Υπολογισιμότητα και Πολυπλοκότητα
Computability and Complexity

Διδάσκων: Στάθης Ζάχος
Επιμέλεια Διαφανειών: Μάκης Αρσένης
CoReLab

ΣΗΜΜΥ - Ε.Μ.Π.

Ιούνιος 2017

Περιεχόμενα

1 Υπολογισιμότητα

2 Αυτόματα και Τυπικές Γλώσσες

3 Πολυπλοκότητα

- Πολυπλοκότητα Αναζήτησης
- Παραμετρική Πολυπλοκότητα
- Κβαντική Πολυπλοκότητα

Πολυπλοκότητα Αναζήτησης Ι

Ορισμός

FNP είναι η κλάση των **μερικών πλειότιμων** (partial multi-valued) συναρτήσεων που υπολογίζονται από μία μη-ντετερμινιστική μηχανή Turing πολυωνυμικού χρόνου, τέτοια ώστε το δέντρο υπολογισμού, για είσοδο x, έχει στα φύλλα είτε ? είτε το πιστοποιητικό y του μονοπατιού που ικανοποιεί το αντίστοιχο κατηγόρημα $R(x, y)$.

Το μη-ντετερμινιστικό μοντέλο, όμως, δημιουργεί προβλήματα στον ορισμό κλάσεων συναρτήσεων, λόγω του ότι για μία δεδομένη είσοδο $x \in \Sigma^*$ δεν υπάρχει μοναδική συμβολοσειρά εξόδου. Η προσπάθεια να αντιμετωπιστεί αυτό το ζήτημα, οδήγησε στον ορισμό των ακόλουθων κλάσεων:

- **NPMV**: *Η κλάση των μερικών πλειότιμων συναρτήσεων που υπολογίζονται από μία μη-ντετερμινιστική μηχανή Turing πολυωνυμικού χρόνου, τέτοια ώστε το δέντρο υπολογισμού, για είσοδο x, έχει στα φύλλα είτε ? είτε κάποια από τα δυνατές απαντήσεις της μηχανής Turing.*
- **NPSV**: *Η κλάση που περιλαμβάνει μονότιμες* **NPMV** *συναρτήσεις.*

Πολυπλοκότητα Αναζήτησης II

Όλες οι κλάσεις που θα δούμε στην συνέχεια του κεφαλαίου είναι υποσύνολα της κλάσης **TFNP**, όπου το "T" δηλώνει ότι οι συναρτήσεις αυτές είναι **ολικές** (total), δηλαδή πάντα υπάρχει τουλάχιστον μία λύση. Η ύπαρξη λύσης για κάθε τέτοια κλάση οφείλεται σε *υπαρξιακές* αποδείξεις κάποιων ιδιοτήτων (συνήθως γραφοθεωρητικών).

Ορισμός

Ένα πρόβλημα αναζήτησης Π αποτελείται από ένα σύνολο **στιγμιοτύπων** (instances), και κάθε στιγμιότυπο I έχει ένα σύνολο $Sol(I)$ **λύσεων**. Δεδομένου ενός στιγμιοτύπου, ζητείται ο υπολογισμός μιας λύσης. Ένα πρόβλημα αναζήτησης είναι *ολικό* αν $Sol(I) \neq \varnothing$, για κάθε στιμιότυπο I.

Προβλήματα Τοπικής Αναζήτησης Ι

Ορισμός

Ένα πρόβλημα Π ανήκει στην κλάση **PLS** (Polynomial Local Search) αν οι λύσεις είναι πολυωνυμικά φραγμένες ως προς το μήκος της εισόδου, και υπάρχουν αλγόριθμοι πολυωνυμικού χρόνου για τα επόμενα:

1. Δοθείσης συμβολοσειράς I, έλεγξε αν το I είναι στιγμιότυπο του Π, και αν ναι υπολόγισε μια αρχική λύση που να ανήκει στο $Sol(I)$.
2. Δοθέντων I, s, έλεγξε αν $s \in Sol(I)$, και αν ναι, υπολόγισε το κόστος της λύσης $c_I(s)$.
3. Δοθέντων I, s, έλεγξε αν η s αποτελεί *τοπικά* βέλτιστη λύση, και αν όχι, βρες μία "καλύτερη" λύση $s' \in N_I(s)$, όπου $N_I(s)$ οι γείτονες της λύσης s για το στιγμιότυπο I.

Κάθε πρόβλημα στην **PLS** δέχεται έναν αλγόριθμο τοπικής αναζήτησης: Χρησιμοποιούμε τον πρώτο αλγόριθμο για να αποκτήσουμε μια αρχική λύση, και μετά επαναληπτικά εφαρμόζουμε τον τρίτο αλγόριθμο μέχρι να φτάσουμε σε μία τοπικά βέλτιστη λύση. Δεδομένου ότι οι εφικτές λύσεις είναι εκθετικά πολλές, η παραπάνω διαδικασία δεν ολοκληρώνεται απαραίτητα σε πολυωνυμικό χρόνο.

Προβλήματα Τοπικής Αναζήτησης II

Παράδειγμα

- Έστω το πρόβλημα MAXCUT, όπου μας δίνεται ένας μη κατευθυνόμενος γράφος $G(V, E)$ και ένα βάρος $w_e \geqslant 0$ για κάθε ακμή. Οι εφικτές λύσεις αντιστοιχούν σε διαμερίσεις $(S, \overline{S})$ του συνόλου των κορυφών, και η αντικειμενική συνάρτηση στην μεγιστοποίηση του συνολικού βάρους των ακμών που ανήκουν στην διαμέριση.
- Δύο λύσεις είναι γειτονικές αν μπορούμε να μεταβούμε από την μία στην άλλη μεταφέροντας μία κορυφή από την διαμέριση στο συμλήρωμά της.
- Ξεκινάμε από μία αυθαίρετη διαμέριση $(S, \overline{S})$, και όσο υπάρχει καλύτερη γειτονική λύση, μεταβαίνουμε σε αυτήν.
- Ο αλγόριθμος τερματίζεται όταν δεν υπάρχει καλύτερη γειτονική λύση, δηλαδή όταν έχουμε φτάσει σε μία τοπικά βέλτιστη λύση.

Παρατηρήστε ότι το πλήθος τον εφικτών λύσεων του MAXCUT είναι εκθετικό ως προς το μήκος της εισόδου.

Προβλήματα Τοπικής Αναζήτησης III

Η δομή του προβλήματος επάγει έναν γράφο G, όπου οι κορυφές είναι οι εφικτές λύσεις, και δύο κορυφές συνδέονται με ακμή αν μπορούμε να μεταβούμε από την μία στην άλλη με μία απλή αλλαγή.

Παρατηρούμε ότι κάθε πρόβλημα στην κλάση **PLS** ανήκει στην κλάση **TFNP**, λόγω του γεγονότος ότι κάθε κατευθυνόμενος ακυκλικός γράφος (DAG) έχει μία καταβόθρα (sink), ή εναλλακτικά, ότι κάθε πεπερασμένο σύνολο αριθμών έχει ελαχιστικό στοιχείο.

Ορισμός

Μία αναγωγή από ένα πρόβλημα αναζήτησης Π_1 σε ένα πρόβλημα Π_2 αποτελείται από δύο αλγορίθμους πολυωνυμικού χρόνου:

1. Ένας αλγόριθμος A που απεικονίζει στιγμιότυπα $x \in \Pi_1$ σε στιγμιότυπα $A(x) \in \Pi_2$.
2. Ένας αλγόριθμος B που απεικονίζει λύσεις y του Π_2 με είσοδο $A(x)$ σε λύσεις $B(y)$ του Π_1 με είσοδο x.

Στην περίπτωση της **PLS**, οι λύσεις που απεικονίζονται από τον B είναι τα τοπικά βέλτιστα.

Προβλήματα Τοπικής Αναζήτησης IV

Τα επόμενα προβλήματα είναι **PLS**-πλήρη:

- MAXCUT
- TSP
- MAXSAT
- PURE NASH EQUILIBRIUM σε παίγνια συμφόρησης.

Αναζήτηση Ισορροπιών Nash I

- Έστω (S, f) ένα παίγνιο n *παικτών*, όπου S_i το σύνολο των *στρατηγικών* του παίκτη i, $S = S_1 \times S_2 \times \cdots \times S_n$ το σύνολο των *στρατηγικών προφίλ* των παικτών, και $f(x) = (f_1(x), \ldots, f_n(x))$ η *συνάρτηση κέρδους* υπολογισμένη στο $x \in S$.
- Έστω x_i το προφίλ στρατηγικής του παίκτη i και x_{-i} τα προφίλ στρατηγικής όλων των υπολοίπων παικτών εκτός του i.
- Δεδομένου ότι κάθε παίκτης $i \in \{1, \ldots, n\}$ επιλέγει την στρατηγική x_i, το προφίλ των στρατηγικών που επιλέγονται περιγράφεται από το διάνυσμα $x = (x_1, \ldots, x_n)$ και το κέρδος κάθε παίκτη υπολογίζεται από τη συνάρτηση κέρδους $f_i(x)$.

Αναζήτηση Ισορροπιών Nash II

Ορισμός (Ισορροπία Nash)

Ένα στρατηγικό προφίλ $x^* \in S$ αποτελεί ισορροπία Nash, εάν κανένας παίκτης δεν μπορεί να βελτιώσει το κέρδος του αλλάζοντας μονομερώς την στρατηγική του. Με άλλα λόγια:

$$\forall i, x_i \in S_i : f_i(x_i^*, x_{-i}^*) \geqslant f_i(x_i, x_{-i}^*)$$

Σημειώνουμε ότι στην περίπτωση όπου η παραπάνω ανισότητα ισχύει γνησίως για όλους τους παίκτες και τις στρατηγικές, έχουμε τον ορισμό της *αυστηρής* Nash ισορροπίας. Αντίστοιχα, εάν κάποιος παίκτης μπορεί να αλλάξει την στρατηγική του διατηρώντας (αλλά όχι απαραίτητα αυξάνοντας) το κέρδος του, γίνεται λόγος για *ασθενή* Nash ισορροπία.

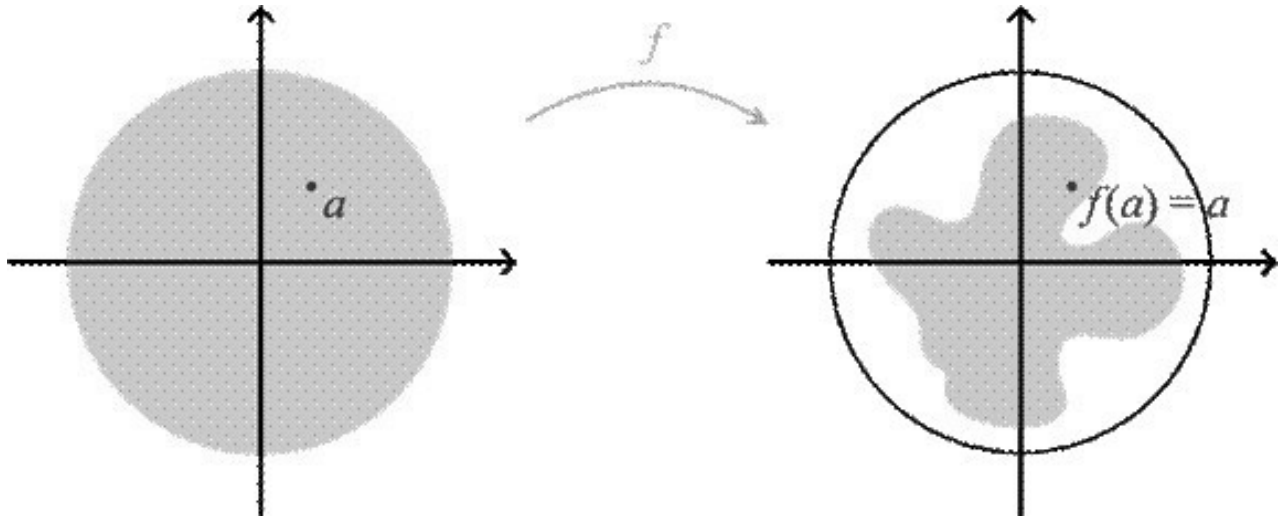
Αναζήτηση Ισορροπιών Nash III

Βασικό ρόλο στην απόδειξη του Nash για την ύπαρξη (μικτών) Nash ισορροπιών σε κάθε πεπερασμένο παίγνιο έπαιξε το παρακάτω τοπολογικό θεώρημα:

Ορισμός (Θεώρημα Σταθερού Σημείου του Brouwer)

Έστω $S \subset \mathcal{R}^n$ ένας κυρτός και συμπαγής (κλειστός και φραγμένος) χώρος. Για κάθε συνεχή συνάρτηση $f : S \to S$, υπάρχει ένα σημείο x_0 τέτοιο ώστε $f(x_0) = x_0$ (σταθερό σημείο).

Αναζήτηση Ισορροπιών Nash IV



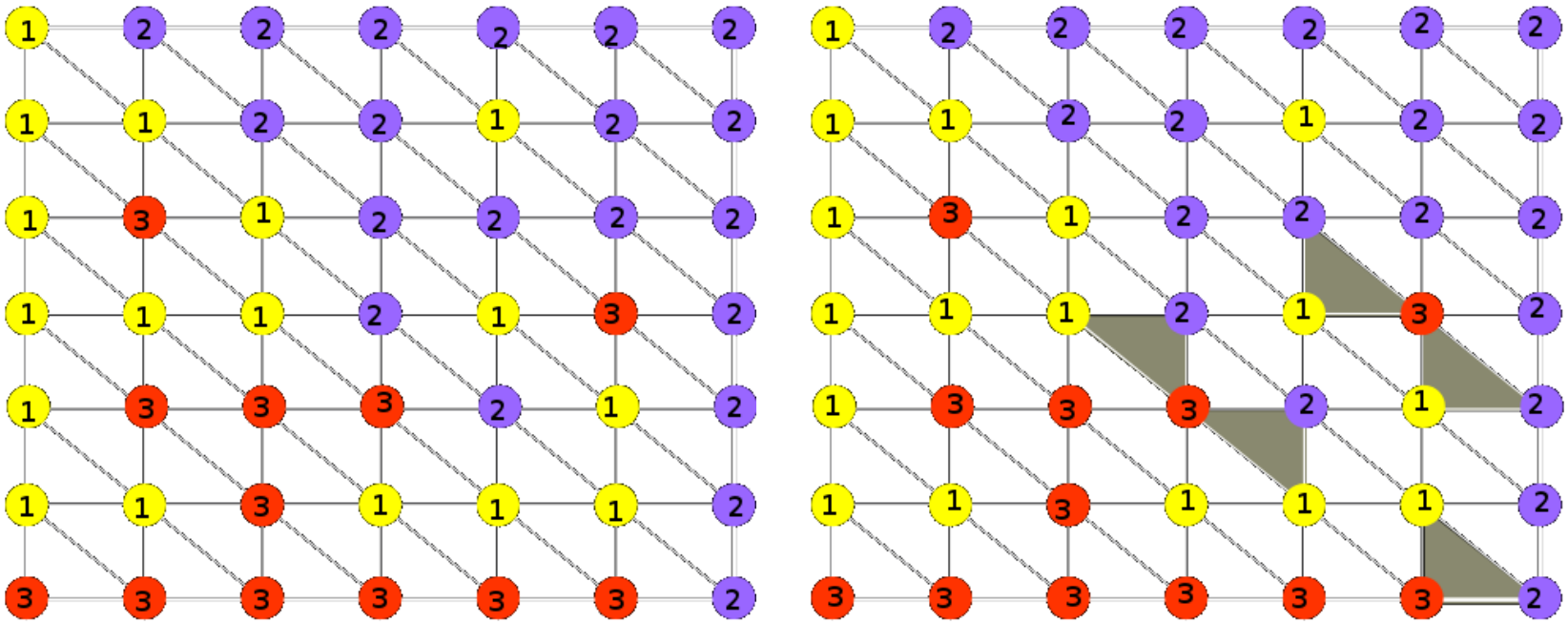
Σχήμα: Σχηματικό παράδειγμα του Θεωρήματος Σταθερού Σημείου.

Αναζήτηση Ισορροπιών Nash V

Η τελευταία έννοια με την οποία θα ασχοληθούμε είναι το *Λήμμα του Sperner*, το οποίο και αποτελεί το συνδυαστικό ανάλογο του παραπάνω Θεωρήματος Σταθερού Σημείου. Για λόγους απλότητας, θα παρουσιάσουμε μια απλοποιημένη εκδοχή του λήμματος στην περίπτωση των δύο διαστάσεων. Ας υποθέσουμε ότι έχουμε ένα ορθογώνιο ΑΒΓΔ και μια τριγωνοποίηση πάνω σε αυτό, όπως ακριβώς βλέπουμε στην επόμενη εικόνα. Επιπλέον, θεωρούμε ότι οι κορυφές που δημιουργούνται από την τριγωνοποίηση χρωματίζονται με *έγκυρο* τρόπο σύμφωνα με τους παρακάτω κανόνες:

1. Οι κορυφές που ακουμπούν στην πλευρά ΑΒ πρέπει να έχουν υποχρεωτικά χρώμα 1 (κίτρινο), στις πλευρές ΒΓ και ΓΔ χρώμα 2 (μπλε) και στην πλευρά ΔΑ χρώμα 3 (κόκκινο).
2. Οι κορυφές που δεν βρίσκονται στα σύνορα του ΑΒΓΔ μπορούν να λάβουν οποιοδήποτε χρώμα.

Αναζήτηση Ισορροπιών Nash VI



Σχήμα: Έγκυρος χρωματισμός σε τυχαία τριγωνοποίηση.

Αναζήτηση Ισορροπιών Nash VII

Λήμμα (2D-Sperner)

Σε κάθε τριγωνοποίηση με τον παραπάνω έγκυρο χρωματισμό υπάρχει κάποιο τρι-χρωματικό τρίγωνο (tri-chromatic triangle), δηλαδή, κάποιο τρίγωνο του οποίου κάθε κορυφή θα έχει χρωματιστεί με διαφορετικό χρώμα. Ισχύει, μάλιστα, ότι ο συνολικός αριθμός των τρι-χρωματικών τριγώνων είναι περιττός.

Απόδειξη:
Δεδομένου κάποιου έγκυρου χρωματισμού, μπορούμε πάντα να κατασκευάσουμε ένα ““τεχνητό”” τρι-χρωματικό τρίγωνο, εκτός του επιπέδου του ορθογωνίου, στην κάτω αριστερά πλευρά του. Ξεκινώντας από το τρίγωνο αυτό, θα ορίσουμε έναν περίπατο ανάμεσα στα τρίγωνα, ο οποίος, όπως θα δείξουμε, θα έχει κάποιο τρι-χρωματικό τρίγωνο σαν τελικό προορισμό. Έστω KL η ακμή του τεχνητού τριγώνου (αφετηρία) που αποτελεί είσοδο στην επιφάνεια ΑΒΓ, και έστω k και l τα χρώματα των δύο κορυφών που την ορίζουν, κίτρινο και κόκκινο αντίστοιχα. Ο κανόνας σύμφωνα με τον οποίο θα περιπλανηθούμε στα τρίγωνα είναι ο παρακάτω: *Οποτεδήποτε βρίσκουμε στο τρέχον τρίγωνο ακμή με χρωματισμό 1 και 3, τη διασχίζουμε, μόνο εάν το χρώμα 1 βρίσκεται στα αριστερά μας*. Μπορούμε εύκολα να επαληθεύσουμε ότι η μόνη περίπτωση όπου ο περίπατος σταματάει είναι όταν βρεθούμε σε τρι-χρωματικό τρίγωνο. Δεδομένου ότι ο

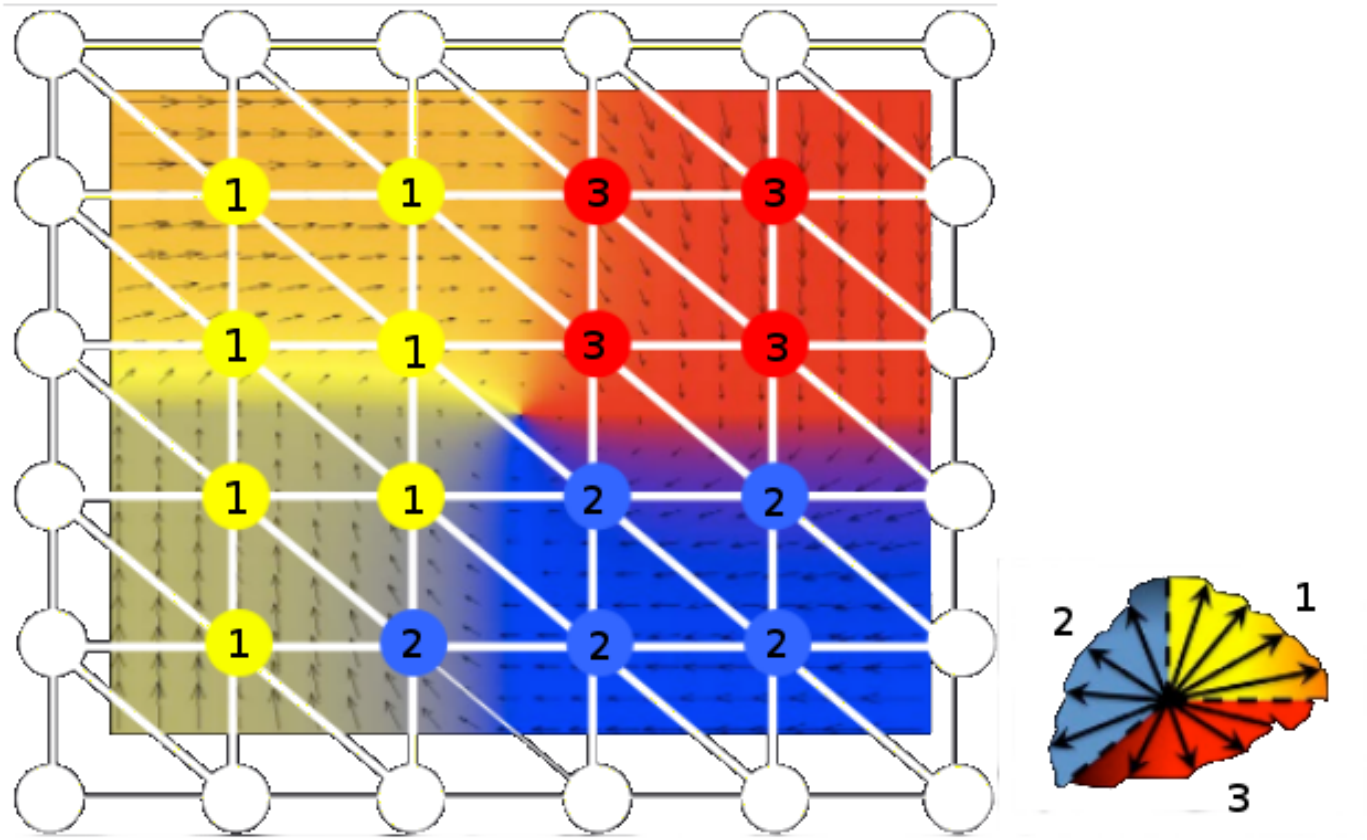
Αναζήτηση Ισορροπιών Nash VIII

αριθμός των τριγώνων είναι πεπερασμένος, ο περίπατός μας πρέπει υποχρεωτικά να σταματήσει, να βρει, δηλαδή, κάποιο τρι-χρωματικό τρίγωνο. Σε αντίθετη περίπτωση, ο περίπατος θα πρέπει να βρεθεί σε ατέρμονα βρόχο, γεγονός το οποίο, εξαιτίας του κανόνα που ορίσαμε, αποκλείεται να συμβεί. Άρα, έχοντας πλέον αποδείξει την ύπαρξη τρι-χρωματικών τριγώνων στο εσωτερικό του ΑΒΓΔ, μπορούμε με παρόμοιο τρόπο να δείξουμε ότι ο αριθμός τους είναι περιττός. Πιο συγκεκριμένα, ξεκινώντας από κάποιο τρι-χρωματικό τρίγωνο και ακολουθώντας τον αντίστροφο περίπατο από αυτόν που περιγράψαμε παραπάνω, μπορούμε να δείξουμε ότι θα βρεθούμε σε κάποιο άλλο τρι-χρωματικό τρίγωνο. Συμπεραίνουμε, λοιπόν, ότι τα τρι-χρωματικά τρίγωνα έρχονται σε ζευγάρια. Δεδομένου, όμως, ότι ένα από αυτά είναι τεχνητό, καταλήγουμε στο ότι ο αριθμός των τρι-χρωματικών τριγώνων είναι περιττός. □

Αναζήτηση Ισορροπιών Nash IX

Το Θεώρημα Σταθερού Σημείου του Brouwer μπορεί να αποδειχθεί μέσω της χρήσης του παραπάνω λήμματος. Πιο συγκεκριμένα, θεωρούμε μια ασθενή μορφή του Θεωρήματος Σταθερού Σημείου, δηλαδή, ότι υπάρχει σταθερό (με την ασθενή έννοια) σημείο x_0 για το οποίο $|f(x_0) - x_0| \leqslant \epsilon$, για $\epsilon > 0$. Στην περίπτωση αυτή, αν θεωρήσουμε μια κατάλληλη τριγωνοποίηση κατά Sperner πάνω στο χώρο που ορίζεται η f, απαιτήσουμε η διάμετρος των τριγώνων να είναι ϵ, και χρωματίσουμε τις κορυφές με τρία χρώματα ανάλογα με την κατεύθυνση που έχει η $f(x) - x$ στα σημεία αυτά, τότε μπορούμε (με αρκετή φαντασία) να δούμε ότι κάθε τρι-χρωματικό τρίγωνο αντιστοιχεί σε ένα ασθενές σταθερό σημείο. Τέλος, μπορούμε να περάσουμε από την ασθενή μορφή του Θεωρήματος Σταθερού Σημείου στην ισχυρή, χρησιμοποιώντας το γεγονός ότι ο χώρος είναι συμπαγής, και παίρνοντας το όριο του ϵ στο μηδέν. Παρακάτω, βλέπουμε ένα παράδειγμα εφαρμογής στις δύο διαστάσεις:

Αναζήτηση Ισορροπιών Nash X



Σχήμα: Η εύρεση του σταθερού σημείου μέσω του λήμματος Sperner στις δύο διαστάσεις

Αναζήτηση Ισορροπιών Nash XI

Ορισμός (NASH)

Δίνονται ως είσοδος ένας αριθμός παικτών n, τα σύνολα των στρατηγικών κάθε παίκτη, S_i, και η συνάρτηση κέρδους $f(x)$. Δίνεται επιπλέον, μια παράμετρος προσέγγισης $\epsilon > 0$. Το πρόβλημα NASH ή $\epsilon - \text{NASH}$ έγκειται στο να βρούμε μια ισορροπία, όπου κανένας παίκτης δεν θα μπορεί, αλλάζοντας μονομερώς την στρατηγική του, να βελτιώσει το κέρδος του περισσότερο απο ϵ.

Ορισμός (SPERNER)

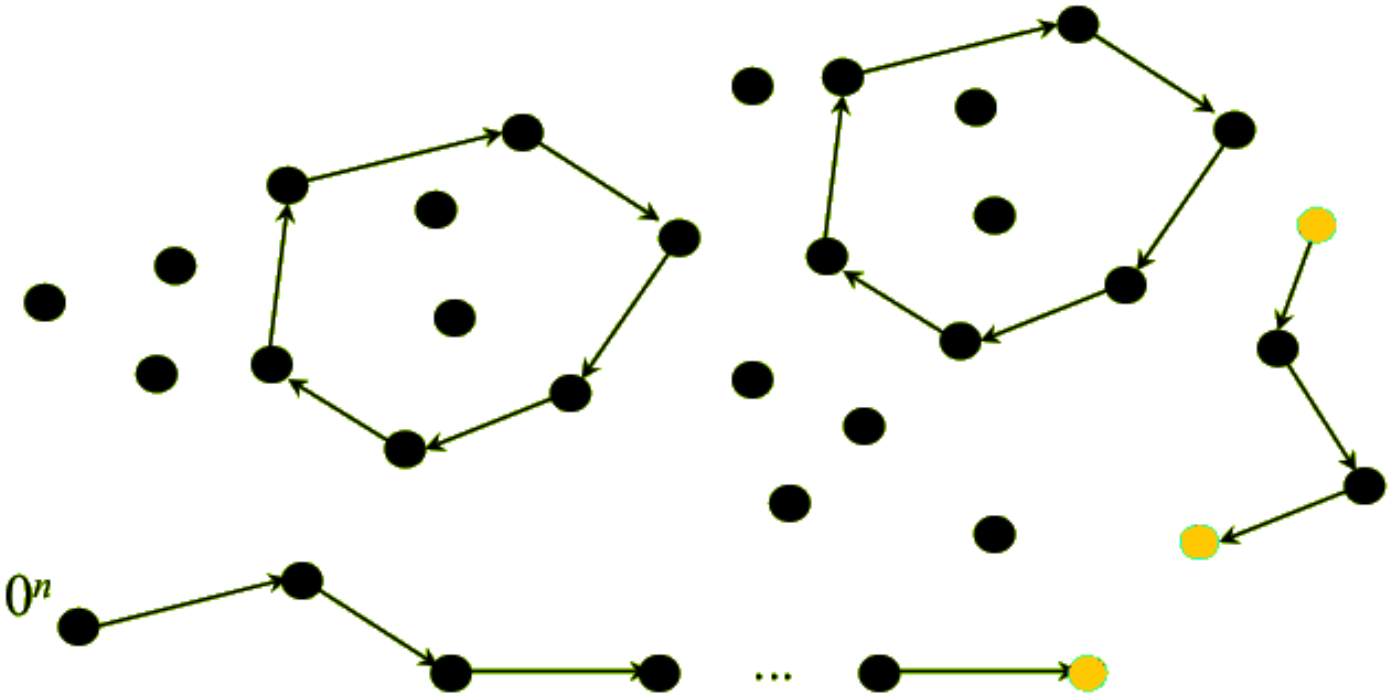
Έστω ότι μας δίνεται ως είσοδος ένα πλέγμα που αποτελείται από $2^n \times 2^n$ κορυφές και ότι οι κορυφές στα σύνορα του πλέγματος έχουν κάποιον κλασικό, έγκυρο χρωματισμό (όπως αυτόν που περιγράψαμε προηγουμένως). Το χρώμα κάθε κορυφής στο εσωτερικό του πλέγματος, θεωρούμε ότι δίνεται από κάποιο κύκλωμα C το οποίο, με είσοδο τις συντεταγμένες x και y μιας κορυφής, επιστρέφει κάποιο από τα τρία χρώματα. Το πρόβλημα SPERNER είναι να βρούμε και να επιστρέψουμε ένα τρι-χρωματικό τρίγωνο.

Αναζήτηση Ισορροπιών Nash XII

Από την προηγούμενη ανάλυση σχετικά με τη σχέση μεταξύ Nash, Θεωρήματος Σταθερού Σημείου και Sperner, μπορεί κάποιος να πεισθεί, έστω διαισθητικά, ότι το $\epsilon - \texttt{NASH}$ πρόβλημα μπορεί να αναχθεί στο αντίστοιχο $\epsilon - \texttt{BROUWER}$, και αυτό με τη σειρά του στο SPERNER. Οι τεχνικές στις οποίες βασίζονται οι αναγωγές θυμίζουν αρκετά τις τεχνικές που χρησιμοποιήθηκαν για την υπαρξιακή σύνδεση των εννοιών. Πιο συγκεκριμένα, μπορούμε να δούμε ότι το πρόβλημα NASH μπορεί λυθεί μέσω του $\epsilon - \texttt{BROUWER}$. Επιπλέον, τα (σχεδόν) σταθερά σημεία του $\epsilon - \texttt{BROUWER}$, μπορούν να βρεθούν μέσω της εύρεσης τρι-χρωματικών τριγώνων στο αντίστοιχο SPERNER πρόβλημα, εάν θεωρήσουμε πλέγμα κατάλληλου μεγέθους, ανάλογου με τον παράγοντα προσέγγισης ϵ.

Φθάνοντας ένα βήμα πλέον πριν τον ακριβή ορισμό της **PPAD** αξίζει να θυμηθούμε την απόδειξη ύπαρξης τρι-χρωματικών τριγώνων στο πλέγμα του Sperner. Σύμφωνα με τον κανόνα τον οποίο ορίσαμε για τον περίπατο μεταξύ των τριγώνων, θεωρούμε έναν βοηθητικό γράφο, στον οποίο και αντιστοιχούμε τα τρίγωνα με κόμβους και τη δυνατότητα μετάβασης από ένα τρίγωνο σε άλλο με ακμή. Ο γράφος που προκύπτει και που φανερώνει την πολυπλοκότητα του προβλήματος αναζήτησης θα αποτελείται από μεμονωμένους κόμβους, απλά μονοπάτια μεταξύ κόμβων και από κύκλους, όπως φαίνεται στο παρακάτω σχήμα:

Αναζήτηση Ισορροπιών Nash XIII



Σχήμα: Η μορφή του γράφου αναζήτησης του προβλήματος SPERNER.

Αναζήτηση Ισορροπιών Nash XIV

Ορισμός

Ένα πρόβλημα Π ανήκει στην κλάση **PPAD** αν οι λύσεις είναι πολυωνυμικά φραγμένες ως προς το μήκος της εισόδου, και υπάρχουν αλγόριθμοι πολυωνυμικού χρόνου για τα επόμενα:

1. Δοθείσης συμβολοσειράς I, έλεγξε αν το I είναι στιγμιότυπο του Π, και αν ναι υπολόγισε μια αρχική λύση $s_0 \in Sol(I)$.
2. Δοθέντων I, s, έλεγξε αν $s \in S(I)$, και αν ναι, επίστρεψε μία λύση $pred(s) \in Sol(I)$, τέτοια ώστε $pred(s_0) = s_0$.
3. Δοθέντων I, s, έλεγξε αν $s \in S(I)$, και αν ναι, επίστρεψε μία λύση $succ(s) \in Sol(I)$, τέτοια ώστε $succ(s_0) \neq s_0$ και $pred(succ(s_0)) = s_0$.

Αναζήτηση Ισορροπιών Nash XV

Όπως και στην περίπτωση της **PLS**, από τον ορισμό της **PPAD** επάγεται ένας κατευθυνόμενος γράφος $G(Sol(I), E)$, όπου οι κορυφές είναι οι εφικτές λύσεις, και $E = \{(u, v) : \ u \neq v, succ(u) = v, pred(v) = u\}$.

Η διαδικασία που περιγράφεται από τον ορισμό της κλάσης αφορά την εύρεση μίας λύσης s, εκτός της s_0, που να έχει $indegree(s) + outdegree(s) = 1$, ακολουθώντας το μονοπάτι στον G που έχει αρχή το s_0. Επειδή για το s_0 ισχύει ότι $indegree(s_0) + outdegree(s_0) = 1$, θα πρέπει να υπάρχει τουλάχιστον μία λύση $s \neq s_0$, λόγω του γνωστού λήμματος:

> *""Κάθε γράφος έχει άρτιο αριθμό κόμβων περιττού βαθμού.""*

Αναζήτηση Ισορροπιών Nash XVI

Παρατηρούμε στο σημείο αυτό, ότι η δομή του γράφου που επάγεται από τον ορισμό της **PPAD** και των συναρτήσεων $succ(u)$ και $pred(u)$ είναι ακριβώς ίδια με τη μορφή του γράφου αναζήτησης του προβλήματος SPERNER. Το γεγονός αυτό, κάθε άλλο παρά τυχαίο είναι, αφού πράγματι SPERNER $\in$ **PPAD**. Επιπλέον, λόγω της αλληλουχίας των αναγωγών που περιγράψαμε, ισχύει ότι BROUWER $\in$ **PPAD** και NASH $\in$ **PPAD**. Στην πρόσφατη εργασία του ""The Complexity of Computing a Nash Equilibrium", οι Daskalakis, Goldberg και Papadimitriou έδειξαν ότι το πρόβλημα NASH για τρεις παίκτες είναι **PPAD**-complete.

Τα επόμενα προβλήματα είναι **PPAD**-πλήρη:

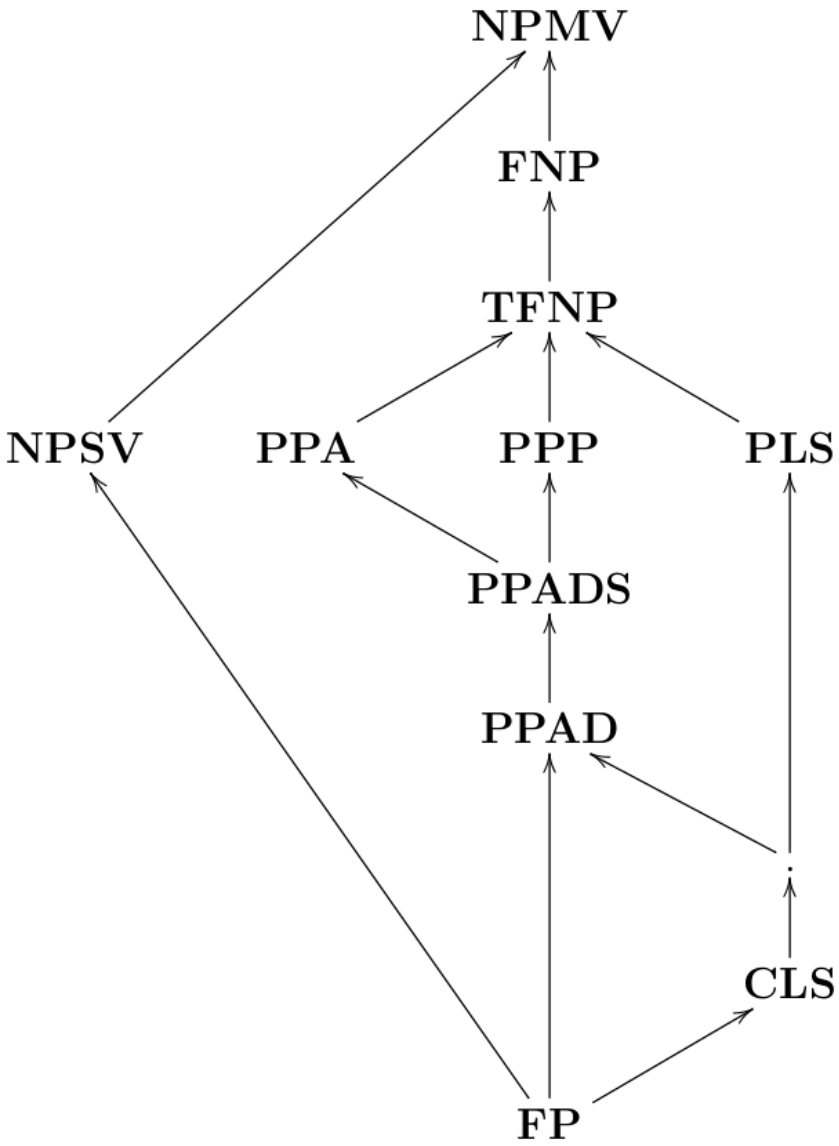
- END OF THE LINE
- SPERNER
- NASH

Άλλες κλάσεις I

Χρησιμοποιώντας διάφορα λήμματα μπορούμε να ορίσουμε και άλλες κλάσεις:

- **PPADS**: Παρόμοια με την **PPAD**, μόνο που σε αυτή την περίπτωση αναζητούμε μία καταβόθρα (sink), δηλαδή λύση με $indegree = 1$ και $outdegree = 0$.
- **PPA**: Το ανάλογο της **PPAD**, αλλά με μη κατευθυνόμενο γράφο (δεν υπάρχουν συναρτήσεις *succ* και *pred*, αλλά μία συνάρτηση γειτονίας).
- **PPP**: Σε αυτή την κλάση ορίζεται μία συνάρτηση f στο σύνολο των λύσεων: Στόχος μας είναι να βρούμε είτε μία λύση που απεικονίζεται στην αρχική λύση, είτε δύο λύσεις y και y', τέτοιες ώστε $f(x, y) = f(x, y')$. Τέτοιες λύσεις υπάρχουν πάντα λόγω της Αρχής του Περιστερεώνα (*Polynomial Pingeonhole Principle*).
- **CLS**: Το ανάλογο της **PLS** για συνεχείς χώρους και συναρτήσεις (Continuous Local Search). Η κλάση **CLS** περιέχει τα προβλήματα αναζήτησης προσεγγιστικού τοπικού βέλτιστου μιας συνεχούς συνάρτησης, με την βοήθεια ενός μαντείου f, όπου και η f είναι συνεχής συνάρτηση.

Άλλες κλάσεις II



Παραμετρική Πολυπλοκότητα Ι

Ορισμός

Μια *παραμετροποίηση* του Σ^* είναι μία *αναδρομική* συνάρτηση $k : \Sigma^* \to \mathbb{N}$. Ένα *παραμετρικό πρόβλημα* είναι ένα διατεταγμένο ζεύγος (L, k), όπου $L \subseteq \Sigma^*$ και k είναι μία παραμετροποίηση του Σ^*.
Ένας αλγόριθμος A είναι FPT-αλγόριθμος (Fixed Parameter Tractable) ως προς την παράμετρο k, αν υπάρχει *υπολογίσιμη* συνάρτηση f και πολυώνυμο p, τέτοια ώστε για κάθε $x \in \Sigma^*$, ο αλγόριθμος A να αποφασίζει το πρόβλημα σε χρόνο $O(f(k(x)) \cdot p(|x|))$.

Ορισμός

Ορίζουμε ως **FPT** την κλάση των παραμετρικών προβλημάτων που επιλύονται από έναν FPT-αλγόριθμο.

Παραμετρική Πολυπλοκότητα II

Το επόμενο βήμα, κατ' αναλογία με την κλασσική Θεωρία Πολυπλοκότητας, είναι να συνδέσουμε τα προβλήματα μέσω αναγωγών:

Ορισμός

Έστω (L, k), (L', k') παραμετρικά προβλήματα. Το (L, k) ανάγεται στο (L', k') μέσω FPT-αναγωγής (συμβ. $L \leqslant_{FPT} L'$) αν υπάρχει αλγόριθμος R τέτοιος ώστε:

1. Για κάθε $x \in \Sigma^*$, $x \in L \Leftrightarrow R(x) \in L'$
2. Η R υπολογίζεται από έναν FPT-αλγόριθμο.
3. $k' = g(k)$, όπου $g : \mathbb{N} \to \mathbb{N}$ υπολογίσιμη συνάρτηση.

Αν $\leqslant_{FPT}$ και $B \leqslant_{FPT} A$, τότε λέμε ότι τα A, B είναι FPT-ισοδύναμα (συμβ. $A \equiv_{FPT} B$).

Παράδειγμα

Έστω το πρόβλημα pSAT, όπου μας δίνεται μία προτασιακή φόρμουλα ϕ, και μία παράμετρος k, που αναπαριστά τον αριθμό των μεταβλητών στην ϕ. Είναι η ϕ ικανοποιήσιμη?

Παραμετρική Πολυπλοκότητα III

Θα επιχειρήσουμε να ορίσουμε το παραμετρικό ανάλογο της κλάσης **NP**:

Ορισμός

Έστω (L, k) παραμετρικό πρόβλημα. Το (L, k) ανήκει στην κλάση **paraNP** αν υπάρχει υπολογίσιμη συνάρτηση $f : \mathbb{N} \to \mathbb{N}$, πολυώνυμο p και *μη-ντετερμινιστικός* αλγόριθμος που για κάθε $x \in \Sigma^*$, αποφασίζει το πρόβλημα σε χρόνο $O(f(k(x)) \cdot p(|x|))$.

Λέμε ότι ένα παραμετρικό πρόβλημα είναι τετριμμένο, αν $L = \varnothing$ ή $L = \Sigma^*$, και ορίζουμε την i-οστή φέτα του προβλήματος (L, k) ως το πρόβλημα:

$$(L, k)_i = \{x \in L | k(x) = i\}$$

Ισχύει ο παρακάτω χαρακτηρισμός της κλάσης **paraNP**:

Θεώρημα

*Έστω $(L, k) \in$ **paraNP** ένα μη-τετριμμένο παραμετρικό πρόβλημα. Τότε η ένωση πεπερασμένων φετών του (L, k) είναι **NP**-complete αν το (L, k) είναι **paraNP**-complete.*

Παραμετρική Πολυπλοκότητα IV

Θα ορίσουμε και το παραμετρικό ανάλογο της κλάσης **EXP**:

Ορισμός

Έστω (L, k) παραμετρικό πρόβλημα. Το (L, k) ανήκει στην κλάση **XP** αν υπάρχει υπολογίσιμη συνάρτηση f, και αλγόριθμος τέτοιος ώστε για κάθε $x \in \Sigma^*$, αποφασίζει το πρόβλημα σε χρόνο $O(|x|^{f(k(x))})$.

Ισχύει ότι $\mathbf{FPT} \subset \mathbf{XP}$, ενώ είναι άγνωστη η σχέση της **paraNP** με την **XP**.

Ορισμός

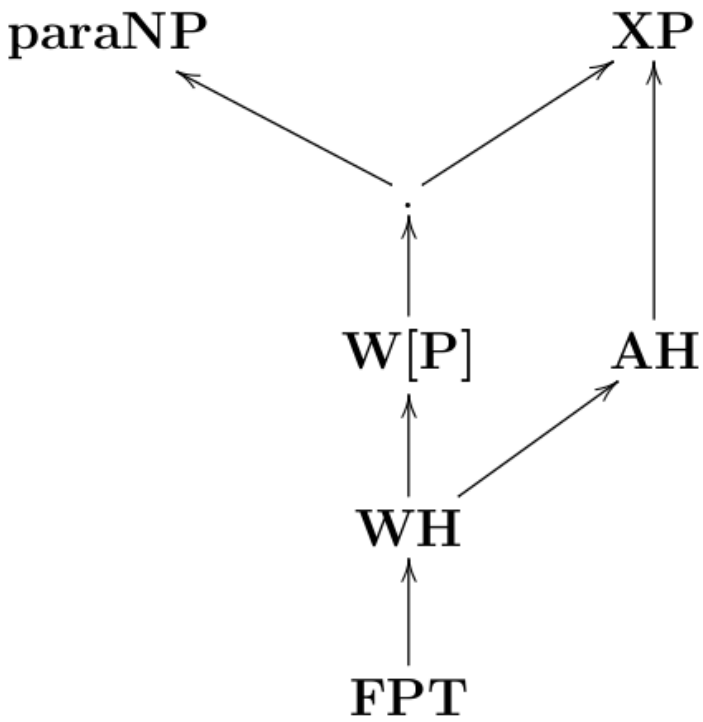
Μία μη-ντετερμινιστική μηχανή Turing καλείται *k-περιορισμένη* αν υπάρχει υπολογίσιμη συνάρτηση $g : \mathbb{N} \to \mathbb{N}$ και ένα πολυώνυμο p τέτοια ώστε η M να χρειάζεται $f(k(x)) \cdot p(|x|)$ υπολογιστικά βήματα, και το πολύ $g(k(x)) \cdot \log |x|$ να είναι μη-ντετερμινιστικά.

Ορισμός

Ορίζουμε την κλάση $\mathbf{W}[\mathbf{P}]$ να περιέχει όλα τα παραμετρικά προβλήματα (L, k) που αποφασίζονται από k-περιορισμένες μηχανές Turing.

Παραμετρική Πολυπλοκότητα V

Τα περισσότερα **NP**-complete προβλήματα παραμετροποιημένα ώστε να *μην* ανήκουν στο **FPT**, ανήκουν στο **W**[**P**].
Ισχύει η σχέση εγκλεισμού: **FPT** $\subseteq$ **W**[**P**] $\subseteq$ **XP** $\cap$ **paraNP**.



Κβαντική Πολυπλοκότητα — Υπολογιστικά Μοντέλα I

Το πιο ευρέως χρησιμοποιούμενο μοντέλο για την μαθηματική περιγραφή κβαντικών υπολογιστών και κβαντικών αλγορίθμων είναι το **κβαντικό κύκλωμα**, και συγκεκριμένα οι οικογένειες **ομοιόμορφων** (με την έννοια ότι υπάρχει κλασσικός αλγόριθμος πολυωνυμικού χρόνου, που εμφανίζει την περιγραφή τους) κβαντικών κυκλωμάτων. Αυτά τα κυκλώματα μοιάζουν αρκετά με τα λογικά κυκλώματα, τα οποία υλοποιούν Boolean συναρτήσεις (θυμίζουμε ότι κάθε Boolean συνάρτηση μπορεί να υπολογιστεί από κάποιο λογικό κύκλωμα που χρησιμοποιεί μονο τις λογικές πύλες not και and).

Οι πύλες που συνθέτουν ένα κβαντικό κύκλωμα μπορούν να κατασκευαστούν ως συνδυασμοί των κβαντικών πυλών cnot,H,T.

Κβαντική Πολυπλοκότητα — Υπολογιστικά Μοντέλα II

Οι πύλες αυτές είναι γραμμικοί ορθομοναδιαίοι (unitary) μετασχηματισμοί: Ένας γραμμικός μετασχηματισμός T, επί ενός μιγαδικού διανυσματικού χώρου, είναι ορθομοναδιαίος (unitary) αν $T^{-1} = T^*$, δηλαδή αν ο αντίστροφός του ισούται με τον αναστροφοσυζυγή (adjoint ή conjugate transpose) του. Οι ορθομοναδιαίοι μετασχηματισμοί διατηρούν την Ευκλείδεια Νόρμα, δηλαδή είναι ισομετρίες.

$$\text{cnot} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

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

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i \cdot \frac{\pi}{4}} \end{pmatrix},$$

με $i^2 = -1$.

Κβαντική Πολυπλοκότητα — Υπολογιστικά Μοντέλα III

- Οι είσοδοι και οι έξοδοι των κβαντικών αλγορίθμων είναι διανύσματα.
- Κάθε λογικό κύκλωμα μετατρέπεται σε κβαντικό κύκλωμα: τα δεύτερα αποτελούν γενίκευση των πρώτων.
- Εκτός από το κβαντικό κύκλωμα έχουν προταθεί άλλα μοντέλα όπως οι κβαντικές Μηχανές Turing.
- 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.
- Ως προς την Υπολογισιμότητα, οι συμβατικοί υπολογιστές είναι ισοδύναμοι με τους κβαντικούς (Church-Turing). Όμως, έχουμε σημαντικές ενδείξεις ότι οι κβαντικοί υπολογιστές είναι πολύ πιο αποδοτικοί από τους συμβατικούς.

Κλάσεις Κβαντικής Πολυπλοκότητας Ι

- Οι πρώτες κλάσεις που θα ορίσουμε είναι κβαντικά ανάλογα κλασσικών κλάσεων: η **BQP** αντιστοιχεί στην **BPP** $\supseteq$ **P**, και η **QMA** στην **MA** $\supseteq$ **NP**.
- Η κύρια διαφορά των κβαντικών καταστάσεων από τις κλασσικές είναι η εξής: για να περιγράψουμε μια κβαντική κατάσταση χρειαζόμαστε εκθετικά μεγάλη, ως προς το μέγεθος του κβαντικού συστήματος που περιγράφει, κλασσική πληροφορία, ενώ για να περιγράψουμε μια κλασσική κατάσταση απαιτείται γραμμικά μεγάλη, ως προς το μέγεθος της κλασσικής κατάστασης που περιγράφει, κλασσική πληροφορία. Δηλαδή, μια κβαντική κατάσταση αποτελεί υπέρθεση κλασσικών καταστάσεων. Για παράδειγμα, μια κβαντική κατάσταση μεγέθους n απαιτεί 2^n μιγαδικούς αριθμούς για να περιγραφεί, ενώ μια κλασσική κατάσταση μεγέθους n απαιτεί μόλις n bits.

Κλάσεις Κβαντικής Πολυπλοκότητας II

Ορισμός (BQP)

Η γλώσσα $L \in \mathbf{BQP}$ αν υπάρχει μια οικογένεια *κβαντικών* κυκλωμάτων πολυωνυμικού χρόνου ως προς i $\{Q_i\}$, ώστε για κάθε $x \in \Sigma^*$:

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

Η κλάση **BQP** αντιπροσωπεύει τα προβλήματα που επιλύονται αποδοτικά με την χρήση κβαντικών υπολογιστών.

Κλάσεις Κβαντικής Πολυπλοκότητας III

Ορισμός (QMA)

Η γλώσσα $L \in \mathbf{QMA}$ αν υπάρχει μια οικογένεια *κβαντικών* κυκλωμάτων πολυωνυμικού χρόνου ως προς i $\{Q_i\}$, ώστε για κάθε $x \in \Sigma^*$:

- $x \in L \Rightarrow$ $\exists$ κβαντική κατάσταση K, μήκους πολυωνυμικού ως προς $|x|$: $Pr\left[\text{το } Q_{|x|} \text{ αποδέχεται το } (x, K)\right] \geqslant \frac{2}{3}$
- $x \notin L \Rightarrow$ $\forall$ κβαντική κατάσταση K, μήκους πολυωνυμικού ως προς $|x|$: $Pr\left[\text{το } Q_{|x|} \text{ αποδέχεται το } (x, K)\right] \leqslant \frac{1}{3}$

Η κλάση **QMA** αντιπροσωπεύει τα προβλήματα που *επαληθεύονται* αποδοτικά με την χρήση κβαντικών υπολογιστών. Ισχύει ότι $\mathbf{BQP} \subseteq \mathbf{QMA}$.

Κλάσεις Κβαντικής Πολυπλοκότητας IV

Ορισμός (QCMA)

Η γλώσσα $L \in \mathbf{QCMA}$ αν υπάρχει μια οικογένεια *κβαντικών* κυκλωμάτων πολυωνυμικού χρόνου ως προς i $\{Q_i\}$, ώστε για κάθε $x \in \Sigma^*$:

- $x \in L \Rightarrow$ $\exists$ κλασσική κατάσταση C, μήκους πολυωνυμικού ως προς $|x|$: $Pr\left[\text{το } Q_{|x|} \text{ αποδέχεται το } (x, C)\right] \geqslant \frac{2}{3}$
- $x \notin L \Rightarrow$ $\forall$ κλασσική κατάσταση C, μήκους πολυωνυμικού ως προς $|x|$: $Pr\left[\text{το } Q_{|x|} \text{ αποδέχεται το } (x, C)\right] \leqslant \frac{1}{3}$

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

Κλάσεις Κβαντικής Πολυπλοκότητας V

Ορισμός (QCMA_1)

Η γλώσσα $L \in \mathbf{QCMA}_1$ αν υπάρχει μια οικογένεια *κβαντικών* κυκλωμάτων πολυωνυμικού χρόνου ως προς i $\{Q_i\}$, ώστε για κάθε $x \in \Sigma^*$:

- $x \in L \Rightarrow$ $\exists$ κλασσική κατάσταση C, μήκους πολυωνυμικού ως προς $|x|$: $Pr\left[\text{το } Q_{|x|} \text{ αποδέχεται το } (x, C)\right] = 1$
- $x \notin L \Rightarrow$ $\forall$ κλασσική κατάσταση C, μήκους πολυωνυμικού ως προς $|x|$: $Pr\left[\text{το } Q_{|x|} \text{ αποδέχεται το } (x, C)\right] \leqslant \frac{1}{3}$

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

Κλάσεις Κβαντικής Πολυπλοκότητας VI

Ορισμός (PQP)

Η γλώσσα $L \in \mathbf{PQP}$ αν υπάρχει μια οικογένεια *κβαντικών* κυκλωμάτων πολυωνυμικού χρόνου ως προς i $\{Q_i\}$, ώστε για κάθε $x \in \Sigma^*$:

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

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

Ορισμός (QIP)

Η γλώσσα $L \in \mathbf{QIP}$ αν υπάρχει μια οικογένεια κβαντικών κυκλωμάτων-επαληθευτών πολυωνυμικού χρόνου ως προς i $\{V_i\}$, ώστε για κάθε $x \in \Sigma^*$:

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

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

Κλάσεις Κβαντικής Πολυπλοκότητας VII

Ορισμός (BQPSPACE)

Η γλώσσα $L \in \mathbf{BQPSPACE}$ αν υπάρχει μια κβαντική μηχανή Turing πολυωνυμικού χώρου M, ώστε για κάθε $x \in \Sigma^*$:

- $x \in L \Rightarrow Pr[\text{η } M \text{ αποδέχεται το } x] \geqslant \frac{2}{3}$
- $x \notin L \Rightarrow Pr[\text{η } M \text{ αποδέχεται το } x] \leqslant \frac{1}{3}$

Ορισμός (PQPSPACE)

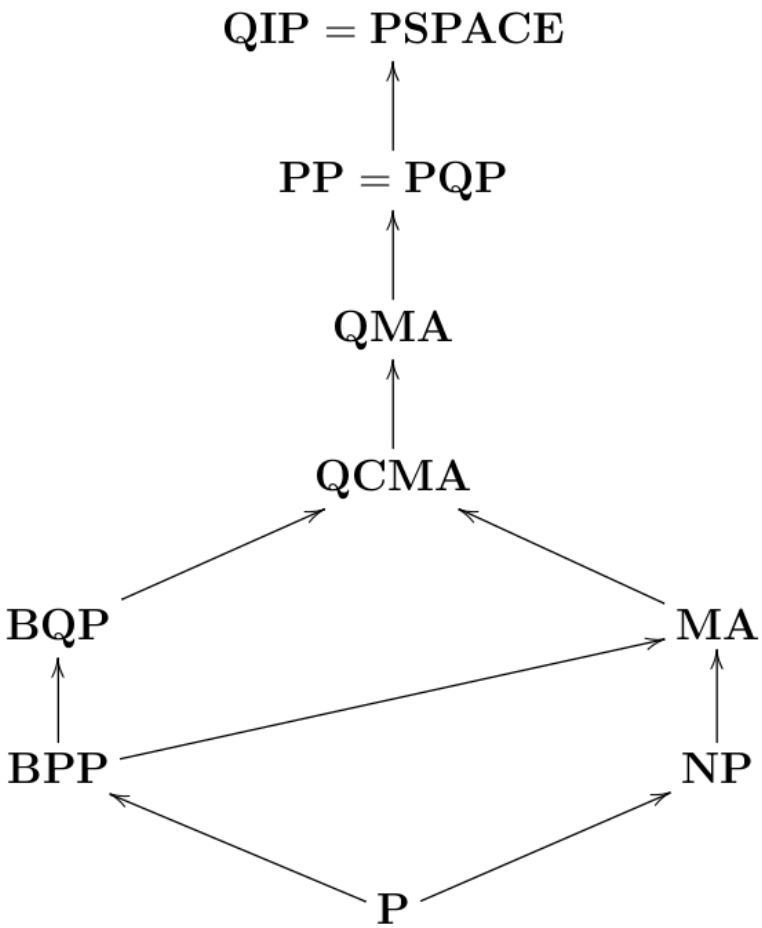
Η γλώσσα $L \in \mathbf{PQPSPACE}$ αν υπάρχει μια κβαντική μηχανή Turing πολυωνυμικού χώρου M, ώστε για κάθε $x \in \Sigma^*$:

- $x \in L \Rightarrow Pr[\text{η } M \text{ αποδέχεται το } x] > \frac{1}{2}$
- $x \notin L \Rightarrow Pr[\text{η } M \text{ αποδέχεται το } x] \leqslant \frac{1}{2}$

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

Κλάσεις Κβαντικής Πολυπλοκότητας VIII

Οι σχέσεις εγκλεισμού φαίνεται στο παρακάτω διάγραμμα:



Κβαντική Πολυπλοκότητα — Θεμελιώδη Αποτελέσματα Ι

Θεώρημα

- $\mathbf{BQP}^{\mathbf{BQP}} = \mathbf{BQP}$
- *Υπάρχει μαντείο* A, *τέτοιο ώστε* $\mathbf{BQP}^A \nsubseteq \mathbf{BPP}^A$.
- *Υπάρχει μαντείο* A, *τέτοιο ώστε* $\mathbf{NP}^A \nsubseteq \mathbf{BQP}^A$.
- $\mathbf{QMA} \subseteq \mathbf{PP} = \mathbf{PQP}$
- $\mathbf{PSPACE} = \mathbf{QIP} = \mathbf{BQPSPACE} = \mathbf{PQPSPACE}$

Θεώρημα (Grover)

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

Κβαντική Πολυπλοκότητα — Θεμελιώδη Αποτελέσματα II

Ορισμός (FACTORING)

Είσοδος: Ένας φυσικός αριθμός n.
Έξοδος: Η παραγοντοποίηση του n σε γινόμενο δυνάμεων πρώτων αριθμών.

Ορισμός (DISCRETE LOGARITHM)

Είσοδος: Δύο στοιχεία a, b μιας ομάδας $(G, \cdot)$. Υπενθυμίζουμε ότι $a^0 = e$, όπου e το ουδέτερο στοιχείο της $(G, \cdot)$, και $a^m = a^{m-1}a$, $\forall m \in \mathbb{N}^{\geq 1}$.
Έξοδος: Ένας φυσικός αριθμός c τέτοιος ώστε $a^c = b$, αν αυτός υπάρχει, αλλιώς κάποια ένδειξη ότι ο c δεν υπάρχει.

Θεώρημα

FACTORING $\in$ **BQP**, *DISCRETE LOGARITHM* $\in$ **BQP** *(για τα αντίστοιχα προβλήματα απόφασης).*

Και για τα δύο προβλήματα, είναι γνωστό ότι είναι στο **NP**, αλλά άγνωστο αν είναι στο **P**.

Κβαντική Πολυπλοκότητα — Θεμελιώδη Αποτελέσματα III

Ορισμός (GROUP NON-MEMBERSHIP)

Είσοδος: Μια υποομάδα $(H, \cdot)$ μιας ομάδας $(G, \cdot)$, και ένα στοιχείο $g \in G$ (η υποομάδα H είναι γνωστή μέσω των γεννητόρων της).
Ερώτηση: Ισχύει ότι $g \notin H$?

Θεώρημα

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

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

Ανάλογα, το πρόβλημα 2-LOCAL HAMILTONIAN είναι **QMA**-complete. Υπάρχουν αρκετά άλλα προβλήματα που επίσης έχουν χαρακτηριστεί **QMA**-complete.

Κβαντική Πολυπλοκότητα — Ανοικτά Προβλήματα Ι

- $\mathbf{NP} \overset{?}{\subseteq} \mathbf{BQP}$, $\mathbf{BQP} \overset{?}{\subseteq} \mathbf{NP}$.
- $\mathbf{QMA} \overset{?}{\subseteq} \mathbf{QCMA}$. Υπάρχει μαντείο A, ώστε $\mathbf{QMA}^A \not\subseteq \mathbf{QCMA}^A$?
- $\mathbf{BQP} \overset{?}{\subseteq} \mathbf{BPP}$, $\mathbf{BQP} \overset{?}{\subseteq} \mathbf{P}$.
- $\mathbf{BQP} \overset{?}{\subseteq} \mathbf{PH}$. Θυμίζουμε ότι $\mathbf{BPP} \subseteq \mathbf{PH}$. Υπάρχει μαντείο A, ώστε $\mathbf{BQP}^A \not\subseteq \mathbf{PH}^A$?
- Υπάρχουν #**P**-complete προβλήματα κβαντικής φύσης?
- GRAPH ISOMORPHISM $\overset{?}{\in}$ **BQP**? Θυμίζουμε ότι GRAPH ISOMORPHISM $\in$ **NP**, αλλά δεν γνωρίζουμε αν GRAPH ISOMORPHISM $\in$ **P**.
- GRAPH NON-ISOMORPHISM $\overset{?}{\in}$ **QMA**? Γνωρίζουμε ότι GRAPH ISOMORPHISM $\in$ *co***NP** $\cap$ **AM**.