



Η συνεκτικότητα μη κατευθυνόμενων
γραφημάτων ανήκει στο L

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αθανάσιος Β. Λιανέας
Επιβλέπων Καθηγητής: κ. Στάθης Ζάχος

Αθήνα, Φεβρουάριος 2009

Αθανάσιος Β. Λιανέας. No rights reserved.

Η γνώση είναι δύναμη. Δεν επιθυμείται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Ευχής έργο η ανατύπωση, αποθήκευση ή διανομή της για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις των εκπαιδευτικών ιδρυμάτων που οργανώνουν το μΠΛΥ.

Συγχωρέστε με για λάθη.

Περίληψη

Ένα από τα πιο σημαντικά και πρόσφατα αποτελέσματα στην υπολογιστική πολυπλοκότητα, αλλά και στην θεωρητική πληροφορική γενικότερα, είναι η απόδειξη πως $L \equiv SL$. Η απόδειξη έγινε από τον Reingold ([Rei05]) παρουσιάζοντας έναν Logspace αλγόριθμο για το USTCON, το σημαντικότερο SL-complete πρόβλημα.

Ο αλγόριθμος αυτός χρειάζεται ένα καλό υπόβαθρο σε θέματα γραφοθεωρίας, γραμμικής άλγεβρας και αναλυτικής γεωμετρίας. Η παρούσα εργασία σκοπό έχει την συγκέντρωση όλων των στοιχείων που χρειάζονται για την πλήρη και αναλυτική παρουσίασή του. Θα δούμε κάποια βασικά πράγματα σχετικά με την κλάση SL, κάποια απαραίτητα θέματα σχετικά με τους expander γράφους (από την αλγεβρική τους κυρίως σκοπιά) και την συμπεριφορά τους σε κάποιες γραφοπράξεις και τελικά θα παρουσιάσουμε τον αλγόριθμο του Reingold, κάνοντας μια πλήρη ανάλυσή του.

Περιεχόμενα

| | | |
|----------|--|-----------|
| 1 | Εισαγωγή | 2 |
| 1.1 | Μηχανές Turing | 2 |
| 1.2 | Πολυπλοκότητα χώρου | 4 |
| 1.3 | Το πρόβλημα <i>USTCON</i> και η κλάση <i>SL</i> | 5 |
| 2 | Γράφοι: πράξεις και expansion | 9 |
| 2.1 | Αναπαράσταση γράφου | 9 |
| 2.1.1 | Πίνακας γειτνίασης | 9 |
| 2.1.2 | Rotation map | 11 |
| 2.2 | Πράξεις επάνω σε γράφους | 12 |
| 2.2.1 | Ύψωση σε δύναμη (powering) | 12 |
| 2.2.2 | Γινόμενο αντικατάστασης, tensor γινόμενο και zig zag γινόμενο | 13 |
| 2.3 | Επεκτατικότητα γράφου (expansion) | 17 |
| 2.3.1 | Μέτρα επεκτατικότητας | 17 |
| 2.3.2 | Spectral expansion \rightarrow Vertex expansion | 19 |
| 2.4 | Υπάρχουν (καλοί) Expander γράφοι; | 21 |
| 2.4.1 | Υπάρχουν πολλοί | 21 |
| 2.4.2 | Μια οικογένεια με καλούς expanders | 23 |
| 3 | Ανάλυση του Zig Zag γινομένου | 27 |
| 3.1 | Η διαίσθηση για το expansion του γινομένου | 27 |
| 3.2 | Το Θεώρημα | 30 |
| 4 | Undirected st Connectivity \in L | 37 |
| 4.1 | Ένας $(D^{16}, D, 1/2)$ -expander της καλής οικογένειας | 38 |
| 4.2 | Από τον G στον G_{reg} | 38 |
| 4.3 | Φουσκώνοντας τον G_{reg} | 40 |
| 4.4 | Το πρόβλημα σε (καλούς) expander γράφους είναι (πιο) εύκολο | 46 |
| 5 | Περί πολυπλοκότητας | 49 |

Κεφάλαιο 1

Εισαγωγή

1.1 Μηχανές Turing

Το μοντέλο που έχει επικρατήσει στην υπολογιστική πολυπλοκότητα για τον υπολογισμό της πολυπλοκότητας αλγορίθμων και προβλημάτων είναι οι Μηχανές Turing. Θα δώσουμε τον ορισμό αυτών και θα καθορίσουμε ακριβώς (ώστε να είμαστε σύμφωνοι) ποιά είναι το μοντέλο επάνω στο οποίο βασιζόμαστε.

Ορισμός 1.1.1. *Μια μηχανή Turing είναι μια τετράδα $M = (K, \Sigma, \delta, s)$ όπου:*

- το K είναι ένα πεπερασμένο σύνολο καταστάσεων
- το s είναι η αρχική κατάσταση της μηχανής, $s \in K$
- το Σ είναι πεπερασμένο σύνολο συμβόλων (το αλφάβητό μας)
- το δ είναι η συνάρτηση μετάβασης

Το K και το Σ είναι ξένα μεταξύ τους σύνολα. Το Σ πάντα περιέχει το κενό σύμβολο \sqcup και το \triangleright , το πρώτο σύμβολο κάθε ταινίας. Η δ είναι η συνάρτηση μετάβασης με πεδίο ορισμού το $K \times \Sigma$ και πεδίο τιμών το $(K \cup \{h, \text{"yes"}, \text{"no"}\}) \times \Sigma \times \{\leftarrow, \rightarrow, -\}$, όπου h η τερματική κατάσταση, το "yes" κατάσταση που αποδέχεται, το "no" κατάσταση που απορρίπτει και τα $\leftarrow, \rightarrow, -$ οι εντολές της μηχανής για κινήσεις της κεφαλής αριστερά, δεξιά και μη κίνησης αντίστοιχα.

Η μηχανή ξεκινά από την αρχική κατάσταση s και δέχεται σαν είσοδο μια συμβολοακολουθία από το αλφάβητο Σ , γραμμένη σε μια ταινία. Η ταινία αυτή ξεκινά με το σύμβολο \triangleright και θεωρούμε ότι εκτείνεται μέχρι το άπειρο. Στις θέσεις της ταινίας μπορεί να δείχνει μια κεφαλή, η οποία αρχικά δείχνει στο πρώτο σύμβολο της ταινίας (στο αριστερό άκρο). Η δ διαβάζει το σύμβολο της

θέσης στην οποία δείχνει η κεφαλή και ανάλογα με την κατάσταση της μηχανής καθορίζει: α) την επόμενη κατάσταση, β) τι θα γραφτεί στην ταινία στην θέση που δείχνει η κεφαλή και γ) την κίνηση της κεφαλής μια θέση δεξιά ή αριστερά ή παραμονή στην ίδια θέση. Η μηχανή σταματά όταν περάσει σε κάποια από τις τρεις τερματικές καταστάσεις $\{h, "yes", "no"\}$.

Στο μοντέλο μας θεωρούμε μηχανές που μπορούν να χρησιμοποιούν περισσότερες από μία ταινίες

Ορισμός 1.1.2. Μηχανή Turing k ταινιών, με $k \geq 1$, είναι μια τετράδα $M = (K, \Sigma, \delta, s)$ όπου τα K, Σ, s είναι ακριβώς όπως πριν αλλά η συνάρτηση δ έχει πεδίο ορισμού το $K \times \Sigma^k$ και πεδίο τιμών το $(K \cup \{h, "yes", "no"\}) \times (\Sigma \times \{\leftarrow, \rightarrow, -\})^k$

Η διαφορά από πριν είναι ότι εδώ έχουμε k ταινίες (με k κεφαλές) από τις οποίες η δ δέχεται το όρισμά της και για τις οποίες αποφασίζει τι θα γραφτεί στην θέση που δείχνει κάθε κεφαλή καθώς και τις κινήσεις της καθεμιάς από τις κεφαλές.

Μπορούμε να θεωρήσουμε ότι από τις k αυτές ταινίες κάποιες μπορούν να είναι μόνο για διάβασμα συμβόλων και κάποιες μόνο για γράψιμο συμβόλων. Το πετυχαίνουμε με κατάλληλο ορισμό της συνάρτησης δ .

Για κάθε μηχανή η "απάντηση" που παίρνουμε για κάθε είσοδο μπορεί να είναι η τελική κατάσταση στην οποία σταμάτησε η μηχανή ή τα περιεχόμενα κάποιας (ή κάποιων) από τις ταινίες της.

Το μοντέλο στο οποίο 'συμφωνούμε' είναι η Μηχανή Turing εισόδου-εξόδου:

Ορισμός 1.1.3. Μηχανή Turing εισόδου-εξόδου είναι μηχανή Turing

- k ταινιών (μη καθορισμένου $k \geq 1$)
- με πρώτη ταινία, την ταινία εισόδου η οποία είναι μόνο για διάβασμα συμβόλων
- τελευταία (k -οστη) ταινία μια ταινία μόνο για γράψιμο συμβόλων
- και την τελευταία αυτή ταινία να είναι και η έξοδος - απάντηση της μηχανής

Από εδώ και πέρα όταν αναφερόμαστε σε μηχανή Turing γενικά θα εννοούμε μια τέτοια μηχανή. Για να ολοκληρώσουμε το πρώτο εισαγωγικό κομμάτι δίνουμε τον ορισμό της μη ντετερμινιστικής μηχανής Turing

Ορισμός 1.1.4. Μη ντετερμινιστική μηχανή Turing k ταινιών, εισόδου-εξόδου, με $k \geq 1$, είναι μια τετράδα $M = (K, \Sigma, \Delta, s)$ όπου τα K, Σ, s είναι ακριβώς όπως πριν αλλά το Δ πλέον δεν είναι συνάρτηση αλλά διμερής σχέση στοιχείων του $K \times \Sigma^k$ με το $(K \cup \{h, "yes", "no"\}) \times (\Sigma \times \{\leftarrow, \rightarrow, -\})^k$

Η ουσία εδώ είναι ότι το Δ παύει να είναι συνάρτηση και σε κάθε βήμα η μηχανή έχει περισσότερες από μια επιλογές να κάνει. Η 'απάντηση' της μηχανής βασίζεται στις απαντήσεις όλων των δυνατών μονοπατιών υπολογισμού. Όσον αφορά τις μηχανές που δέχονται ή απορρίπτουν την είσοδο τότε για την αποδοχή (και μη απόρριψη) της εισόδου αρκεί ένα μονοπάτι υπολογισμού να αποδέχεται.

Παρακάτω θα ορίσουμε και θα ασχοληθούμε με το χώρο που χρησιμοποιεί μια μηχανή κατά τα τρεξίματα της στις διαφορές εισόδους.

1.2 Πολυπλοκότητα χώρου

Σαν χώρο μηχανής εννοούμε το πλήθος των θέσεων των ταινιών που χρησιμοποιήθηκαν κατά την λειτουργία της. Στο μοντέλο που χρησιμοποιείτε εδώ τα πλήθη των θέσεων της ταινίας εισόδου και της ταινίας εξόδου δεν λαμβάνονται σαν χώρος της μηχανής. Λίγο πιο τυπικά:

Ορισμός 1.2.1. Έστω μηχανή k ταινιών, κι έστω a_i το πλήθος των θέσεων της i -οστής ταινίας που υπέστησαν επεξεργασία κατά την λειτουργία της μηχανής σε κάποια είσοδο. Ο χώρος που χρειάζεται η μηχανή για την είσοδο αυτή ορίζεται ως το $\sum_{i=2}^{k-1} a_i$.

Όσον αφορά τις κλάσεις πολυπλοκότητας χώρου ορίαουμε

Ορισμός 1.2.2. • Ένα πρόβλημα ανήκει στην κλάση $SPACE(f(n))$ αν υπάρχει μηχανή *Turing* εισόδου-εξόδου που για κάθε στιγμιότυπο του προβλήματος μήκους n χρησιμοποιεί χώρο το πολύ $f(n)$

• Ένα πρόβλημα ανήκει στην κλάση $NSPACE(f(n))$ αν υπάρχει μη ν-τετερμινιστική μηχανή *Turing* που για κάθε στιγμιότυπο του προβλήματος μήκους n χρησιμοποιεί χώρο το πολύ $f(n)$

Παραθέτουμε παρακάτω ένα σημαντικότατο θεώρημα (με τις συνέπειες γνωστές σε όλους). Η απόδειξη δεν εξυπηρετεί κάποιον από τους σκοπούς της εισαγωγής μας και για αυτο την παραλείπουμε.

Θεώρημα 1.2.1. Αν κάποιο πρόβλημα ανήκει στην κλάση $SPACE(f(n))$ (ή $NSPACE(f(n))$) τότε για τυχαίο $\epsilon > 0$ θα ανήκει και στην κλάση $SPACE(2 + \epsilon f(n))$ (ή $NSPACE(2 + \epsilon f(n))$)

Αποτέλεσμα αυτού είναι να παραλείπουμε τις σταθερές και να μπορούμε να μιλάμε για κλάσεις $SPACE(O(f(n)))$ και $NSPACE(O(f(n)))$. Σημαντικότερες είναι οι κλάσεις $L = SPACE(O(\log n)) = SPACE(\log n)$ και $NL = NSPACE(O(\log n)) = NSPACE(\log n)$

Από τους ορισμούς και επειδή μια συνάρτηση δ μπορούμε να την δούμε σαν σχέση προκύπτει ότι $SPACE(f(n)) \subseteq NSPACE(f(n))$. Κατά συνέπεια $L \subseteq NL$

Μία πρόταση που θα μας χρειαστεί στο κυρίως μέρος της εργασίας, στον αλγόριθμο του Reinglod, είναι η ακόλουθη (η ιδέα από σελίδα 164 του [Pap94]):

Πρόταση 1.2.1. Έστω δύο προβλήματα A και B που *i*) αποφασίζονται από δύο ντετερμινιστικές μηχανές M_1 και M_2 αντίστοιχα σε χώρο $SPACE(\log n)$, *ii*) έχουν έξοδο μήκους $O(\text{poly}(n))$ και *iii*) είναι τέτοια ώστε η απάντηση του πρώτου να αποτελεί είσοδο για το δεύτερο. Υπάρχει ντετερμινιστική μηχανή M , λογαριθμικού χώρου, που δεχόμενη σαν είσοδο μια είσοδο για το A πρόβλημα απαντά αυτό που θα απαντούσε η M_2 με είσοδο την λύση του A προβλήματος (με είσοδο την απάντηση της M_1).

Απόδειξη. Η απόδειξη δεν είναι εντελώς προφανής. Μια πρώτη λύση που έρχεται στο μυαλό είναι να βάλουμε σε σειρά τις μηχανές ούτως ώστε η M_1 να παράγει την έξοδό της, να την δίνει στην M_2 και μετά η M_2 να δίνει την απάντηση. Το πρόβλημα εδώ είναι ότι η απάντηση της M_1 μπορεί να μην είναι λογαριθμικού μήκους, επιτρεπτό γιατί πρόκειται για την ταινία εξόδου.

Παρ' όλα αυτά η απάντηση σε αυτό το πρόβλημα είναι απλή. Είναι δεδομένο ότι κάθε φορά η M_2 διαβάζει μόνο ένα στοιχείο από την είσοδό της. Κάθε φορά που η M_2 θέλει να διαβάσει ένα στοιχείο από την είσοδό της σημειώνουμε την θέση αυτού του στοιχείου (μεριμνώντας από πριν για κάποιο μετρητή) και "τρέχουμε" την M_1 μέχρι να δούμε με τι συμπληρώνει την θέση που σημειώσαμε (χρησιμοποιώντας άλλο ένα μετρητή). Επειδή η έξοδος της μηχανής είναι το πολύ πολυωνυμικού μήκους ως προς το μήκος της εισόδου, οι μετρητές είναι μήκους λογαριθμικό ως προς αυτό το πολυώνυμο και συνεπώς $O(\log n)$. \square

Εδώ δώσαμε κάποιους βασικούς ορισμούς για να βεβαιωθούμε για ποιο μοντέλο μηχανής μιλάμε και ίσα ίσα για να μπορέσουμε να αποδείξουμε το πιο πάνω θεώρημα. Δεν θα δώσουμε ορισμούς μήτε για τις αναγωγές προβλημάτων μηδέ για την πληρότητα των κλάσεων, θεωρώντας αυτές γνωστές.

1.3 Το πρόβλημα $USTCON$ και η κλάση SL

Ένα από τα πιο παλιά, γνωστά και σημαντικά προβλήματα της θεωρίας πολυπλοκότητας αλλά και της επιστήμης των υπολογιστών γενικότερα, είναι το

Ορισμός 1.3.1. *ST Connectivity* πρόβλημα ($STCON$)

Δοσμένου κατευθυνόμενου γράφου G και δύο κόμβων του s και t , υπάρχει μονοπάτι στον G που συνδέει τα s και t ;

Το πρόβλημα αυτό αναφέρεται σε κατευθυνόμενους γράφους. Υπάρχει και το αντίστοιχο για μη κατευθυνόμενους γράφους.

Ορισμός 1.3.2. *Undirected ST Connectivity* πρόβλημα (*USTCON*)

Δοσμένου μη κατευθυνόμενου γράφου G και δύο κόμβων του s και t , υπάρχει μονοπάτι στον G που συνδέει τα s και t ;

Η πρώτη έκδοση του προβλήματος αποδεικνύεται σχετικά εύκολα ότι είναι NL-complete. Για μη κατευθυνόμενους γράφους όμως, κάτι τέτοιο δεν φαινόταν και ούτε φαίνεται να ισχύει. Παρότι τώρα ξέρουμε ότι το πρόβλημα ανήκει στο L και είναι L -πλήρες (και άρα η ερώτηση ισοδυναμεί με το ερώτημα $L = NL$), για καιρό γινόταν αναζήτηση τρόπου ώστε το USTCON να τοποθετηθεί πλήρως σε κάποια κλάση.

Μια ουσιαστική προσπάθεια που έδωσε αποτέλεσμα ήταν στο [LP82] όπου οι συγγραφείς ορίζουν μια νέα μηχανή Turing με βάση την οποία δημιουργούνται νέες κλάσεις πολυπλοκότητας χώρου και χρόνου. Η μηχανή αυτή είναι μη ντετερμινιστική αλλά έχει κάποιους περιορισμούς στην σχέση Δ που καθορίζει τα βήματα της μηχανής και η δύναμή της βρίσκεται ανάμεσα σε αυτές των δύο μηχανών που ορίσαμε νωρίτερα. Δεν θα γίνουμε πολύ συγκεκριμένοι.

Έστω μηχανή Turing k ταινιών. Πολύ γενικά θυμίζουμε ότι κάθε φορά η 'εικόνα' της μηχανής μπορεί να περιγραφεί πλήρως από τις 'εικόνες' των ταινιών της και τις θέσεις των κεφαλών των ταινιών. Η περιγραφή γίνεται και έτσι:

$$(s, w_1, u_1, \dots, w_k, u_k)$$

όπου s η κατάσταση στην οποία βρίσκεται η μηχανή και $w_i || u_i$ τα περιεχόμενα της i -οστής ταινίας με το τελευταίο σύμβολο του w_i να είναι και αυτό στο οποίο βρίσκεται η κεφαλή της αντίστοιχης ταινίας. Από μια εικόνα της μηχανής μέσω της Δ πηγαίνουμε σε κάποια άλλη (αν δεν τερματίζει η μηχανή). Τότε λέμε και ότι η μια εικόνα οδηγεί στην άλλη.

Η ιδέα για να την NL -πληρότητα του STCON είναι περίπου έτσι: Έστω πρόβλημα που επιλύεται με μηχανή Turing M λογαριθμικού χώρου. Η M έχει πλήθος πιθανών εικόνων εκθετικό ως προς τον χώρο της και άρα πολυωνυμικό ως προς την είσοδο. Έτσι μπορούμε να δούμε κάθε πιθανή εικόνα σαν κόμβο γράφου, να δημιουργήσουμε ένα γράφο που θα έχει σαν κατευθυνόμενες ακμές μεταξύ εικόνων που οδηγούν η μία στην άλλη μέσω της M και να επιλύσουμε σε λογαριθμικό χώρο μη ντετερμινιστικά το STCON για αυτό το γράφο.

Για να ακολουθήσουμε περίπου το ίδιο σκεπτικό και να βρεθεί μια κλάση για την οποία το USTCON θα ήταν πλήρες θα έπρεπε ο αντίστοιχος γράφος της μηχανής του κάθε προβλήματος της κλάσης να έχει μη κατευθυνόμενες ακμές. Αυτό πετυχαίνεται αλλάζοντας μηχανή! Χονδρικά:

Ορισμός 1.3.3. Συμμετρική μηχανή Turing είναι κάθε μη ντετερμινιστική μηχανή Turing που είναι τέτοια ώστε αν μια εικόνα της, έστω α , οδηγεί σε μια εικόνα της, έστω β , τότε και η β οδηγεί στην α .

Αντίστοιχα με τις ήδη γνωστές μηχανές ορίζουμε:

Ορισμός 1.3.4. Ένα πρόβλημα ανήκει στην κλάση $SSPACE(f(n))$ αν υπάρχει συμμετρική μηχανή Turing εισόδου-εξόδου που για κάθε στιγμιότυπο του προβλήματος μήκους n χρησιμοποιεί χώρο το πολύ $f(n)$

Αποδεικνύεται ότι και για την πολυπλοκότητα χώρου συμμετρικών μηχανών ισχύει το αντίστοιχο του θεωρήματος 1.2.1. Έτσι μπορούμε να ορίσουμε πλέον την κλάση SL .

$$SL = SSPACE(\log n)$$

Όμοια με το σκεπτικό για την NL -πληρότητα του $STCON$ μπορούμε να καταλήξουμε ότι το $USTCON$ είναι SL -hard.

Μια λύση για το $USTCON$ είναι σε κάθε βήμα η επιλογή μη ντετερμινιστικά ενός άλλου κόμβου του γράφου από αυτόν που είμαστε (κρατώντας στην μνήμη τον κόμβο που είμαστε, βλέπε και υποσημείωση) και

- αν δεν υπάρχει ακμή ανάμεσα στον παλιό και στον καινούριο τότε γυρνάμε στον προηγούμενο
- αν υπάρχει επαναλαμβάνουμε με τον ίδιο τρόπο ¹

Μια τέτοια μηχανή, αν προσέξουμε τις λεπτομέρειες, μπορεί (με τη χρήση ίσως άλλης μιας θέσης για κόμβο ή και κάτι παραπάνω, και πειράζοντας την σχέση μετάβασης) να είναι συμμετρική. Όπως και να 'χει πάντως μια τέτοια μη ντετερμινιστική μηχανή, (σχεδόν) ανεξάρτητα από την ακριβή υλοποίησή της, έχει συμμετρικό κλείσιμο που αποφασίζει την ίδια γλώσσα στον ίδιο χώρο ([LP82])². Συμπεραίνουμε λοιπόν ότι υπάρχει συμμετρική μηχανή που επιλύει το πρόβλημα σε λογαριθμικό χώρο.

Διαισθητικά μπορούμε να δούμε ότι το $USTCON$ ανήκει στην κλάση SL ακριβώς γιατί από ένα κόμβο μπορούμε να γυρίσουμε πίσω σε αυτόν από τον οποίο ήρθαμε, μέσω της ίδιας ακμής, είναι μία από τις μη ντετερμινιστικές μας επιλογές, και άρα κάθε δύο συνεχόμενες εικόνες μπορούν να οδηγήσουν η μία στην άλλη.

¹για να είμαστε λίγο πιο τυπικοί: αν υπάρχει ακμή ανάμεσα στον παλιό και τον καινούριο τότε κρατά στις δύο θέσεις τον καινούριο κόμβο, αλλιώς κρατά στις δύο θέσεις τον παλιό κόμβο (κάθε βήμα που περιγράφουμε δηλαδή είναι στη ουσία δύο βήματα).

²οι εικόνες στα βήματα που αναφέραμε πιο πάνω, είναι οι ειδικές εικόνες της μηχανής όπως αναφέρονται στο λήμμα του [LP82]

Καταλήγουμε λοιπόν στο συμπέρασμα ότι το USTCON είναι SL -πλήρες. Έτσι η κλάση SL μπορεί ισοδύναμα να οριστεί σαν η κλάση των προβλημάτων που ανάγονται με logspace αναγωγή στο USTCON. Για περισσότερη ανάλυση, ορισμούς, αποτελέσματα και πλήρη προβλήματα της κλάσης μπορεί κανείς να αντρέξει στα [LP82] και [Gre96].

Η εικόνα με την μεγαλύτερη δυνατή πληροφορία που υπήρχε πριν τον αλγόριθμο του Reingold έδειχνε σαν

$$L \subseteq SL \subseteq RL \subseteq NL \subseteq L^2$$

Δύο από τα πιο σημαντικά ερωτήματα της θεωρίας πολυπλοκότητας (τουλάχιστον σε ότι αφορά τον χώρο) είναι τα $L \stackrel{?}{=} RL$ και $L \stackrel{?}{=} NL$. Η κλάση SL (και γενικότερα η συμμετρικότητα) έδωσε νέο ενδιαφέρον και νέες κατευθύνσεις στην αναζήτηση για απαντήσεις αυτών των ερωτημάτων (αλλά και άλλων). Μεγάλη λοιπόν η σημαντικότητα του αλγορίθμου του Reingold τον οποίο θα παρουσιάσουμε και θα στηρίξουμε όσο το δυνατόν πληρέστερα μέσα από τα επόμενα κεφάλαια.

Κεφάλαιο 2

Γράφοι: πράξεις και expansion

Στο κομμάτι αυτό θα αναφερθούμε εκτεταμένα σε κάποιους ορισμούς που αφορούν τους γράφους, σε κάποιες πράξεις που εφαρμόζονται επάνω σε αυτούς και στους δύο τρόπους που μας ενδιαφέρουν για την μέτρηση της επεκτατικότητάς τους - του expansion τους. Τυπικά δίνουμε τον ορισμό ενός γράφου:

Ορισμός 2.0.5. Γράφος $G = (V, E)$ είναι ένα ζεύγος συνόλων V και E για το οποίο

- V είναι ένα σύνολο κορυφών (ή κόμβων)
- E είναι ένα σύνολο μη διατεταγμένων ζευγών του V .

Θεωρούμε γενικούς γράφους όπου στο σύνολο E μπορούν να εμφανίζονται οι ίδιες ακμές (δισύνολα) περισσότερες από μία φορές καθώς και ακμές της μορφής $\{i, i\}$ (δηλαδή self-loops).

2.1 Αναπαράσταση γράφου

Η αναπαράσταση ενός γράφου μπορεί να γίνει με διάφορους τρόπους. Εδώ θα δούμε δύο από τους πιο συνηθισμένους, που είναι και αυτοί που θα χρειαστούμε παρακάτω. Το σημαντικό που σημειώνουμε είναι ότι για κάθε γράφο το πέρασμα από μια αναπαράσταση σε κάποια άλλη μπορεί να γίνει σε $SPACE(\log n)$

2.1.1 Πίνακας γειτνίασης

Ο πρώτος τρόπος με τον οποίο μπορούμε να αναπαραστήσουμε ένα γράφο είναι ο πίνακας γειτνίασης.

Ορισμός 2.1.1. Πίνακας γειτνίασης ενός γράφου $G = (V, E)$ με $|V| = n$ κόμβους είναι ο $n \times n$ πίνακας που στην (i, j) θέση περιέχει τον αριθμό των ακμών $\{i, j\}$ που περιέχονται στο σύνολο E του γράφου.

Κάθε ακμή $\{i, j\}$ λέμε ότι έχει άκρα τους κόμβους i και j και μπορούμε να λέμε ότι ξεκινά από οποιαδήποτε από αυτούς. Ένας γράφος είναι k -κανονικός αν από κάθε κόμβο του ξεκινούν ακριβώς k ακμές. Τυπικότερα και σε σχέση με τον πίνακα γειτνίασης:

Ορισμός 2.1.2. Ένας γράφος είναι k -κανονικός αν το άθροισμα οποιασδήποτε γραμμής ή στήλης του πίνακα γειτνίασης ισούται με k .

Για τους k -κανονικούς γράφους χρησιμοποιούμε τον κανονικοποιημένο πίνακα γειτνίασης

Ορισμός 2.1.3. Κανονικοποιημένος πίνακας γειτνίασης ενός k -κανονικού γράφου με πίνακα γειτνίασης M είναι ο πίνακας $M' = \frac{1}{k}M$

Η σημαντική ιδιότητα είναι πως ο κανονικοποιημένος πίνακας δίνει τις πιθανότητες για τις μεταβάσεις από κόμβο σε κόμβο ενός τυχαίου περιπάτου στον γράφο με κάθε γραμμή ή στήλη να έχει άθροισμα στοιχείων ίσο με 1.

Έστω M κανονικοποιημένος πίνακας γειτνίασης k -κανονικού γράφου G . Αν πάμε να υπολογίσουμε τις ιδιοτιμές του M ($\lambda : \lambda X = MX$) θα δούμε ότι:

Πρόταση 2.1.1. Έστω M κανονικοποιημένος πίνακας γειτνίασης k -κανονικού γράφου G , n κόμβων. Οι ιδιοτιμές του M έχουν αντίστοιχα ιδιοδιανύσματα κάθετα μεταξύ τους και για κάθε ιδιοτιμή λ του M ισχύει: $\lambda \leq 1$. Το $\lambda = 1$ είναι ιδιοτιμή του M με ιδιοδιάνυσμα το $u = 1_N = (1, \dots, 1)$

Απόδειξη. Αφού ο G είναι μη κατευθυνόμενος, ο M είναι συμμετρικός και άρα οι ιδιοτιμές έχουν αντίστοιχα ιδιοδιανύσματα κάθετα μεταξύ τους.

Έστω λ μια ιδιοτιμή του M με αντίστοιχο ιδιοδιάνυσμα το X . Έστω x_i το μεγαλύτερο κατά απόλυτη τιμή στοιχείο του διανύσματος X . Τότε από την θέση i του λX έχουμε:

$$\lambda X = MX \Rightarrow |\lambda| = \frac{|m_{i1}x_1 + \dots + m_{in}x_n|}{|x_i|} \leq \frac{m_{i1}|x_1|}{|x_i|} + \dots + \frac{m_{in}|x_n|}{|x_i|} \leq 1$$

Μια επαλήθευση αρκεί για να δούμε ότι το $\lambda = 1$ είναι ιδιοτιμή του M με ιδιοδιάνυσμα το $1_N = (1, \dots, 1)$. \square

Κάποια βασικά στοιχεία από άλγεβρα σε σχέση με τις ιδιοτιμές τέτοιων πινάκων (όπως μια παρόμοια απόδειξη αλλά και κάποια στοιχεία για την επεκτατικότητα γράφων) βρίσκονται στο [SeN93].

Ορίζουμε σαν $\lambda(G)$ την δεύτερη (κατ' απόλυτη τιμή) μεγαλύτερη ιδιοτιμή του πίνακα M . Επειδή μιλάμε για συμμετρικούς πίνακες μπορούμε πιο τυπικά να ορίσουμε:

Ορισμός 2.1.4. Ορίζουμε $\lambda(G)$ να είναι

$$\lambda(G) = \max_{x \perp u} \frac{\|Mx\|}{\|x\|} = \max_{x \perp u} \frac{|\langle Mx, x \rangle|}{\langle x, x \rangle}$$

Το γιατί ακριβώς η δεύτερη (κατ' απόλυτη τιμή) μεγαλύτερη ιδιοτιμή λ_2 ισούται με αυτά τα μέγιστα προκύπτει από τις σχέσεις:

$$\|Mx\| = \|M(k_2x_2 + \dots + k_nx_n)\| = \|\lambda_2k_2x_2 + \dots + \lambda_nk_nx_n\| \leq |\lambda_2| \cdot \|x\|$$

και

$$\begin{aligned} |\langle Mx, x \rangle| &= |\langle M(k_2x_2 + \dots + k_nx_n), k_2x_2 + \dots + k_nx_n \rangle| = \\ &|\langle Mk_2x_2 + \dots + Mk_nx_n, k_2x_2 + \dots + k_nx_n \rangle| = |\langle \lambda_2k_2x_2 + \dots + \lambda_nk_nx_n, k_2x_2 + \dots + k_nx_n \rangle| \\ &\leq |\lambda_2 \langle k_2x_2, k_2x_2 \rangle| + \dots + |\lambda_n \langle k_nx_n, k_nx_n \rangle| \leq |\lambda_2| (\langle k_2x_2, k_2x_2 \rangle + \dots + \langle k_nx_n, k_nx_n \rangle) \\ &= |\lambda_2| \langle x, x \rangle \end{aligned}$$

για τις οποίες η ισότητα ισχύει για κάθε x ιδιοδιάνυσμα του λ_2 .

Παρακάτω θα δούμε ότι το $\lambda(G)$ είναι ένα καλό μέτρο για την μέτρηση της επεκτατικότητας (του expansion) ενός γράφου, του πόσο γρήγορα μπορούμε να επεκταθούμε σε όλους τους κόμβους.

Ορισμός 2.1.5. Έστω k -κανονικός γράφος N κόμβων. Τότε για κάθε $\lambda \geq \lambda(G)$ ο G καλείται (N, k, λ) -γράφος.

Θα δούμε παρακάτω έναν άλλο χρήσιμο τρόπο αναπαράστασης γράφων και θα επανέλθουμε αργότερα για να δούμε κάποιες ιδιότητες των (N, k, λ) -γράφων που τις εμφανίζονται όταν τους εφαρμόσουμε κάποιες πράξεις (που θα περιγράψουμε).

2.1.2 Rotation map

Ο πίνακας γειτνίασης σαν τρόπος αναπαράστασης είναι κομβοκεντρικός κατα μία έννοια. Εδώ θα δούμε έναν άλλο τρόπο που θα μπορούσαμε να τον πούμε "ακμοκεντρικό".

Έστω ένας γράφος $G = (V, E)$. Σε κάθε κόμβο του, αντιστοιχούν κάποιες ακμές. Έστω $u, v \in V$ δυο κόμβοι του και $\{u, v\} \in E$ μια ακμή του. Ονομάζουμε τις ακμές κάθε κόμβου (τις αριθμούμε). Έστω η ακμή $\{u, v\}$ είναι η i -οστή του κόμβου u και j -οστή του κόμβου v . Τότε μπορούμε να πούμε ότι ο κόμβος u με την ακμή i πηγαίνει στον κόμβο v και ο v με την ακμή j πηγαίνει στην u . Έτσι λοιπόν ορίζουμε τον χάρτη εναλλαγής του G :

Ορισμός 2.1.6. *Χάρτης εναλλαγής (Rotation map) του γράφου $G = (V, E)$ είναι μια συνάρτηση $Rot_G : V \times E \rightarrow V \times E$ τέτοια ώστε:*

$$Rot_G(u, i) = (v, j) \iff e = (u, v) \in E \text{ και } e \begin{cases} i - \text{οστη του } u \text{ και} \\ j - \text{οστη του } v \end{cases}$$

Μια απλή παρατήρηση είναι ότι για k -κανονικούς γράφους η αρίθμηση των ακμών για κάθε κόμβο έχει πλήθος k και για προφανείς λόγους θεωρούμε ότι χρησιμοποιούνται οι αριθμοί $1, \dots, k$.

Ολοκληρώνουμε το κομμάτι των αναπαραστάσεων υπενθυμίζοντας ότι η μετάβαση από τον ένα τρόπο αναπαράστασης στον άλλο μπορεί να γίνει σε $SPACE(\log n)$.

2.2 Πράξεις επάνω σε γράφους

Θα περιγράψουμε τρεις πράξεις που εφαρμόζονται σε γράφους και θα μας χρησιμεύσουν στον αλγόριθμο του Reingold.

2.2.1 Ύψωση σε δύναμη (powering)

Πρόκειται για μια απλή πράξη που παίρνει τον γράφο $G = (V, E)$ και για κάθε t δημιουργεί έναν γράφο $G^t = (V', E')$ με $V' = V$ και σύνολο ακμών αυτό για το οποίο για κάθε δύο κορυφές u, v , έχει ακριβώς τόσες ακμές $\{u, v\}$ όσες τα διαφορετικά μονοπάτια μήκους t που τις ενώνουν.

Πρόταση 2.2.1. Έστω G ένας (N, k, λ) -γράφος, τότε ο G^t είναι ένας (N, k^t, λ^t) -γράφος

Απόδειξη. Χωρίζουμε την απόδειξη σε τρεις επιμέρους αποδείξεις κι έχουμε:

1. Οι κόμβοι του G^t παραμένουν οι ίδιοι και άρα N σε πλήθος.
2. Αφού ο G είναι k -κανονικός τα μονοπάτια μήκους t που ξεκινούν από κάθε κόμβο είναι k^t σε πλήθος, καθώς υπάρχουν k επιλογές σε κάθε κόμβο. Άρα το πλήθος ακμών θα είναι k^t .
3. Αρκεί να δείξουμε ότι ο πίνακας γειτνίασης του G^t είναι η t -οστή δύναμη του πίνακα γειτνίασης του G καθώς τότε οι ιδιοτιμές του πίνακα του G^t θα είναι οι ιδιοτιμές του πίνακα του G υψωμένες στην t -στή δύναμη και άρα $\lambda(G^t) = \lambda^t(G)$.

Με επαγωγή για $t = 1$ έχουμε $G^t = G$ και άρα ισχύει η υπόθεση.

Έστω ισχύει για $t = m$. Τότε για $t = m + 1$ τα μονοπάτια μήκους $m + 1$ μπορούμε να τα δούμε σαν ένωση δύο μονοπατιών μήκους m και μήκους 1. Έστω M_1 και M_2 οι πίνακες αναπαράστασης των G^m και G αντίστοιχα. Ο πίνακας M_1 έχει στην θέση $\{u, w\}$ το πλήθος των μονοπατιών μήκους m από το u στο w . Ο πίνακας M_2 έχει στην θέση $\{w, v\}$ το πλήθος των ακμών στον G από το w στο v . Έτσι ο πίνακας $M_1 \cdot M_2$ θα έχει στην θέση $\{u, v\}$ το πλήθος των μονοπατιών του G μήκους $m + 1$ από το u στο v (λόγω γινομένου πινάκων, αφήνοντας το w να τρέξει από 1 έως n). Έστω M ο πίνακας γειτνίασης του G . Από επαγωγική υπόθεση ο πίνακας M_1 θα είναι $M_1 = M^m$. Συνεπώς ο πίνακας γειτνίασης του G^{m+1} θα είναι ο $M^m \cdot M = M^{m+1}$.

□

Μια παρατήρηση που κάνουμε εδώ είναι ότι αν μια μηχανή έχει στην είσοδό της τον χάρτη εναλλαγής του G τότε ο χάρτης εναλλαγής του G^t για t σταθερό μπορεί να υπολογιστεί σε χώρο $O(\log n)$. Αυτό γιατί έστω u ένας κόμβος του G και (i_1, \dots, i_t) μια ακμή του G^t . Τότε αν μας ζητείται το $Rot_{G^t}(u, (i_1, \dots, i_t))$ μπορούμε μέσω του Rot_G να γράφουμε στην ταινία στις ίδιες θέσεις:

$$(u, (i_1, \dots, i_t)) \rightarrow (w_1, (j_1, i_2, \dots, i_t)) \rightarrow \dots \rightarrow (v, (j_1, \dots, j_t))$$

και αντιστρέφοντας τα j_r να πάρουμε στην ίδια θέση το $(v, (j_t, \dots, j_1)) = Rot_{G^t}(u, (i_1, \dots, i_t))$. Τυπώνουμε στην έξοδο και ελευθερώνουμε τον χώρο ώστε αυτός πλέον μπορεί να χρησιμοποιηθεί για υπολογισμό κάποιου άλλου $Rot_{G^t}(u', (i'_1, \dots, i'_t))$

Μια δεύτερη παρατήρηση είναι πως αν σε ένα γράφο δύο κόμβοι ενώνονται με μονοπάτι, τότε για κάποιο t στον G^t θα υπάρχει ακμή ανάμεσά τους. Θα μπορούσαμε έτσι να αποφασίσουμε αν συνδέονται απλά παράγοντας τους γράφους G^t για τα διάφορα t και κοιτάζοντας κάθε φορά τις ακμές των. Το πρόβλημα που θα παρουσιαζόταν και θα μας σπαταλούσε χώρο είναι πως οι ακμές γίνονται πολλές ζητώντας πολύ χώρο για την αναπαράστασή τους, αφού δεν μπορούμε να φράξουμε το t για το οποίο μπορεί να υπάρχει ακμή. Για την λύση αυτού του προβλήματος μπορούμε να βοηθηθούμε από τα ακόλουθα "γινόμενα" γράφων.

2.2.2 Γινόμενο αντικατάστασης, tensor γινόμενο και zig zag γινόμενο

Στην υποενότητα αυτή θα δούμε τρία είδη γινομένων μεταξύ γράφων. Ο αλγόριθμος του Reingold μπορεί να δουλέψει στον επιθυμητό χώρο και με το γινόμενο αντικατάστασης και με το zig zag γινόμενο. Το γινόμενο tensor θα

μας χρειαστεί στο κεφάλαιο 3 όπου θα αναλύσουμε το zig zag γινόμενο. Στον αλγόριθμο που θα παρουσιάσουμε θα χρησιμοποιήσουμε το zig zag γινόμενο καθώς οι αποδείξεις προκύπτουν λιγότερο περίπλοκα. Οι συμβολισμοί και τα σχήμα είναι από τα [RVW00] και [Rei08]

Γινόμενο αντικατάστασης (replacement product)

Το γινόμενο αντικατάστασης είναι το πιο απλό από τα τρία και βοηθά στην κατανόηση του zig zag γινομένου.

Έστω G , K -κανονικός γράφος N κορυφών και H , k -κανονικός γράφος K κορυφών. Το γινόμενο αντικατάστασης του G με τον H δίνει έναν γράφο $N \times K$ κορυφών ως εξής:

- Κάθε κόμβος u του G τον αντικαθιστά με ένα αντίγραφο του H , το H_u
- Κάθε κόμβος του H_u συνδέεται με τους k κόμβους μέσα στο H_u αλλά και με έναν κόμβο του H_w αν $\{u, w\}$ ακμή του G .

Δεν θα προχωρήσουμε σε πιο επίσημο ορισμό κρίνοντας ότι δεν χρειάζεται. Το χρήσιμο εδώ είναι πως ο βαθμός του γινομένου αντικατάστασης είναι κοντά στον βαθμό του δεύτερου γράφου ($k + 1$ και k αντίστοιχα) και ο βαθμός του δεύτερου γράφου μπορεί να είναι πολύ πιο μικρός από τον βαθμό του πρώτου ($k \ll K$).

Tensor γινόμενο (tensor product)

Έστω G_1 , D_1 -κανονικός γράφος N_1 κόμβων και G_2 , D_2 -κανονικός γράφος N_2 κόμβων. Το tensor γινόμενό τους είναι ο γράφος $G_1 \otimes G_2$ με $N_1 \cdot N_2$ κόμβους και $D_1 \cdot D_2$ κανονικότητα που δίνεται από τον χάρτη εναλλαγής $Rot_{G_1 \otimes G_2}$: $Rot_{G_1 \otimes G_2}((u, w), (i, j)) = ((u', w'), (i', j'))$, με $(u', i') = Rot_{G_1}(u, i)$ και $(w', j') = Rot_{G_2}(w, j)$.

Αυτό που γίνεται διαισθητικά είναι πως αντικαθιστούμε κάθε κόμβο u του G_1 με ένα αντίγραφο G_{2u} του G_2 . Ο κόμβος (u, w) με την (i, j) ακμή πηγαίνει από το G_{2u} αντίγραφο στον αντίστοιχο του κόμβο στο $G_{2w'}$, με την ακμή i , και μέσα στο αντίγραφο πηγαίνει από τον (u', w) κόμβο στον (u', w') κόμβο με την j ακμή.

Το tensor γινόμενο των δύο γράφων έχει άμεση σχέση με το γνωστό από την γραμμική άλγεβρα γινόμενο kronecker. Υπενθυμίζουμε ότι για διανύσματα $a \in \mathbb{R}^{N_1}$, $b \in \mathbb{R}^{N_2}$, το γινόμενο kronecker είναι το $c \in \mathbb{R}^{N_1 \cdot N_2}$: $c_{(i,j)} = a_i \cdot b_j$:

$$c = (a_1 b_1, \dots, a_1 b_{N_2}, \dots, a_{N_1} b_1, \dots, a_{N_1} b_{N_2})$$

Για πίνακες A, B διαστάσεων $N_1 \times N_1$ και $N_2 \times N_2$ αντίστοιχα το γινόμενο kronecker αυτών είναι ο C διάστασης $N_1 \cdot N_2 \times N_1 \cdot N_2$ με $c_{(i,k),(j,l)} = a_{(i,j)} \cdot b_{(k,l)}$

$$C = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1N_2}B \\ a_{21}B & a_{22}B & \dots & a_{2N_2}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{N_11}B & a_{N_12}B & \dots & a_{N_1N_2}B \end{pmatrix}$$

Είναι εύκολο να διαπιστώσει κανείς ότι ο κανονικοποιημένος πίνακας γειτνίασης του γινομένου $G_1 \otimes G_2$ είναι ο ο πίνακας που προκύπτει από το γινόμενο kronecker των κανονικοποιημένων πινάκων γειτνίασης των G_1, G_2 . Καθότι δεν θα χρειαστούμε περισσότερα δεν επεκτεινόμαστε άλλο και συνεχίζουμε στο σημαντικό γινόμενο το οποίο θα χρειαστούμε στον αλγόριθμο.

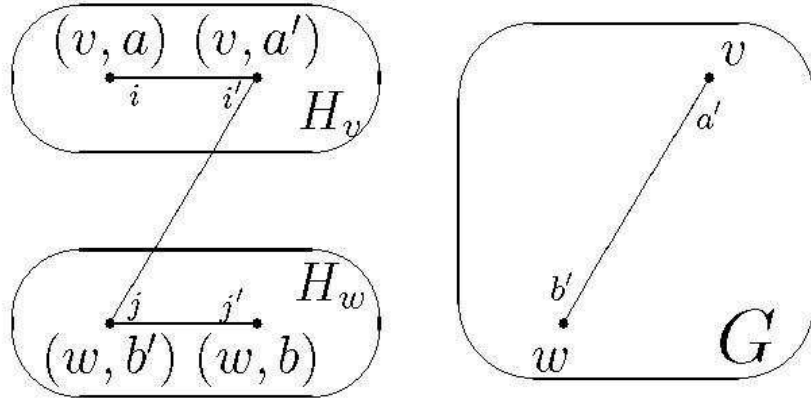
Zig zag γινόμενο (zig zag product)

Ένα πιο περίπλοκο γινόμενο είναι το zig zag γινόμενο. Έστω πάλι G , K -κανονικός γράφος N κορυφών και H , k -κανονικός γράφος K κορυφών. Εδώ πάλι αντικαθιστούμε κάθε κόμβο u του G με ένα αντίγραφο H_u του H . Οι κόμβοι του γινομένου συνεπώς έχουν πλήθος $N \times K$ (όσοι και στο γινόμενο αντικατάστασης). Οι ακμές του γινομένου προκύπτουν διαφορετικά.

Διαισθητικά, κάθε ακμή αντιστοιχεί σε ένα μονοπάτι μήκους 3 του γινομένου αντικατάστασης των G και H . Το μονοπάτι αυτό έχει την πρώτη και την τρίτη του ακμή σε δύο διαφορετικά αντίγραφα του H_u και ενδιάμεσα μια ακμή που συνδέει αυτά τα δύο αντίγραφα. Κάθε κόμβος του γινομένου έχει k^2 ακμές όσες και οι συνδυασμοί ακμών δύο κόμβων που βρίσκονται σε δυο διαφορετικά αντίγραφα του H . Αυτές οι k^2 ακμές καθορίζουν πλήρως τα μονοπάτια μήκους 3 (και άρα και τις ακμές του γινομένου).

Έστω ο κόμβος (u, a) ($u \in G$ και $a \in H$) και η ακμή (i, j) του zig zag γινομένου. Θα περιγράψουμε που μας πηγαίνει αυτή η ακμή (βοήθεια και στο σχήμα). Σημειώνουμε ότι ο G είναι K -κανονικός και ο H έχει K κόμβους και άρα τους αριθμούς $1 \dots K$ μπορούμε να τους δούμε σαν όνομα ακμής του G ή σαν όνομα κορυφής του H . Ας δούμε το μονοπάτι μήκους 3.

- Με το i πηγαίνουμε από τον (u, a) στον (u, a') , όπου a και a' συνδέονται με την i -οστή ακμή του x (στον H_u).
- Με το a' που βρήκαμε προηγουμένως (από τα i και a) πηγαίνουμε από τον κόμβο (u, a') στον (w, b') , όπου u και w συνδέονται με την a' -οστή ακμή του u και b' -οστή ακμή του w (στον G).
- Με το j πηγαίνουμε από τον (w, b') στον (w, b) , όπου b' και b συνδέονται με την j -οστή ακμή του b' (στον H_w).



Σχήμα 2.1: Το μονοπάτι μήκους 3 που δίνει τελικά την αντίστοιχη ακμή $\{(u, a), (w, b)\}$ στον γράφο του γινομένου.

Από το μονοπάτι μήκους 3 παίρνουμε και την ακμή του γινομένου. Έτσι ο (u, a) με την ακμή (i, j) πηγαίνει στον (w, b) . Εύκολα μπορούμε να βρούμε ποια ακμή του (w, b) μας πηγαίνει 'πίσω' στον (u, a) , αρκεί στα βήματα 1 και 3 να σημειώνουμε ποια ακμή μας πηγαίνει 'πίσω' στον κόμβο από όπου φύγαμε. Αυτό θέλουμε να μπορούμε να το κάνουμε για να μπορούμε να περιγράψουμε τον παραγόμενο γράφο του zig zag γινομένου με χάρτη εναλλαγής. Ο τυπικός ορισμός με χάρτη εναλλαγής ακολουθεί.

Ορισμός 2.2.1. Έστω G : K -κανονικός γράφος N κορυφών με χάρτη εναλλαγής Rot_G και H : k -κανονικός γράφος K κορυφών με χάρτη εναλλαγής Rot_H . Το zig zag γινόμενο $G \tilde{z} H$ των γράφων G και H ορίζεται να είναι ο k^2 κανονικός γράφος $N \times K$ κορυφών με χάρτη εναλλαγής αυτόν που προκύπτει με τους παρακάτω υπολογισμούς:

1. $(a', i') = Rot_H(a, i)$
2. $(w, b') = Rot_G(u, a')$
3. $(b, j') = Rot_H(b', j)$
4. $Rot_{G \tilde{z} H}((u, a), (i, j)) = ((w, b), (j', i'))$

Πρώτη παρατήρηση είναι ότι χάρτης εναλλαγής του $G\bar{z}H$ μπορεί να παραχθεί σε λογαριθμικό χώρο (αν K και k σταθερές) αν στην είσοδο υπάρχουν οι χάρτες εναλλαγής των G και H . Αυτό το συμπέρασμα βγαίνει με τον ίδιο τρόπο που συμπεράναμε την αντίστοιχη ιδιότητα για την ύψωση σε δύναμη. Δοσμένου $((u, a), (i, j))$ υπολογίζουμε σε λογαριθμικό χώρο τα βήματα που πρέπει να γίνουν από τον ορισμό, τυπώνουμε στην έξοδο το αποτέλεσμα και ελευθερώνουμε το χώρο για τον υπολογισμό κάποιου άλλου $Rot_{G\bar{z}H}((u', a'), (i', j'))$.

Ένα δεύτερο σημαντικό δεδομένο θα το δούμε στην ανάλυση του zig zag γινομένου και αφορά την δεύτερη ιδιοτιμή του παραγόμενου υπογράφου.

Στην επόμενη ενότητα θα ορίσουμε ένα μέτρο για την επεκτατικότητα των γράφων ώστε ακολούθως να δούμε κάποιες σημαντικές ιδιότητες που θα αφορούν όλα οσα θα έχουμε αναφέρει μέχρι εκείνο το σημείο.

2.3 Επεκτατικότητα γράφου (expansion)

Ο όρος επεκτατικότητα θέλει να περιγράψει κατά κάποιο τρόπο την συνεκτικότητα του γράφου υπό την έννοια του πόσο γρήγορα μπορούμε να επεκταθούμε από ένα σύνολο κόμβων στους υπόλοιπους κόμβους του γράφου.

2.3.1 Μέτρα επεκτατικότητας

Υπάρχουν αρκετοί τρόποι με τους οποίους μπορούμε να 'μετρήσουμε' την επεκτατικότητα ενός γράφου. Κάποιος μπορεί να αντρέξει στο [HLW06] και να δει αρκετούς τρόπους και σχέσεις μεταξύ τους. Εδώ θα δώσουμε τρεις από αυτούς δίνοντας περισσότερη προσοχή στους δύο που χρειάζονται για τον σκοπό μας. Ο ένας έχει σχέση με τους κόμβους και την καλή γειτονία μεταξύ τους, και είναι ο πιο άμεσος τρόπος που έρχεται στο μυαλό. Ο άλλος έχει να κάνει με την δεύτερη ιδιοτιμή του κανονικοποιημένου πίνακα αναπαράστασης του γράφου και η σχέση του με την επεκτατικότητα δεν φαίνεται εύκολα. Επάνω σε αυτόν όμως βασίζεται ο αλγόριθμος του Reingold. Τελικά αποδεικνύεται ότι οι δυο τρόποι είναι ισοδύναμοι (στο $[BAA^+]$), κάτι που επίσης μας χρειάζεται και θα δούμε (την μια κατεύθυνση).

Vertex expansion

Έστω ένα τυχαίο σύνολο κόμβων του γράφου. Έστω ότι μπορούμε για κάθε τέτοιο να εγγυηθούμε ότι η γειτονιά του, είναι μεγαλύτερη του σε πληθικότητα κατά ένα παράγοντα. Τότε ανάλογα με τον παράγοντα αυτό θα μπορούμε να μιλάμε για γρήγορη ή αργή επέκταση σε μεγαλύτερα σύνολα κόμβων. Η ιδέα για επεκτατικότητα μέσω κόμβων (Vertex expansion) είναι αυτή και απεικονίζεται στον ακόλουθο ορισμό.

Ορισμός 2.3.1. Ένας γράφος $G = (V, E)$ καλείται (K, A) vertex expander αν για κάθε σύνολο $S \subseteq V$ με το πολύ K κόμβους η γειτονιά $N(S) = \{u \mid \exists v \in S : (u, v) \in E\}$ έχει πληθικότητα $|N(S)| \geq A|S|$.

Edge expansion

Με όμοιο με πριν σκεπτικό για κάθε σύνολο κόμβων θα μπορούσαμε αντί για το σύνολο των εξωτερικών γειτόνων να βλέπουμε το σύνολο των ακμών που φεύγουν έξω από το σύνολο.

Ορισμός 2.3.2. Ένας γράφος $G = (V, E)$ καλείται (K, ϵ) edge expander αν για κάθε σύνολο $S \subseteq V$ με το πολύ K κόμβους το σύνολο $e(S, \bar{S}) = \{\{x, y\} : x \in S, y \in \bar{S}, \{x, y\} \in E\}$ έχει πληθικότητα τουλάχιστον $\epsilon \cdot |S|$

Spectral expansion

Δεδομένου του κανονικοποιημένου πίνακα γειτνίασης μη κατευθυνόμενου γράφου υπολογίζουμε την δεύτερη (κατ' απόλυτο) μεγαλύτερη ιδιοτιμή του (όπως περιγράψαμε σε προηγούμενη ενότητα). Αυτή αποδεικνύεται όπως θα δούμε ότι αποτελεί καλό μέτρο για την επεκτατικότητα του γράφου. Όσο μικρότερη τόσο καλύτερη επεκτατικότητα.

Ορισμός 2.3.3. Έστω k -κανονικός γράφος G , N κόμβων. Τότε για κάθε $\lambda : \lambda \geq \lambda(G)$ ο G καλείται (N, k, λ) -expander.

Καλούμε φασματική απόσταση (spectral gap) το $\gamma(G) = 1 - \lambda(G)$

Αυτό που πριν καλούσαμε (N, k, λ) -γράφο, πλέον μπορούμε να το μετονομάσουμε σε (N, k, λ) -expander και να μας δίνει πληροφορίες για την επεκτατικότητα του G . Όσον αφορά το $\gamma(G)$ όσο μεγαλύτερο τόσο καλύτερη επεκτατικότητα.

Μια σχέση της ιδιοτιμής αυτής με τον γράφο είναι πως μας δείχνει πόσο γρήγορα ένας τυχαίος περίπατος θα καταλήγει σε όλους τους κόμβους του γράφου με (σχεδόν) την ίδια πιθανότητα. Δεν θα επεκταθούμε πολύ. Εκτεταμένη ανάλυση γύρω από τους τυχαίους περιπάτους υπάρχει στο [LE93].

Έστω π μια κατανομή πιθανότητας να βρεθούμε αρχικά σε κάποιον από τους κόμβους του G που έχει κανονικοποιημένο πίνακα γειτνίασης τον M . Έστω $\lambda = 1$ και $u = (1/n)_n$ η μεγαλύτερη ιδιοτιμή του M με ένα αντίστοιχο της ιδιοδιάνυσμα και $\lambda_2, \dots, \lambda_n$ οι υπόλοιπες ιδιοτιμές με αντίστοιχά τους ιδιοδιανύσματα u_2, \dots, u_n , με λ_2 μεγαλύτερη κατά απόλυτη τιμή από τις υπόλοιπες, και τα ιδιοδιανύσματα που επιλέγουμε είναι κατανομές πιθανότητας.

Τα u_2, \dots, u_n μπορούν να παράγουν τον χώρο των κάθετων στο u διανυσμάτων (u, u_2, \dots, u_n) γραμμικά ανεξάρτητα και βάση του χώρου) και άρα μπορούν να παράγουν και το $\pi - u$ (καθώς $(\pi - u) \perp u$). Έστω λοιπόν

$\pi = u + c_2 u_2 + \dots + c_n u_n$. Έστω ένας τυχαίος περίπατος k βημάτων. Ο M όπως έχουμε επισημάνει σε προηγούμενη ενότητα είναι πίνακας μετάβασης τυχαίου περιπάτου. Στο 1^ο βήμα λοιπόν η πιθανότητα να βρεθούμε στον κάθε κόμβο δίνεται από το διάνυσμα $M\pi$. Στο 2^ο βήμα δίνεται από το διάνυσμα $M^2\pi$ και με την ίδια λογική στο k -οστό βήμα η πιθανότητα να βρεθούμε στον κάθε κόμβο δίνεται από το διάνυσμα $M^k\pi$. Μα τότε με γραμμική άλγεβρα έχουμε:

$$M^k\pi = M^k u + c_2 M^k u_2 + \dots + c_n M^k u_n = u + c_2 \lambda_2^k u_2 + \dots + c_n \lambda_n^k u_n$$

Έτσι όσο πιο μικρό είναι το $|\lambda_2|$ με τόσο λιγότερα βήματα (μικρότερο k) θα φτάνουμε πιο κοντά στην ομοιόμορφη κατανομή u .

Η παραπάνω συζήτηση μας δίνει μια διαίσθηση γιατί θεωρούμε ότι το $\lambda(G)$ μπορεί να μας δώσει πληροφορίες για την επεκτατικότητα του γράφου. Παρακάτω το αποδεικνύουμε και τυπικά.

2.3.2 Spectral expansion \rightarrow Vertex expansion

Για να δώσουμε την διαίσθηση του καλού μέτρου επεκτατικότητας για το $\lambda(G)$ εισάγαμε την έννοια της κατανομής πιθανότητας να βρεθούμε αρχικά σε κάποιον από τους κόμβους του G . Την ονομάσαμε π και θυμίζουμε ότι $u = (1/n, \dots, 1/n)$ είναι η ομοιόμορφη κατανομή. Με βάση τις τυχαίες κατανομές πιθανότητας μπορούμε να χαρακτηρίσουμε πλήρως το $\lambda(G)$

Πρόταση 2.3.1.

$$\lambda(G) = \max_{\pi} \frac{\|M\pi - u\|}{\|\pi - u\|}$$

Απόδειξη. Από τον ορισμό 2.1.4 έχουμε $\lambda(G) = \max_{x \perp u} \frac{\|Mx\|}{\|x\|}$.

Για κάθε π κατανομή πιθανότητας και κάθε διάνυσμα $x : x \perp u$ τα x και $\pi - u$ είναι συγγραμικά (γιατί $(\pi - u) \perp u$) και άρα $ax = \pi - u \rightarrow x = \frac{1}{a}(\pi - u) = b(\pi - u)$. Έτσι:

$$\frac{\|Mx\|}{\|x\|} = \frac{\|bM(\pi - u)\|}{\|b(\pi - u)\|} = \frac{\|M(\pi - u)\|}{\|\pi - u\|} = \frac{\|M\pi - u\|}{\|\pi - u\|}$$

και συνεπώς

$$\forall x \forall \pi : \frac{\|Mx\|}{\|x\|} = \frac{\|M\pi - u\|}{\|\pi - u\|} \Rightarrow \max_{x \perp u} \frac{\|Mx\|}{\|x\|} = \max_{\pi} \frac{\|M\pi - u\|}{\|\pi - u\|}$$

□

Για να αποδείξουμε ότι Spectral expansion \rightarrow Vertex expansion θα χρειαστούμε τον ακόλουθο ορισμό και το ακόλουθο λήμμα.

Ορισμός 2.3.4. Έστω μια κατανομή πιθανότητας π . Ορίζουμε:

- Πιθανότητα σύγκρουσης (*collision probability*) να είναι η πιθανότητα δύο τυχαίες επιλογές θέσεων του π να είναι ίδιες. Τυπικά: $CP(\pi) = \sum_x \pi_x^2$.
- Υποστηρίζον σύνολο (*Support*) του π να είναι το σύνολο των θέσεων με μη μηδενική πιθανότητα. Τυπικά $Supp(\pi) = \{x : \pi_x > 0\}$

Λήμμα 2.3.1. Για κάθε π , κατανομή πιθανότητας n θέσεων, έχουμε:

1. $CP(\pi) = \|\pi\|^2 = \|\pi - u\|^2 + 1/n$
2. $CP(\pi) \geq 1/|Supp(\pi)|$, με την ισότητα αν και μόνο αν $\pi = u$

Απόδειξη. Για τα δύο μέρη του λήμματος:

1. Από τον ορισμό του $CP(\pi)$: $CP(\pi) = \|\pi\|^2$. Επειδή $(\pi - u) \perp u$ έχουμε $\|\pi\|^2 = \|(\pi - u) + u\|^2 = \|(\pi - u)\|^2 + \|u\|^2 = \|(\pi - u)\|^2 + 1/N$
2. Έστω $a \in \{0, 1\}^n$ με τους άσσους να εμφανίζονται ακριβώς και μόνο στις θέσεις $i : \pi_i > 0$. Το a έχει τόσους άσσους όσους το πλήθος του $Supp(\pi)$. Λαμβάνοντας υποψιν και την ανισότητα Cauchy-Schwarz έχουμε:

$$1 = |a \cdot \pi| \leq \|a\| \cdot \|\pi\| = \sqrt{|Supp(\pi)|} \cdot \sqrt{\sum_x \pi_x^2} \Rightarrow CP(\pi) \geq \frac{1}{|Supp(\pi)|}$$

□

Πλέον μπορούμε να αποδείξουμε το

Θεώρημα 2.3.1. Έστω G είναι (N, K, λ) -expander τότε $\forall a \in [0, 1]$ ο G είναι ένας $(aN, \frac{1}{(1-a)\lambda^2+a})$ vertex expander.

Απόδειξη. Από την πρόταση 2.3.1 και το λήμμα 2.3.1, για την τυχαία π έχουμε για κάθε $\lambda \geq \lambda(G)$:

$$\lambda^2 \geq \lambda(G)^2 \geq \frac{\|M\pi - u\|^2}{\|\pi - u\|^2} \Rightarrow CP(M\pi) - \frac{1}{N} \leq \lambda^2 \left(CP(\pi) - \frac{1}{N} \right)$$

Έστω S τυχαίο υποσύνολο κόμβων πληθικότητας το πολύ aN , για τυχαίο $a \in [0, 1]$. Έστω u_s η ομοιόμορφη κατανομή στο S . Τότε $CP(u_s) = 1/|S|$ (από τον ορισμό) και $CP(Mu_s) \geq 1/|Supp(Mu_s)| = 1/N(S)$ (από το λήμμα

με $N(S)$ την γειτονιά του S , δες ορισμό 2.3.1). Συνεπώς από την προηγούμενη σχέση έχουμε:

$$\left(\frac{1}{|N(S)|} - \frac{1}{N} \right) \leq \lambda^2 \left(\frac{1}{|S|} - \frac{1}{N} \right)$$

Λύνοντας ως προς $|N(S)|$ έχουμε

$$\frac{1}{|N(S)|} \leq \frac{\lambda^2}{|S|} + \frac{1 - \lambda^2}{N} \Rightarrow |N(S)| \geq \frac{N|S|}{\lambda^2 N + |S| - \lambda^2 |S|}$$

Όμως $|S| \leq aN \Rightarrow N \geq |S|/a$ κι οπότε:

$$|N(S)| \geq \frac{|S|^2/a}{\lambda^2 |S|/a + |S| - \lambda^2 |S|} = \frac{|S|}{\lambda^2 + a - a\lambda^2} = \frac{|S|}{(1-a)\lambda^2 + a}$$

Συνεπώς το τυχαίο S πληθικότητας το πολύ aN (για τυχαίο $a \in [0, 1]$) έχει πλήθος γειτόνων τουλάχιστον ίσο με $\frac{1}{(1-a)\lambda^2 + a}|S|$ και άρα ο G είναι ένας $(aN, \frac{1}{(1-a)\lambda^2 + a})$ vertex expander. \square

Στο επόμενο κεφάλαιο, όταν θα χρειαστούμε αυτό το θεώρημα στον αλγόριθμο του Reingold, θα σταθεροποιήσουμε το a σε μια βολική τιμή.

Πριν ξεκινήσουμε να συζητάμε για το πρόβλημα αυτό καθεαυτό θα δούμε δύο (τελευταίες) χρήσιμες ιδιότητες.

2.4 Υπάρχουν (καλοί) Expander γράφοι;

2.4.1 Υπάρχουν πολλοί

Οποιοδήποτε μέτρο επεκτατικότητας και αν πάρουμε για την μέτρηση του expansion ενός γράφου υπάρχουν ανεξάρτητοι μεταξύ τους τρόποι για να μας δείξουν ότι expander γράφοι υπάρχουν πολλοί. Για το spectral expansion η ακόλουθη πρόταση μας δίνει και μια τέτοια πληροφορία.

Πρόταση 2.4.1. Κάθε d -κανονικός, συνεκτικός, μη διμερής, n κόμβων γράφος G έχει $\lambda(G) \leq 1 - 1/dn^2$

Εμείς θα αποδείξουμε μια ασθενέστερη μορφή της κατά την οποία ο γράφος G έχει μόνο θετικές ιδιοτιμές και μας αρκεί για τον αλγόριθμο του Reingold. Για το πλήρες θεώρημα παραπέμπουμε στο [AS00] και πιο πίσω στο [Lov93] όπου (μάλλον) υπάρχει ολοκληρωμένο.

Απόδειξη. Ο G έχει μόνο θετικές ιδιοτιμές και άρα από τον ορισμό 2.1.4 έχουμε

$$\lambda(G) = \max_{x \perp u, \|x\|=1} \langle Ax, x \rangle = \max_{x \perp u, \|x\|=1} \frac{1}{d} \sum_{(u,v) \in E} 2x_u x_v$$

με την δεύτερη ισότητα να προκύπτει αν σκεφτούμε τι περιέχει ο πίνακας A και τι σημαίνει $\langle Ax, x \rangle$. Με πράξεις έχουμε

$$\begin{aligned} \lambda(G) &= \max_{x \perp u, \|x\|=1} \frac{1}{d} \sum_{(u,v) \in E} (x_u^2 + x_v^2 - (x_u - x_v)^2) = \\ &= \max_{x \perp u, \|x\|=1} \frac{1}{d} \left(\sum_{i=1}^n x_i^2 d - \sum_{(u,v) \in E} (x_u - x_v)^2 \right) = 1 - \min_{x \perp u, \|x\|=1} \sum_{(u,v) \in E} (x_u - x_v)^2 \end{aligned}$$

σχεπτόμενοι όμοια με πριν για να βεβαιώσουμε της ισότητας (και επιπλέον την d -κανονικότητα του γράφου), και τελικά έχουμε

$$1 - \lambda(G) = \frac{1}{d} \min_{x \perp u, \|x\|=1} \sum_{(u,v) \in E} (x_u - x_v)^2$$

Έστω y το μοναδιαίο διάνυσμα για το οποίο ισχύει η ισότητα. Επειδή ακριβώς είναι μοναδιαίο θα υπάρχει j τέτοιο ώστε: $|y_j| \geq \frac{1}{\sqrt{n}}$.

Παράλληλα ισχύει όμως και $y \perp u$ και άρα $\sum_{i=1}^n y_i = 0$. Κατά συνέπεια θα υπάρχει k τέτοιο που οι y_j, y_k να είναι εταίροσημοι. Έτσι $|y_j - y_k| \geq \frac{1}{\sqrt{n}}$.

Επειδή ο G είναι συνεκτικός έχουμε ότι οι κόμβοι j, k του γράφου συνδέονται με κάποιο ελάχιστο μονοπάτι μήκους έστω a , το $j(= w_0), w_1, \dots, w_{a-1}, k(= w_a)$. Έχουμε

$$|y_k - y_j| = |y_k - y_{w_1} + y_{w_1} - \dots - y_{w_{a-1}} + y_{w_{a-1}} - y_j| \leq \sum_{i=0}^{a-1} |y_{w_i} - y_{w_{i+1}}|$$

και άρα

$$\sum_{i=0}^{a-1} |y_{w_i} - y_{w_{i+1}}| \geq \frac{1}{\sqrt{n}}$$

Κατά συνέπεια

$$1 - \lambda(G) = \frac{1}{d} \sum_{(u,v) \in E} (y_u - y_v)^2 \geq \frac{1}{d} \sum_{i=0}^{a-1} (y_{w_i} - y_{w_{i+1}})^2 \geq \frac{1}{da} \left(\sum_{i=0}^{a-1} |y_{w_i} - y_{w_{i+1}}| \right)^2$$

με την τελευταία ανισότητα να προκύπτει από την ανισότητα *Cauchy–Schwartz*.

Από τις δύο τελευταίες σχέσεις και το γεγονός ότι $a \leq n$ έχουμε

$$1 - \lambda(G) \geq \frac{1}{d} \left(\sum_{i=0}^{a-1} |y_{w_i} - y_{w_{i+1}}| \right)^2 \geq \frac{1}{dan} \geq \frac{1}{dn^2}$$

□

Για κάθε γράφο συνεκτικό μη διμερή G ο γράφος G^2 έχει μόνο θετικές ιδιοτιμές και άρα μπορούμε να εφαρμόσουμε την υποπερίπτωση του θεωρήματος που αποδείξαμε (σχετικά εύκολα βγαίνει μη διμερής). Έτσι

$$1 - \lambda(G^2) \geq \frac{1}{d^2n^2} \Rightarrow 1 - \lambda(G)^2 \geq \frac{1}{d^2n^2} \Rightarrow \lambda(G) \leq \sqrt{1 - \frac{1}{d^2n^2}}$$

Στο τέταρτο κεφάλαιο στον αλγόριθμο του Reingold θα χρησιμοποιήσουμε την αρχική πρόταση. Θα δώσουμε όμως σε σημείωση τι αλλάζει αν χρησιμοποιήσουμε την ασθενή περίπτωση που αποδείξαμε εδώ (δεν αλλάζει σχεδόν τίποτα).

2.4.2 Μια οικογένεια με καλούς expanders

Θα δώσουμε μια κατασκευή που απορρέει από κατασκευές που παρουσιάζονται στο [AR94], τους Cayley γράφους (περισσότερα στην αντίστοιχη δημοσίευση), και βρίσκεται στο [RVW00].

Έστω ένας πρώτος αριθμός q και κάποιο $d \in \mathbb{N}$. Ορίζουμε q^2 -κανονικό γράφο $LD_{q,d}$ με κόμβους τα στοιχεία του συνόλου \mathfrak{F}_q^{d+1} έτσι ώστε για κάθε $a \in \mathfrak{F}_q^{d+1}$ και $x, y \in \mathfrak{F}_q$ ο (x, y) -στός γείτονας του a να είναι ο $a + (y, yx, yx^2, \dots, yx^d)$.

Μια πρώτη παρατήρηση είναι ότι ο γράφος είναι οντως μη κατευθυνόμενος όπως θέλουμε καθώς αν a (x, y) -στός γείτονας του b τότε b $(x^{-1}, -y)$ -στός γείτονας του a (τα $-y$ και x^{-1} είναι modulo q .)

Αυτοί οι γράφοι έχουν πολύ καλή επεκτατικότητα (που ασυμπτωτικά πλησιάζει την βέλτιστη). Για να το αποδείξουμε θα χρειαστεί να ανακαλέσουμε στη μνήμη μας κάποια βασικά πράγματα από την θεωρία των μιγαδικών αριθμών. Αυτό θα γίνει γιατί θα περιγράψουμε πλήρως τις ιδιοτιμές και τα ιδιοδιανύσματα του πίνακα γειτνίασης του εκάστοτε γράφου. Για τα διάφορα q, d ισχύει

Πρόταση 2.4.2. $LD_{q,d}$ είναι ένας $(q^{d+1}, q^2, d/q)$ -expander.

Απόδειξη. Για το πλήθος των κόμβων και το βαθμό κανονικότητας δεν υπάρχει αμφιβολία.

Έστω M ο κανονικοποιημένος πίνακας γειτνίασης του $LD_{q,d}$ και για απλούστευση στις αναπαραστάσεις έστω $\mathfrak{F} = \mathfrak{F}_q$. Τα διανύσματα του χώρου $\mathbb{C}^{q^{d+1}}$ μπορούμε να τα δούμε σαν συναρτήσεις $f : \mathfrak{F}^{d+1} \rightarrow \mathbb{C}$ αφού κάθε f με πεδίο ορισμού το \mathfrak{F}^{d+1} πρέπει να δίνει μιγαδική τιμή σε κάθε ένα από τα q^{d+1} σε πλήθος στοιχεία του πεδίου ορισμού. Έστω $\zeta = e^{2\pi i/q}$. Από την μιγαδική ανάλυση ξέρουμε ότι το $\zeta^k = 1$ μόνο για τα k που είναι ακέραια πολλαπλάσια του q .

Για κάθε $a = (a_0, \dots, a_d) \in \mathfrak{F}^{d+1}$ ορίζουμε την συνάρτηση $\chi_a : \mathfrak{F}^{d+1} \rightarrow \mathbb{C}$ ώστε $\chi_a(b) = \zeta^{\sum a_i b_i}$. Εύκολα προκύπτει ότι $\chi_a(b+c) = \chi_a(b)\chi_a(c)$.

Ισχυρισμός. Τα χ_a είναι κάθετα μεταξύ τους (με το σύνηθες εσωτερικό γινόμενο: $(f, g) = \sum_c f(c)g(c)^*$).

Πράγματι ισχύει και για να το δούμε αρκεί να ομαδοποιήσουμε τα c σε A_i σύνολα τοποθετώντας στο ίδιο σύνολο τα c που έχουν ίδιες τις συντεταγμένες τους εκτός από την πρώτη. Τότε

$$(\chi_a, \chi_b) = \sum_{c \in \mathfrak{F}^{d+1}} \chi_a(c)\chi_b(c)^* = \sum_{c \in A_1} \chi_a(c)\chi_b(c)^* + \dots + \sum_{c \in A_{qd}} \chi_a(c)\chi_b(c)^*$$

Το κάθε A_i έχει q σε πλήθος στοιχεία. Έστω c ένα τυχαίο από αυτά. Τότε

$$\chi_a(c)\chi_b(c)^* = e^{\frac{2\pi i}{q} \sum a_i c_i} \cdot e^{-\frac{2\pi i}{q} \sum b_i c_i} = e^{\frac{2\pi i}{q} \sum_{i \neq 1} (a_i - b_i)c_i + \frac{2\pi i}{q} (a_1 - b_1)c_1}$$

Για όλα τα τυχαία $c \in A_i$ το πρώτο μέρος του εκθέτη είναι ίδιο. Το $(a_1 - b_1)c_1$ του δεύτερου μέρους, για τα $c_1 \in \{1, \dots, q\}$ παίρνει modulo q όλες τις τιμές $1, \dots, q$ γιατί

$$(c_1, d_1 \in \mathfrak{F} \& c_1 \neq d_1 \& (c_1(a_1 - b_1) \equiv d_1(a_1 - b_1) \pmod{q}) \rightarrow$$

$$c_1 - d_1 = \frac{k}{a_1 - b_1} q \rightarrow c_1 = d_1$$

άτοπο. Κατά συνέπεια, για τα $c \in A_i$, τα $e^{\frac{2\pi i}{q} \sum_{i \neq 1} (a_i - b_i)c_i + \frac{2\pi i}{q} (a_1 - b_1)c_1}$ κατανέμονται ομοιόμορφα πάνω στον τριγωνομετρικό κύκλο και άρα το άθροισμά τους για τα $c \in A_i$ βγαίνει 0. Αυτό ισχύει για κάθε A_i και άρα και το εσωτερικό γινόμενο των χ_a, χ_b βγαίνει μηδέν όσο λέει και ο ισχυρισμός.

Οι συναρτήσεις χ_a είναι q^{d+1} σε πλήθος, και συνεπώς ίσες με την διάσταση του χώρου των συναρτήσεων $h : \mathfrak{F}^{d+1} \rightarrow \mathbb{C}$ ο οποίος με την σειρά του ταυτίζεται με το $\mathbb{C}^{q^{d+1}}$. Αποτέλεσμα του ισχυρισμού λοιπόν είναι τα κάθετα μεταξύ τους χ_a να αποτελούν βάση του χώρου $\mathbb{C}^{q^{d+1}}$.

Όπως παρατηρήσαμε νωρίτερα ο γράφος είναι μη κατευθυνόμενος, άρα ο M είναι συμμετρικός και άρα τα ιδιοδιανύσματά του είναι κάθετα μεταξύ τους. Αν

αποδείξουμε λοιπόν ότι κάθε χ_a είναι ιδιοδιάνυσμα του M τότε τα έχουμε βρει όλα. Με υπολογισμούς έχουμε για κάθε b :

$$(M\chi_a)(b) = \frac{1}{q^2} \sum_{c \in \mathfrak{F}^{d+1}} M_{bc} \chi_a(c) = \frac{1}{q^2} \sum_{x, y \in \mathfrak{F}} \chi_a(b + (y, yx, \dots, yx^d))$$

Η πρώτη ισότητα προκύπτει από τον ορισμό του γινομένου πίνακα με διάνυσμα (ή πινάκων γενικότερα) και το γεγονός ότι ο πίνακας είναι κανονικοποιημένος (για το $\frac{1}{q^2}$).

Η δεύτερη ισότητα προκύπτει από το γεγονός ότι στην θέση M_{bc} βρίσκεται το πλήθος των ακμών (διαιρεμένο με q^2) από το b στο c . Από τον ορισμό του γράφου όμως υπάρχουν τόσες ακμές όσες και τα ζεύγη (x, y) τέτοια ώστε $c = b + (y, yx, \dots, yx^d)$. Άρα στο πρώτο άθροισμα για κάθε c θα εμφανιστούν M_{bc} σε πλήθος $\chi_a(c)$ όσα και τα $\chi_a(b + (y, yx, \dots, yx^d))$ που θα εμφανιστούν στο δεύτερο άθροισμα για τα $(x, y) : c = b + (y, yx, \dots, yx^d)$

Όμως $\chi_a(b + c) = \chi_a(b)\chi_a(c)$ και άρα

$$(M\chi_a)(b) = \left(\frac{\sum_{x, y \in \mathfrak{F}} \chi_a(y, yx, \dots, yx^d)}{q^2} \right) \cdot \chi_a(b)$$

Ορίζουμε $\lambda_a = \frac{\sum_{x, y \in \mathfrak{F}} \chi_a(y, yx, \dots, yx^d)}{q^2}$ και έχουμε τελικά για κάθε b :

$$(M\chi_a)(b) = \lambda_a \chi_a(b)$$

Άρα $M\chi_a = \lambda_a \chi_a$ και το λ_a είναι ιδιοτιμή του M για κάθε a . Για την απόδειξη της πρότασης λοιπόν αρκεί να δείξουμε ότι για όλα τα $a \in \mathfrak{F}^{d+1}$ εκτός από ένα ισχύει $|\lambda_a| \leq d/q$. Έχουμε από τον ορισμό του χ_a :

$$\lambda_a = \frac{1}{q^2} \sum_{x, y \in \mathfrak{F}} \chi_a(y, yx, \dots, yx^d) = \frac{1}{q^2} \sum_{x, y \in \mathfrak{F}} \zeta^{y \cdot p_a(x)}$$

όπου $p_a(x) = a_0 + a_1x + \dots + a_dx^d$ με $a = (a_0, \dots, a_d)$.

Κοιτώντας το άθροισμα έχουμε:

- Όταν το x είναι ρίζα του $p_a(x)$ τότε για όλα τα y , $\zeta^{y p_a(x)} = 1$ και άρα κάθε τέτοιο x συνεισφέρει στο άθροισμα το πολύ $q/q^2 = 1/q$

- Όταν το x δεν είναι ρίζα του $p_a(x)$ τότε

Ισχυρισμός. Για τα $y \in \mathfrak{F}$ τα $yp_a(x)$ παίρνουν όλες τις τιμές

$$e^{1 \frac{2\pi i}{q}}, e^{2 \frac{2\pi i}{q}}, \dots, e^{q \frac{2\pi i}{q}}$$

Πράγματι ισχύει και αρκεί να δείξουμε ότι $[(y_1 \neq y_2) \& (y_1, y_2 \in \mathfrak{F})] \Rightarrow y_1 p_a(x) \not\equiv y_2 p_a(x) \pmod{q}$ γιατί τότε κάθε $y_1 \in \mathfrak{F}$ θα έχει διαφορετικό υπόλοιπο από κάθε άλλο $y_2 \in \mathfrak{F}$ και συνεπώς θα έχουμε τα q σε πλήθος y να δίνουν q σε πλήθος $e^{(y \pmod{q}) \frac{2\pi i}{q}}$ και άρα όσα λέει ο ισχυρισμός.

Ότι $[(y_1 \neq y_2) \& (y_1, y_2 \in \mathfrak{F})] \Rightarrow y_1 p_a(x) \not\equiv y_2 p_a(x) \pmod{q}$ ισχύει γιατί:

$$(y_1, y_2 \in \mathfrak{F} \& y_1 \neq y_2 \& (y_1 p_a(x) \equiv y_2 p_a(x) \pmod{q}) \rightarrow$$

$$y_1 - y_2 = \frac{k}{p_a(x)} q \rightarrow y_1 = y_2$$

που είναι άτοπο και άρα ο ισχυρισμός θεμελιώνεται.

Αν πάμε να υπολογίσουμε την προσφορά στο άθροισμα όλων των y για ένα τέτοιο x θα δούμε ότι είναι μηδενική καθώς λόγω του ισχυρισμού τα y θα δώσουν τις τιμές $e^{1 \frac{2\pi i}{q}}, e^{2 \frac{2\pi i}{q}}, \dots, e^{q \frac{2\pi i}{q}}$ οι οποίες κατανέμονται ομοιόμορφα επάνω στον τριγωνομετρικό κύκλο. Συνέπεια αυτού να δίνουν συνολικά άθροισμα 0.

Αν $a = 0$ τότε παίρνουμε την αναμενόμενη ιδιοτιμή 1.

Αν $a \neq 0$ τότε το $p_a(x)$ έχει το πολύ d ρίζες και άρα λόγω του προηγούμενου διαχωρισμού στα x θα είναι $|\lambda(a)| \leq d/q$.

Άρα $\lambda(LD_{q,d}) \leq d/q$ και ολοκληρώνεται η απόδειξη. \square

Δημιουργήσαμε έτσι μια οικογένεια καλών expanders που προκύπτει από τις διάφορες (επιτρεπτές) τιμές των q, d . Από αυτή την καλή οικογένεια θα πάρουμε ένα κατάλληλο γράφο τον οποίο θα χρησιμοποιήσουμε σαν βάση στον αλγόριθμο του Reingold, και θα εφαρμόσουμε κάποιες από τις πράξεις που δώσαμε νωρίτερα. Μια από αυτές τις πράξεις είναι και το zig zag γινόμενο το οποίο και θα αναλύσουμε στο επόμενο κεφάλαιο.

Κεφάλαιο 3

Ανάλυση του Zig Zag γινομένου

Το κύριο αποτέλεσμα του κεφαλαίου έχει να κάνει με το spectral expansion του γράφου του zig zag γινομένου. Δίνει τον τρόπο εξάρτησης του λ του γινομένου από τα λ των δύο γράφων επάνω στους οποίους γίνεται η πράξη.

3.1 Η διαίσθηση για το expansion του γινομένου

Έστω δύο γράφοι G και H . Θυμίζουμε τα τρία βήματα που ορίζουν την τυχαία ακμή (i, j) του κόμβου (u, a) στον $G\tilde{z}H$ και δίνουν την ακμή $((u, a), (w, c))$.

1. $(Rot_H(a, i) = (b_1, k)) : (u, a) \rightarrow (u, b_1)$
2. $(Rot_G(u, b_1) = (w, b_2)) : (u, b_1) \rightarrow (w, b_2)$
3. $(Rot_H(b_1, j) = (c, l)) : (w, b_2) \rightarrow (w, c)$

Τα βήματα 1 και 3 είναι βήματα που γίνονται στα αντίγραφα H_u και H_w του H . Για το βήμα 2 υπάρχει μια σημαντική παρατήρηση: ο χάρτης εναλλαγής του γράφου G είναι μια 1-1 και επί αντιστοιχία του συνόλου $N \times K$ στον εαυτό του (όπου N και K τα σύνολα των κόμβων των G και H αντίστοιχα). Για αυτό το λόγο μπορούμε να τον βλέπουμε και ως μετάθεση των κόμβων του γράφου $G\tilde{z}H$ που έχει ακριβώς σαν σύνολο κόμβων το $N \times K$.

Στην υποενότητα 2.3.1 μιλήσαμε για τυχαίους περιπάτους και για το πως αυτοί μας δίνουν την διαίσθηση της στενής σχέσης του spectral expansion με την έννοια της επεκτατικότητας ενός γράφου. Στους τυχαίους περιπάτους θα

βασιστούμε για να δούμε την σχέση των spectral expansions των γράφων G και H με το spectral expansion του $G\tilde{z}H$.

Η επεκτατικότητα του γινομένου είναι διαισθητικά κάπως έτσι: Αν υποθέσουμε ότι ο G είναι μεγάλος (συνεκτικός) γράφος (σε βαθμό και πλήθος κόμβων) και ο H (συνεκτικός) μικρός (σε βαθμό και πλήθος κόμβων), τότε το zig zag γινόμενο κατά μια έννοια:

- Παίρνει το μέγεθος του από τον μεγάλο G .
- Παίρνει τον βαθμό του (βαθμό κανονικότητας του) από τον μικρό H .
- Κληρονομεί τις επεκτατικές ιδιότητες και από τους δύο, και αν υποθέσουμε ότι ο μικρός H έχει καλή επεκτατικότητα τότε η επεκτατικότητα του γινομένου βρίσκεται κοντά στο μεγάλο.

Τα δύο πρώτα είναι, λίγο έως πολύ, προφανή. Για το τρίτο θα προσπαθήσουμε να δούμε την συμπεριφορά των τυχαίων περιπάτων μέσα στον γράφο $G\tilde{z}H$.

Κάνουμε μια ακόμη παρατήρηση. Έστω ότι επιλέγουμε μια τυχαία ακμή (i, j) του $G\tilde{z}H$. Τότε, λόγω των βημάτων που υπενθυμίσαμε νωρίτερα, αυτή την τυχαία επιλογή μπορούμε να την δούμε σαν δύο ανεξάρτητες μεταξύ τους τυχαίες επιλογές δύο ακμών του H , μια για το H_u και μια για τον H_v που καθορίζουν παράλληλα και το βήμα στον G (το βήμα 2 για την εύρεση της ακμής του γινομένου).

Έστω u μια κατανομή πιθανότητας να βρεθούμε αρχικά σε κάποιον από τους κόμβους του $G\tilde{z}H$. Μετά από k τυχαία βήματα η κατανομή πιθανότητας θα δίνεται κατά τα γνωστά από το διάνυσμα $M^k u$, όπου M ο κανονικοποιημένος πίνακας γειτνίασης του $G\tilde{z}H$. Αν το u απέχει από την ομοιόμορφη κατανομή τότε με αυτά τα βήματα θα πλησιάζουμε σε αυτήν (ομοιόμορφη στις συνεκτικές συνιστώσες αλλά υποθέτουμε ότι οι γράφοι είναι συνεκτικοί και άρα και το γινόμενο τους) με ταχύτητα-τρόπο που εξαρτάται από τις ιδιοτιμές του γράφου.

Υποθέτουμε ότι έχουμε μια αρχική πιθανότητα μακριά από την ομοιόμορφη κατανομή και θέλουμε να δούμε διαισθητικά τι καταφέρνει το γινόμενο. Υπάρχουν δύο ακραίες περιπτώσεις:

Οι επιμέρους κατανομές στα αντίγραφα H_v του H είναι μακριά από την ομοιόμορφη κατανομή.

Οι επιμέρους κατανομές στα αντίγραφα του H είναι ομοιόμορφες, που τότε όμως θα πρέπει η κατανομή των H_v για όλα τα v να μην είναι ομοιόμορφη γιατί η αρχική κατανομή είναι μακριά από την ομοιόμορφη.

Η παρατήρηση κλειδί είναι πως οποιαδήποτε άλλη κατανομή (μακριά από την ομοιόμορφη) μπορεί να εκφραστεί σαν γραμμικός συνδυασμός αυτών των

δύο ακραίων περιπτώσεων. Έτσι για να καταλάβουμε την διαίσθηση, θα μιλήσουμε μόνο για αυτές τις δύο περιπτώσεις και θα μιλήσουμε μετά για το πως με γραμμική άλγεβρα μπορούμε να χειριστούμε κάθε περίπτωση μέσω αυτών των δύο.

Παίρνουμε ένα τυχαίο βήμα στον $G\tilde{z}H$. Τότε όπως σημειώσαμε νωρίτερα αυτό μπορούμε να το δούμε σαν τυχαίο μονοπάτι μήκους 3 με το πρώτο και τρίτο βήμα να γίνεται στα αντίγραφα του H και το μεσαίο βήμα πηδώντας από κάποιο αντίγραφο σε κάποιο άλλο.

1. Αν είμαστε στην πρώτη ακραία περίπτωση τότε με το πρώτο βήμα στο αντίγραφο πλησιάζουμε την ομοιόμορφη κατανομή (από την οποία είμαστε μακριά) και μάλιστα με τρόπο ανάλογο με το πόσο καλό expansion έχει ο γράφος H .

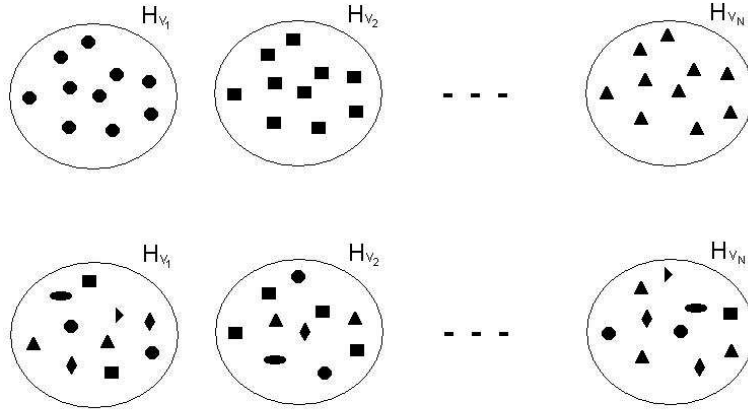
Τα άλλα δύο βήματα του μονοπατιού δεν μπορούν να αναιρέσουν αυτή την πρόοδο (το δεύτερο είναι όπως είδαμε μια μετάθεση των κόμβων του $N \times K$ και το τρίτο είναι βήμα σε κανονικό γράφο) μόνο να βοηθήσουν στην πρόοδο.

2. Αν είμαστε στην δεύτερη περίπτωση τότε το πρώτο βήμα δεν μπορεί να μας φέρει πιο κοντά στην ομοιόμορφη κατανομή καθώς σε όποιο αντίγραφο κι αν είμαστε η κατανομή εκεί είναι ομοιόμορφη και άρα δεν έχει σημασία σε ποιο κόμβο του αντιγράφου είμαστε. Ο κόμβος όμως που θα βρεθούμε παίζει ρόλο για το δεύτερο βήμα καθώς αυτός καθορίζει σε ποιο αντίγραφο θα μεταπηδήσουμε.

Το δεύτερο βήμα φέρνει την κατανομή των αντιγράφων του H πιο κοντά στην ομοιόμορφη. Όμως το μεσαίο βήμα είναι αυτό που καθορίζεται από τον Rot_G και όπως σημειώσαμε νωρίτερα τον Rot_G μπορούμε να τον δούμε σαν μια μετάθεση των κόμβων του $N \times K$. Άρα αυτό το βήμα δεν μπορεί να μας φέρει κοντά στην ομοιόμορφη κατανομή των κόμβων του $G\tilde{z}H$ (των κόμβων του συνόλου $N \times K$). Αυτό που κάνει αυτό το βήμα όμως είναι να χαλά τις ομοιόμορφες κατανομές στα H_v . Αυτό γιατί με μη ομοιόμορφο τρόπο το βήμα 2 μας πηγαίνει σε κόμβους μέσα στα αντίγραφα και άρα κάνει μη ομοιόμορφες τις κατανομές τους (εξήγηση και στο σχήμα).

Το τρίτο βήμα πλέον θα γίνει σε γράφο (αντίγραφο του H) με μη ομοιόμορφη κατανομή κι έτσι μπορεί να μας φέρει κοντά στην ομοιόμορφη κατανομή (με τον ίδιο τρόπο που το πρώτο βήμα δρα στην πρώτη περίπτωση).

Στο πάνω μέρος του σχήματος φαίνονται τα αντίγραφα του H με τις ίδιες πιθανότητες κατανομής εντός τους. Στο κάτω μέρος φαίνεται η εικόνα των αντιγράφων μετά το μεσαίο βήμα που ανακατέβει τους κόμβους των αντιγράφων.



Σχήμα 3.1: Η εικόνα πριν και μετά το μεσαίο-δεύτερο βήμα. Τα διαφορετικά σχήματα εντός των κύκλων αντιπροσωπεύουν τις διαφορετικές πιθανότητες.

Συνέπεια αυτού του βήματος είναι να χαλάνε οι ομοιόμορφες κατανομές πιθανότητας εντός των αντιγράφων και να δημιουργείται έτσι χώρος για βελτίωση στο τρίτο βήμα, βήμα το οποίο θα γίνει μέσα στα αντίγραφα (κύκλους) και άρα θα μας φέρει τόσο πιο κοντά στην ομοιόμορφη κατανομή όσο καλύτερο είναι το expansion του μικρού γράφου.

Κάθε τυχαία κατανομή που δεν είναι ομοιόμορφη μπορεί να εκφραστεί σαν γραμμικός συνδυασμός των δύο παραπάνω περιπτώσεων. Στην απόδειξη που ακολουθεί θα δούμε πως εκφράζονται αυτές οι δύο ακραίες περιπτώσεις και πως και γιατί με αυτές τις δύο μπορούμε να εκφράσουμε κάθε μη ομοιόμορφη κατανομή. Ακολουθώντας κατά κάποιο τρόπο την διαίσθηση που περιγράψαμε πιο πάνω θα φτάσουμε στο σημαντικό θεώρημα που αφορά το expansion του γινομένου.

3.2 Το Θεώρημα

Θεώρημα 3.2.1. Έστω G ένας (N, D, λ_1) -expander και H ένας (D, d, λ_2) -expander τότε ο $G\tilde{z}H$ είναι ένας $(N \cdot D, d^2, f(\lambda_1, \lambda_2))$ -expander, με

$$f(\lambda_1, \lambda_2) = \frac{1}{2}(1 - \lambda_2^2)\lambda_1 + \frac{1}{2}\sqrt{(1 - \lambda_2^2)\lambda_1^2 + 4\lambda_2^2}$$

Θα πάρουμε την απόδειξη εξ ολοκλήρου από το [RVW00].

Απόδειξη. Για τον βαθμό και το μέγεθος του παραγόμενου γράφου έχουμε μιλήσει νωρίτερα και τα αντίστοιχα αποτελέσματα προκύπτουν εύκολα. Το δύσκολο κομμάτι είναι να καθορίσουμε το $f(\lambda_1, \lambda_2)$.

Έστω M ο κανονικοποιημένος πίνακας του γινομένου $G\tilde{z}H$. Σύμφωνα με τον ορισμό 2.1.4 αρκεί να δείξουμε ότι για κάθε διάνυσμα $a \in \mathbb{R}^{ND}$ κάθετο στην ομοιόμορφη κατανομή το $\langle Ma, a \rangle$ είναι μικρότερο από το $\langle a, a \rangle$ κατά τον παράγοντα $f(\lambda_1, \lambda_2)$.

Για να ακολουθήσουμε την διαίσθηση που δώσαμε νωρίτερα, θα αναλύσουμε το τυχαίο διάνυσμα $a \perp 1_{ND}$ (που λόγω αυτής της καθετότητας βρίσκεται μακριά από τη ομοιόμορφη κατανομή) σε γραμμικό συνδυασμό των δύο διανυσμάτων που αντιστοιχούν το ένα στην ομοιόμορφη κατανομή εντός των αντιγράφων και το άλλο στην ομοιόμορφη κατανομή των αντιγράφων. Στα επόμενα u_k και 1_k η ομοιόμορφη κατανομή k θέσεων και το ‘ολα 1’ διάνυσμα k θέσεων αντίστοιχα.

Έστω τυχαίο $a \perp 1_{ND}$. Ορίζουμε:

- για κάθε $v \in [N]$ διάνυσμα $a_v \in \mathbb{R}^D$ τέτοιο που $(a_v)_k = a_{vk}$
- μια συνάρτηση $C : \mathbb{R}^{ND} \rightarrow \mathbb{R}^N : (Ca)_v = \sum_{k=1}^D a_{vk}$

Το a_v δίνει την κατανομή στο v αντίγραφο. Ο C είναι ακριβώς αυτός που δίνει για κάθε κατανομή π το $C\pi$ το οποίο είναι ακριβώς η κατανομή των αντιγράφων.

Έστω e_1, \dots, e_N η στάνταρ ορθοκανονική βάση του \mathbb{R}^N . Τότε από τους ορισμούς εύκολα προκύπτει ότι $a = \sum_{v=1}^N e_v \otimes a_v$. Με γραμμική άλγεβρα μπορούμε να βρούμε διάνυσμα a_v^{\parallel} τέτοιο ώστε: $a_v^{\parallel} \parallel u_D$ και $a_v - a_v^{\parallel} \perp a_v$ (παιρνώντας την ιδέα από το $\pi - u \perp u$). Έτσι μπορούμε να αναλύσουμε το a_v σε $a_v = a_v^{\parallel} + a_v^{\perp}$ με $a_v^{\perp} \perp u_D$. Έτσι τελικά έχουμε για το αρχικό a :

$$a = \sum_{v=1}^N e_v \otimes a_v = \sum_{v=1}^N e_v \otimes a_v^{\parallel} + \sum_{v=1}^N e_v \otimes a_v^{\perp} = a^{\parallel} + a^{\perp}$$

Ο όρος a_v^{\parallel} λόγω της παραλληλίας του με το διάνυσμα της ομοιόμορφης κατανομής έχει στις θέσεις τον ίδιο αριθμό και αντιστοιχεί στην ομοιόμορφη κατανομή εντός του αντιγράφου H_v . Έτσι το $e_v \otimes a_v$ είναι το διάνυσμα που έχει παντού μηδέν εκτός (ίσως) από τις θέσεις που αφορούν το αντίγραφο H_v . Εκεί έχει τον αριθμό που υπάρχει στις θέσεις του a_v^{\parallel} . Κατά συνέπεια το διάνυσμα $a^{\parallel} = \sum_{v=1}^N e_v \otimes a_v^{\parallel}$ είναι αυτό που αντιστοιχεί σε μια κατανομή που είναι ομοιόμορφη εντός των αντιγράφων του H .

Ο όρος a_v^\perp είναι κάθετος στην ομοιόμορφη κατανομή. Κατ' επέκταση το διάνυσμα $a^\perp = \sum_{v=1}^N e_v \otimes a_v^\perp$ αντιστοιχεί σε μια κατανομή η οποία σε κάθε αντίγραφο είναι μακριά από την ομοιόμορφη.

Έστω M ο κανονικοποιημένος πίνακας γειτνίασης του $G\tilde{z}H$. Οι όροι a^\parallel και a^\perp είναι ακριβώς οι όροι που χρησιμοποιήσαμε στην διαισθητική ανάλυση που κάναμε νωρίτερα. Για να δούμε πως δρα ο M επάνω στο a (ακολουθώντας την διαίσθηση) θα δούμε πως δρα στα a^\parallel και a^\perp συσχετίζοντάς τον με τους κανονικοποιημένους πίνακες A, B των G, H αντίστοιχα.

Ο M είναι προφανώς πίνακας που εξαρτάται από τους A, B . Θα τον αναλύσουμε σε γινόμενο τριών πινάκων που αντιστοιχούν στα τρία βήματα του γινομένου (τα οποία εξαρτώνται από τους A, B). Έστω \tilde{B} ο πίνακας που αντιστοιχεί στο πρώτο και τρίτο βήμα (βήματα μέσα στα αντίγραφα). Αυτός θα πρέπει να ενώνει τους κόμβους των αντιγράφων του H ακριβώς όπως στον H . Έτσι αυτός είναι ακριβώς το γινόμενο kronecker $\tilde{B} = I_{N \times N} \otimes B$ με $I_{N \otimes N}$ ο μοναδιαίος $N \times N$ πίνακας. Προφανώς ο \tilde{B} είναι συμμετρικός.

Το μεσαίο βήμα περιγράφεται από έναν \tilde{A} που καθορίζει την μετάθεση των κόμβων και έχει σχέση περιεργη με τον A . Δεν θα τον καθορίσουμε εδώ αλλά ιδιότητές του θα δούμε στην συνέχεια της απόδειξης. Μια από αυτές είναι ότι είναι συμμετρικός γιατί ο G είναι μη κατευθυνόμενος.

Ο M πλέον μπορεί να γραφτεί σαν $M = \tilde{B}\tilde{A}\tilde{B}$ (από τον ορισμό του γινομένου). Στη αρχή είδαμε πως θέλουμε να φράξουμε το $\frac{\langle Ma, a \rangle}{\langle a, a \rangle}$. Από την συμμετρία του \tilde{B} έχουμε

$$\langle Ma, a \rangle = \langle \tilde{B}\tilde{A}\tilde{B}a, a \rangle = \langle \tilde{A}\tilde{B}a, \tilde{B}a \rangle$$

Το a^\parallel είναι η κατανομή που είναι ομοιόμορφη εντός των αντιγράφων. Η συνάρτηση C που ορίσαμε προηγουμένως εφαρμοζόμενη στο a θα δώσει την κατανομή των αντιγράφων. Έτσι $a^\parallel = Ca \otimes 1_D/D$, γιατί παίρνουμε την συνολική πιθανότητα για ένα αντίγραφο και την μοιράζουμε ομοιόμορφα στους κόμβους του.

Από τις ιδιότητες του γινομένου kronecker και το ότι $B1_D = 1_D$ έχουμε:

$$\tilde{B}a^\parallel = (I_N \otimes B) \cdot (Ca \otimes 1_D/D) = (I_N \cdot Ca/D) \otimes (B \cdot 1_D) = Ca \otimes 1_D/D = a^\parallel$$

Έτσι $\tilde{B}a = \tilde{B}a^\parallel + \tilde{B}a^\perp = a^\parallel + \tilde{B}a^\perp$ και άρα τελικά αυτό που θέλουμε να φράξουμε είναι το

$$\frac{\langle Ma, a \rangle}{\langle a, a \rangle} = \frac{\langle \tilde{B}\tilde{A}\tilde{B}a, a \rangle}{\|a\|^2} = \frac{\langle \tilde{A}(a^\parallel + \tilde{B}a^\perp), a^\parallel + \tilde{B}a^\perp \rangle}{\|a^\parallel + a^\perp\|^2}$$

Ισχυρισμός 1. Ο \tilde{A} ανακλά κάθε διάνυσμα v μέσω ενός υποχώρου S του \mathbb{R}^{ND} .

Απόδειξη. Ο \tilde{A} είναι ο πίνακας που περιγράφει την μετάθεση των κόμβων όπως αυτή δίνεται από τον χάρτη εναλλαγής του G . Έτσι είναι $\tilde{A}^2 = I_{ND}$. Οι ιδιοτιμές του \tilde{A} συνεπώς είναι οι $1, -1$. Επειδή παράλληλα είναι και συμμετρικός, αυτές έχουν κάθετα μεταξύ τους ιδιοδιανύσματα που παράγουν το χώρο \mathbb{R}^{ND} . Έστω x_1, \dots, x_k και x_{k+1}, \dots, x_{ND} τα ιδιοδιανύσματα που αντιστοιχούν στις ιδιοτιμές $\lambda_1 = 1$ και $\lambda_2 = -1$ αντίστοιχα. Τότε

$$\begin{aligned}\tilde{A}v &= \tilde{A}(c_1x_1 + \dots + x_{ND}) = \tilde{A}c_1x_1 + \dots + \tilde{A}x_{ND} = \\ &\lambda_1c_1x_1 + \dots + \lambda_1c_kx_k + \lambda_2c_{k+1}x_{k+1} + \dots + \lambda_2c_{ND}x_{ND} = \\ &c_1x_1 + \dots + \lambda_1c_kx_k - c_{k+1}x_{k+1} - \dots - c_{ND}x_{ND}\end{aligned}$$

Παίρνοντας σαν υπόχωρο S το χώρο της γραμμικής θήκης $\langle x_1, \dots, x_k \rangle$ αποδεικνύουμε τον ισχυρισμό. \square

Αποτέλεσμα του ισχυρισμού είναι για κάθε διάνυσμα v το εσωτερικό γινόμενο $\langle \tilde{A}v, v \rangle$ να είναι

$$\langle \tilde{A}v, v \rangle = (\cos 2\theta) \|v\|^2$$

με θ την γωνία μεταξύ S και v .

Έτσι πλέον θέλουμε να φράξουμε το

$$\frac{|\langle Ma, a \rangle|}{\langle a, a \rangle} = |\cos 2\theta| \frac{\|a^{\parallel} + \tilde{B}a^{\perp}\|^2}{\|a^{\parallel} + a^{\perp}\|^2}$$

με θ την γωνία μεταξύ S και $a^{\parallel} + \tilde{B}a^{\perp}$.

Έστω $\phi \in [0, \pi/2]$ η γωνία μεταξύ των a^{\parallel} και $a^{\parallel} + a^{\perp}$ και ϕ' η γωνία μεταξύ a^{\parallel} και $a^{\parallel} + \tilde{B}a^{\perp}$. Τότε

$$\frac{\|a^{\parallel} + \tilde{B}a^{\perp}\|^2}{\|a^{\parallel} + a^{\perp}\|^2} = \left(\frac{\|a^{\parallel} + \tilde{B}a^{\perp}\| \cdot \|a^{\parallel}\|}{\|a^{\parallel} + a^{\perp}\| \cdot \|a^{\parallel}\|} \right)^2 = \left(\frac{\langle a^{\parallel} + \tilde{B}a^{\perp}, a^{\parallel} \rangle \cdot \cos \phi}{\langle a^{\parallel} + a^{\perp}, a^{\parallel} \rangle \cdot \cos \phi'} \right)^2 = \frac{\cos^2 \phi}{\cos^2 \phi'}$$

(γιατι $\langle a^{\perp}, a^{\parallel} \rangle = \langle a^{\perp}, \tilde{B}a^{\parallel} \rangle = \langle \tilde{B}a^{\perp}, a^{\parallel} \rangle \Rightarrow \langle a^{\parallel} + \tilde{B}a^{\perp}, a^{\parallel} \rangle = \langle a^{\parallel} + a^{\perp}, a^{\parallel} \rangle$)

Αν ψ η γωνία ανάμεσα στο a^{\parallel} και το S τότε $\theta \in [\psi - \phi', \psi + \phi']$ (εύκολα από γεωμετρία με ένα απλό σχηματάκι).

Έτσι καταλήγουμε να θέλουμε να φράξουμε το

$$\frac{|\langle Ma, a \rangle|}{\langle a, a \rangle} = |\cos 2\theta| \frac{\cos^2 \phi}{\cos^2 \phi'}$$

με τις γωνίες να ικανοποιούν όσα περιγράψαμε νωρίτερα.

Θα δούμε κάποιους περιορισμούς για αυτές τις γωνίες. Ένας περιορισμός πηγάζει από τον ισχυρισμό

Ισχυρισμός 2. $\|\tilde{B}a^\perp\| \leq \lambda_2 \|a^\perp\|$

Απόδειξη. Από την επεκτατικότητα του H ισχύει $\|Ba_v^\perp\| \leq \lambda_2 \cdot \|a_v^\perp\|$ και άρα

$$\|\tilde{B}a^\perp\| = \|\tilde{B}\left(\sum_{v=1}^N e_v \otimes a_v^\perp\right)\| = \left\|\sum_{v=1}^N e_v \otimes Ba_v^\perp\right\| \leq \lambda_2 \left\|\sum_{v=1}^N e_v \otimes a_v^\perp\right\| = \lambda_2 \|a^\perp\|$$

□

Άμεση συνέπεια του ισχυρισμού είναι

$$\frac{\tan \phi}{\tan \phi'} = \frac{\|\tilde{B}a^\perp\|}{\|a^\perp\|} \leq \lambda_2$$

$$\text{γιατι } \frac{\tan \phi}{\tan \phi'} = \frac{\|\tilde{B}a^\perp + a^\parallel\| \cdot \sin \phi'}{\|a^\perp + a^\parallel\| \cdot \sin \phi} = \frac{\|\tilde{B}a^\perp\|}{\|a^\perp\|}$$

Ένας ακόμη περιορισμός πηγάζει από τον

Ισχυρισμός 3. $|\langle \tilde{A}a^\parallel, a^\parallel \rangle| \leq \lambda_1 \langle a^\parallel, a^\parallel \rangle$

Απόδειξη. Αυτό ισχύει διαισθητικά ακριβώς για τους λόγους που ίσχυε και ο προηγούμενος ισχυρισμός. Για να το αποδείξουμε τυπικά πρέπει να δώσουμε τον ακριβή συσχετισμό του A με το \tilde{A} .

Έστω e_1, \dots, e_N η στάνταρ ορθοκανονική βάση του \mathfrak{R}^N . Για κάθε v το Ae_v δίνει τις πιθανότητες να πάμε σε ένα βήμα από τον v στους γείτονές του.

Το $(e_v \otimes 1_D/D)$ είναι διάνυσμα που παριστάνει την ομοιόμορφη κατανομή στο αντίγραφο H_v . Από τη φύση του ο \tilde{A} είναι τέτοιος που το $\tilde{A}(e_v \otimes 1_D/D)$ δίνει την κατανομή πιθανότητας των κόμβων του $G\tilde{z}H$ μετά από ένα βήμα, δεδομένου ότι ξεκινήσαμε ισοπίθανα από κάποιον από τους κόμβους του αντιγράφου H_v .

Έτσι το $C[\tilde{A}(e_v \otimes 1_D/D)]$ δίνει την κατανομή πιθανότητας για τα αντίγραφα που θα πρέπει να είναι Ae_v λόγω της εξάρτησης του \tilde{A} από τον A . Έτσι $C[\tilde{A}(e_v \otimes 1_D/D)] = Ae_v$.

Αυτό ισχύει για κάθε e_v της βάσης του \mathfrak{R}^N και άρα και για κάθε στοιχείο του \mathfrak{R}^N . Επομένως ισχύει και για το στοιχείο $Ca \in \mathfrak{R}^N$ και οπότε παίρνουμε $C[\tilde{A}(Ca \otimes 1_D/D)] = ACa$ και θυμίζουμε ότι $a^\parallel = Ca \otimes 1_D/D$. Επομένως έχουμε $C[\tilde{A}a^\parallel] = ACa$. Συνεπώς

$$\langle \tilde{A}a^\parallel, a^\parallel \rangle = \langle \tilde{A}a^\parallel, Ca \otimes 1_D \rangle / D = \langle C[\tilde{A}a^\parallel], Ca \rangle / D = \langle ACa, Ca \rangle / D$$

(με την μεσαία ισότητα να προκύπτει από τον ορισμό του εσωτερικού γινομένου)

Θυμίζουμε ότι το a είναι $a \perp 1_{ND}$ (άθροισμα στοιχείων 0). Άρα το Ca είναι αντίστοιχα $Ca \perp 1_N$ (ακριβώς το ίδιο άθροισμα στοιχείων με το a). Από τον ορισμό 2.1.4 του λ_2 για τον γράφο G έχουμε τελικά:

$$\langle \tilde{A}a^\parallel, a^\parallel \rangle \leq \lambda_1 \langle Ca, Ca \rangle / D = \lambda_1 \langle Ca \otimes 1_D, Ca \otimes 1_D \rangle / D^2 = \lambda_1 \langle a^\parallel, a^\parallel \rangle$$

(με την πρώτη ισότητα να προκύπτει από τον ορισμό του εσωτερικού γινομένου) \square

Ο ισχυρισμός αυτός, λόγω του ισχυρισμού 1, έχει άμεση συνέπεια την σχέση

$$|\cos 2\psi| \leq \lambda_1$$

Ορίζουμε $\mu_1 = \frac{\tan \phi}{\tan \phi'}$ και $\mu_2 = |\cos 2\psi|$ και τους χρησιμοποιούμε μέχρι το τέλος της απόδειξης όπου και θα τους φράξουμε με τα λ_1 και λ_2 .

Υπενθυμίζουμε ότι νωρίτερα καταλήξαμε στο

$$\frac{|\langle Ma, a \rangle|}{\langle a, a \rangle} = |\cos 2\theta| \cdot \frac{\cos^2 \phi}{\cos^2 \phi'}$$

Θα ξεχωρίσουμε δύο περιπτώσεις για να μπορέσουμε τελικά να φράξουμε την ποσότητα $|\cos 2\theta| \cdot \frac{\cos^2 \phi}{\cos^2 \phi'}$.

Περίπτωση 1η: $\phi' \leq \min\{\psi, \pi/2 - \psi\}$

$$|\cos 2\theta| = \max\{|\cos 2(\psi + \phi')|, |\cos 2(\psi - \phi')|\} = |\cos 2\psi \cdot \cos 2\phi'| + |\sin 2\psi \cdot \sin 2\phi'|.$$

Με τριγωνομετρία έχουμε:

$$|\cos 2\theta| \frac{\cos^2 \phi}{\cos^2 \phi'} = \frac{1}{2} \left| (1 - \mu_2^2) \cos 2\psi + (1 + \mu_2^2) \cos 2\psi \cos 2\phi' \right| + \frac{1}{2} \left| 2\mu_2 \sin 2\psi \sin 2\phi' \right|$$

Η επιλογή του ϕ που μεγιστοποιεί αυτή την ποσότητα είναι αυτή που κάνει το $(\cos 2\phi, \sin 2\phi)$ να είναι μοναδιαίο διάνυσμα το οποίο έχει την κατεύθυνση του διανύσματος $(\pm(1 + \mu_2^2) \cos 2\psi, 2\mu_2 \sin 2\psi)$ κι έτσι

$$|\cos 2\theta| \frac{\cos^2 \phi}{\cos^2 \phi'} \leq \frac{1}{2} (1 - \mu_2^2) |\cos 2\psi| + \frac{1}{2} \sqrt{(1 + \mu_2^2)^2 \cos^2 2\psi + 4\mu_2^2 \sin^2 2\psi}$$

\Downarrow

$$|\cos 2\theta| \frac{\cos^2 \phi}{\cos^2 \phi'} \leq \frac{1}{2} (1 - \mu_2^2) \mu_1 + \frac{1}{2} \sqrt{(1 + \mu_2^2)^2 \mu_1^2 + 4\mu_2^2 (1 - \mu_1^2)}$$

Περίπτωση 2η: $\phi' > \min\{\psi, \pi/2 - \psi\}$

Σε αυτή την περίπτωση δεν μπορούμε να φράξουμε (μη τετριμμένα) το $|\cos 2\theta|$ κι έτσι μετά από τριγωνομετρία αρκούμαστε να φράξουμε την ποσότητα

$$|\cos 2\theta| \frac{\cos^2 \phi}{\cos^2 \phi'} \leq \frac{\cos^2 \phi}{\cos^2 \phi'} = \mu_2^2 + (1 - \mu_2^2) \cos^2 \phi$$

Με τριγωνομετρία έχουμε

$$\cos 2\phi' = \frac{(1 + \mu_2^2)\cos^2\phi - \mu_2^2}{(1 - \mu_2^2)\cos^2\phi + \mu_2^2}$$

Επίσης έχουμε $\phi' > \min\{\psi, \pi/2 - \psi\} \Rightarrow \cos 2\phi' < |\cos 2\psi| = \mu_1$ το οποίο είναι ισοδύναμο με το

$$\cos^2\phi < \frac{\mu_2^2(1 + \mu_1)}{(1 - \mu_1) + \mu_2^2(1 + \mu_1)}$$

Συνδυάζοντας τις τρεις τελευταίες σχέσεις έχουμε

$$|\cos 2\theta| \frac{\cos^2\phi}{\cos^2\phi'} < \frac{2\mu_2^2}{1 - \mu_1 + \mu_2^2(1 + \mu_1)}$$

Αποδεικνύεται ότι το φράγμα της πρώτης περίπτωσης είναι πάντα μεγαλύτερο από το φράγμα της δεύτερης περίπτωσης κι ότι είναι και αύξουσα συνάρτηση των μ_1, μ_2 . Έτσι αντικαθιστώντας τα λ_1, λ_2 στη θέση των μ_1, μ_2 παίρνουμε το θεώρημα

$$\frac{|\langle Ma, a \rangle|}{\langle a, a \rangle} = |\cos 2\theta| \frac{\cos^2\phi}{\cos^2\phi'} \leq \frac{1}{2}(1 - \lambda_2^2)\lambda_1 + \frac{1}{2}\sqrt{(1 - \lambda_2^2)\lambda_1^2 + 4\lambda_2^2}$$

□

Συνέπεια του θεωρήματος είναι το ακόλουθο

Πόρισμα 3.2.1. Αν G είναι ένας (N, D, λ_1) -expander και H είναι ένας (D, d, λ_2) -expander τότε ο $G\tilde{z}H$ είναι ένας $(N \cdot D, d^2, f(\lambda_1, \lambda_2))$ -expander με:

$$\lambda(G\tilde{z}H) \leq 1 - \frac{1}{2}(1 - \lambda_2^2)(1 - \lambda_1)$$

Απόδειξη. Είναι $\lambda_1 \leq 1$ και άρα

$$\frac{1}{2}\sqrt{(1 - \lambda_2^2)\lambda_1^2 + 4\lambda_2^2} \leq \frac{1}{2}\sqrt{(1 - \lambda_2^2) + 4\lambda_2^2} = \frac{1}{2}(1 + \lambda_2^2) = 1 - \frac{1}{2}(1 - \lambda_2^2)$$

Ισχύει προφανώς λόγω του θεωρήματος $\lambda(G\tilde{z}H) \leq f(\lambda_1, \lambda_2)$. Τελικά συνδυάζοντας με το θεώρημα έχουμε:

$$f(\lambda_1, \lambda_2) = \frac{1}{2}(1 - \lambda_2^2)\lambda_1 + \frac{1}{2}\sqrt{(1 - \lambda_2^2)\lambda_1^2 + 4\lambda_2^2} \leq \frac{1}{2}(1 - \lambda_2^2)\lambda_1 + 1 - \frac{1}{2}(1 - \lambda_2^2)$$

και άρα

$$\lambda(G\tilde{z}H) \leq 1 - \frac{1}{2}(1 - \lambda_2^2)(1 - \lambda_1)$$

□

Κεφάλαιο 4

Undirected st Connectivity $\in \mathbf{L}$

Στο κεφάλαιο αυτό θα κάνουμε μια πλήρη παρουσίαση και ανάλυση του αλγορίθμου του Reingold. Ο αλγόριθμος διαισθητικά στηρίζεται σε μια πολύ απλή ιδέα για την επίλυση του προβλήματος της st -συννεκτικότητας.

Μας δίνετε ένας γράφος G και δύο κόμβοι του s, t . Θέλουμε να δούμε αν οι s και t συνδέονται με μονοπάτι. Αν οι δυο κόμβοι συνδέονται τότε αυτό θα γίνεται με μονοπάτι μήκους έστω k . Άρα αν δημιουργήσουμε τον γράφο G^k (κεφάλαιο 2.2.1) τότε ο γράφος αυτός θα έχει ακμή ανάμεσα στις s και t και άρα το πρόβλημα θα επιλυόταν. Η κατασκευή θα γινόταν βήμα βήμα με πρόβλημα όμως να προκύπτει στο γεγονός ότι ο βαθμός του γράφου θα αυξάνει με μεγάλο ρυθμό, χωρίς να ξέρουμε πότε πρέπει να σταματήσουμε.

Αν με κάποιο τρόπο μπορούσαμε να κρατήσουμε τον βαθμό του γράφου χαμηλά, φέρνοντας ταυτόχρονα 'κοντά' τους επικοινωνούντες κόμβους τότε θα λύναμε και το πρόβλημα σε επιθυμητό χώρο. Αυτό επιτυγχάνεται με την βοήθεια του zig zag γινομένου. Δίνουμε παρακάτω τα βασικά σημεία του αλγορίθμου κάνοντας μια γενική περιγραφή.

Ο αλγόριθμος του Reingold:

1. Δημιουργεί έναν expander της οικογένειας 2.4.2 με κατάλληλα καλό spectral expansion.
2. Μετατρέπει τον γράφο της εισόδου σε ένα κανονικό, μη διμερή γράφο χωρίς να χαλάσει τις αντιστοιχίες ανάμεσα στις συνεκτικές συνιστώσες του. Εχμεταλεύεται έτσι την πρόταση 2.4.1 και δημιουργεί γράφο με που έχει για συνιστώσες (ίσως κακούς) expanders.
3. Εφαρμόζει στους δυο γράφους πράξεις ύψωσης σε δύναμη και zig zag γινομένου και δημιουργεί προκαθορισμένα κανονικό γράφο με καλό spectral expansion (εχμεταλευόμενος το θεώρημα 3.2.1).

4. Επιλύει το πρόβλημα της st -συνεκτικότητας για δύο αντίστοιχους με τους αρχικούς κόμβους του νέου γράφου

Το σημαντικό είναι ότι όλα αυτά τα πετυχαίνει σε λογαριθμικό χώρο! Αυτό φυσικά θα το δείξουμε. Στις επόμενες ενότητες θα παρουσιάσουμε τι ακριβώς κάνει σε κάθε βήμα ο αλγόριθμος δείχνοντας παράλληλα ότι κάθε βήμα μπορεί να γίνει με χρήση λογαριθμικού χώρου. Μετά θα εκμεταλευτούμε την πρόταση 1.2.1 για να συμπεράνουμε ότι όντως ο αλγόριθμος συνολικά χρησιμοποιεί λογαριθμικό χώρο.

4.1 Ένας $(D^{16}, D, 1/2)$ -expander της καλής οικογένειας

Ο αλγόριθμος στο πρώτο βήμα κατασκευάζει έναν καλό expander. Ένας γράφος που κάνει την δουλειά είναι ο $LD_{67,31}$ που σύμφωνα με την πρόταση 2.4.2 είναι ένας $(67^{32}, 67^2, 31/67)$ -expander.

Αυτός ο γράφος μπορεί να είναι μεγάλος αλλά δεν εξαρτάται σε καμία περίπτωση από την είσοδο. Συνεπώς μπορεί να παραχθεί με οποιαδήποτε αναπαράσταση σε χώρο σταθερό και να είναι καθ' όλη την διάρκεια του τρεξίματος του αλγορίθμου σε κάποια από τις ταινίες εργασίας. Άρα κατ' επέκταση λογαριθμικός χώρος αρκεί.

Η επικεφαλίδα της ενότητας μιλά για έναν $(D^{16}, D, 1/2)$ -expander. Είναι αυτός ακριβώς που περιγράψαμε ($31/67 < 1/2$), τον ονομάζουμε H , και το D καθορίζεται να είναι το ακριβώς $D = 67^2 = 4489$. Το D αυτό θα χρησιμοποιείτε και παρακάτω καθόλη την ανάλυση.

4.2 Από τον G στον G_{reg}

Όπως είπαμε στην φάση αυτή πρέπει να μετατραπεί ο γράφος G , N κόμβων, της εισόδου σε ένα μη διμερή κανονικό γράφο G_{reg} . Ο G_{reg} θέλουμε να είναι D^{16} κανονικός και να δίνεται μέσω χάρτη εναλλαγής. Για ορθότητα υποθέτουμε πως ο G μας δίνετε μέσω πίνακα γειτνίασης.

Υπάρχουν αρκετοί τρόποι με τους οποίους εξυπηρετείτε ο σκοπός μας. Ένας, όχι και ο καλύτερος, που παρ' όλα αυτά μας αρκεί είναι να αντικαταστήσουμε κάθε κόμβο του γράφου με ένα κύκλο N κόμβων δημιουργώντας έτσι γράφο με κόμβους το σύνολο $N \times N$. Οι ακμές μεταξύ των κόμβων του G_{reg} θα καθορίζονται από τους κύκλους με επιπλέον ακμές να υπάρχουν μεταξύ των κόμβων (u, w) και (w, u) αν και μόνο αν οι u, w συνδέονται με ακμή στον G . Για να συμπληρωθεί η κανονικότητα προστίθενται επιπλέον self loops. Ο χάρτης

ενναλλαγής του G_{reg} είναι ο $Rot_{G_{reg}} : (N \times N) \times D^{16} \rightarrow (N \times N) \times D^{16}$ που δίνεται από τους κανόνες:

- $Rot_{G_{reg}}((u, w), 1) = ((u, w'), 2)$, με $w' = \begin{cases} w + 1, & w < N \\ 1, & \text{αλλιώς.} \end{cases}$
- $Rot_{G_{reg}}((u, w), 2) = ((u, w'), 1)$, με $w' = \begin{cases} w - 1, & w < N \\ N, & \text{αλλιώς.} \end{cases}$
- $Rot_{G_{reg}}((u, w), 3) = \begin{cases} ((w, u), 3), & \text{αν } (u, w) \text{ ακμή του } G \\ ((u, w), 3), & \text{αλλιώς.} \end{cases}$
- Για $3 < i \leq |D^{16}| : Rot_{G_{reg}}((u, w), i) = ((u, w), i)$

Ο χάρτης ενναλλαγής του $Rot_{G_{reg}}$ μπορεί να υπολογιστεί σε λογαριθμικό χώρο γιατί πολύ απλά, για τις περιπτώσεις ένα και δύο κάνει έναν έλεγχο μιας ισότητας που γίνεται σε λογαριθμικό χώρο, για την τέταρτη περίπτωση δεν χρειάζεται να κάνει τίποτα (αντιγράφει απλά την είσοδο της ερώτησης) ενώ για την τρίτη περίπτωση απλά ανατρέχει στον πίνακα γειτνίασης και χρησιμοποιώντας ίσως λογαριθμικού μήκους μετρητές κοιτάζει για ύπαρξη ακμής ανάμεσα στους δύο κόμβους που χρειάζεται.

Κάτι άλλο που χρειαζόμαστε και εξυπηρετεί αυτή η μετατροπή είναι να μην επηρεάζονται οι συνεκτικές συνιστώσες με την έννοια του ότι δυο κόμβοι s, t συνδέονται στον G αν και μόνο αν οι αντίστοιχοι $s' = (s, s), t' = (t, t)$ συνδέονται στον $Rot_{G_{reg}}$.

- προς την μια κατεύθυνση αν οι s, t συνδέονται, τότε στον G υπάρχει μονοπάτι s, a_1, \dots, a_k, t . Στον G_{reg} τότε, μέσω των κύκλων, θα υπάρχει το μονοπάτι

$$(s, s), (s, a_1), (a_1, s), (a_1, a_2), \dots, (a_{k-1}, a_k), (a_k, a_{k-1}), (a_k, t), (t, a_k), (t, t)$$

- αν αντίστοιχα οι δύο κόμβοι $(s, s), (t, t)$ συνδέονται στον G_{reg} , θα υπάρχει μονοπάτι $(s, s), (a_1, b_1), \dots, (a_k, b_k), (t, t)$. Διπλανοί κόμβοι $(a_m, b_m), (a_{m+1}, b_{m+1})$ στο μονοπάτι ή θα ανήκουν στον ίδιο κύκλο, ή θα είναι $(a_m, b_m) = (b_m, a_m)$. Η δεύτερη περίπτωση ισχύει μόνο όταν στον G υπάρχει η ακμή (a_m, b_m) . Μπορούμε τώρα να δούμε το μονοπάτι σαν ακολουθία διαδοχικών κύκλων. Κάθε κύκλος αντιστοιχεί σε ένα κόμβο του γράφου και λόγω της δεύτερης περίπτωσης δύο κύκλοι συνδέονται μόνο αν οι αντίστοιχοι κόμβοι συνδέονται στον G . Έτσι από το μονοπάτι του G_{reg} παίρνουμε μονοπάτι μεταξύ των κόμβων s και t .

Αυτά τα δύο πρώτα μέρη του αλγορίθμου είναι τα πιο απλά και επιτυγχάνονται σε λογαριθμικό χώρο (όπως εύκολα είδαμε). Παρακάτω θα περάσουμε στο κύριο μέρος του αλγορίθμου που επιλύει το πρόβλημα για τους κόμβους (s, s) και (t, t) του G_{reg} .

4.3 Φουσκώνοντας τον G_{reg}

Δυο κόμβοι ενώνονται με μονοπάτι αν και μόνο αν ανήκουν στην ίδια συνεκτική συνιστώσα του γράφου. Στο κομμάτι αυτό θα δώσουμε έναν τρόπο με τον οποίο κάθε συνεκτική συνιστώσα του γράφου G_{reg} μετατρέπεται σε καλό expander. Αυτό όπως θα δούμε στην επόμενη ενότητα μας διευκολύνει πολύ.

Ο μετασχηματισμός που θα δώσουμε θα δέχεται σαν είσοδο τους δύο γράφους G και H , μέσω των χαρτών εναλλαγής τους και θα δίνει σαν έξοδο έναν γράφο με καλές συνεκτικές συνιστώσες κάνοντας χρήση λογαριθμικού χώρου.

Ορισμός 4.3.1. Έστω G ένας D^{16} -κανονικός γράφος N κόμβων και H ένας D -κανονικός γράφος D^{16} κόμβων. Αν δίνονται μέσω των χαρτών εναλλαγής τους, τότε ο T δίνει σαν έξοδο τον χάρτη εναλλαγής του G_{exp} (του 'φουσκωμένου' G) ως εξής:

- Βρίσκει το μικρότερο l για το οποίο¹ $(1 - 1/DN^2)^{2^l} < 1/2$
- Θέτει $G_0 = G$ και βρίσκει αναδρομικά τους G_i μέσω του κανόνα

$$G_i = (G_{i-1} \tilde{z} H)^8$$

- $G_{exp} = T(G, H) = G_l$.

Ακολουθώντας θα αποδείξουμε κάποιες χρήσιμες για το σκοπό μας ιδιότητες που αφορούν αυτό τον μετασχηματισμό.

Κατ' αρχήν ο μετασχηματισμός αυτός είναι σωστά ορισμένος. Αυτό γιατί κάθε G_i εύκολα αποδεικνύεται ότι είναι D^{16} -κανονικός και άρα το zig zag γινόμενο μπορεί να εφαρμοστεί.

Δεύτερη παρατήρηση είναι ότι αν το D είναι σταθερό (που επιλέγουμε να είναι, τότε το l είναι της τάξης τους $O(\log n)$ (από τον ορισμό του και λόγω του $1 + x \leq e^x$ για $||x|| \leq 1$) και το G_i έχει $poly(N)$ κόμβους (γιατί κάθε G_i αποδεικνύεται αναδρομικά ότι έχει $N \cdot (D^{16})^i$ κόμβους) και άρα οι κόμβοι για να ονομαστούν χρειάζονται $O(\log n)$ χώρο².

¹Μπορούμε εδώ αντί αυτού του l να βρίσκουμε το μικρότερο l για το οποίο $(\sqrt{1 - 1/D^2N^2})^{2^l} < 1/2$ για να είμαστε πιο συμβατοί με αυτά που έχουμε αποδείξει.

²Αν χρησιμοποιήσουμε το εναλλακτικό l που αναφέραμε επίσης με όμοιο σκεπτικό το l είναι της τάξης του $O(\log n)$ και αυτό μας αρκεί.

Το λήμμα που ακολουθεί μας δείχνει πως αν ο H είναι καλός expander, τότε ο μετασχηματισμός μετατρέπει κάθε μη διμερή συνεκτικό γράφο σε καλό expander.

Λήμμα 4.3.1. Έστω G και H είσοδοι του T τέτοιοι ώστε $\lambda(H) \leq 1/2$ και G συνεκτικός και μη διμερής. Τότε $\lambda(T(G, H)) \leq 1/2$

Απόδειξη. Στην αρχικοποίηση έχουμε $G_0 = G$. Επειδή G συνεκτικός και μη διμερής, από την πρόταση³ 2.4.1 έχουμε $\lambda(G_0) \leq 1 - 1/DN^2$.

Ισχυρισμός. Για κάθε $i > 0$, $\lambda(G_i) \leq \max\{\lambda(G_{i-1})^2, 1/2\}$.

Πράγματι ο ισχυρισμός ισχύει. Για απλούστευση των αναπαραστάσεων, έστω $\lambda = \lambda(G_{i-1})$. Από την υπόθεση έχουμε $\lambda(H) \leq 1/2$ και άρα από το πόρισμα 3.2.1 έχουμε

$$\lambda(G_{i-1} \tilde{z} H) \leq 1 - \frac{1}{2}(1 - (\frac{1}{2})^2)(1 - \lambda_1) \leq 1 - \frac{3}{8}(1 - \lambda) < 1 - \frac{1}{3}(1 - \lambda)$$

Από τον ορισμό του G_i και την πρόταση 2.2.1 έχουμε:

$$\lambda(G_i) < \left(1 - \frac{1}{3}(1 - \lambda)\right)^8$$

Θα διακρίνουμε δύο περιπτώσεις σχετικά με το λ

- Αν $\lambda < 1/2$ τότε $\lambda(G_i) < \left(1 - \frac{1}{3}(1 - \lambda)\right)^8 \leq (5/6)^8 < 1/2$
- Αν $\lambda \geq 1/2$ τότε με υπολογισμούς παίρνουμε εύκολα ότι $\left(1 - \frac{1}{3}(1 - \lambda)\right)^4 \leq \lambda$ και άρα $\lambda(G_i) \leq \lambda^2$

Συνεπώς πάντα $\lambda(G_i) \leq \lambda(G_{i-1})^2$ ή $\lambda(G_i) \leq 1/2$ και ο ισχυρισμός αποδεικνύεται.

Από την απόδειξη του ισχυρισμού μπορούμε να ισχυριστούμε κάτι πιο δυνατό:

Ισχυρισμός. Αν για κάποιο $j \geq 0$ ισχύει $\lambda(G_j) < 1/2$ τότε για κάθε $i \geq j$ θα ισχύει $\lambda(G_i) < 1/2$

Ο ισχυρισμός αποδεικνύεται εύκολα με επαγωγή καθώς αν για κάποιο $i \geq j$ ισχύει $\lambda(G_i) < 1/2$ τότε βρισκόμαστε στην πρώτη από τις δύο προηγούμενες περιπτώσεις και άρα $\lambda(G_{i+1}) < 1/2$.

Πλέον μπορούμε εύκολα να αποδείξουμε το λήμμα καθώς

³εναλλακτικά από την ασθενέστερη πρόταση που αποδείξαμε (σελίδα 23) έχουμε $\lambda(G) \leq \sqrt{1 - \frac{1}{d^2 n^2}}$

- αν για κάποιο $0 \leq i < l$ ίσχυε $\lambda(G_i) < 1/2$ τότε και $\lambda(G_l) < 1/2$
- αν δεν ίσχυε για κανένα τέτοιο i , τότε για κάθε $i > 0$ θα είχαμε $\lambda(G_i) \leq \lambda(G_{i-1})^2$. Δεδομένου ότι $\lambda(G_0) \leq 1 - 1/DN^2$ και του καθορισμού το l παίρνουμε τελικά ⁴:

$$\lambda(G_l) \leq \lambda(G_{l-1})^2 \leq \dots \leq \lambda(G_0)^{2^l} \leq (1 - 1/DN^2)^{2^l} < 1/2$$

□

Μέσω αυτού του λήμματος είδαμε ότι θα μπορούσαμε με την βοήθεια ενός καλού H να μετατρέψουμε τον G_{reg} σε ένα G_{exp} με πολύ καλή συνεκτικότητα με την προϋπόθεση όμως ότι ο G_{reg} είναι συνεκτικός. Αυτό σαν ιδέα ακούγεται λίγο χαζό καθώς τότε δεν θα είχε νόημα να ψάχνουμε για τον αν συνδέονται δυο κόμβοι στον G_{reg} . Η ιδέα όμως που κρύβεται πίσω από αυτό το κομμάτι είναι πως όπως θα δούμε ο μετασχηματισμός T μετατρέπει κάθε συνεκτική συνιστώσα του γράφου σε συνεκτική συνιστώσα με καλή συνεκτικότητα. Πριν δούμε το αντίστοιχο λήμμα θα δούμε τυπικά κάποιους συμβολισμούς.

Έστω γράφος G και S ένα υποσύνολο των κόμβων του. Συμβολίζουμε με $G|_S$ τον επαγόμενο από της κορυφές του S υπογράφο του G (τον υπογράφο με σύνολο κόμβων το S και σύνολο ακμών τις ακμές του G που έχουν και τα δυο άκρα τους στο S). Προφανώς αν για κάποιο S οι κόμβοι του $G - G|_S$ και του $G|_S$ δεν έχουν καμία κοινή ακμή τότε και μόνο τότε το σύνολο S αποτελεί συνεκτική συνιστώσα του G .

Λήμμα 4.3.2. Έστω G και H γράφοι σωστής εισόδου του T .

Αν S συνεκτική συνιστώσα του G τότε

$$T(G|_S, H) = T(G, H)|_{S \times (D^{16})^i}$$

Απόδειξη. Έστω S μια συνεκτική συνιστώσα του G . Ονομάζουμε $T_i(G, H)$ τους ενδιάμεσους γράφους G_i του ορισμού 4.3.1. Θα αποδείξουμε με επαγωγή ότι $T_i(G|_S, H) = T_i(G, H)|_{S \times (D^{16})^i}$ και ότι το $S \times (D^{16})^i$ είναι αποκομμένο από τον υπόλοιπο γράφο $T_i(G, H)$.

Στην βάση της επαγωγής, για $i = 0$, έχουμε τετριμμένα το $S \times (D^{16})^0 = S$ να είναι αποκομμένο από τον υπόλοιπο γράφο $T_i(G, H) = G_0$ και παράλληλα

$$T_0(G|_S, H) = G|_S = T_0(G, H)|_S = T_0(G, H)|_{S \times (D^{16})^0}$$

⁴αν ορίζαμε διαφορετικά το l θα είχαμε όμοια $\lambda(G_l) \leq \lambda(G_{l-1})^2 \leq \dots \leq \lambda(G_0)^{2^l} \leq (\sqrt{1 - 1/D^2N^2})^{2^l} < 1/2$ από τον εναλλακτικό ορισμό του l

Στο επαγωγικό βήμα έχουμε σαν υπόθεση ότι για $i = k$: $T_k(G|_S, H) = T_k(G, H)|_{S \times (D^{16})^k}$ και ότι το $S \times (D^{16})^k$ είναι αποκομμένο από τον υπόλοιπο γράφο $T_k(G, H)$. Έστω $G_k = T_k(G, H)$ και $S_k = S \times (D^{16})^k$. Από την επαγωγική υπόθεση το S_k είναι αποκομμένο από τον υπόλοιπο G_k . Έτσι από τον ορισμό του zig zag γινομένου το $S_k \times D^{16}$ είναι αποκομμένο από το υπόλοιπο $G_k \tilde{z} H$ και οι ακμές που αφορούν τους κόμβους του $S_k \times D^{16}$ στον $G_k \tilde{z} H$ είναι ακριβώς όπως στον $G_k|_{S_k \times D^{16}} \tilde{z} H$. Παρόμοια, από τον ορισμό της ύψωσης σε δύναμη έχουμε το $S_k \times D^{16}$ είναι αποκομμένο από τον υπόλοιπο $(G_k \tilde{z} H)^8$ και οι ακμές που αφορούν τους κόμβους του $S_k \times D^{16}$ στον $(G_k \tilde{z} H)^8$ είναι ακριβώς όπως στον $(G_k|_{S_k \times D^{16}} \tilde{z} H)^8$. Έτσι τελικά αποδείχτηκε ότι η υπόθεση ισχύει και για $i = k + 1$.

Άρα και για $i = l$ έχουμε

$$T(G|_S, H) = T(G, H)|_{S \times (D^{16})^l}$$

και αποδεικνύεται το λήμμα. □

Συνδυάζοντας τα λήμματα 4.3.1 και 4.3.2 μπορούμε να δούμε ότι αν ο μετασχηματισμός T εφαρμοστεί στους G_{reg} και H που έχουμε από το προηγούμενο βήμα του αλγορίθμου, τότε κάθε συνεκτική συνιστώσα του παραγόμενου G_{exp} θα έχει $\lambda \leq 1/2$. Αυτό ο αλγόριθμος το εκμεταλεύεται στο τελευταίο βήμα, όπως θα δούμε στην επόμενη ενότητα.

Ένα τελευταίο κομμάτι που μας ενδιαφέρει να δείξουμε είναι πως

Πρόταση 4.3.1. Αν στην είσοδο υπάρχουν οι χάρτες εναλλαγής των G και H τότε χάρτης εναλλαγής του $T(G, H)$ μπορεί να υπολογιστεί με χρήση λογαριθμικού χώρου.

Απόδειξη. Θα δώσουμε λίγο περιγραφικά την απόδειξη εξηγώντας πως μπορεί να λειτουργήσει μια μηχανή και να χρησιμοποιήσει λογαριθμικό χώρο. Στο [Gol08] υπάρχει αναλυτικότερη απόδειξη που ακολουθεί παρόμοια λογική.

Η γενική ιδέα βασίζεται στο γεγονός ότι στην πραγματικότητα κανείς δεν μας ζητά να κατασκευάσουμε όλους τους ενδιάμεσους γράφους. Ο σκοπός είναι για κάθε κόμβο του $T(G, H)$ και ακμή του κόμβου να μπορούμε να υπολογίσουμε σε ποιον καταλήγει. Αποτυπώνουμε σε κάποια ταινία την πληροφορία για τον κόμβο και την ακμή του και αναδρομικά (ταξιδεύοντας μέσα στην πληροφορία) φτάνουμε σε σημείο όπου μπορούμε να υπολογίσουμε κάποια γειτονία.

Κάθε φορά χρειαζόμαστε χώρο για να βρούμε έναν μόνο γείτονα και αυτός ο χώρος είναι λογαριθμικού μήκους και μετά την εύρεση μπορεί να ελευθερώνεται. Παρακάτω μπαίνουμε σε περισσότερες λεπτομέρειες.

Όπως είδαμε πιο πάνω στον μετασχηματισμό $l = O(\log n)$. Έτσι αρκεί να αποδείξουμε ότι $space(G_{i+1}) = space(G_i) + O(1)$, γιατί ο $G_0 = G$ υπάρχει στην είσοδο και άρα τότε ο G_l θα θέλει χώρο $lO(1) + space(G_0) = O(\log n)$.

Χωρίζουμε την απόδειξη σε δύο μέρη.

$space(G_i \tilde{z} H) = space(G_i) + O(1)$: Για κάθε κόμβο, (u, i) και ακμή (a_1, a_2) του $G_i \tilde{z} H$ μας δίνεται το $((u, i), (a_1, a_2))$ και μας ζητείται το

$$Rot_{G_i \tilde{z} H}((u, i), (a_1, a_2)).$$

Κάνουμε συνολικά δύο ερωτήσεις στο Rot_H και μια ερώτηση στο Rot_{G_i} και πηγαίνουμε:

$$Rot_H(i, a_1) = (k_1, b_2) : ((u, i), (a_1, a_2)) \rightarrow ((u, k_1)(b_2, a_2))$$

$$Rot_{G_i}(u, k_1) = (w, k_2) : ((u, k_1)(b_2, a_2)) \rightarrow ((w, k_2), (b_2, a_2))$$

$$Rot_H(k_2, a_2) = (j, b_1) : ((w, k_2), (b_2, a_2)) \rightarrow ((w, j), (b_2, b_1))$$

και τελικά η έξοδος είναι το $((w, j), (b_1, b_2))$.

Την έξοδο (για να μας βγεί ο χώρος) την τυπώνουμε στην ταινία που τυπώσαμε αρχικά την πρώτη πληροφορία, στις θέσεις των κόμβων και των ακμών που μας οδήγησαν εκεί (και με ξεχωριστά ίσως σύμβολα ώστε να ξέρουμε ότι υπολογίστηκαν).

Επειδή το D είναι μια σταθερά που έχουμε προκαθορίσει, ο χώρος που χρειαζόμαστε για τις δύο ερωτήσεις στον Rot_H και ο χώρος των μετρητών για το πέρασμα $((u, i), (a_1, a_2)) \rightarrow ((u, k_1)(b_2, a_2))$ και $((w, k_2), (b_2, a_2)) \rightarrow ((w, j), (b_2, b_1))$, μπορεί να θεωρηθεί σταθερός, καθώς η απάντηση στις ερωτήσεις υπάρχει στην είσοδο και μόνο τα u, w εξαρτώνται από το n που εδώ δεν τα πειράζουμε.

Στο ενδιάμεσο βήμα χρειαζόμαστε $space(G_i)$ χώρο για την ερώτηση στον Rot_{G_i} και κάποιον χώρο πάλι για μετρητές για το πέρασμα $((u, k_1)(b_2, a_2)) \rightarrow ((w, k_2), (b_2, a_2))$. Αυτός ο μετρητής είναι της τάξης του $O(\log n)$ όσος και τα u, w (όπως είδαμε στην αρχή της ανάλυσης του μετασχηματισμού). Όμως αν δούμε μέσα στον $space(G_i)$, θα βρούμε κάποιον αντίστοιχο χώρο που χρησιμοποιήθηκε για την εύρεση του G_i από τον G_{i-1} . Αυτός ο χώρος μετά την εύρεση του G_i ελευθερώνεται και μπορεί να χρησιμοποιηθεί. Αν τον αυξήσουμε κατά $poly(D)$ θα μπορεί να χρησιμοποιηθεί για μέτρημα μέχρι τα u, w (που χρειαζόμαστε για το πέρασμα). Αυτό γιατί τα u, w σε σχέση με τα αντίστοιχα τους στο προηγούμενο βήμα ($G_{i-1} \rightarrow G_i$) είναι κατά $poly(D)$ μεγαλύτερα. Βέβαια το $poly(D)$ είναι μια σταθερά.

Έτσι τελικά $space(G_i \tilde{z} H) = space(G_i) + O(1)$.

$space(G_{i+1}) = space(G_i \tilde{z}H) + O(1)$: Από τον ορισμό του μετασχηματισμού έχουμε: $space(G_{i+1}) = space((G_i \tilde{z}H)^8)$. Για κάθε κόμβο και ακμή του G_{i+1} μας δίνεται το $(u, (i_1, \dots, i_8))$ και μας ζητείται το $Rot_{G_{i+1}}(u, (i_1, \dots, i_8))$.

- Από το $(u, (i_1, \dots, i_8))$ πηγαίνουμε μέσω του $Rot_{G_i \tilde{z}H}$ στο $(w_1, (j_1, i_2, \dots, i_8))$ με ερώτηση στο $Rot_{G_i \tilde{z}H}$: $Rot_{G_i \tilde{z}H}(u, i_1) = (w_1, j_1)$.
- Από το $(w_1, (j_1, i_2, \dots, i_8))$ πηγαίνουμε μέσω του $Rot_{G_i \tilde{z}H}$ στο $(w_2, (j_1, j_2, i_3, \dots, i_8))$ με ερώτηση στο $Rot_{G_i \tilde{z}H}$: $Rot_{G_i \tilde{z}H}(w_1, i_2) = (w_2, j_2)$.
- ...
- Από το $(w_7, (j_1, \dots, j_7, i_8))$ πηγαίνουμε μέσω του $Rot_{G_i \tilde{z}H}$ στο $(v, (j_1, \dots, j_8))$ με ερώτηση στο $Rot_{G_i \tilde{z}H}$: $Rot_{G_i \tilde{z}H}(w_7, i_8) = (v, j_8)$.

Τέλος αντιστρέφουμε τα j_1, \dots, j_8 και έχουμε τελικά σαν έξοδο το $(v, (j_8, \dots, j_1))$ που είναι όντως $Rot_{G_i \tilde{z}H}(u, (i_1, \dots, i_8)) = (v, (j_8, \dots, j_1))$.

Εδώ, πάλι, την έξοδο την τυπώνουμε στην ταινία που τυπώσαμε αρχικά την πρώτη πληροφορία, στις θέσεις των κόμβων και των ακμών που μας οδήγησαν εκεί.

Σε κάθε ένα από τα 8 βήματα που περιγράφουμε μπορούμε να χρησιμοποιούμε τον ίδιο χώρο. Όμοια με πριν ο χώρος που χρειάζεται για την αναπαράσταση των u, w_1, \dots, w_7, v στον προσδιορισμό του G_{i+1} είναι κατα μια σταθερά μεγαλύτερος από αυτόν που χρησιμοποιείται για τον προσδιορισμό του G_i .

Έτσι τελικά $space((G_i \tilde{z}H)^8) = space(G_i \tilde{z}H) + O(1)$.

Συνδυάζοντας τα δύο αποτελέσματα έχουμε

$$space(G_{i+1}) = space(G_i \tilde{z}H) + O(1) = space(G_i) + 2O(1) = space(G_i) + O(1)$$

Άρα και

$$space(G_l) = space(G_0) + lO(1) = O(\log n)$$

□

Αφού ο μετασχηματισμός T έχει τις ωραίες ιδιότητες που είδαμε πιο πάνω, τον εκμεταλευόμαστε και από τους H και G_{reg} των βημάτων 1 και 2 του αλγορίθμου δημιουργούμε τον $G_{exp} = T(G_{reg}, H)$.

Στο βήμα 2 ανάγαμε το πρόβλημα της st -συνεκτικότητας στον G στο πρόβλημα της $s't'$ -συνεκτικότητας στον G_{reg} . Στο τρίτο αυτό βήμα που βρισκόμαστε ανάγουμε την $s't'$ -συνεκτικότητα στον G_{reg} στην $s''t''$ -συνεκτικότητα στον G_{exp} με $s'' = (s, a_1, \dots, a_l)$, με $a_i \in D^{16}$ και $t'' = (t, b_1, \dots, b_l)$, με $b_i \in D^{16}$.

Η ισοδυναμία στα δύο προβλήματα προκύπτει εύκολα από το λήμμα 4.3.2 και την απόδειξή του.

Τα βήματα 1 και 2 δείξαμε νωρίτερα ότι μπορούν να γίνουν σε λογαριθμικό χώρο. Αυτά παράγουν την είσοδο του μετασχηματισμού T ο οποίος όταν τα έχει στην είσοδό του επίσης εξάγει τον G_{exp} σε λογαριθμικό χώρο. Από την πρόταση 1.2.1 έχουμε ότι ο G_{exp} μπορεί να παραχθεί από την αρχική είσοδο σε λογαριθμικό χώρο. Επίσης εύκολα μπορούν να παραχθούν σε λογαριθμικό χώρο τα s'', t'' απλά προσθέτοντας συνολικά $O(\log n)$ χώρο δίπλα από τα s', t' , απαιτώντας συνολικά $O(\log n)$ χώρο για την αναπαράστασή τους και άρα δυνατότητα φύλαξής τους σε μια ταινία εργασίας με χρήση λογαριθμικού χώρου.

Από όλα τα προηγούμενα διαπιστώνουμε ότι το αρχικό πρόβλημα συνεκτικότητας το ανάγαμε, σε λογαριθμικό χώρο, σε πρόβλημα συνεκτικότητας σε ένα γράφο με πολύ καλό expansion στις συνιστώσες του. Στην επόμενη ενότητα θα δούμε ένα τρόπο επίλυσης του προβλήματος σε γράφους με όμοιο με το παραπάνω, καλό expansion.

4.4 Το πρόβλημα σε (καλούς) expander γράφους είναι (πιο) εύκολο

Με τον όρο καλός γράφος G εδώ εννοούμε ότι είναι $\lambda(G) \leq 1/2$. Από το θεώρημα 2.3.1 έχουμε:

Πόρισμα 4.4.1. Αν G γράφος n κόμβων με $\lambda(G) \leq 1/2$, τότε κάθε δύο κόμβοι του γράφου συνδέονται με μονοπάτι μήκους το πολύ $2 \log_{8/5} \frac{n}{2} + 2$

Απόδειξη. Έστω s, t δύο τυχαίοι κόμβοι του G . Το μονοσύνολο $a_0 = \{s\}$, από το θεώρημα 2.3.1 για $a = 1/2$ θα έχει τουλάχιστον $\frac{1}{(1/2)(1/2)^2+1/2}|a_0| = 8/5$ γείτονες. Έστω a_1 αυτό το σύνολο. Με την σειρά του, αυτό θα έχει $(8/5)|a_1| \geq (8/5)^2|a_0|$ γείτονες, το σύνολο a_2 . Συνεχίζουμε ομοιτρόπως μέχρι να φτάσουμε σε κάποιο a_k που να έχει γείτονες περισσότερους από τους μισούς κόμβους του γράφου. Από την κατασκευή των a_k θα είναι $|a_k| \geq (8/5)^k|a_0| = (8/5)^k$. Έτσι

$$\frac{n}{2} \geq |a_k| \geq (8/5)^k \Rightarrow k \leq \log_{8/5} \frac{n}{2}$$

Αν ξεκινήσουμε από το s και πάρουμε όλα τα μονοπάτια μήκους $k + 1$ θα επισκεφτούμε τουλάχιστον τους μισούς από τους κόμβους του γράφου. Με ίδια ανάλυση αν ξεκινήσουμε από το t θα επισκεφτούμε επίσης τουλάχιστον τους μισούς κόμβους. Συνεπώς θα υπάρχει κόμβος που θα τον επισκεφτούμε και από τον s και από τον t , με μονοπάτια μήκους $k + 1$. Άρα οι s, t θα συνδέονται σίγουρα με μονοπάτι μήκους $\leq 2(k + 1) \leq 2 \log_{8/5} \frac{n}{2} + 2$. \square

Το πρόβλημα της st -συνεκτικότητας σε τέτοιους γράφους, λόγω του προηγούμενου πορίσματος, δεν θα απαιτούσε πολύ χώρο αν μπορούσαμε σε λίγο χώρο να ελέγξουμε όλα τα μονοπάτια που ξεκινούν από τον s (ή τον t) μήκους $2 \log_{\frac{d}{2}} \frac{n}{2} + 2$.

Αν ο γράφος μας είναι d -κανονικός τότε όλα τα μονοπάτια μήκους $2 \log_{\frac{d}{2}} \frac{n}{2} + 2$ θα μπορούσαν να περιγραφούν σε χώρο $\log d (2 \log_{\frac{d}{2}} \frac{n}{2} + 2)$ απλά ονομάζοντας κάθε μια από τις ακμές του μονοπατιού σε χώρο $\log d$. Επιπλέον στην περίπτωση που μας ενδιαφέρει το d είναι σταθερό. Η ιδέα για την επίλυση του προβλήματος είναι να απαριθμούμε ένα ένα τα μονοπάτια από τον s , μέσω των "ονομάτων" των ακμών, μέχρι είτε να βρούμε σε κάποιο από αυτά το t και να απαντήσουμε ναι, είτε να μην το βρούμε σε κανένα έχοντας ελέγξει όλα τα $d^{2 \log_{\frac{d}{2}} \frac{n}{2} + 2}$ μονοπάτια, απαντώντας όχι.

Πρόταση 4.4.1. Έστω G d -κανονικός γράφος n κορυφών, που δίνεται μέσω χάρτη εναλλαγής. Υπάρχει αλγόριθμος που για κάθε k χρησιμοποιεί χώρο $O(\log d \cdot k)$ και δίνει όλους τους κόμβους που απέχουν απόσταση το πολύ k από ένα κόμβο εκκίνησης έστω s .

Απόδειξη. Ο αλγόριθμος εκμεταλεύεται αυτά που είπαμε νωρίτερα. Έστω κάποιο k . Δεδομένου αυτού του k κρατά k το πλήθος μετρητές οι οποίοι ονομάζουν ακμές κορυφών και άρα έχουν μεγεθος το πολύ $\log d$.

Ο αλγόριθμος ξεκινά από τον t , παίρνει την ακμή που του υποδεικνύει ο πρώτος μετρητής, και μέσω του χάρτη εναλλαγής πηγαίνει στον s_1 τον οποίο και γράφει στην έξοδο. Ακολούθως ακολουθεί την ακμή που του υποδεικνύει ο δεύτερος μετρητής και πηγαίνει στον s_2 τον οποίο επίσης και γράφει στην έξοδο. Όμοια φτάνει μέχρι τον s_k , γράφοντας τον στην έξοδο και έχοντας γράψει τελικά όλους τους κόμβους του μονοπατιού που του υποδεικνύουν οι μετρητές.

Στην συνέχεια αυξάνει τον τελευταίο μετρητή κατά 1 δημιουργώντας καινούριο μονοπάτι. Αν ο τελευταίος μετρητής δείχνει αριθμό μεγαλύτερο από d , τότε τον μηδενίζει και αυξάνει κατά 1 τον αμέσως προηγούμενο του και αν κι αυτός δείχνει αριθμό μεγαλύτερο από d πράττει όμοια μέχρι να βρεί κάποιον που έχει περιθώρια και δημιουργεί καινούριο μονοπάτι. Για τις καινούριες τιμές των μετρητών, όμοια με προηγουμένως, ακολουθεί την πορεία του μονοπατιού από τον t στα s_1, \dots, s_k γράφοντας κάθε κόμβο του μονοπατιού στην έξοδο. Αν σε κάποια φάση δεν μπορεί να αυξήσει κανένα μετρητή (γιατί όλοι ξεπερνούν το d) τότε σταματά γιατί έχει ακολουθήσει όλα τα $d^{2 \log_{\frac{d}{2}} \frac{n}{2} + 2}$ μονοπάτια.

Ο αλγόριθμος συνεπώς αποτυπώνει στην έξοδο όλους τους κόμβους όλων των μονοπατιών μήκους k που ξεκινούν από τον t , χρησιμοποιώντας $O(\log d \cdot k)$ χώρο. \square

Είναι ξεκάθαρο τώρα τι θα κάνουμε. Θα εφαρμόσουμε τον αλγόριθμο στον γράφο G_{exp} με κόμβο εκκίνησης τον s'' και $k = 2 \log_{\frac{8}{5}} \frac{n}{2} + 2$. Έτσι αν οι s'' και t'' συνδέονται με μονοπάτι ο αλγόριθμος που παρουσιάσαμε εδώ θα τυπώσει τον t'' στην έξοδο σε κάποια θέση ενώ αν δεν συνδέονται δεν θα τον τυπώσει. Έτσι λύνουμε το πρόβλημα της $s''t''$ -συνεκτικότητας στον G_{exp} και άρα και της st -συνεκτικότητας στον αρχικό γράφο G .

Σε λογαριθμικό χώρο, από την (αρχική) είσοδο των s, t, G , δίνουμε μέσω των βημάτων 1,2,3 την έξοδο s'', t'', G_{exp} . Αυτό αποτελεί είσοδο του αλγορίθμου που δώσαμε εδώ. Αυτός με τη σειρά του αν δεχτεί αυτή την είσοδο, θα χρειαστεί όπως είδαμε χώρο $O(\log D^{16} \cdot k) = O(\log n)$ (γιατί D σταθερά και $k = O(\log n)$). Χρησιμοποιώντας την πρόταση 1.2.1 καταλήγουμε ότι το αρχικό πρόβλημα της st -συνεκτικότητας μπορεί να υπολογιστεί σε λογαριθμικό χώρο. Έτσι αποδεικνύεται το

Θεώρημα 4.4.1. $USTCON \in L$.

Στο επόμενο κεφάλαιο θα μιλήσουμε λίγο για τις συνέπειες που προκύπτουν από αυτό το σημαντικότατο αποτέλεσμα, ολοκληρώνοντας έτσι την εργασία.

Κεφάλαιο 5

Περί πολυπλοκότητας

Άμεσες συνέπειες

Στην εισαγωγή (υπο)δείξαμε γιατί το *USTCON* πρόβλημα είναι *SL*-πλήρες. Μια πρώτη άμεση συνέπεια λοιπόν είναι το

Θεώρημα 1. $L = SL$.

Μια επίσης άμεση συνέπεια είναι πως το πρόβλημα της συνεκτικότητας ενός γράφου ανήκει στο *L*. Αυτό γιατί με δυο μετρητές λογαριθμικού μήκους μπορούμε βήμα βήμα να δημιουργήσουμε όλα τα δυνατά ζευγάρια κόμβων και σε λογαριθμικό χώρο σε κάθε βήμα να λύνουμε το πρόβλημα της συνεκτικότητας του εκάστοτε ζευγαριού. Έτσι

Θεώρημα 2. $Connectivity \in L$

Λόγω της *SL*-πληρότητας του *USTCON* προβλήματος και του θεωρήματος 1 έχουμε

Θεώρημα 3. $A \in L \Rightarrow A$ αναγεται στο *USTCON*

Αυτό το θεώρημα χρησιμεύει κυρίως από την αντιθετοαντίστροφη πλευρά του, για να αποδείξουμε ότι ένα πρόβλημα δεν ανήκει στο *L*.

Κοιτώντας βαθύτερα

Το *USTCON* αποτελούσε και αποτελεί ένα από τα σημαντικά (και πρώτα ως προς την απόδειξή τους) προβλήματα που ανήκουν στο *RL*.

Ένας αλγόριθμος που το επιλύει σε λογαριθμικό χώρο και το τοποθετεί σε αυτή την κλάση είναι αυτός που δόθηκε στο [AKL⁺79]. Η ιδέα είναι: Από τον κόμβο που βρισκόμαστε επιλέγουμε τυχαία έναν γειτονικό του κόμβο κάνοντας έναν πολυωνυμικού μήκους τυχαίο περίπατο. Αν υπάρχει μονοπάτι τότε αποδεικνύεται ότι ένα τυχαίο μονοπάτι μήκους $O(|V| \cdot |E|) = O(n^3)$ που ξεκινά

από τον ένα κόμβο θα επισκεφτεί τον άλλο κόμβο με πιθανότητα τουλάχιστον $1/2$.

Αμέσως μετά την εμφάνιση του παραπάνω αλγορίθμου, έγιναν προσπάθειες αποτυχαιοποίησής του με όσο το δυνατόν λιγότερο κόστος σε χώρο. Σαν παράλληλο ή και απώτερο στόχο αυτές οι προσπάθειες είχαν να δώσουν μια ώθηση στην απάντηση του ερωτήματος $L \stackrel{?}{=} RL$, ενός από τα σημαντικότερα ερωτήματα στην θεωρία πολυπλοκότητας. Παραπέμπουμε στα [SZ95] [ATSWZ97] για λεπτομέρειες.

Βασικό ερώτημα αποτελεί κατά πόσο το αποτέλεσμα που παρουσιάσαμε εδώ μπορεί να χρησιμοποιηθεί στις προσπάθειες απάντησης του παραπάνω ερωτήματος, είτε αυτό καθαυτό, είτε οι τεχνικές για την απόδειξή του.

Πρώτες προσπάθειες αμέσως μετά το αποτέλεσμα του Reingold έγιναν στα [RTV06] και [RV05] όπου στο δεύτερο σε αντίθεση με την ιδέα που παρουσιάστηκε εδώ (αυξάνουμε το expansion, κρατάμε σταθερό το βαθμό κανονικότητας, αυξάνουμε 'λίγο' το μέγεθος του γράφου), υλοποιείται μια ιδέα της μορφής: βελτιώνουμε το expansion, κρατάμε σταθερό το μέγεθος, αυξάνουμε 'λίγο' το βαθμό κανονικότητας.

Η υλοποίηση της ιδέας βελτιώνει τα γνωστά αποτελέσματα για το $USTCON$ και δίνει μια ώθηση στο ερώτημα $L \stackrel{?}{=} RL$ αφήνοντας παρ' όλα αυτά πολύ χώρο για πρόοδο. Η εικόνα μετά την δημοσίευση του Reingold έχει κάπως έτσι

$$L = SL \subseteq RL \subseteq NL \subseteq L^2$$

με σημεία ανοικτά για έρευνα και επαναπροσδιορισμό ικανά να της προκαλέσουν σημαντικές αλλαγές.

Bibliography

- [AKL⁺79] Romas Aleliunas, Richard M. Karp, Richard J. Lipton, Laszlo Lovasz, and Charles Rackoff. Random walks, universal traversal sequences, and the complexity of maze problems. In *SFCS '79: Proceedings of the 20th Annual Symposium on Foundations of Computer Science (sfcs 1979)*, pages 218–223, Washington, DC, USA, 1979. IEEE Computer Society.
- [AR94] Noga Alon and Yuval Roichman. Random cayley graphs and expanders. *Random Structures Algorithms*, 5:271–284, 1994.
- [AS00] Noga Alon and Benny Sudakov. Bipartite subgraphs and the smallest eigenvalue. *Combinatorics, Probability & Computing*, 9:1–12, 2000.
- [ATSWZ97] Roy Armoni, Amnon Ta-Shma, Avi Wigderson, and Shiyu Zhou. $SI \subseteq 14/3$. In *STOC '97: Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pages 230–239, New York, NY, USA, 1997. ACM.
- [BAA⁺] J. Combinatorial Theory B, N. Alon, S. Arora, C. Lund, R. Motwani, M. Sudan, M. Szegedy Proof Verification, and Hardness Of. [2] n. alon: Eigenvalues and expanders, *combinatorica* 6(1986), 83•96.
- [Gol08] Oded Goldreich. *Computational Complexity: A Conceptual Perspective*. Cambridge University Press, 1 edition, April 2008.
- [Gre96] Raymond Greenlaw. A compendium of problems complete for symmetric logarithmic space. *Computational Complexity*, 9:2000, 1996.
- [HLWO06] Shlomo Hoory, Nathan Linial, Avi Wigderson, and An Overview. Expander graphs and their applications. *Bull. AMS*, 43:439–561, 2006.

- [LE93] L. Lov and Of Paul Erdos. Random walks on graphs: A survey, 1993.
- [Lov93] Laszlo Lovász. *Combinatorial Problems and Exercises: Problem 11.29*. Elsevier North-Holland, 1993.
- [LP82] Harry R. Lewis and Christos H. Papadimitriou. Symmetric space-bounded computation. *Theor. Comput. Sci.*, 19:161–187, 1982.
- [Pap94] Christos H. Papadimitriou. *Computational Complexity*. Addison Wesley Longman, 1994.
- [Rei05] Omer Reingold. Undirected st-connectivity in log-space. In *STOC '05: Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, pages 376–385, New York, NY, USA, 2005. ACM.
- [Rei08] Omer Reingold. Undirected connectivity in log-space. *J. ACM*, 55(4):1–24, 2008.
- [RTV06] Omer Reingold, Luca Trevisan, and Salil Vadhan. Pseudorandom walks on regular digraphs and the rl vs. l problem. In *STOC '06: Proceedings of the thirty-eighth annual ACM symposium on Theory of computing*, pages 457–466, New York, NY, USA, 2006. ACM.
- [RV05] Eyal Rozenman and Salil Vadhan. Derandomized squaring of graphs. In *In Proceedings of the 8th International Workshop on Randomization and Computation (RANDOM)*, pages 436–447. Springer, 2005.
- [RVW00] Omer Reingold, Salil Vadhan, and Avi Wigderson. Entropy waves, the zig-zag graph product, and new constant-degree expanders and extractors. *Annals of Mathematics*, 155:3–13, 2000.
- [SeN93] SeNaor. Probabilistic methods in computer science (course notes), 1993.
- [SZ95] M. Saks and S. Zhou. $Rspace(s) \subseteq dspace(s^{3/2})$. In *FOCS '95: Proceedings of the 36th Annual Symposium on Foundations of Computer Science (FOCS'95)*, page 344, Washington, DC, USA, 1995. IEEE Computer Society.