Κεφάλαιο 35

Κβαντική Πολυπλοκότητα

Η προβολή της [κλασσικής] *Θεωρίας Υπολογιστικής Πολυπλοκότητας*, στον χώρο της *Κβαντικής Μηχανικής*, ορίζει την *Θεωρία Κβαντικής Υπολογιστικής Πολυπλοκότητας*: μίας νέας θεωρίας με τα δικά της βασικά αποτελέσματα και ανοικτά προβλήματα. Η Κβαντική Θεωρία Πολυπλοκότητας μελετά κλάσεις πολυπλοκότητας που ορίζονται με την χρήση των υπολογιστικών μοντέλων της κβαντικής πληροφορίας και κβαντικών υπολογιστών. Εξετάζει την δυσκολία προβλημάτων σε σχέση με αυτές τις κλάσεις πολυπλοκότητας καθώς και τις σχέσεις μεταξύ κβαντικών και κλασσικών κλάσεων.

35.1 Σύντομη Ιστορική Αναδρομή

Η κβαντική πολυπλοκότητα, όπως και η *Κβαντική Υπολογιστική*, γενικότερα, αναπτύχθηκε κατά τις δεκαετίες του 1980 και του 1990: με τις εργασίες των Richard Feynman, David Deutsch, Umesh Vazirani, Ethan Bernstein, Peter Shor, Emanuel Knill, κ.ά., οι οποίες βασίστηκαν στις εργασίες προγενέστερων, όπως οι Albert Einstein, Boris Podolsky, Nathan Rosen, και John Bell.

Παρακάτω αναφέρονται κάποιες από τις πλέον επιδραστικές, στην διαμόρφωση του χώρου, εργασίες:

1. Einstein, A., Podolsky, B., and Rosen, N., "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" 1935.
2. Bell, J., "On the Einstein-Podolsky-Rosen Paradox," 1964.
3. Feynman, R., "Simulating Physics with Computers," 1982.
4. Deutsch, D., "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer," 1985.
5. Shor, P., "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," 1994.
6. Kerenidis I., de Wolf R., "Exponential lower bound for 2-query locally decodable codes via a quantum argument," 2004.
7. Knill, E., "Quantum Randomness and Nondeterminism," 1996.

8. Benett, C., Bernstein, E., Brassard, G., and Vazirani, U., "Strengths and Weaknesses of Quantum Computing," 1997.

9. Bernstein, E., and Vazirani, U., "Quantum Complexity Theory," 1997.

10. Beals, R., Buhrman, H., Cleve, R., and Mosca, M., "Quantum Lower Bounds by Polynomials," 1998.

11. Vazirani, U., "On the Power of Quantum Computation," 1998.

35.2 Κβαντική Πληροφορία

Τα κλασσικά συστήματα χρησιμοποιούν τα συμβατικά bits για να αναπαραστήσουν πληροφορία και τα χρησιμοποιούν για την επικοινωνία μεταξύ τους, καθώς και για τους υπολογισμούς τους. Τα κβαντικά συστήματα όμως, χρησιμοποιούν μια διαφορετική αναπαράσταση, τα *quantum bits - qubits*. Ένα qubit αποτελεί ένα κβαντομηχανικό σύστημα δύο καταστάσεων, όπως η πόλωση ενός φωτονίου. Σε ένα τέτοιο σύστημα για παράδειγμα, οι δύο καταστάσεις είναι η οριζόντια και η κάθετη πόλωση. Αντίθετα με τα κλασσικά συστήματα, όπου ένα bit βρίσκεται σε μία από τις δύο καταστάσεις, η κβαντομηχανική επιτρέπει στο qubit να βρίσκεται σε υπέρθεση (superposition) και των δύο καταστάσεων ταυτόχρονα, μια ιδιότητα που αποτελεί θεμέλιο των κβαντικών υπολογισμών.

Όταν μετρήσουμε (παρατηρήσουμε) το qubit, η υπέρθεση στην οποία βρίσκεται θα καταρρεύσει[1], και θα καταλήξει σε δύο δυνατές καταστάσεις, συνήθως 0 και 1 όπως ένα κλασσικό bit. Οι δύο καταστάσεις στις οποίες μπορεί να μετρηθεί ένα qubit, χρησιμοποιώντας τον συμβολισμό Dirac (ή bra-ket notation) είναι οι ακόλουθες:

$$0 \longrightarrow |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$1 \longrightarrow |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Μια κβαντική κατάσταση, είναι μια γραμμική υπέρθεση των καταστάσεων βάσης, δηλαδή το qubit μπορεί να αναπαρασταθεί σαν γραμμικός συνδιασμός των $|0\rangle$ και $|1\rangle$:

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

όπου τα α, β είναι πλάτη πιθανότητας και μπορούν να είναι μιγαδικοί αριθμοί στην γενική περίπτωση. Όταν μετρήσουμε το qubit αυτό την κανονική βάση, η πιθανότητα το αποτέλεσμα να είναι $|0\rangle$ είναι $|\alpha|^2$, ενώ αντίστοιχα το αποτέλεσμα είναι $|1\rangle$ με πιθανότητα $|\beta|^2$. Ακόμη, επειδή τα πλάτη αυτά εξισώνονται με πιθανότητες, έχουμε τον ακόλουθο περιορισμό: $|\alpha|^2+|\beta|^2 = 1$.

35.3 Υπολογιστικά Μοντέλα

Το πιο ευρέως χρησιμοποιούμενο μοντέλο για την μαθηματική περιγραφή κβαντικών υπολογιστών, και κβαντικών αλγορίθμων, κατά συνέπεια, είναι το *κβαντικό*

[1] Με αποτέλεσμα απώλεια πληροφορίας!

κύκλωμα και, πιο συγκεκριμένα, οι οικογένειες *ομοιόμορφων*[2] κβαντικών κυκλωμάτων. Αυτά τα κυκλώματα ομοιάζουν αρκετά με τα λογικά κυκλώματα, τα οποία υλοποιούν Boolean συναρτήσεις,[3] που συναντά κάποιος σε μαθήματα μαθηματικής λογικής, ή διακριτών μαθηματικών.

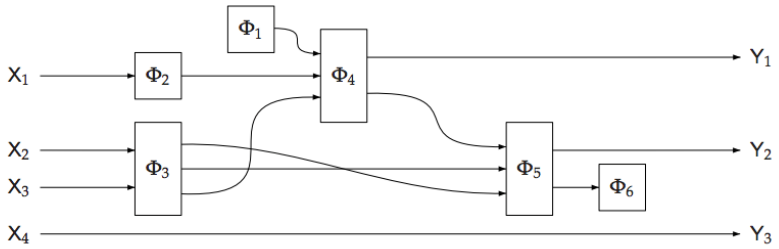
Οι πύλες που συνθέτουν ένα οποιοδήποτε κβαντικό κύκλωμα δύνανται όλες να κατασκευαστούν ως συνδυασμοί κβαντικών πυλών από το σύνολο

$$\{\text{CNOT}, H, T\}.$$

Οι πύλες αυτές είναι γραμμικοί unitary[4] μετασχηματισμοί:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$
$$H = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$
$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i \cdot \frac{\pi}{4}} \end{pmatrix},$$

με $i^2 = -1$. Η μορφή αυτών των μετασχηματισμών συνεπάγεται ότι οι είσοδοι και έξοδοι των κβαντικών αλγορίθμων μοντελοποιούνται ως *διανύσματα*.



Σχήμα 35.1: Ένα κβαντικό κύκλωμα

Σημείωση 35.3.1. Κάθε [κλασσικό] λογικό κύκλωμα δύναται να μετατραπεί σε ισοδύναμο κβαντικό κύκλωμα: τα κβαντικά κυκλώματα αποτελούν *γενίκευση* των κλασσικών κυκλωμάτων. [Παραλείπουμε τις λεπτομέρειες της μετατροπής!]

Εκτός από το κβαντικό κύκλωμα έχουν προταθεί και άλλα μοντέλα όπως, π.χ., οι *κβαντικές μηχανές Turing*.

[2] Με την έννοια ότι υπάρχει κλασσικός αλγόριθμος, πολυωνυμικού χρόνου, που εμφανίζει την [κλασσική] περιγραφή τους.

[3] Θυμίζουμε ότι κάθε Boolean συνάρτηση δύναται να υπολογισθεί από κάποιο λογικό κύκλωμα που χρησιμοποιεί μόνο τις λογικές πύλες NOT και AND.

[4] Ένας γραμμικός μετασχηματισμός T, επί ενός μιγαδικού διανυσματικού χώρου, είναι unitary αν $T^{-1} = T^*$: δηλαδή, αν ο αντίστροφός του ισούται με τον αναστροφοσυζυγή του. Οι unitary μετασχηματισμοί διατηρούν την *Ευκλείδεια νόρμα*: αυτό είναι χρήσιμο, για λόγους, όμως, που δεν θα καλύψουμε εδώ.

Σημείωση 35.3.2. Όπως θα γίνει φανερό, λίγο αργότερα, τα κβαντικά κυκλώματα χρησιμοποιούνται κυρίως στον ορισμό των κβαντικών κλάσεων *χρονικής* πολυπλοκότητας, ενώ οι κβαντικές μηχανές Turing χρησιμοποιούνται κυρίως στον ορισμό των κβαντικών κλάσεων *χωρικής* πολυπλοκότητας.

Σημείωση 35.3.3. Από την σκοπιά της *Θεωρίας Υπολογισιμότητας*, οι συμβατικοί, κλασσικοί, υπολογιστές είναι ισοδύναμοι με τους κβαντικούς: κάθε κβαντικός υπολογιστής δύναται να προσομοιωθεί πλήρως από έναν κλασσικό—με δυσανάλογα μεγάλο υπολογιστικό κόστος, όμως, στην γενική περίπτωση. Απλά, έχουμε σημαντικές ενδείξεις ότι, γενικά, οι κβαντικοί υπολογιστές είναι πολύ πιο αποδοτικοί από τους κλασσικούς.

35.4 Κβαντικές Κλάσεις Πολυπλοκοτητας

Ποιές είναι οι σημαντικότερες κβαντικές κλάσεις πολυπλοκότητας; Καταρχάς, αυτές που αναγνωρίζονται ως κβαντικά ανάλογα σημαντικών κλασσικών κλάσεων: η **BQP** μπορεί να ιδωθεί ως γενίκευση της **BPP** $\supseteq$ **P**, και η **QMA** ως γενίκευση της **MA** $\supseteq$ **NP**.

Ακολουθούν οι ορισμοί κάποιων κβαντικών κλάσεων.

Σημείωση 35.4.1. Στα επόμενα, ως *κβαντική κατάσταση* καλούμε την κατάσταση ενός *κβαντικού συστήματος*. Χωρίς να θέλουμε να εισέλθουμε σε λεπτομέρειες, η κύρια διαφορά από μία *κλασσική κατάσταση*, που περιγράφει, δηλαδή, την κατάσταση ενός *κλασσικού συστήματος*, είναι η εξής: για να περιγράψουμε μία κβαντική κατάσταση χρειαζόμαστε εκθετικά-μεγάλη, ως προς το μέγεθος του κβαντικού συστήματος που περιγράφει, κλασσική πληροφορία, ενώ για να περιγράψουμε μία κλασσική κατάσταση απαιτείται γραμμικά-μεγάλη, ως προς το μέγεθος της κλασσικής κατάστασης που περιγράφει, κλασσική πληροφορία. Γενικά: μία κβαντική κατάσταση μπορεί να ιδωθεί ως μία *υπέρθεση* ενός συνόλου κλασσικών καταστάσεων. Για παράδειγμα, μία κβαντική κατάσταση μεγέθους n απαιτεί 2^n μιγαδικούς αριθμούς για να περιγραφεί—ενώ μία αντιστοίχου μεγέθους κλασσική απαιτεί μόλις n bits.

Σημείωση 35.4.2. Έστω $\Sigma = \{0,1\}$. Με $L \subseteq \Sigma^* = \bigcup_{i=1}^{\infty} \Sigma^i$ συμβολίζουμε γλώσσες, [δηλαδή, σύνολα πεπερασμένων συμβολοσειρών,] και με $|x|$ το μήκος κάθε [πεπερασμένης] συμβολοσειράς $x \in \Sigma^*$. Τέλος, με $\Pr[E]$ συμβολίζουμε την πιθανότητα να συμβεί το ενδεχόμενο E.

Ορισμός 35.4.3 (Η κλάση **BQP**)**.** Αν $L \in$ **BQP**, τότε υπάρχει μία οικογένεια κβαντικών κυκλωμάτων $\{Q_i\}_i$ πολυωνυμικού χρόνου ως προς i, για κάθε i, [υπάρχει, δηλαδή, ένα κύκλωμα Q_i για κάθε μήκος εισόδου i,] τέτοια ώστε για κάθε $x \in \Sigma^*$ έχουμε ότι:

- $x \in L \Rightarrow \Pr\left[\text{το } Q_{|x|} \text{ αποδέχεται το } x\right] \geq \frac{2}{3}$.
- $x \notin L \Rightarrow \Pr\left[\text{το } Q_{|x|} \text{ αποδέχεται το } x\right] \leq \frac{1}{3}$.

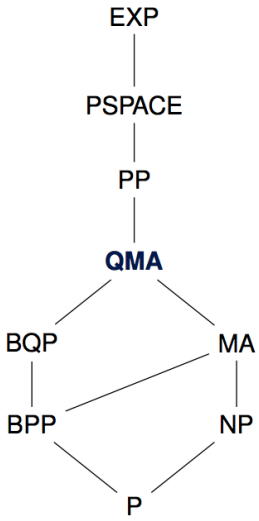
Η κλάση **BQP** είναι η πιο μελετημένη κβαντική κλάση πολυπλοκότητας, γιατί αντιπροσωπεύει το σύνολο των προβλημάτων που *επιλύονται* αποδοτικά με την χρήση κβαντικών υπολογιστών.

Ορισμός 35.4.4 (Η κλάση **QMA**). Αν $L \in \mathbf{QMA}$, τότε υπάρχει μία οικογένεια κβαντικών κυκλωμάτων $\{Q_i\}_i$ πολυωνυμικού χρόνου ως προς i, για κάθε i, [υπάρχει, δηλαδή, ένα κύκλωμα Q_i για κάθε μήκος εισόδου i,] τέτοια ώστε για κάθε $x \in \Sigma^*$ έχουμε ότι:

- $x \in L \Rightarrow$ υπάρχει μία κβαντική κατάσταση $\mathcal{K}$, πολυωνυμικού [ως προς το $|x|$] μήκους, τέτοια ώστε $\Pr\left[\text{το } Q_{|x|} \text{ αποδέχεται το ζεύγος } (x, \mathcal{K})\right] \geq \frac{2}{3}$.
- $x \notin L \Rightarrow$, κάθε κβαντική κατάσταση $\mathcal{K}$, πολυωνυμικού [ως προς το $|x|$] μήκους, είναι τέτοια ώστε $\Pr\left[\text{το } Q_{|x|} \text{ αποδέχεται το ζεύγος } (x, \mathcal{K})\right] \leq \frac{1}{3}$.

Η κλάση **QMA** είναι αντιπροσωπεύει το σύνολο των προβλημάτων των οποίων οι λύσεις *επαληθεύονται* αποδοτικά με την χρήση κβαντικών υπολογιστών.

Ισχύει ότι $\mathbf{BQP} \subseteq \mathbf{QMA}$.



Ορισμός 35.4.5 (Η κλάση **QCMA**). Αν $L \in \mathbf{QCMA}$, τότε υπάρχει μία οικογένεια κβαντικών κυκλωμάτων $\{Q_i\}_i$ πολυωνυμικού χρόνου ως προς i, για κάθε i, [υπάρχει, δηλαδή, ένα κύκλωμα Q_i για κάθε μήκος εισόδου i,] τέτοια ώστε για κάθε $x \in \Sigma^*$ έχουμε ότι:

- $x \in L \Rightarrow$ υπάρχει μία κλασσική κατάσταση $\mathscr{K}$, πολυωνυμικού [ως προς το $|x|$] μήκους, τέτοια ώστε $\Pr\left[\text{το } Q_{|x|} \text{ αποδέχεται το ζεύγος } (x, \mathscr{K})\right] \geq \frac{2}{3}$.
- $x \notin L \Rightarrow$, κάθε κλασσική κατάσταση $\mathscr{K}$, πολυωνυμικού [ως προς το $|x|$] μήκους, είναι τέτοια ώστε $\Pr\left[\text{το } Q_{|x|} \text{ αποδέχεται το ζεύγος } (x, \mathscr{K})\right] \leq \frac{1}{3}$.

Ισχύει ότι $\mathbf{QCMA} \subseteq \mathbf{QMA}$: κάθε κλασσικός μάρτυρας-κατάσταση μπορεί να ιδωθεί ως ειδική περίπτωση κβαντικού μάρτυρα-κατάστασης. Επίσης, $\mathbf{BQP} \subseteq \mathbf{QCMA}$.

Η κλάση **QCMA** απαντάται και ως **CMQA**, ή **MQA**.

Σημείωση 35.4.6. Παρατηρούμε ότι:

$$\mathbf{P} \subseteq \mathbf{BPP} \subseteq \mathbf{BQP} \subseteq \mathbf{QCMA} \subseteq \mathbf{QMA},$$

και

$$\mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{MA} \subseteq \mathbf{QCMA}.$$

Ορισμός 35.4.7 (Η κλάση $\mathbf{QCMA}_1$)**.** Αν $L \in \mathbf{QCMA}_1$, τότε υπάρχει μία οικογένεια κβαντικών κυκλωμάτων $\{Q_i\}_i$ πολυωνυμικού χρόνου ως προς i, για κάθε i, [υπάρχει, δηλαδή, ένα κύκλωμα Q_i για κάθε μήκος εισόδου i,] τέτοια ώστε για κάθε $x \in \Sigma^*$ έχουμε ότι:

- $x \in L \Rightarrow$ υπάρχει μία κλασσική κατάσταση $\mathscr{K}$, πολυωνυμικού [ως προς το $|x|$] μήκους, τέτοια ώστε $\Pr\left[\text{το } Q_{|x|} \text{ αποδέχεται το ζεύγος } (x, \mathscr{K})\right] = 1$.
- $x \notin L \Rightarrow$, κάθε κλασσική κατάσταση $\mathscr{K}$, πολυωνυμικού [ως προς το $|x|$] μήκους, είναι τέτοια ώστε $\Pr\left[\text{το } Q_{|x|} \text{ αποδέχεται το ζεύγος } (x, \mathscr{K})\right] \leq \frac{1}{3}$.

Αποδεικνύεται ότι $\mathbf{QCMA}_1 = \mathbf{QCMA}$.

Ορισμός 35.4.8 (Η κλάση **PQP**)**.** Αν $L \in \mathbf{PQP}$, τότε υπάρχει μία οικογένεια κβαντικών κυκλωμάτων $\{Q_i\}_i$ πολυωνυμικού χρόνου ως προς i, για κάθε i, [υπάρχει, δηλαδή, ένα κύκλωμα Q_i για κάθε μήκος εισόδου i,] τέτοια ώστε για κάθε $x \in \Sigma^*$ έχουμε ότι:

- $x \in L \Rightarrow \Pr\left[\text{το } Q_{|x|} \text{ αποδέχεται το } x\right] > \frac{1}{2}$.
- $x \notin L \Rightarrow \Pr\left[\text{το } Q_{|x|} \text{ αποδέχεται το } x\right] \leq \frac{1}{2}$.

Ισχύει ότι $\mathbf{PP} \subseteq \mathbf{PQP}$.

Ορισμός 35.4.9 (Η κλάση **QIP**)**.** Αν $L \in \mathbf{QIP}$, τότε υπάρχει μία οικογένεια κβαντικών κυκλωμάτων-*επαληθευτών* $\{V_i\}_i$ πολυωνυμικού χρόνου ως προς i, για κάθε i, [υπάρχει, δηλαδή, ένα κύκλωμα-επαληθευτής V_i για κάθε μήκος εισόδου i,] τέτοια ώστε για κάθε $x \in \Sigma^*$ έχουμε ότι:[5]

- $x \in L \Rightarrow (\exists P\ Prover)\left[\Pr\left[\text{ο } P \text{ πείθει τον } V_{|x|} \text{ να αποδεχτεί το } x\right] \geq \frac{2}{3}\right]$.
- $x \notin L \Rightarrow (\forall P\ Provers)\left[\Pr\left[\text{ο } P \text{ πείθει τον } V_{|x|} \text{ να αποδεχτεί το } x\right] \leq \frac{1}{3}\right]$.

Ισχύει ότι $\mathbf{IP} \subseteq \mathbf{QIP}$.

Ακόμη, υπάρχει η κλάση $QIP(m)$ η οποία περιορίζει σε m τα μηνύματα που ανταλλάσσονται συνολικά μεταξύ του prover και του verifier.

Ορισμός 35.4.10 (Η κλάση **BQPSPACE**)**.** Αν $L \in \mathbf{BQPSPACE}$, τότε υπάρχει μία κβαντική μηχανή Turing M, πολυωνυμικού [ως προς το μέγεθος της εισόδου της] χώρου, τέτοια ώστε για κάθε $x \in \Sigma^*$ έχουμε ότι:

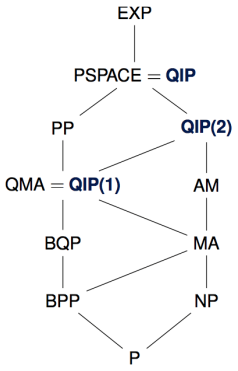
- $x \in L \Rightarrow \Pr\left[\eta\ M \text{ αποδέχεται το } x\right] \geq \frac{2}{3}$.
- $x \notin L \Rightarrow \Pr\left[\eta\ M \text{ αποδέχεται το } x\right] \leq \frac{1}{3}$.

Ορισμός 35.4.11 (Η κλάση **PQPSPACE**)**.** Αν $L \in \mathbf{PQPSPACE}$, τότε υπάρχει μία κβαντική μηχανή Turing M, πολυωνυμικού [ως προς το μέγεθος της εισόδου της] χώρου, τέτοια ώστε για κάθε $x \in \Sigma^*$ έχουμε ότι:

- $x \in L \Rightarrow \Pr\left[\eta\ M \text{ αποδέχεται το } x\right] > \frac{1}{2}$.
- $x \notin L \Rightarrow \Pr\left[\eta\ M \text{ αποδέχεται το } x\right] \leq \frac{1}{2}$.

Ισχύει ότι $\mathbf{PSPACE} = \mathbf{BBPSPACE} \subseteq \mathbf{BQPSPACE} \subseteq \mathbf{PQPSPACE}$.

[5] Όπου με ΑΠΟΔΕΙΚΤΕΣ συμβολίζουμε το σύνολο των δυνατών *αποδεικτών*.



35.5 Θεμελιώδη Αποτελέσματα

Εδώ παρουσιάζονται κάποια βασικά αποτελέσματα της κβαντικής πολυπλοκότητας.

Θεώρημα 35.5.1. $\mathbf{BQP}^{\mathbf{BQP}} = \mathbf{BQP}$*: η κλάση* $\mathbf{BQP}$ *δεν γίνεται ισχυρότερη αν επιτρέψουμε την χρήση υπο-ρουτινών που επιλύουν προβλήματα που ανήκουν στην* $\mathbf{BQP}$.

Θεώρημα 35.5.2. *Υπάρχει μαντείο* $\mathcal{A}$*, τέτοιο ώστε* $\mathbf{BQP}^{\mathcal{A}} \not\subseteq \mathbf{BPP}^{\mathcal{A}}$.

Θεώρημα 35.5.3. *Υπάρχει μαντείο* $\mathcal{A}$*, τέτοιο ώστε* $\mathbf{NP}^{\mathcal{A}} \not\subseteq \mathbf{BQP}^{\mathcal{A}}$.

Θεώρημα 35.5.4. $\mathbf{QMA} \subseteq \mathbf{PP}$.

Θεώρημα 35.5.5. $\mathbf{PQP} = \mathbf{PP}$.

Θεώρημα 35.5.6. $\mathbf{QIP} = \mathbf{PSPACE} = \mathbf{IP}$.

Θεώρημα 35.5.7. $\mathbf{BQPSPACE} = \mathbf{PQPSPACE} = \mathbf{PSPACE}$.

Θεώρημα 35.5.8 (Grover)**.** *Υπάρχει κβαντικός αλγόριθμος που υπολογίζει την θέση ενός [έστω μοναδικού] αντικειμένου* s*, που ανήκει σε μία λίστα μεγέθους* $N \in \mathbb{N}$*, σε* $\mathcal{O}\left(\sqrt{N}\right)$ *βήματα. Η απόδοση του κβαντικού αυτού αλγορίθμου αποδεικνύεται ότι είναι βέλτιστη.*

Παρατηρούμε ότι κάθε κλασσικός αλγόριθμος απαιτεί $\Omega(N)$ βήματα για την εκτέλεση της παραπάνω λειτουργίας αναζήτησης.

Ορισμός 35.5.9 (FACTORING)**.**
Είσοδος: ένας φυσικός αριθμός n.
Έξοδος: η παραγοντοποίηση του n σε γινόμενο δυνάμεων πρώτων αριθμών.

Θεώρημα 35.5.10. FACTORING $\in \mathbf{BQP}$.

Δεν γνωρίζουμε αν FACTORING $\in \mathbf{P}$, ενώ ισχύει ότι FACTORING $\in \mathbf{TFNP}$.

Ορισμός 35.5.11 (DISCRETE LOGARITHM)**.**
Είσοδος: δύο στοιχεία a και b μίας ομάδας G: $a, b \in G$. Η πράξη της ομάδας G δηλώνεται με '$\cdot$,' και έχουμε ότι

$$a^0 = e, \text{ το ουδέτερο στοιχείο της πράξης '}\cdot\text{' στην } G, \qquad \text{και}$$
$$a^m = a^{m-1} \cdot a, \qquad \forall m \in \mathbb{N}_{\geq 1}.$$

Έξοδος: ένας φυσικός αριθμός c τέτοιος ώστε $a^c = b$, αν αυτός υπάρχει, αλλιώς, κάποια ένδειξη ότι ο c δεν υπάρχει.

Θεώρημα 35.5.12. DISCRETE LOGARITHM $\in$ **BQP**.

Δεν γνωρίζουμε αν DISCRETE LOGARITHM $\in$ **P**, ενώ ισχύει ότι DISCRETE LOGARITHM $\in$ **TFNP**.

Ορισμός 35.5.13 (GROUP NON-MEMBERSHIP)**.**
Είσοδος: μία υποομάδα H, κάποιας ομάδας G, και ένα στοιχείο $g \in G$. [Η υποομάδα H είναι γνωστή μέσω των γεννητόρων της.]
Ερώτηση: ισχύει ότι $g \notin H$;

Θεώρημα 35.5.14. GROUP NON-MEMBERSHIP $\in$ **QMA**.

Δεν γνωρίζουμε αν GROUP NON-MEMBERSHIP $\in$ **NP**.

Ορισμός 35.5.15 (k-LOCAL HAMILTONIAN)**.** [Αναζητήστε το!]

Θεώρημα 35.5.16. *Το πρόβλημα* 2-LOCAL HAMILTONIAN *είναι* **QMA**-complete.

Υπάρχουν αρκετά άλλα προβλήματα που έχουν επίσης χαρακτηριστεί ως **QMA**-complete.

35.6 Ανοικτά Προβλήματα

Ο χώρος της κβαντικής πολυπλοκότητας χαρακτηρίζεται από ενδιαφέροντα ανοικτά προβλήματα. Παρακάτω αναφέρονται κάποια από αυτά:

1. **NP** $\overset{?}{\subseteq}$ **BQP**. Το συγκεκριμένο ερώτημα είναι πολύ σημαντικό: αν η απάντηση σε αυτό είναι ΝΑΙ, τότε ένας κβαντικός υπολογιστής μπορεί να λύσει σε πολυωνυμικό χρόνο κάθε ένα από τα ενδιαφέροντα, και καθημερινώς ανακύπτοντα, προβλήματα της κλάσης **NP**.

2. **BQP** $\overset{?}{\subseteq}$ **NP**. Αλλιώς: *είναι ο πολυωνυμικός μη-ντετερμινισμός ισχυρότερος από τους πολυωνυμικούς κβαντικούς υπολογιστές;*

3. **QMA** $\overset{?}{\subseteq}$ **QCMA**: αν ΝΑΙ, τότε δεν είναι απαραίτητο ο μάρτυρας στον ορισμό της **QMA** να είναι κάποια κβαντική κατάσταση, αλλά μπορεί να είναι κλασσικός, π.χ., μία πεπερασμένη ακολουθία από bits. Σε αυτή την περίπτωση έχουμε ότι **QMA** = **QCMA**.

4. Υπάρχει [κλασσικό] μαντείο $\mathcal{A}$, τέτοιο ώστε $\mathbf{QMA}^{\mathcal{A}} \not\subseteq \mathbf{QCMA}^{\mathcal{A}}$;

5. **BQP** $\overset{?}{\subseteq}$ **BPP**. Αν ΝΑΙ, τότε οι κβαντικοί υπολογιστές δεν προσφέρουν τίποτε περισσότερο από τους κλασσικούς πιθανοκρατικούς υπολογιστές. Θεωρείται απίθανο.

6. **BQP** $\overset{?}{\subseteq}$ **P**. Αν ΝΑΙ, τότε οι κβαντικοί υπολογιστές δεν προσφέρουν τίποτε περισσότερο από τους κλασσικούς ντετερμινιστικούς υπολογιστές. Θεωρείται απίθανο.

7. $\mathbf{BQP} \stackrel{?}{\subseteq} \mathbf{PH}$. Θυμίζουμε ότι $\mathbf{BPP} \subseteq \mathbf{PH}$.

8. Υπάρχει μαντείο $\mathcal{A}$, τέτοιο ώστε $\mathbf{BQP}^{\mathcal{A}} \not\subseteq \mathbf{PH}^{\mathcal{A}}$;

9. Υπάρχουν *κλειστές χρονο-ομοιάζουσες καμπύλες, CTCs*,[6] στην φύση; Αν ΝΑΙ, τότε αν θέσουμε ως

   $\mathbf{P}_{\mathsf{CTC}}$ = το σύνολο των γλωσσών που δύνανται να αποφασιστούν από ένα κλασσικό υπολογιστή, εφοδιασμένο με CTCs, σε πολυωνυμικό χρόνο, και με μηδενικό σφάλμα,

   και

   $\mathbf{BQP}_{\mathsf{CTC}}$ = το σύνολο των γλωσσών που δύνανται να αποφασιστούν από ένα κβαντικό υπολογιστή, εφοδιασμένο με CTCs, σε πολυωνυμικό χρόνο, και με φραγμένο σφάλμα,

   έχουμε ότι

   $$\mathbf{P}_{\mathsf{CTC}} = \mathbf{PSPACE} = \mathbf{BQP}_{\mathsf{CTC}}.$$

   Πιο απλά: ένας ντετερμινιστικός υπολογιστής πολυωνυμικού χρόνου, εφοδιασμένος με τέτοιου είδους καμπύλες, μπορεί να αποφασίζει όλη την κλάση **PSPACE**, και, ακόμα, είναι ισοδύναμος με έναν αντίστοιχα-εφοδιασμένο κβαντικό υπολογιστή πολυωνυμικού χρόνου!

10. Υπάρχουν #**P**-complete προβλήματα κβαντικής φύσης;

Ορισμός 35.6.1 (GRAPH ISOMORPHISM)**.**
Είσοδος: δύο γραφήματα G_1 και G_2.
Ερώτηση: είναι τα G_1 και G_2 ισομορφικά;

11. GRAPH ISOMORPHISM $\stackrel{?}{\in}$ **BQP**. Θυμίζουμε ότι GRAPH ISOMORPHISM $\in$ **NP**, ενώ δεν γνωρίζουμε αν GRAPH ISOMORPHISM $\in$ **P**. Επίσης, δεν γνωρίζουμε αν το GRAPH ISOMORPHISM είναι **NP**-complete.

Ορισμός 35.6.2 (GRAPH NON-ISOMORPHISM)**.**
Είσοδος: δύο γραφήματα G_1 και G_2.
Ερώτηση: είναι τα G_1 και G_2 μη-ισομορφικά;

12. GRAPH NON-ISOMORPHISM $\stackrel{?}{\in}$ **QMA**. Γνωρίζουμε ότι GRAPH NON-ISOMORPHISM $\in$ *co***NP** $\cap$ **AM**.

[6] Closed timelike curves.