# Quantum computation

Κουβαράς Μάριος
Κωνσταντινίδης Ορέστης

# Κβαντικό σύστημα

Οι υπολογιστές δεν είναι πλέον ένα κλασσικό αντικείμενο, αλλά ένα *κβαντικό σύστημα*.

Για κάθε $bit$ εκτός από 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 $|\alpha|^2 + |\beta|^2 = 1$, όπου $|\alpha|^2$ η πιθανότητα να καταρρεύσει στο $|0\rangle$ και αντίστοιχα για το $\beta$.

# Κβαντικός υπολογιστής *αναπόφευκτο (1)*

*Νόμος του Moore:*

κάθε δύο χρόνια η χωρητικότητα της μνήμης των κλασικών υπολογιστών διπλασιάζεται.

σμίκρυνση της βασικής μονάδας μνήμης,

η μονάδα αυτή θα αποκτήσει ατομικές διαστάσεις.

Η εφαρμογή των κβαντικών νόμων θα είναι αναγκαστική.

# Κβαντικός υπολογιστής *αναπόφευκτο (2)*

Richard Feynman το 1982:

η υπολογιστική πολυπλοκότητα των κβαντικών συστημάτων αυξάνεται *εκθετικά* συναρτήσει του αριθμού των σωματιδίων τους

μπορεί να αντιμετωπιστεί μόνο με έναν υπολογιστή που θα είναι κι αυτός ένα κβαντικό σύστημα

ύπαρξη ενός κβαντικού συστήματος $\Longrightarrow$ *έμπρακτη επίλυση* των σχετικών εξισώσεων

# Quantum Bit = qubit

*δυαδικό ψηφίο = ελάχιστο κομμάτι μνήμης = μονάδα πληροφορίας*

δυνατές καταστάσεις του συστήματος

$$|00\rangle \equiv |0\rangle|0\rangle \qquad |01\rangle \equiv |0\rangle|1\rangle$$

$$|10\rangle \equiv |1\rangle|0\rangle \qquad |11\rangle \equiv |1\rangle|1\rangle$$

γενική κατάσταση της μνήμης

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

# Γενική κβαντική κατάσταση της μνήμης

$$|\psi\rangle = \sum_{x} c_x \, |x\rangle \equiv \sum_{x_1, x_2, \ldots, x_N} c_{x_1, x_2, \ldots, x_N} \, |x_1, x_2, \ldots, x_N\rangle,$$

Με συνθήκη κανονικοποίησης

$$\sum_{x} |c_x|^2 = 1.$$

διακόσιες μόνο θέσεις μνήμης μπορεί να «φορτωθεί» και να γίνει αντικείμενο επεξεργασίας πληροφορία

$$2^{200} \; bit \equiv \; 2^{200}$$

δυαδικών ψηφίων

# Μέτρηση

με τη μέτρηση το qubit θα καταρρεύσει στη μία ή την άλλη από τις καταστάσεις $|0\rangle$ ή $|1\rangle$

ουδεμία τέτοια μέτρηση πραγματοποιείται στη διάρκεια ενός υπολογισμού

το υπολογιστικό πρόγραμμα εκτελείται ταυτόχρονα –ή «παράλληλα»– και για τις δύο τιμές της δυαδικής μεταβλητής του κάθε qubit

*μαζικός κβαντικός παραλληλισμός* ⇒

θεμελιώδη μηχανισμό λειτουργίας ενός κβαντικού υπολογιστή

# Διάβασμα αποτελέσματος

η απάντηση δεν χρειάζεται να είναι τόσο μακροσκελής όσο η μνήμη του υπολογιστή

ΝΑΙ ή ΟΧΙ

«ξανατρέχουμε» το πρόγραμμα όσες φορές χρειαστεί

για να περιορίσουμε το ενδεχόμενο σφάλματος κάτω από ένα ανεκτό επίπεδο

*ο κβαντικός υπολογιστής δεν είναι μια ντετερμινιστική μηχανή*

# καταστάσεις Bell (1)

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

$$|B_{10}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

$$|B_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

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

# καταστάσεις Bell (2)

αμοιβαία ορθογώνιες

*σύμπλεκτες καταστάσεις*

$$|0\rangle \equiv |\uparrow\rangle, |1\rangle \equiv |\downarrow\rangle$$

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

η κβαντική σύμπλεξη θα αποτελέσει συστατικό στοιχείο της λειτουργίας ενός κβαντικού υπολογιστή

# Χειρισμοί qubits

υποχρεωτικά μοναδιαίοι

ο καθιερωμένος όρος γι’ αυτές τις μοναδιαίες «πράξεις» είναι *κβαντικές πύλες*

Αρκεί ένας μικρός αριθμός πυλών που δρουν μόνο πάνω σε *ένα* $qubit$, σε συνδυασμό με *μία μόνο πύλη* που δρα σε *δύο* $qubits$

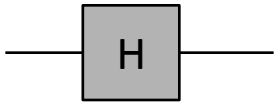
για να υλοποιηθεί μέσω αυτών (έστω προσεγγιστικά) κάθε δυνατός μοναδιαίος μετασχηματισμός επί του συνόλου των $qubits$ του καταχωρητή

# μονοψηψιακές πύλες

Μονάδα

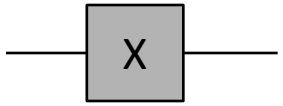

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Hadamard



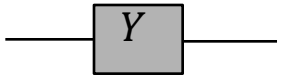

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Pauli X



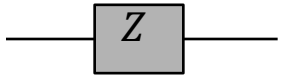

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Pauli Y



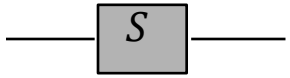

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Pauli Z




$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Φάση S




$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

# Πύλες δύο qubit

$$Controlled - NOT \equiv CNOT$$

$$CNOT|0\rangle|y\rangle = |0\rangle|y\rangle \qquad CNOT|1\rangle|y\rangle = |1\rangle|\bar{y}\rangle$$

Και με μορφή μήτρας

$$WCNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

# *πύλη Hadamard*

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

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

# *πύλη X*

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

# Θέση υπέρθεσης

$$X(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle$$

$$Y(\alpha|0\rangle + \beta|1\rangle) = -i\beta|0\rangle + i\alpha|1\rangle$$

$$Z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$$

$$S(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle + i\beta|1\rangle$$

# Hadamard

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

# $Controlled - U$

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 target $qubit$.

# Ο κβαντικός αντιγραφέας

θα επιθυμούσαμε να εκτελεί μια εργασία ανάλογη με την *αντιγραφή αρχείων* σε έναν κλασικό υπολογιστή

$$U|\psi\rangle|\varphi\rangle = |\psi\rangle|\psi\rangle$$

Όμως ισχύει

$$U(c_1|\psi_1\rangle + c_2|\psi_2\rangle)|\varphi\rangle = c_1(U|\psi_1\rangle|\varphi\rangle) + c_2(U|\psi_2\rangle|\varphi\rangle)$$

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

$$\neq (c_1|\psi_1\rangle + c_2|\psi_2\rangle)(c_1|\psi_1\rangle + c_2|\psi_2\rangle)$$

# Θεώρημα μη αντιγραφής

Αυτό που αποκλείει είναι η δημιουργία πανομοιότυπων αντιγράφων μιας *άγνωστης κβαντικής κατάστασης*

*κατασκευή* (μέσω μέτρησης) προαποφασισμένων κβαντικών καταστάσεων μπορούμε να υλοποιήσουμε

Το θεώρημα της μη αντιγραφής αναφέρεται λοιπόν σε γνήσια αντιγραφή μιας άγνωστης κβαντικής κατάστασης και όχι στην πολλαπλή δημιουργία μιας γνωστής.

# Θεώρημα μη αντιγραφής

αν πράγματι μπορούσαμε να βγάλουμε όσα αντίγραφα θέλουμε μιας άγνωστης κβαντικής κατάστασης, τότε θα είχαμε τη δυνατότητα – να μάθουμε ό,τι θέλουμε για την κατάσταση αυτή διατηρώντας άθικτο το «πρωτότυπο»

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*

# BQP (1)

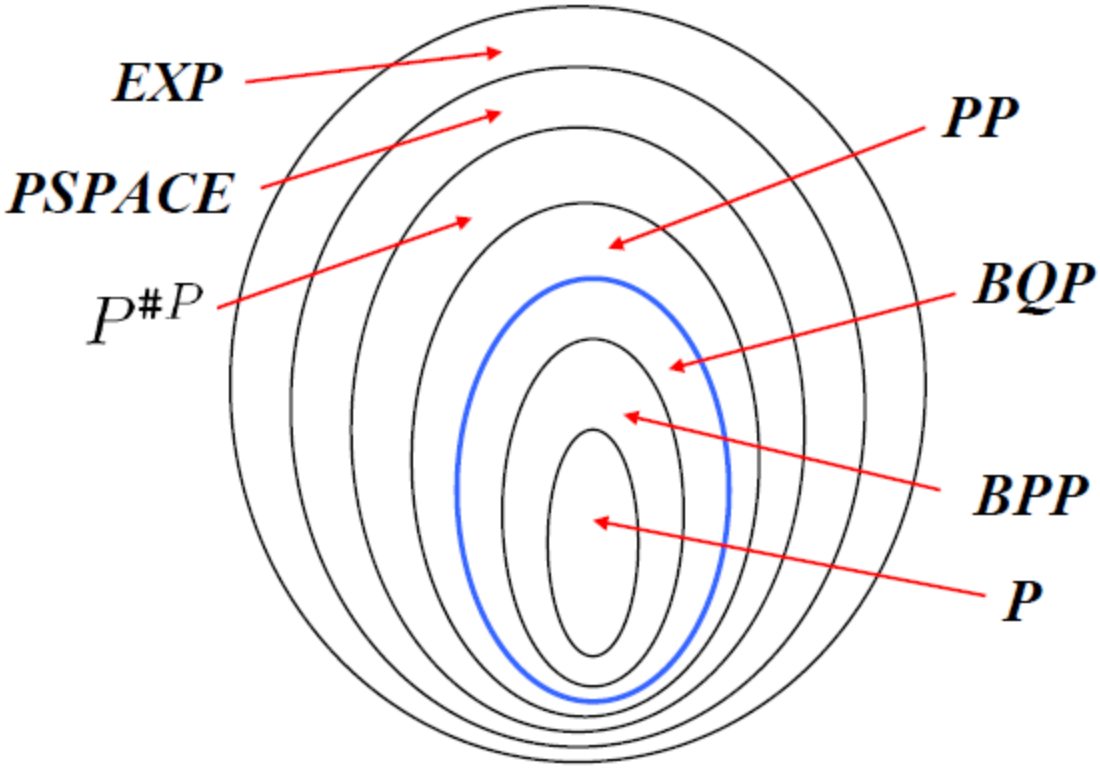
L ∈ $\boldsymbol{BQP}$ ⇔ ∃ ομοιόμορφη οικογένεια πολυωνυμικών κβαντικών κυκλωμάτων $\{Q_n : n \in \mathbb{N}\}$, τέτοια ώστε:

$n \in \mathbb{N}$: $n$ *qubits* ως είσοδος, 1 *qubit* ως έξοδος.

$$x \in L: \Pr\left(Q_{|x|}(x) = 1\right) \geq \frac{2}{3}$$

$$x \notin L: \Pr\left(Q_{|x|}(x) = 0\right) \geq \frac{2}{3}$$

# BQP (2)



# BQP relations

$\boldsymbol{P \subseteq BQP}$

$\boldsymbol{BPP \subseteq BQP}$: (Η πύλη Hadamard με $|0\rangle$ δίνει τυχαιότητα)

$\boldsymbol{BQP \subseteq EXP}$

$\boldsymbol{BQP \subseteq PSPACE}$: (Feynmann's path integral)

$\boldsymbol{BQP \subseteq P^{\#P} \subseteq PSPACE}$: (#$\boldsymbol{P}$ μπορεί να τρέξει όλα τα πιθανά μονοπάτια μη ντετερμινιστικά στο Feynmann's path integral)

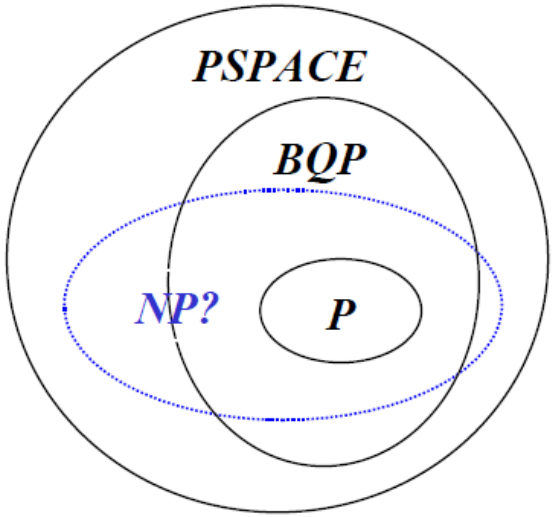
# Open problems

Ο κβαντικός υπολογιστής υπερέχει του κλασσικού?

Αυτό θα σήμαινε $\boldsymbol{P \neq PSPACE}$.

$\boldsymbol{NP}$ ?

Υποθέτουμε ότι $\boldsymbol{NP \subsetneq BQP}$, και δεν γνωρίζουμε όμως τίποτα για το αν $\boldsymbol{BQP \subsetneq NP}$.



# $BQP^{BQP} = BQP$?

Input $|0\rangle \longrightarrow |work(0)\rangle|output(0)\rangle$

Input $|1\rangle \longrightarrow |work(1)\rangle|output(1)\rangle$

... όμως ...

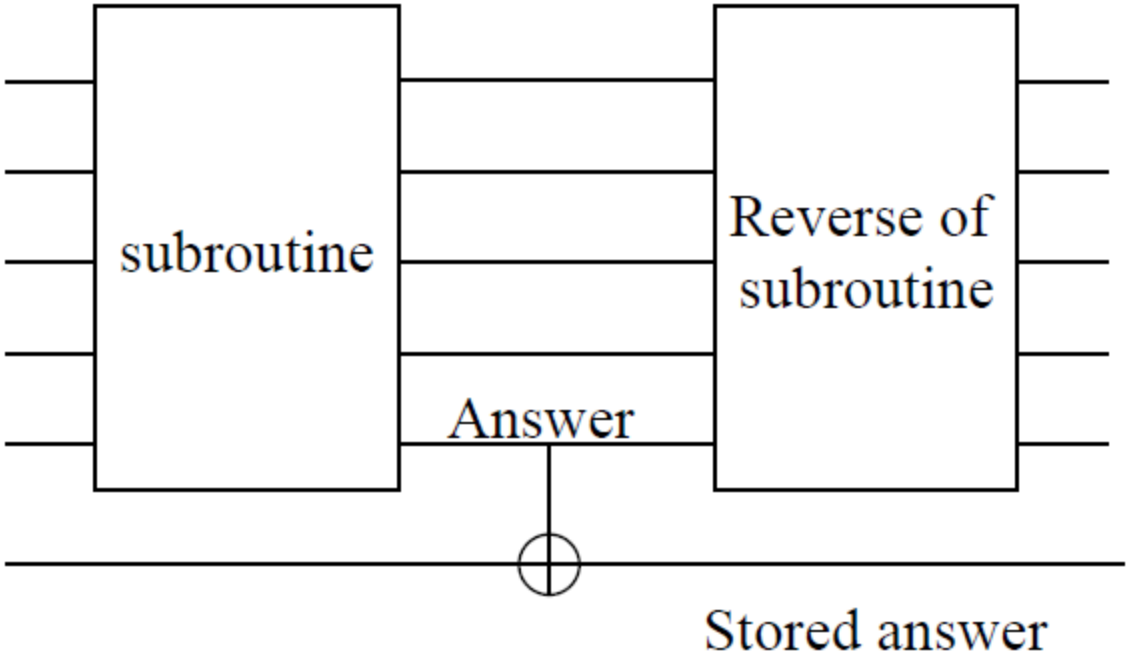
Input $|0\rangle+|1\rangle \longrightarrow$

$$|work(0)\rangle|output(0)\rangle + |work(1)\rangle|output(1)\rangle$$

Σύμπλεξη work space και output space!!!

# Uncomputing

Αφού ρωτήσω το oracle εφαρμόζω $CNOT$ gate στην απάντηση και τρέχω αντίστροφα την υπορουτίνα για να σβήσω τα πάντα εκτός από την απάντηση.



# With the power of uncomputing…

Μειώνουμε το λάθος εκθετικά και…

$$BQP^{BQP} = BQP$$

# QMA

$L \in \boldsymbol{QMA}$, αν υπάρχει ένα κβαντικό πολυωνυμικό κύκλωμα A, τέτοιο ώστε:

$$x \in L: \exists\ witness\ state\ |\varphi\rangle: \Pr\left(\mathrm{A}(x, |\varphi\rangle) = 1\right) \geq \frac{2}{3}$$

$$x \in L: \forall\ witness\ state\ |\varphi\rangle: \Pr\left(\mathrm{A}(x, |\varphi\rangle) = 1\right) \leq \frac{1}{3}$$

# Amplifying QMA

Πολλά πειράματα → πολλά πιστοποιητικά.

Λόγω του θεωρήματος μη αντιγραφής, θα πρέπει ο Merlin να κατασκευάσει πολλά πιστοποιητικά.

Μπορούμε να τον εμπιστευτούμε όμως?

- Πολλά αλλά διαφορετικά πιστοποιητικά → αυτό με την μεγαλύτερη πιθανότητα αποδοχής.
- Σύμπλεξη με random qubits → Προσθέτει στην πιθανότητα αποδοχής → αυτό με την μεγαλύτερη πιθανότητα αποδοχής.
- Σύμπλεξη μεταξύ των πιστοποιητικών → αυτό με την μεγαλύτερη πιθανότητα αποδοχής, χωρίς σύμπλεξη.

Αποτέλεσμα: Μπορούμε να τον εμπιστευτούμε.

# Group Membership

Ορισμός: Δεδομένου συνόλου $G$, υποσυνόλου του $H$ ( σαν λίστα γεννητόρων ) και στοιχείου $x \in G, x \in H$ ;

Λίστα γεννητόρων → πάντα πολυωνυμικού μεγέθους (όταν τα σύνολα είναι το πολύ εκθετικού μεγέθους).

ΝΑΙ: Εύκολο να δείξουμε ότι είναι στο **NP**.

ΟΧΙ: Θα δείξουμε ότι ανήκει στην **QMA**.

# GMP ∈ QMA(1)

Ο Merlin στέλνει στον Arthur την κατάσταση:

$$|H\rangle = \frac{1}{\sqrt{|\mathrm{H}|}} \sum_{h \in H} |h\rangle$$

Σημείωση: Δεν θα μπορούσε να την κατασκευάσει μόνος του γιατί χρησιμοποιώντας τυχαιότητα και όχι κβαντική κατάσταση θα είχε το εξής αποτέλεσμα:

$$|H\rangle = \frac{1}{\sqrt{|\mathrm{H}|}} \sum_{h \in H} |h\rangle\, |garbage_h\rangle$$

# GMP ∈ QMA(2)

Ο Arthur υπολογίζει την κατάσταση:

$$|Hx\rangle = \frac{1}{\sqrt{|\mathrm{H}|}} \sum_{h \in H} |hx\rangle$$

Μετά κατασκευάζεται η κατάσταση $|0\rangle|H\rangle + |1\rangle|Hx\rangle$.

Τελικά ο Arthur εφαρμόζει πύλη Hadamard στο πρώτο qubit και μετράει.

# $GMP \in QMA(3)$

Αν, $x \in H$: $|H\rangle = |Hx\rangle$. Οπότε η κατάσταση γίνεται:

$$|0\rangle|H\rangle + |1\rangle|H\rangle = (|0\rangle + |1\rangle)\,|H\rangle$$

Και με την πύλη Hadamard στο πρώτο qubit πάντα θα παράγεται η κατάσταση $|0\rangle$.

Αν, $x \notin H$: οι $|H\rangle, |Hx\rangle$ θα είναι ορθογώνιες μεταξύ τους.

Άρα, μετά την πύλη Hadamard, η μέτρηση θα μου δώσει $|1\rangle$ με πιθανότητα $\frac{1}{2}$.

# If Merlin cheats…

Ο Arthur υπολογίζει ένα τυχαίο στοιχείο $y$, είτε του $H$, είτε του $G$. Έστω $H'$ αυτό που μας έστειλε ο Merlin. Τότε υπολογίζουμε

$$|0\rangle|H'\rangle + |1\rangle|H'y\rangle.$$

Αν τα παραπάνω tests επιτύχουν, τότε η $|H'\rangle$ είναι είτε ίση με την $|H\rangle$, είτε συμπεριφέρεται με τον ίδιο τρόπο, για τον σκοπό που την χρησιμοποιούμε.

Αν εφαρμόσουμε την τεχνική για amplifying probability, θα έχουμε και αρκετά αντίγραφα για να τρέξουμε τα tests.

# QMA-complete problem

K-local Hamiltonians:

Δοθέντος 2-outcome μετρήσεων $E_1, \dots, E_M$ σε το πολύ $k$ qubits, υπάρχει $n$-qubit $|\varphi\rangle$ έτσι ώστε,

$$\sum_{i=1}^{M} \Pr[E_i(|\varphi\rangle)\ accepts] \geq b$$

Δεδομένου ότι το άθροισμα θα είναι πάντα $\geq b$ ή $\leq a$, όπου

$$b - a = \Omega\left(\frac{1}{poly(n)}\right)?$$


That's all Folks!