είναι τοποθετημένη σε ένα είδος «μαύρου κουτιού» που λειτουργεί ως βασικό στοιχείο της πύλης U_f χωρίς όμως να είναι προσβάσιμο από εμάς. Και στην ουσία εμείς καλούμαστε να αποφανθούμε –μετρώντας την έξοδο του υπολογιστή μας– αν η συνάρτηση που βρίσκεται μέσα στο κουτί είναι σταθερή ή όχι.

και

$$U_f|x\rangle|1\rangle = \begin{cases} \xrightarrow{f(x)=0} & |x\rangle|1\rangle \\ \xrightarrow{f(x)=1} & |x\rangle|0\rangle \end{cases}$$

$$\Rightarrow \quad U_f|x\rangle\big(|0\rangle - |1\rangle\big) = \left.\begin{cases} \xrightarrow{f(x)=0} & |x\rangle\big(|0\rangle - |1\rangle\big) \\ \xrightarrow{f(x)=1} & -|x\rangle\big(|0\rangle - |1\rangle\big) \end{cases}\right\} = (-1)^{f(x)}|x\rangle\big(|0\rangle - |1\rangle\big)$$

που είναι, βεβαίως, το αποτέλεσμα (15.7) χωρίς τον παράγοντα κανονικοποίησης $1/\sqrt{2}$ που δεν έχει προφανώς σημασία για την ισχύ αυτής της σχέσης.

Επιστρέφοντας στον αλγόριθμο του Deutsch θα έχουμε διαδοχικά

$$\blacktriangleright \qquad |\psi_0\rangle = |0\rangle|1\rangle \qquad \text{(Είσοδος)}$$

$$\blacktriangleright \qquad |\psi_1\rangle = \big(H|0\rangle\big)\big(H|1\rangle\big) = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\,\frac{|0\rangle - |1\rangle}{\sqrt{2}} \qquad \text{(Αποτέλεσμα 1)}$$

$$\begin{aligned}\blacktriangleright \qquad |\psi_2\rangle = U_f|\psi_1\rangle &= \frac{1}{\sqrt{2}}U_f\left(\big(|0\rangle + |1\rangle\big)\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\\ &= \frac{1}{\sqrt{2}}U_f\left(|0\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) + \frac{1}{\sqrt{2}}U_f\left(|1\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\\ &= \frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}} + \frac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}}\end{aligned}$$

$$\Rightarrow \quad |\psi_2\rangle = \begin{cases} \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}\,\dfrac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{αν } f(0) = f(1)\\[2ex] \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}\,\dfrac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{αν } f(0) \neq f(1)\end{cases} \qquad \text{(Αποτέλεσμα 2)}$$

$$\blacktriangleright \qquad |\psi_3\rangle = \begin{cases} H\left(\dfrac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\dfrac{|0\rangle - |1\rangle}{\sqrt{2}} & : \ f(0) = f(1)\\[2ex] H\left(\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\dfrac{|0\rangle - |1\rangle}{\sqrt{2}} & : \ f(0) \neq f(1)\end{cases}$$

$$\Rightarrow \quad |\psi_3\rangle = \begin{cases} |0\rangle\dfrac{|0\rangle - |1\rangle}{\sqrt{2}} & : \ f(0) = f(1)\\[2ex] |1\rangle\dfrac{|0\rangle - |1\rangle}{\sqrt{2}} & : \ f(0) \neq f(1)\end{cases} \qquad \text{(Αποτέλεσμα 3)}$$

οπότε, βέβαια, αρκεί να μετρήσουμε το πρώτο κβαντοδυφίο πάνω στην $|\psi_3\rangle$ για να αποφανθούμε αν η f είναι σταθερή ή όχι. Αν το κβαντοδυφίο αυτό «βγει» $|0\rangle$ τότε η f θα είναι σταθερή ενώ αν βγει $|1\rangle$ θα είναι ισοζυγισμένη.

3.2. Η φυσική πίσω από τον αλγόριθμο: Ο κβαντικός παραλληλισμός και πώς επιτυγχάνεται

Όπως είδαμε, η εφαρμογή του αλγορίθμου έδωσε πράγματι αυτό που υποσχεθήκαμε. Απάντησε το ερώτημά μας με ένα μόνο «τρέξιμο» της μηχανής έναντι δύο που θα απαιτούσε ένας κλασικός υπολογιστής. Και ο λόγος γι' αυτή την «οικονομία πράξεων» είναι γνωστός. Οφείλεται σε ένα θεμελιώδες χαρακτηριστικό του

τρόπου λειτουργίας ενός κβαντικού υπολογιστή. Τον *κβαντικό παραλληλισμό*: Ότι δηλαδή ο υπολογιστής εκμεταλλεύεται τη δυνατότητα των κβαντοδυφίων να υπάρχουν σε κάθε δυνατή επαλληλία των καταστάσεων $|0\rangle$ και $|1\rangle$ και εκτελεί έτσι το εκάστοτε πρόγραμμα και για τη μια και για την άλλη τιμή της δυαδικής μεταβλητής $x(= 0$ ή $1)$. Σ' αυτό το πνεύμα η πρώτη «κίνηση» του αλγορίθμου, να φέρουμε τα δύο κβαντοδυφία σε κατάσταση επαλληλίας –ώστε η βασική πράξη U_f να εφαρμοστεί παράλληλα για $x = 0$ και $x = 1$– ήταν απολύτως αναμενόμενη. Εύλογο ήταν επίσης αυτές οι επαλληλίες να είναι ισοβαρείς –50% για κάθε κατάσταση– ώστε ο αλγόριθμος να είναι «αμερόληπτος» απέναντι στις δύο τιμές του x. Έτσι η χρήση της πύλης Hadamard στο πρώτο στάδιο του αλγορίθμου ήταν περίπου αυτονόητη, αφού αυτή ακριβώς είναι η δουλειά της: Να δημιουργεί ισοβαρείς επαλληλίες των δύο βασικών καταστάσεων $|0\rangle$ και $|1\rangle$.

Πέρα όμως από τον ρόλο των υπερθέσεων στη λειτουργία του αλγορίθμου Deutsch, εξίσου σημαντική είναι και η σημασία της *συμβολής* των παράλληλων διαδικασιών που συντελούνται ώστε το τελικό αποτέλεσμα –η *έξοδος*– να έχει τη μορφή ιδιοκαταστάσεων της υπολογιστικής βάσης $|0\rangle$ και $|1\rangle$ και να είναι *εύκολα αναγνώσιμο*. Στην πραγματικότητα, αν το καλοσκεφτείτε, η λειτουργία του αλγορίθμου Deutsch είναι απολύτως όμοια με εκείνη των γνωστών πειραμάτων συμβολής στα οποία η αρχική δέσμη –ηλεκτρονίων ή φωτονίων– διαχωρίζεται σε ένα πρώτο στάδιο και οι δύο επιμέρους δέσμες ανασυντίθενται μετά ώστε να αναδημιουργήσουν μια νέα σύμφωνη δέσμη με χαρακτηριστικά που εξαρτώνται καίρια από τη διαφορά φάσεως μεταξύ των δεσμών λόγω των διαφορετικών διαδρομών που ακολουθήθηκαν. Στην ουσία –αν τα δούμε διαφορετικά– τέτοιου είδους πειράματα διαχωρισμού και ανασύνθεσης μιας δέσμης συνιστούν ένα είδος κβαντικού υπολογισμού αφού ο διαχωρισμός επιτρέπει να «σαρωθούν» ταυτόχρονα δύο ενδεχόμενα –να μάθουμε δηλαδή «τι συμβαίνει» σε δυο κλασικά αλληλοαποκλειόμενες διαδρομές– και να αποτυπώσουμε αυτές τις «παράλληλες εμπειρίες» στην τελική ενιαία δέσμη μέσω των διαφορών φάσεως που προκλήθηκαν καθ' οδόν. Και είναι φανερό από αυτή την «εικόνα» ότι κάτι ανάλογο συμβαίνει και στον αλγόριθμο του Deutsch, όπου οι αρχικές πύλες Hadamard δρουν ως «διαχωριστές δέσμης» (beam splitters) ενώ η ίδια πύλη στην πάνω έξοδο ανασυνθέτει τα δύο μέρη αυτής της δέσμης ώστε να την επαναφέρει στη μια ή την άλλη από τις βασικές καταστάσεις $|0\rangle$ ή $|1\rangle$.

Σημειώστε ακόμα τον... υπόγειο ρόλο της σύμπλεξης των δύο κβαντοδυφίων –μέσω της πύλης U_f που δρα ως ένα είδος γενικευμένης CNOT– χάρις στην οποία αυτό που «υπολογίζουμε» είναι ένα *ολικό* (global) *χαρακτηριστικό* της συνάρτησης f –αν είναι σταθερή ή ισοζυγισμένη– και όχι επιμέρους τιμές της. Το οποίο βέβαια είναι και το θεμελιώδες φυσικό χαρακτηριστικό των σύμπλεκτων καταστάσεων:

Ότι έχουν έναν ισχυρά *ολιστικό χαρακτήρα* με απώλεια της αυτονομίας των μερών τους. Αλλά σ' αυτό το θέμα θα χρειαστεί να επανέλθουμε.

3.3. Ανάγνωση του αποτελέσματος και ο ρόλος των σφαλμάτων

Όμως τούτη είναι μια καλή ευκαιρία να συζητήσουμε και το θέμα της *ανάγνωσης των αποτελεσμάτων* ενός κβαντικού υπολογιστή. Όπως θυμάστε, για το θέμα αυτό μιλήσαμε ήδη από την πρώτη παράγραφο τούτου του κεφαλαίου ξεχωρίζοντας μάλιστα μια ειδική περίπτωση, που είναι ακριβώς αυτή που έχουμε μπροστά μας τώρα. Το ερώτημα που θέτουμε στον υπολογιστή μας να είναι τέτοιο ώστε να μπορεί να απαντηθεί με ένα *ναι* ή ένα *όχι*, οπότε η απάντηση θα μπορούσε να δοθεί μέσω της τελικής κατάστασης του πρώτου μόνο κβαντοδυφίου του καταχωρητή: $|0\rangle$ αν η απάντηση είναι *ναι*, $|1\rangle$ αν η απάντηση είναι *όχι*. Αυτή λοιπόν είναι η τωρινή περίπτωση και πάνω σ' αυτήν είναι χρήσιμο να συζητήσουμε ξανά το βασικό ερώτημα της ανάγνωσης του αποτελέσματος κάθε κβαντικού υπολογισμού. Το ζήτημα είναι γνωστό: Αν π.χ. η μέτρηση «έβγαλε» την απάντηση $|1\rangle$, αυτό δεν σημαίνει ότι αυτή όντως ήταν η κατάσταση του κβαντοδυφίου πριν τη μέτρηση. Μπορούσε κάλλιστα η κατάσταση αυτή να είχε τη μορφή της επαλληλίας $\alpha|0\rangle + \beta|1\rangle$ με $|\alpha|^2 = 0{,}999$ και $|\beta|^2 = 0{,}001$ και στη δική μας μέτρηση να προέκυψε το πιο απίθανο –πλην όμως υπαρκτό– ενδεχόμενο της κατάστασης $|1\rangle$. Οπότε βέβαια –αν είχαμε βασιστεί σε αυτό και μόνο το αποτέλεσμα– θα είχαμε οδηγηθεί στο λανθασμένο συμπέρασμα ότι η απάντηση του υπολογιστή ήταν αρνητική στο ερώτημά μας, ενώ ίσχυε ακριβώς το αντίθετο. Πώς όμως προέκυψε στο πρώτο κβαντοδυφίο μια κατάσταση επαλληλίας του παραπάνω τύπου, αφού ο αλγόριθμος του Deutsch προβλέπει μόνο $|0\rangle$ ή μόνο $|1\rangle$ ανάλογα με το είδος της συνάρτησης f που βρίσκεται στο μαύρο κουτί; Η απάντηση είναι απλή όσο και σημαντική. Ο κβαντικός, όπως και ο κλασικός, υπολογιστής δεν είναι «τέλειες μηχανές» αλλά πραγματικά φυσικά συστήματα που λειτουργούν με ένα ενδεχόμενο σφάλματος, τόσο μεγαλύτερο όσο περισσότερες είναι οι «πράξεις» που καλούνται να εκτελέσουν μέσω των κατάλληλων πυλών. Έτσι λοιπόν ακόμα και όταν ο ιδεατός αλγόριθμος του προβλήματος προβλέπει την έκβαση $|0\rangle$ σε μια συγκεκριμένη περίπτωση, η πραγματική λειτουργία του υπολογιστή δεν θα δώσει ακριβώς $|0\rangle$ αλλά μια κατάσταση υπέρθεσης του τύπου που αναφέραμε πριν, όπου η σωστή απάντηση $|0\rangle$ έχει «μολυνθεί» με την παρουσία μιας ελαφράς «πρόσμειξης» από την λάθος απάντηση $|1\rangle$. Τι κάνουμε τότε; Απλούστατα επαναλαμβάνουμε τον υπολογισμό –δηλαδή «ξανατρέχουμε» το πρόγραμμα– όσες φορές χρειαστεί ώστε να βεβαιωθούμε (πάντα με ένα ανεκτό περιθώριο λάθους) ότι η απάντηση είναι όντως $|0\rangle$ (δηλαδή ΝΑΙ) και όχι $|1\rangle$ (δηλαδή ΟΧΙ) όπως είχαμε παραπλανηθεί να συμπεράνουμε από τη μία μόνο αρχική μέτρηση.

Ωραίος υπολογιστής! – θα σχολίαζε ειρωνικά ο δύσπιστος Θωμάς του πεδίου. Φτιάξαμε έναν (πανάκριβο!) κβαντικό υπολογιστή για να απαντά το ερώτημά μας σε έναν μόνο γύρο αντί δύο –σιγά την οικονομία!– αλλά χρειάζεται να τον τρέξουμε καμιά εκατοστή φορές για να βεβαιωθούμε ότι διαβάσαμε σωστά τον... χρησμό του! Αν είπε ΝΑΙ ή αν είπε ΟΧΙ! Και ακόμα και τότε να μην είμαστε απόλυτα σίγουροι ότι δεν έχουμε κάνει λάθος. Ότι το... ιερό τέρας δεν μας ξεγέλασε!

Η κριτική του Θωμά είναι ταυτόχρονα υπερβολική και ... βάσιμη. Υπερβολική διότι σε ένα ρεαλιστικό πρόβλημα –και όχι σε ένα πρόβλημα-παιγνίδι όπως το παρόν– η οικονομία πράξεων που αναμένεται από την εφαρμογή ενός κβαντικού αλγορίθμου είναι τόσο γιγάντια ώστε το κόστος της επανάληψης του υπολογισμού για εκατό ή χίλιες φορές να είναι κυριολεκτικά αστείο. Η κριτική όμως είναι ταυτόχρονα και βάσιμη διότι φέρνει στο προσκήνιο το θεμελιώδες ζήτημα της συσσώρευσης των σφαλμάτων σε έναν κβαντικό υπολογιστή και κατά πόσο έχουμε τη δυνατότητα «διόρθωσής» τους με κατάλληλους κβαντικούς κώδικες όπως και στους κλασικούς υπολογιστές. Το πρόβλημα όχι μόνο δεν είναι τετριμμένο αλλά και για κάποιο διάστημα έμοιαζε περίπου άλυτο. Σε σημείο που να έχει οδηγήσει πολλούς... Θωμάδες στο στάδιο της πλήρους... απιστίας: Ότι ο κβαντικός υπολογιστής είναι μια χίμαιρα με μηδενική πιθανότητα πραγματοποίησης. Και χρειάστηκε να επέμβει εκ νέου ο Schor(*) –αλλά όχι μόνο– για να αποδειχθεί ότι η *επιδιόρθωση* ή το *σβήσιμο* των κβαντικών σφαλμάτων είναι δυνατόν να γίνει με αποτελεσματικό τρόπο που δεν ακυρώνει την αναμενόμενη οικονομία πράξεων του ιδεατού αλγορίθμου.

Σημειώστε τέλος ότι η αναγνωσιμότητα του αποτελέσματος δεν περιορίζεται στην ειδική περίπτωση που αναλύσαμε πριν αλλά εκτείνεται σε κάθε περίπτωση που η έξοδος του υπολογιστή είναι μια ιδιοκατάσταση της υπολογιστικής βάσης –δηλαδή ένα «διάνυσμα» της μορφής $|001110\ldots\rangle$– οπότε κάθε κβαντοδυφίο διαβάζεται χωριστά και, βέβαια, για να μειώσουμε το ενδεχόμενο σφάλματος «ξανατρέχουμε» το πρόγραμμα όσες φορές χρειαστεί.

3.4. Και μια εναλλακτική παρουσίαση του αλγορίθμου του Deutsch

Θα κλείσουμε τούτη τη (βασική) παράγραφο με μια διαφορετική παρουσίαση του αλγορίθμου του Deutsch, που βασίζεται στην αναγωγή της πύλης U_f σε ισοδύναμες πύλες U_{f_i} $(i = 1, \ldots, 4)$ ανάλογα με την εκάστοτε μορφή της μπουλεανής συνάρτησης f.

Σ' αυτό το πνεύμα είναι αμέσως φανερό από το Σχήμα 15.2 ότι στην περίπτωση I $-f =$ σταθ.– η πύλη U_f στο κύκλωμα του Deutsch (Σχ. 15.3) θα αντικατασταθεί

(*) P.W. Schor, Scheme for reducing decoherence in quantum computer memory, *Phys. Rev.* A52, R2493 (1995).

με δύο *μη «αλληλεπιδρώντα» στοιχεία* εκ των οποίων το πάνω είναι πάντα η ταυτοτική πύλη, οπότε οι δύο πύλες Hadamard της ίδιας γραμμής του κυκλώματος θα πολλαπλασιαστούν μεταξύ τους με αποτέλεσμα $H^2 = 1$. Έτσι το πρώτο κβαντοδυφίο του υπολογιστή θα «διαδοθεί» ως έχει κατά μήκος αυτής της γραμμής και άρα θα φτάσει ως $|0\rangle$ στην πάνω έξοδο, ακριβώς όπως δείξαμε προηγουμένως. Η περίπτωση II –$f(x) \neq$ σταθ.– είναι πιο σύνθετη διότι τώρα υπάρχει αλληλεπίδραση μεταξύ πάνω και κάτω κβαντοδυφίου, αφού είναι

$$U_{f_3} = \text{CNOT}, \qquad U_{f_4} = \overline{\text{CNOT}}.$$

Και δεδομένου ότι η κατάσταση $|\psi_1\rangle$ στο κύκλωμα του Deutsch –βλ. Σχ. 15.3– είναι

$$|\psi_1\rangle = |+\rangle|-\rangle, \qquad |\pm\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle \pm |1\rangle\big)$$

και δεδομένου επίσης ότι (δείξτε το)

$$\text{CNOT}\,|+\rangle|-\rangle = |-\rangle|-\rangle, \qquad \overline{\text{CNOT}}\,|+\rangle|-\rangle = -|-\rangle|-\rangle,$$

η κατάσταση $|\psi_2\rangle$ –μετά την πύλη $U_f \equiv$ CNOT ή $\overline{\text{CNOT}}$– θα είναι η

$$|\psi_2\rangle = |-\rangle|-\rangle \qquad \text{ή} \qquad |\psi_2\rangle = -|-\rangle|-\rangle$$

οπότε η δράση της πύλης H στο πρώτο κβαντοδυφίο θα δώσει –θυμηθείτε ότι $H|-\rangle = |1\rangle$–

$$|\psi_3\rangle = \pm|1\rangle|-\rangle,$$

που είναι ξανά το προηγούμενό μας αποτέλεσμα: Η απάντηση είναι γραμμένη στο πρώτο κβαντοδυφίο που είναι $|1\rangle$ στην παρούσα περίπτωση, έναντι $|0\rangle$ της προηγούμενης.

Βλέπετε έτσι, καθώς εξοικειωνόμαστε βαθμιαία με το κυκλωματικό μοντέλο του κβαντικού υπολογιστή, ότι τα πράγματα –παρά τις θεμελιώδεις διαφορές τους– αρχίζουν να θυμίζουν σιγά-σιγά τα κλασικά ηλεκτρικά κυκλώματα στην «προολοκληρωμένη» εποχή τους. Λίγα βασικά στοιχεία –πηνία, πυκνωτές, αντιστάσεις, δίοδοι, τρανζίστορ, μπαταρίες, κ.λπ.– που πρέπει να μάθουμε πρώτα τι κάνει το καθένα και μετά πώς να τα συνδυάζουμε ώστε να επιτύχουμε την εκτέλεση ενός σύνθετου καθήκοντος.

Οι εποχές αλλάζουν αλλά κάποιοι βασικοί τρόποι σκέψης –όπως η ανάλυση ενός σύνθετου καθήκοντος σε λίγες βασικές «πράξεις»– φαίνεται να διατηρούν αναλλοίωτη την αξία τους.