Μαθημα Πρωτο

'Αρης Παγουρτζης, Βασιλης Νακος ΑΛΜΑ

Τι είναι η Λεπτομερής Πολυπλοκότητα;

Θεωρία NP-πληρότητας διαχωρίζει τα προβλήματα σε εύκολα (επιλύσιμα σε πολυωνυμικό χρόνο) και δύσκολα (μη επιλύσιμα σε πολυωνυμικό χρόνο).

Τι είναι η Λεπτομερής Πολυπλοκότητα;

Θεωρία NP-πληρότητας διαχωρίζει τα προβλήματα σε εύκολα (επιλύσιμα σε πολυωνυμικό χρόνο) και δύσκολα (μη επιλύσιμα σε πολυωνυμικό χρόνο).

Ωστόσο, δε μπορεί να απαντήσει σε ερωτήματα της μορφής: Δύναται το πρόβλημα της μέγιστης κοινής υπακολουθίας να επιλυθεί σε αυστηρά υποτετραγωνικό ($n^{2-\delta}$) χρόνο;

Τι είναι η Λεπτομερής Πολυπλοκότητα;

Θεωρία NP-πληρότητας διαχωρίζει τα προβλήματα σε εύκολα (επιλύσιμα σε πολυωνυμικό χρόνο) και δύσκολα (μη επιλύσιμα σε πολυωνυμικό χρόνο).

Ωστόσο, δε μπορεί να απαντήσει σε ερωτήματα της μορφής: Δύναται το πρόβλημα της μέγιστης κοινής υπακολουθίας να επιλυθεί σε αυστηρά υποτετραγωνικό ($n^{2-\delta}$) χρόνο;

Κατασκευή μίας θεωρίας που καλύπτει τα προαναφερθέντα υπολογιστικά κενά: Θεωρία Λεπτομερούς Πολυπλοκότητας.

Αρχικές Υποθέσεις

Ξεκινάμε από αρχικές υποθέσεις *δυσκολίας* προβλημάτων, και δείχνουμε δυσκολία άλλων προβλημάτων.

Αρχικές Υποθέσεις

Ξεκινάμε από αρχικές υποθέσεις *δυσκολίας* προβλημάτων, και δείχνουμε δυσκολία άλλων προβλημάτων.

- Πρόβλημα Συντομότερων Μονοπατιών (APSP).
  Δίνεται ένας γράφος με n κορυφές και βάρη στις ακμές. Να βρεθεί το μήκους του συντομότερου μονοπατιού μεταξύ οποιονδήποτε δύο κόμβων.

Αρχικές Υποθέσεις

Ξεκινάμε από αρχικές υποθέσεις *δυσκολίας* προβλημάτων, και δείχνουμε δυσκολία άλλων προβλημάτων.

- Πρόβλημα Συντομότερων Μονοπατιών (APSP).
  Δίνεται ένας γράφος με n κορυφές και βάρη στις ακμές. Να βρεθεί το μήκους του συντομότερου μονοπατιού μεταξύ οποιονδήποτε δύο κόμβων.
  Υπόθεση. Δεν υπάρχει αλγόριθμος χρόνου $n^{3-\epsilon}$, για $\epsilon > 0$.

Αρχικές Υποθέσεις

- Πρόβλημα 3SUM.
  Δίνονται σύνολο A θετικών ακεραίων. Να βρεθεί αν υπάρχουν διακεκριμένοι αριθμοί $a_1, a_2, a_3 \in A$ ώστε $a_1 + a_2 + a_3 = 0$.

Αρχικές Υποθέσεις

- Πρόβλημα 3SUM.
  Δίνονται σύνολο A θετικών ακεραίων. Να βρεθεί αν υπάρχουν διακεκριμένοι αριθμοί $a_1, a_2, a_3 \in A$ ώστε $a_1 + a_2 + a_3 = 0$.
  Υπόθεση. Δεν υπάρχει αλγόριθμος χρόνου $n^{2-\epsilon}$, για $\epsilon > 0$.

Αρχικές Υποθέσεις

- Πρόβλημα CNF-SAT.
  Δίνεται μία φόρμουλα Μπουλ ϕ σε κανονική μορφή (conjuctive normal form), με *N* μεταβλητές, *M* clauses. Υπάρχει αποτίμηση τιμών αληθείας στις μεταβλητές που κάνουν την ϕ αληθή;

Αρχικές Υποθέσεις

- Πρόβλημα CNF-SAT.
  Δίνεται μία φόρμουλα Μπουλ ϕ σε κανονική μορφή (conjuctive normal form), με N μεταβλητές, M clauses. Υπάρχει αποτίμηση τιμών αληθείας στις μεταβλητές που κάνουν την ϕ αληθή;
  Υπόθεση. Για κάθε $k \geq 3$ υπάρχει $\epsilon > 0$ έτσι ώστε να μην υπάρχει αλγόριθμος χρόνου $2^{(1-\epsilon)\cdot n} \cdot \mathrm{poly}(\log M)$.

Αρχικές Υποθέσεις

- Πρόβλημα Ορθογώνιων Διανυσμάτων.
  Δίνονται δύο συλλογές διανυσμάτων $A, B \subseteq \{0,1\}^d$, με $|A| = |B| = n$.
  Υπάρχουν δύο διανύματα $(a, b) \in A \times B$ με εσωτερικό γινόμενο 0;

Αρχικές Υποθέσεις

- Πρόβλημα Ορθογώνιων Διανυσμάτων.
  Δίνονται δύο συλλογές διανυσμάτων $A, B \subseteq \{0,1\}^d$, με $|A| = |B| = n$.
  Υπάρχουν δύο διανύματα $(a, b) \in A \times B$ με εσωτερικό γινόμενο 0;
  Υπόθεση. Δεν υπάρχει αλγόριθμος χρόνου $n^{2-\epsilon}$, για $\epsilon > 0$.

Είδη Αναγωγών

Έστω προβλήματα Π_1, Π_2. Θα δούμε δύο ειδών αναγωγές:

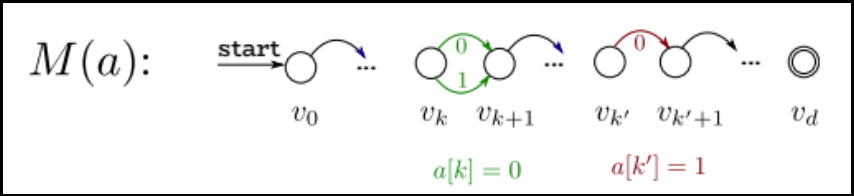
1. Π_1 αναγέται με έναν αλγόριθμο χρόνου $r(n)$ σε ένα στιγμιότυπο μεγέθους $s(n)$ του προβλήματος Π_2. Αυτό δίνει έναν αλγόριθμο $r(n) + T_2(s(n))$ για το Π_1, όπου T_2 ο χρόνος να λύσει το Π_2.
2. Π_1 αναγέται με έναν αλγόριθμο χρόνου $r(n)$ σε k στιγμιότυπα μεγέθους $s_1(n), s_2(n), \ldots, s_k(n)$ του Π_2. Αυτό δίνει έναν αλγόριθμο $r(n) + T_2(s_1(n)) + \ldots + T_2(s_k(n))$ για το Π_1.

Η πρώτη μας αναγωγή

- Πρόβλημα Αποδοχής Μη Ντετερμινιστικού Αυτόματου (NFA). Δίνεται ένα NFA με M καταστάσεις, και μια συμβολοσειρά x. Αποφανθείτε αν το εν λόγω NFA αποδέχεται ή όχι την x. **Αλγόριθμος**. Με δυναμικό προγραμματισμό, ή (αναζήτηση κατά βάθος) σε χρόνο $O(M \cdot |x|)$. Έστω $S[i]$ το σύνολο των καταστάσεων στις οποίες βρίσκεται το NFA μετά από i βήματα.

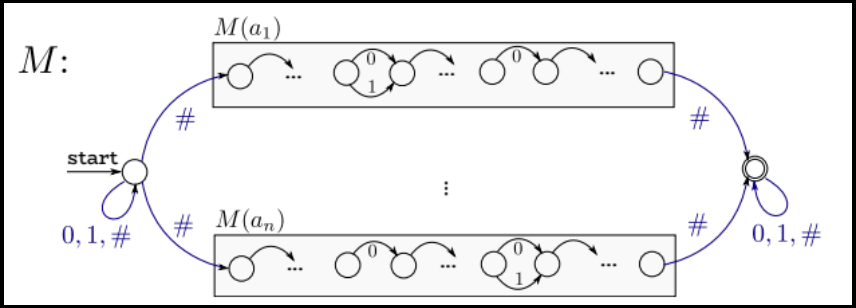
Θεώρημα: Αν υπάρχει αλγόριθμος χρόνου $(M \cdot |x|)^{1-\epsilon}$ για το Πρόβλημα Αποδοχής Μη Ντετερμινιστικού Αυτόματου, τότε η Υπόθεση των Ορθογώνιων Διανυσμάτων καταρρέει.

Για κάθε $a \in \{0,1\}^d$ φτιάχνουμε το NFA $\mathcal{M}_a$ ως εξής.

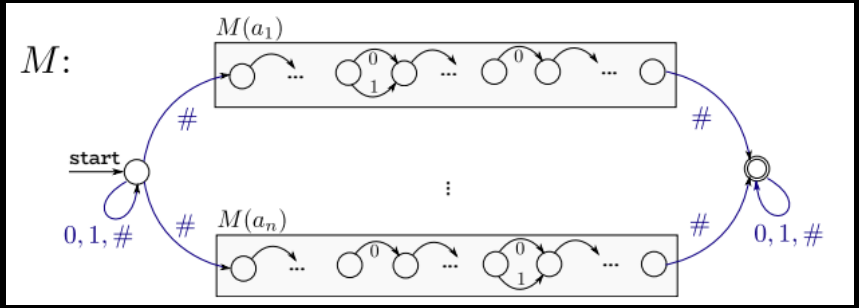


Ισχυρισμός: Για κάθε $b \in \{0,1\}^d$, το $\mathcal{M}_a$ αποδέχεται το το b αν και μόνο αν τα a, b είναι ορθογώνια.

Φτιάχνουμε το $\mathcal{M}$ ως ¨λογικό Ή¨ όλων των $\mathcal{M}_a$, για $a \in A$.



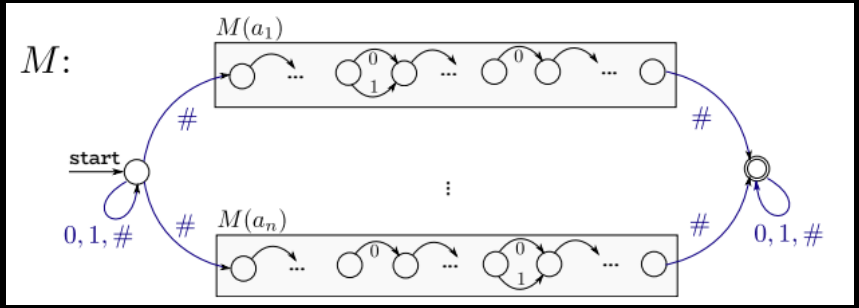
Φτιάχνουμε το $\mathcal{M}$ ως ¨λογικό Ή¨ όλων των $\mathcal{M}_a$, για $a \in A$.



Φτιάχνουμε τη συμβολοσειρά

$$x = \#b_1[1] \dots b_1[d]\#b_2[1] \dots b_2[d]\# \dots \# \dots \#b_n[1] \dots b_n[d]$$

Φτιάχνουμε το $\mathcal{M}$ ως ¨λογικό Ή¨ όλων των $\mathcal{M}_a$, για $a \in A$.



Φτιάχνουμε τη συμβολοσειρά

$$x = \#b_1[1] \dots b_1[d] \# b_2[1] \dots b_2[d] \# \dots \# \dots \# b_n[1] \dots b_n[d]$$

$\mathcal{M}$ αποδέχεται την x αν και μόνο αν υπάρχουν δύο ορθογώνια διανύσματα.

- Πρόβλημα 3-SAT.
  Δίνεται μία φόρμουλα Μπουλ ϕ σε κανονική μορφή (conjuctive normal form), με *N* μεταβλητές, *M* clauses. Υπάρχει αποτίμηση τιμών αληθείας στις μεταβλητές που κάνουν την ϕ αληθή;

- Πρόβλημα 3-SAT.
  Δίνεται μία φόρμουλα Μπουλ ϕ σε κανονική μορφή (conjuctive normal form), με N μεταβλητές, M clauses. Υπάρχει αποτίμηση τιμών αληθείας στις μεταβλητές που κάνουν την ϕ αληθή;
  Υπόθεση. Υυπάρχει δ για το οποίο δεν υπάρχει αλγόριθμος χρόνου $2^{\delta \cdot n}$ για το 3-SAT.

$$\phi := (x_1 \vee x_2 \vee x_N) \wedge \ldots \wedge (x_4 \vee x_7 \vee x_9)$$

Κυρίαρχο σύνολο ενός γράφους $G = (V, E)$ είναι ένα σύνολο $S \subseteq V$, έτσι ώστε κάθε $u \in V$ είτε ανήκει στο S, είτε έχει έναν γείτονα στο S.

- Πρόβλημα Κυρίαρχου Συνόλου.
  Δίνεται ένας γράφος $G = (V, E)$ με n κορυφές, m ακμές, και ένας φυσικός αριθμός q.

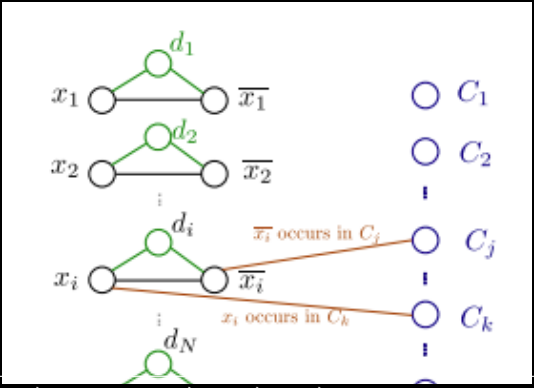
Κυρίαρχο σύνολο ενός γράφους $G = (V, E)$ είναι ένα σύνολο $S \subseteq V$, έτσι ώστε κάθε $u \in V$ είτε ανήκει στο S, είτε έχει έναν γείτονα στο S.

- Πρόβλημα Κυρίαρχου Συνόλου.
  Δίνεται ένας γράφος $G = (V, E)$ με n κορυφές, m ακμές, και ένας φυσικός αριθμός q.
  Ερώτηση: Υπάρχει κυρίαρχο σύνολο μεγέθους q ;

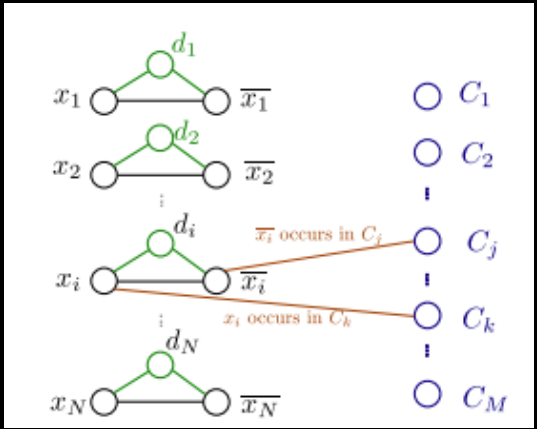
Θεώρημα: Το Πρόβλημα του Κυρίαρχου Συνόλου δεν μπορεί να λυθεί σε $2^{\delta \cdot n^{1/3}}$ χρόνο, εκτός αν η ETH καταρρέει.

Ξεκινάμε από την κλασική απόδειξη NP-πληρότητας του Προβλήματος Κυρίαρχου Συνόλου (αναγωγή από 3-SAT).

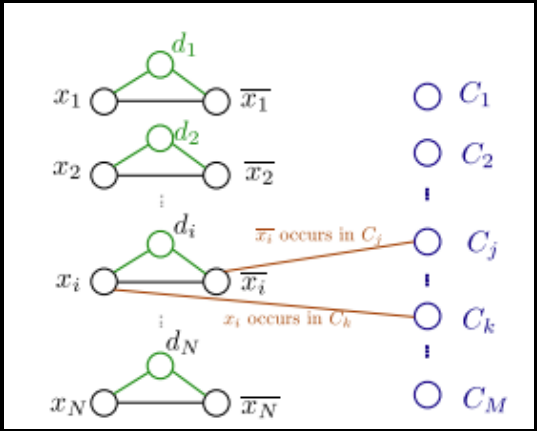
$\star$ ϕ με N μεταβλητές, M clauses $\underbrace{\rightarrow}_{O(N+M)}$ γράφος με $3N + M$ κόμβους



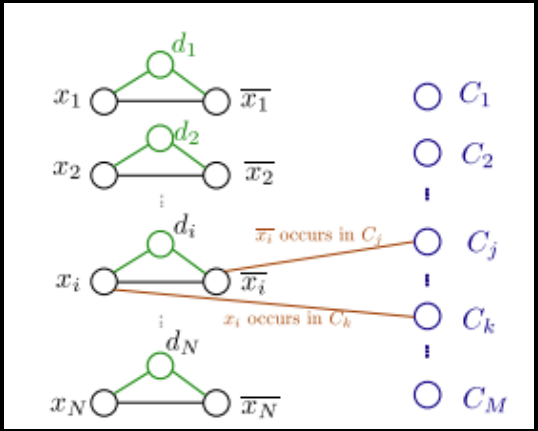
Ισχυρισμός: Ο κατασκευόμενος γράφος έχει κυρίαρχο σύνολο μεγέθους N αν και μόνο αν η φόρμουλα ϕ είναι ικανοποιήσιμη.



Πλήθος κόμβων $\leq N + \binom{N}{3} 2^3 = 9N^3$



Πλήθος κόμβων $\leq N + \binom{N}{3}2^3 = 9N^3$



$2^{\delta' n^{1/3}}$ αλγόριθμος για Κυρίαρχο Σύνολο δίνει
$2^{\delta(9N^3)^{1/3}} = 2^{\delta N}$ αλγόριθμο για 3-SAT

Πιο ισχυρά κάτω φράγματα

- $\star$ Το $2^{\delta n^{1/3}}$ στον εκθέτη προέκυψε λόγω του ότι το πλήθος των πιθανών clauses είναι κυβικό στο N.

Πιο ισχυρά κάτω φράγματα

- $\star$ Το $2^{\delta n^{1/3}}$ στον εκθέτη προέκυψε λόγω του ότι το πλήθος των πιθανών clauses είναι κυβικό στο N.
- $\star$ Σχεδιασμός πιο ¨σφιχτής¨ αναγωγής (οι σταθερές μετράνε!)

Πιο ισχυρά κάτω φράγματα

- $\star$ Το $2^{\delta n^{1/3}}$ στον εκθέτη προέκυψε λόγω του ότι το πλήθος των πιθανών clauses είναι κυβικό στο N.
- $\star$ Σχεδιασμός πιο ¨σφιχτής¨ αναγωγής (οι σταθερές μετράνε!)
- **Λήμμα Αραιοποίησης** (Impagliazzo, Paturi, Zane): Μπορούμε να μεταμορφώσουμε κάθε k-SAT στιγμιότυπο σε ένα *υποεκθετικό* πλήθος *αραιών* k-SAT στιγμιοτύπων.

Λήμμα Αραιοποίησης. Έστω θετικός ακέραιος $k \geq 3$ και $\epsilon > 0$. Τότε υπάρχει αριθμός $C := C(k, \epsilon)$ και αλγόριθμος $\mathcal{A}$ έτσι ώστε

Λήμμα Αραιοποίησης. Έστω θετικός ακέραιος $k \geq 3$ και $\epsilon > 0$. Τότε υπάρχει αριθμός $C := C(k, \epsilon)$ και αλγόριθμος $\mathcal{A}$ έτσι ώστε

- Δοσμένης μίας k-CNF φόρμουλα ϕ, ο $\mathcal{A}(\phi)$ επιστρέφει φόρμουλες $\phi_1, \ldots, \phi_t$ ώστε

$$\phi = \phi_1 \vee \phi_2 \vee \ldots \phi_t.$$

Λήμμα Αραιοποίησης. Έστω θετικός ακέραιος $k \geq 3$ και $\epsilon > 0$. Τότε υπάρχει αριθμός $C := C(k, \epsilon)$ και αλγόριθμος $\mathcal{A}$ έτσι ώστε

- Δοσμένης μίας k-CNF φόρμουλα ϕ, ο $\mathcal{A}(\phi)$ επιστρέφει φόρμουλες $\phi_1, \ldots, \phi_t$ ώστε
$$\phi = \phi_1 \vee \phi_2 \vee \ldots \phi_t.$$

- $t \leq 2^{\epsilon N}$.

Λήμμα Αραιοποίησης. Έστω θετικός ακέραιος $k \geq 3$ και $\epsilon > 0$. Τότε υπάρχει αριθμός $C := C(k, \epsilon)$ και αλγόριθμος $\mathcal{A}$ έτσι ώστε

- Δοσμένης μίας k-CNF φόρμουλα ϕ, ο $\mathcal{A}(\phi)$ επιστρέφει φόρμουλες $\phi_1, \ldots, \phi_t$ ώστε
$$\phi = \phi_1 \vee \phi_2 \vee \ldots \phi_t.$$

- $t \leq 2^{\epsilon N}$.
- Ο $\mathcal{A}$ τρέχει σε χρόνο $\tilde{O}(2^{\epsilon N})$.

Λήμμα Αραιοποίησης. Έστω θετικός ακέραιος $k \geq 3$ και $\epsilon > 0$. Τότε υπάρχει αριθμός $C := C(k, \epsilon)$ και αλγόριθμος $\mathcal{A}$ έτσι ώστε

- Δοσμένης μίας k-CNF φόρμουλα ϕ, ο $\mathcal{A}(\phi)$ επιστρέφει φόρμουλες $\phi_1, \ldots, \phi_t$ ώστε
$$\phi = \phi_1 \vee \phi_2 \vee \ldots \phi_t.$$

- $t \leq 2^{\epsilon N}$.
- Ο $\mathcal{A}$ τρέχει σε χρόνο $\tilde{O}(2^{\epsilon N})$.
- Κάθε ϕ_j είναι k-CNF φόρμουλα με N μεταβλητές και το πολύ $M_j = C \cdot N$ clauses.

Λήμμα Αραιοποίησης. Έστω θετικός ακέραιος $k \geq 3$ και $\epsilon > 0$. Τότε υπάρχει αριθμός $C := C(k, \epsilon)$ και αλγόριθμος $\mathcal{A}$ έτσι ώστε

- Δοσμένης μίας k-CNF φόρμουλα ϕ, ο $\mathcal{A}(\phi)$ επιστρέφει φορμουλες $\phi_1, \ldots, \phi_t$ ώστε
$$\phi = \phi_1 \vee \phi_2 \vee \ldots \phi_t.$$

- $t \leq 2^{\epsilon N}$.
- Ο $\mathcal{A}$ τρέχει σε χρόνο $\tilde{O}(2^{\epsilon N})$.
- Κάθε ϕ_j είναι k-CNF φόρμουλα με N μεταβλητές και το πολύ $M_j = C \cdot N$ clauses.

Κυρίαρχο σύνολο δε λύνεται σε $O(2^{\delta' n})$ χρόνο:

$$\underbrace{2^{\epsilon N}}_{\text{πλήθος στιγμιοτύπων}} \cdot \underbrace{2^{\delta'(3N+M_j)}}_{\text{χρόνος ανά στιγμιότυπο}} = 2^{\epsilon N + \delta'(3+C)N} < 2^{\delta n}.$$

ΕΤΗ και πολυωνυμικοί αλγόριθμοι

- Πρόβλημα q-Κυρίαρχου Συνόλου.
  Δίνεται ένας γράφος $G = (V, E)$ με n κορυφές, m ακμές, και ένας φυσικός αριθμός q.

ΕΤΗ και πολυωνυμικοί αλγόριθμοι

- Πρόβλημα q-Κυρίαρχου Συνόλου.
  Δίνεται ένας γράφος $G = (V, E)$ με n κορυφές, m ακμές, και ένας φυσικός αριθμός q.
  Ερώτηση: Υπάρχει κυρίαρχο σύνολο μεγέθους q ;

Άμεσο: $\binom{n}{q} \cdot nq \approx n^{q+1}$ αλγόριθμος.

Προχωρημένο: Για $q \geq 7$, $n^{q+o(1)}$ αλγόριθμος

ΕΤΗ και πολυωνυμικοί αλγόριθμοι

- Πρόβλημα q-Κυρίαρχου Συνόλου.
  Δίνεται ένας γράφος $G = (V, E)$ με n κορυφές, m ακμές, και ένας φυσικός αριθμός q.
  Ερώτηση: Υπάρχει κυρίαρχο σύνολο μεγέθους q ;

Άμεσο: $\binom{n}{q} \cdot nq \approx n^{q+1}$ αλγόριθμος.

Προχωρημένο: Για $q \geq 7$, $n^{q+o(1)}$ αλγόριθμος

Θεώρημα: Για όλα τα επαρκώς μεγάλα q, υπάρχει ένα δ έτσι ώστε να μην υπάρχει αλγόριθμος χρόνου $n^{\delta q}$ για το q-Κυρίαρχο Σύνολο.

- Χωρίζουμε τις μεταβλητές σε q ίσες ομάδες $G^{(i)} = \{x_{(i-1)\cdot N/q+1}, x_{i\cdot N/q}\}$.

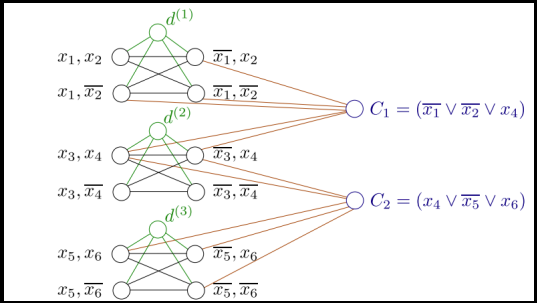
- Χωρίζουμε τις μεταβλητές σε q ίσες ομάδες $G^{(i)} = \{x_{(i-1)\cdot N/q+1}, x_{i\cdot N/q}\}$.
- Για κάθε ομάδα και για κάθε μερική αποτίμηση τιμών αληθείας p, φτιάχνουμε μία κορυφή $\alpha_p^{(i)}$.

- Χωρίζουμε τις μεταβλητές σε q ίσες ομάδες $G^{(i)} = \{x_{(i-1)\cdot N/q+1}, x_{i\cdot N/q}\}$.
- Για κάθε ομάδα και για κάθε μερική αποτίμηση τιμών αληθείας p, φτιάχνουμε μία κορυφή $\alpha_p^{(i)}$.
- Ορίζουμε μία κορυφή $d^{(i)}, \forall i$.

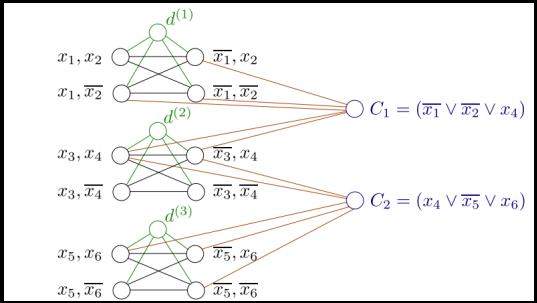
- Χωρίζουμε τις μεταβλητές σε q ίσες ομάδες $G^{(i)} = \{x_{(i-1)\cdot N/q+1}, x_{i\cdot N/q}\}$.
- Για κάθε ομάδα και για κάθε μερική αποτίμηση τιμών αληθείας p, φτιάχνουμε μία κορυφή $\alpha_p^{(i)}$.
- Ορίζουμε μία κορυφή $d^{(i)}, \forall i$.
- Για το ίδιο i, οι κορυφές $a_p^{(i)}$ σχηματίζουν κλίκα.

- Χωρίζουμε τις μεταβλητές σε q ίσες ομάδες $G^{(i)} = \{x_{(i-1)\cdot N/q+1}, x_{i\cdot N/q}\}$.
- Για κάθε ομάδα και για κάθε μερική αποτίμηση τιμών αληθείας p, φτιάχνουμε μία κορυφή $\alpha_p^{(i)}$.
- Ορίζουμε μία κορυφή $d^{(i)}, \forall i$.
- Για το ίδιο i, οι κορυφές $a_p^{(i)}$ σχηματίζουν κλίκα.
- Για το j-οστό clause, ορίζουμε μια κορυφή C_j.

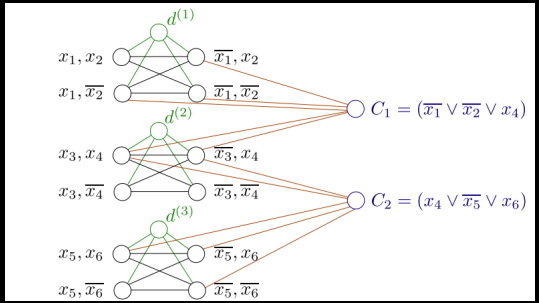
- Χωρίζουμε τις μεταβλητές σε q ίσες ομάδες $G^{(i)} = \{x_{(i-1)\cdot N/q+1}, x_{i\cdot N/q}\}$.
- Για κάθε ομάδα και για κάθε μερική αποτίμηση τιμών αληθείας p, φτιάχνουμε μία κορυφή $\alpha_p^{(i)}$.
- Ορίζουμε μία κορυφή $d^{(i)}, \forall i$.
- Για το ίδιο i, οι κορυφές $a_p^{(i)}$ σχηματίζουν κλίκα.
- Για το j-οστό clause, ορίζουμε μια κορυφή C_j.
- Συνδέουμε μία κορυφή C_j με το $a_p^{(i)}$ αν η αποτίμηση που αντιστοιχεί στην $a_p^{(i)}$, κάνει αληθές το clause C_j



Ισχυρισμός: Η ϕ είναι ικανοποιήσιμη, αν και μόνο αν ο κατασκευασμένος γράφος έχει κυρίαρχο σύνολο μεγέθους q.



Ισχυρισμός: Η ϕ είναι ικανοποιήσιμη, αν και μόνο αν ο κατασκευασμένος γράφος έχει κυρίαρχο σύνολο μεγέθους q.
Άρα $O(n^{\delta' q})$ αλγόριθμος για το q-Κυρίαρχο Σύνολο θα έδινε
$O\left(\left(q2^{N/q}\right)^{\delta' q}\right) = O(2^{\delta N})$ για 3-SAT.



Ισχυρισμός: Η ϕ είναι ικανοποιήσιμη, αν και μόνο αν ο κατασκευασμένος γράφος έχει κυρίαρχο σύνολο μεγέθους q.

Άρα $O(n^{\delta' q})$ αλγόριθμος για το q-Κυρίαρχο Σύνολο θα έδινε $O((q2^{N/q})^{\delta' q}) = O(2^{\delta N})$ για 3-SAT.

$\star$ Χρόνος Αναγωγής $2^{O(N/q)}$, άρα $q = \Omega(1/\delta)$.

Ευχαριστούμε!