REU 2022 témák

2022. március 27.

1. Klasszikus és kvantumos bolyongások

Legyen $G = (V, E)$ egy irányítatlan $|V| = n$ csúcsú gráf. Definiálhatunk egy véletlen bolyongást a gráf csúcsain a következő szabály szerint: az aktuális pontból válasszunk egy véletlen élet és annak mentén lépjünk a következő csúcsra. Ennek a bolyongásnak az átmenti mátrixa $P \in \mathbb{R}^{n\times n}$, ahol $P_{uv} = \frac{1}{\deg(v)}$ ha $uv \in E$ és 0 egyébként. A bolyongás k lépésének átmeneti mátrixa értelemszerűen P^k.

Szegedy Márió konstruált minden ilyen P bolyongáshoz egy kvantumos bolyongást ami bizonyos szempontból kvadratikusan gyorsabban konvergál mint P [Szeg04]. Ma már értjük [AGJK20], hogy ennek a kvantumos bolyongásnak k lépését lényegében a $T_k(P)$ mátrix írja le, ahol T_k a k-dik Csebisev polinom. ($T_k(x) = \cos(k \cdot \arccos(x))$, ami egész k estén egy $|k|$ fokú polinom, $T_k(P)$-t pedig úgy kell érteni, hogy x^i helyébe P^i-t helyettesítünk.)

A kvantumos bolyongások megértése kapcsán tehát fontos megérteni a $T_k(P)$ alakú mátrixok viselkedését. Egy nagyon konkrét kérdés amiknek a megválaszolása jobb megértését adná bizonyos kvantumos algoritmusoknak:

- Vegyünk egy (páros) n csúcsú utat, amely minden élének súlya $\sqrt{2}/3$, kivéve a középső él aminek a súlya $2/3$, illetve a végpontokban van egy-egy $1/3$ súlyú hurokél. Ennek az élsúlyozott gráfnak az A adjacencia mátrixa bizonyos értemben két összeragasztott bináris fán való bolyongást ír le [CCD+03]. A szimulációk azt mutatják, hogy ha az egyik végpontból indulunk akkor $k = \mathcal{O}(n)$ lépés után nagy valószínűséggel átjutunk a túloldalra, vagyis $T_k(A)$ jobb felső sarkában egy konstans nagy szám található. Ez még nincs rendesen bebizonyítva, csak n nagyobb hatványára és kis valószínűséggel, és egy kicsit másik gráfra. Ebben a formában a kérdést szerintem más még nem vizsgálta.

Egy másik, kvantumos relevanciájú, de teljesen klasszikus kérdés:

- Legyen $M \subseteq V$ egy csúcshalmaz ami a csúcsok legfeljebb 1/9-ed részét tartalmazza. Igaz-e, hogy ha egy reguláris (súlyozatlan) gráfon bolyongunk $\overline{M} := V \setminus M$ egy uniform véletlen pontjából indulva, és T a várható lépésszám mielőtt eljutunk egy M-beli csúcsba, akkor mindig van olyan t érték hogy M csúcsain átlagosan t ideig várva a bolyongás úgy módosul, hogy $\mathcal{O}(T)$ lépés után nagy valószínűséggel M-beli

csúcson leszünk, majd újabb $\mathcal{O}(T)$ lépés után nagy valószínűséggel $\overline{M}$-beli csúcsban leszünk? Az állítás csak $\sim 1/\log(T)$ valószínűséggel ismert [AGJK20], de nem tudunk ellenpéldáról.

Vannak még kapcsolódó érdekes kérdések, csak azokhoz kicsi hosszabb bevezető dukál.

2. Strukturált unitér mátrixszorzatok által generált polinomok

Az elmúlt években kiderült, hogy a következő alakú mátrixszorzatok:

$$U_0 W U_1 W U_2 W \cdots W U_k,$$

ahol $W = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$ és $U_i \in \mathbb{C}^{2\times 2}$, vizsgálatával rengeteg kvantumos algoritmus sokkal jobban megérthető és egyszerűbben leírható [GSLW18]. (Intuitíve érdemes ω-ra mint a $\mathbb{T}$ komplex egységkörön mozgó változóra gondolni.)

Az ilyen alakú mátrixok karakterizációja ezért nagy áttörést hozott a kvantumos algoritmusok fejlesztésének terén. A fenti alakú mátrixok mint kiderült pontosan azok a 2×2-es mátrix értékű $L(\omega)$ Laurent polinomok, amik legfeljebb k-ad fokúak ω-ban, mint ω-beli függvények a paritásuk megegyezik k-ával, és minden $\omega \in \mathbb{T}$ értékre egy unitér mátrixot írnak le [Haa19, Theorem 2].

Ennek kapcsán több nyitott kérdés is van. Egy a feltételeknek megfelelő Laurent polinom esetén hogyan tudjuk megtalálni az $U_0, U_1, U_2, \ldots, U_k$ sorozatot hatékonyan? Vannak egészen jó algoritmusok [CDG+20] amik $\sim k^3$ időben futnak, de még jobbakat szeretnénk.

Természetes és a kvantumos algoritmusok szempontjából is érdekes kérdés, hogy mi történik, ha például $W = \begin{pmatrix} \omega_1 & 0 \\ 0 & \omega_2 \end{pmatrix}$ alakú? Vagy esetleg 4×4-es mátrixokat vizsgálunk, és $W = \begin{pmatrix} \omega_1 & 0 & 0 & 0 \\ 0 & \omega_1^{-1} & 0 & 0 \\ 0 & 0 & \omega_2 & 0 \\ 0 & 0 & 0 & \omega_2^{-1} \end{pmatrix}$. Tudunk jó karakterizációt adni az így előálló mátrix értékű (Laurent) polinomokra?

Hivatkozások

[AGJK20] Andris Ambainis, András Gilyén, Stacey Jeffery, and Martins Kokainis. Quadratic speedup for finding marked vertices by quantum walks. In *Proceedings of the 52nd ACM Symposium on the Theory of Computing (STOC)*, page 412–424, 2020. arXiv: 1903.07493

[CCD+03] Andrew M. Childs, Richard Cleve, Enrico Deotto, Edward Farhi, Sam Gutmann, and Daniel A. Spielman. Exponential algorithmic speedup by a quantum

walk. In *Proceedings of the 35th ACM Symposium on the Theory of Computing (STOC)*, pages 59–68, 2003. arXiv: quant-ph/0209131

[CDG+20] Rui Chao, Dawei Ding, András Gilyén, Cupjin Huang, and Mário Szegedy. Finding angles for quantum signal processing with machine precision. arXiv: 2003.02831, 2020.

[GSLW18] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. Quantum singular value transformation and beyond: Exponential improvements for quantum matrix arithmetics [full version], 2018. arXiv: 1806.01838

[Haa19] Jeongwan Haah. Product Decomposition of Periodic Functions in Quantum Signal Processing. *Quantum*, 3:190, 2019. arXiv: 1806.10236

[Szeg04] Mário Szegedy. Quantum speed-up of Markov chain based algorithms. In *Proceedings of the 45th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 32–41, 2004. arXiv: quant-ph/0401053

3. Lokális algoritmusok, játékok és Borel kombinatorika

Az elosztott számítás Linial-féle modelljében [6] egy nagy gráfon akarunk megoldani valamilyen gráfelméleti problémát. Mindegyik csúcsban egy számítógép van, amely a szomszédainak tud üzenetet küldeni, és rendelkezik egy egyedi azonosítóval. A számítás körökre van osztva, egy körben a számítógépek üzenetet küldhetnek a szomszédaiknak és végezhetnek valamilyen számítást. Mindegyik számítógépen ugyanaz az algoritmus fut. A számítás hosszára vagy az üzenetek nagyságára nem teszünk megszorítást, a cél a probléma megoldása a lehető legkevesebb körben. Egy, ezeknek a feltételeknek megfelelő (t-körig futó) algoritmust, (t-körű) *lokális algoritmusnak* nevezünk. Könnyű belátni például a következőt:

1. Állítás. *Legyen G egy N hosszú út. Ekkor, nincs olyan lokális algoritmus, amely $< \frac{N}{10}$ körben 2-színezné G-t.*

Meglepő módon, utak 3-színezésére létezik $\ll N$ körben futó algoritmus [5]; valójában $\log^* N$ lépés elérhető, ahol $\log^*$ az iterált logaritmus függvény. Nevezzük ezeket az algoritmusokat *gyorsnak*.

A célunk lokális algoritmusok vizsgálata d-reguláris fákon (pontosabban olyan véges fákon, melyek minden csúcsa vagy d vagy 1 fokú, és az 1-fokú csúcsokon nem kell megoldanunk a problémát). Az alábbi egy klasszikus, nemtriviális tétel (lásd pl. [2]).

1. Tétel. *Legyen $d \geq 2$. Létezik gyors lokális algoritmus, mely d-reguláris fákat $d+1$ színnel színez, de nincs olyan gyors lokális algoritmus, mely d színnel színezne.*

Egy nemrégi gyönyörű észrevétel [4, 1], hogy konkrét összefüggés építhető ki a fenti modell és a halmazelméletben vizsgált végtelen gráfok viselkedése között. Kiderül például,

hogy a tétel következik egy, a halmazelméletben felfedezett mély technikából [7, 3]: játékok segítségével kizárható a gyors algoritmusok létezése.

A fő cél, hogy megértsük, pontosan mit adnak ezek a játékok. A szokásos gráf színezési probléma általánosítása a H-színezési probléma: adott H gráfra találjunk homomorfizmust G-ből H-ba. Egy természetes tesztkérdés tehát az alábbi:

1. Kérdés. *Karakterizáljuk azon H véges gráfokat, melyekre létezik a d-reguláris fákat H-színező gyors lokális algoritmus!*

Egy gráf csúcsainak két színosztályra való osztását *barátságtalan színezésnek* nevezzük, ha minden csúcsnak több tőle különböző színű szomszédja van, mint vele azonos színű. Egy másik érdekes tesztkérdés, ami várhatóan egy régóta megoldatlan problémára is választ adna a következő:

2. Kérdés. *Bizonyítsuk játékkal, hogy nincs gyors algoritmus, amely 3-reguláris fáknak barátságtalan színezését adja meg.*

Hivatkozások

[1] A. Bernshteyn. Probabilistic constructions in continuous combinatorics and a bridge to distributed algorithms. *arXiv preprint arXiv:2102.08797*, 2021.

[2] S. Brandt. An automatic speedup theorem for distributed problems. In *Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing*, pages 379–388, 2019.

[3] S. Brandt, Y.-J. Chang, J. Grebík, C. Grunau, V. Rozhoň, and Z. Vidnyánszky. On homomorphism graphs. *arXiv preprint arXiv:2111.03683*, 2021.

[4] G. Elek. Qualitative graph limit theory. cantor dynamical systems and constant-time distributed algorithms. *arXiv preprint arXiv:1812.07511*, 2018.

[5] F. Kuhn and R. Wattenhofer. On the complexity of distributed graph coloring. In *Proceedings of the twenty-fifth annual ACM symposium on Principles of distributed computing*, pages 7–15. ACM, 2006.

[6] N. Linial. Locality in distributed graph algorithms. *SIAM J. Comput.*, 21(1):193–201, 1992.

[7] A. S. Marks. A determinacy approach to Borel combinatorics. *J. Amer. Math. Soc.*, 29(2):579–600, 2016.

4. Nagy véletlen gráfok

A véletlen gráfok meglepő tulajdonságokkal bírnak. Például vegyünk egy $n \to \infty$ csúcsú véletlen gráfot, amiben minden csúcs fokszáma 10, és kérdezzük meg, hogy mekkora benne a maximális független csúcshalmaz mérete (a legnagyobb olyan csúcshalmaz, ami az üres gráfot feszíti). Majd tegyük fel ugyanezt a kérdést 10 helyett 100-as fokszámra. Kevesen gondolnák, hogy ez két külön probléma lenne. Pedig ez olyasmi, mint hogy kiszámolni a víz sűrűségét +20°C-on vagy +50°C-on (100 kPa nyomáson) szinte ugyanolyan a feladat, de -50°C-on már teljesen más, mert közben a víz megfagy, és a legtöbb tulajdonsága megváltozik. Hasonlóan „fagy meg" a független halmaz is kb. 19,14 fokon.

Ilyen gráfelméleti kérdéseket kutatunk többek között a gráflimeszelmélet, a statisztikus fizika és az algoritmuselmélet eszközeivel, és ugyanezek a témák adják a kutatás fő motivációját is. Például nem érthetjük meg a nagy gráfok szerkezetét, amíg azt sem tudjuk, hogy a véletlen gráf milyen. Vagy a fizikai fázisátalakulásokat sem érthetjük meg, amíg a sokkal egyszerűbb absztrakt matematikai modellekben megjelenő fázisátalakulásokat sem értjük.

Ehhez a kutatáshoz sok esetben olyan elemi matematikai kérdéseket kell megválaszolnunk, mint hogy egy n csúcsú d-reguláris véletlen gráfnak:

- hány feszítőfája vagy feszítő erdeje van?
- hány olyan adott méretű párosítása (független élhalmaz) van, ami nem tartalmaz alternáló kört?

Ilyen elemi kérdésekkel fogunk foglalkozni, de ezeken keresztül igyekszünk bepillantást adni a kérdések eredetére, kapcsolataira is.

5. Normál felület szingularitások topológiája és generikus analitikus típusainak kombinatorikája

Az algebrai geometria egyik klasszikus és szép ága a komplex normál felület szingularitások elmélete. Ez két dimenziós komplex felületek (4 valós dimenziós) csúnya pontjait vizsgálja ahol lokálisan nem úgy néznek ki mint R^4. Egy szinguláris pont kis környezete úgy néz ki mint egy 3 dimenziós kompakt tér fölé állított kúp. Egy sima pont esetén ez a tér egy 3 dimenziós gömb, szinguláris pont esetén azonban egy bonyolultabb 3-dimenziós tér úgy nevezett gráf 3 sokaság. Ezt kombinatorikailag egy gráf, és rajta két féle dekoráció, az önmetszés számok és génusz számok írják le.

Egy klasszikus kérdése a normál felület szingularitások elméletének hogy analitikus invariánsok mint a geometriai génusz, multiplicitás vagy Milnor szám milyen szinten olvashatóak le a gráf kombinatorikájából. Az utóbbi években egy új lendületet kapott a téma azáltal, hogy fix gráf mellett a lehető leggenerikusabb analitikus típusra számtalan invariánst sikerült leírni, mint például a geometriai génuszt vagy a multiplicitást. A formulák sajátos jellege hogy legtöbbjük egy a gráfhoz rendelt egyszerű kvadratikus függvényből olvashatóak le kombinatorikus képletekkel.

A módszer egyes általánosításai esélyt adnak arra, hogy egy általános szingularitás kohomológikus invariánsára erős kombinatorikus megszorításokat adjunk. A témához szükség van elméleti alapozásra, de utána elemi kombinatorikus kérdések is megfogalmazhatóak amelyek jó alapot nyújthatnak egy kutatás megkezdésére már egyetemistáknak is.

6. Számtani sorozatokat tartalmazó és nem tartalmazó halmazok

Olyan kérdéseket vizsgálunk, melyeknél vagy azt írjuk elő, hogy egy halmazban sok számtani sorozat legyen (további előírt feltételeknek is eleget téve), és emellett a mérete legyen minél kisebb, vagy pedig azt, hogy egyáltalán ne legyen számtani sorozat, és legyen a lehető legnagyobb.

Mi a lehetséges legkisebb mérete egy olyan $A \subseteq \mathbb{F}_p$ halmaznak, melynek minden eleme egy 3 hosszú A-beli számtani sorozat középső eleme? (Azaz minden $a \in A$ esetén van $b, c \in A \setminus \{a\}$ úgy, hogy $2a = b + c$.) És ha $2k + 1$ hosszú számtani sorozat létezését írjuk elő, vagyis minden $a \in A$ esetén kell legyen olyan $d \neq 0$, hogy $a \pm d, a \pm 2d, \ldots, a \pm kd$ mind A-beliek? És ha emellett még azt is megköveteljük, hogy minden $a \notin A$ esetén legyen olyan $d \neq 0$, hogy $a + d, a + 2d, \ldots, a + kd \in A$? Ezek a kérdések az Alon-Jaeger-Tarsi sejtéshez kapcsolódnak, mely azt állítja, hogy ha M egy nemszinguláris mátrix egy legalább 4 elemű test felett, akkor van olyan x, hogy sem x-nek, sem Mx-nek nincs 0 koordinátája.

Mekkora lehet $\mathbb{Z}_m^n$ egy olyan részhalmaza, ami nem tartalmaz k hosszú számtani sorozatot? A kérdést elsősorban úgy néznénk, hogy m, k rögzített, és $n \to \infty$. Az extremális méretet jelölje $r_k(\mathbb{Z}_m^n)$. A kérdés már $k = 3$-ra is nyitott. Ismert, hogy

$$2.217^n \leq r_3(\mathbb{Z}_3^n) \leq 2.756^n,$$

$$3^n/\sqrt{n} \leq r_3(\mathbb{Z}_4^n) \leq 3.611^n.$$

Ezeken a becsléseken javítani talán túl ambíciózus célkitűzés lenne, de pl. bizonyos összetett m-ekre a jelenleg ismert becslések javítása, vagy akár $k > 3$ mellett az eddigieknél jobb konstrukciók találása már sokkal reménytelibb. Érdekes lehet más aritmetikai konfigurációkat is nézni, pl. híres kérdés, hogy mekkora lehet egy corner-free halmaz, vagyis egy olyan $A \subseteq \mathbb{F}_p^n \times \mathbb{F}_p^n$, melyben nem fordul elő az $(a, b), (a+d, b), (a, b+d)$ konfiguráció. Felső becslésekhez a polinom módszer lehet hasznos (például a "slice rank" segítségével), alsó becsléseknél Behrend, és Salem-Spencer konstrukciói adhatnak ihletet, de a kérdések sok más területhez (számítástudomány és információelmélet, geometria), illetve hipergráfokkal kapcsolatos kérdésekhez is kapcsolódnak.

7. Szimplexek r-szeresen metsző halmazrendszerekben

Egy $\mathcal{F}$ halmazrendszer r-szeresen metsző, ha minden $F_1, F_2, \ldots, F_r \in \mathcal{F}$ esetén $\cap_{i=1}^r F_i \neq \emptyset$. A $G_1, G_2, \ldots, G_s$ halmazok s-szimplexet alkotnak, ha bármelyiket elhagyva a többiek

metszete nem-üres, de $\cap_{i=1}^{s} G_i = \emptyset$. Legfeljebb hány $(r+1)$-szimplexet tartalmazhat egy r-szeresen metsző $\mathcal{F} \subseteq 2^{[n]}$ halmazrendszer? A sejtett extremális konstrukció: $\mathcal{F}_r = \{F \subseteq [n] : |F \cap [r+1]| \geq r\}$. A k-uniform esetben az analóg konstrukció valóban extremális elég nagy k-tól függő n esetén:

D. Nagy, B. Patkós: Triangles in intersecting families, https://arxiv.org/abs/2201.02452

8. Turán-problémák q-gráfokra

Egy q-él egy n-hosszú vektor, melynek pontosan két nem nulla eleme van, és minden eleme a $\{0, 1, \ldots, q\}$ halmazból való. (Azaz a $q = 1$ eset egy n csúcsú gráf egy élének a karakterisztikus vektora, vagy a gráf incidencia-mátrixának egy oszlopa.) A q-él tartója a nem-nulla elemek indexeiből álló pár. Egy n csúcsú q-gráf egy csomó q-él együtt. Definiálni szeretnénk, hogy egy H q-gráf mikor alkotja egy hagyományos F gráf egy s-példányát (itt $s \geq 2$ egész). Akkor mondjuk ezt, ha $|H| = E(F)$, a H tartóiból álló gráf izomorf F-fel és minden $v \in e, e' \in F$ esetén az e-nek és e'-nek megfelelő q-élek v-nek megfelelő koordinátáinak összege legalább s.

Példa: $(1, 3, 0, 0, 0)$, $(0, 1, 0, 0, 3)$, $(3, 0, 0, 0, 1)$ egy 4-háromszöget alkot, de $(3, 1, 0, 0, 0)$, $(0, 1, 0, 0, 3)$, $(3, 0, 0, 0, 1)$ csak egy 2-háromszöget.

Probléma: $ex(n, F, q, s)$ jelöli a legnagyobb n-csúcsú q-gráf méretét, ami nem tartalmazza F s-példányát. Tehát $ex(n, F) = ex(n, F, 1, 2)$. Van néhány eredmény $ex(n, F, q) = ex(n, F, q, q+1)$-ről. Gyűjtsünk még.

Pl.: $ex(n, C_3, q)$ ha ≥ 3. Sejtés: $q^2 \cdot ex(n, C_3)$. Ugyanez hosszabb páratlan körökre.

$ex(n, T, q)$ ha $q \geq 3$ és T fa. ($q = 2$ esetén ismert az aszimptotika.)

$ex(n, K_r, q)$ ha $r \geq 4$. Van egy általános alsó és felső korlát.

9. Véletlenített átlagolás

Néhány, egyelőre kettő entitás szeretné a méréseit (mondjuk 1 és -1) kiátlagolni. Ha hatékonyan szinkron kommunikálnának, ez menne is gyorsan. Ehelyett annyit engedünk, hogy egyirányú üzeneteket küldjenek egymásnak. Egy működő séma erre az esetre az ún. ratio consensus (másutt push-sum, weighted gossip), ahol az i entitás a mért x^i mellett egy másodlagos w^i változót is kap, fixen 1-re inicializálva. Egy $i \to j$ üzenet esetén a frissítés

$$x^i_{t+1} = x^i_t/2, \qquad x^j_{t+1} = x^j_t + x^i_t/2,$$
$$w^i_{t+1} = w^i_t/2, \qquad w^j_{t+1} = w^j_t + w^i_t/2.$$

Bizonyított, hogy nemtriviális iid üzengetések esetén x^i_t/w^i_t mindkét szereplőre tart az átlaghoz (most 0-hoz) 1 valószínűséggel.

Elképzelhető azonban, hogy az üzenetek elvesznek az éterben. Tegyük fel, hogy p valószínűséggel a fenti művelet helyett az alábbi megy végbe:

$$x^i_{t+1} = x^i_t/2, \qquad x^j_{t+1} = x^j_t,$$
$$w^i_{t+1} = w^i_t/2, \qquad w^j_{t+1} = w^j_t.$$

Tehát a küldő teszi a dolgát, de semmi nem érkezik. A hányadosok ekkor is konvergálnak, azonban egy közös véletlen értékhez.

A kihívás az, hogy a kapott érték négyzetes hibáját becsüljük a tényleges átlagtól, a 0-tól. Vannak részeredmények és kezdetleges becslések amik $p \to 0$ és $p \to 1$ konzisztensek, de van hova javítani bőven. Részletek olvashatók a https://arxiv.org/abs/1504.08193 cikkben, valamint a https://www.renyi.hu/~balazsg/anim_u3d_140808.webm videó mutatja 3 szereplő esetén a kapott érték (szimulált) eloszlását, ahogy p-t növeljük 0-ról 1-re.