FOCS: Annual IEEE Symposium on Foundations of Computer Science 2023

Stare, Matic Starič, Martin Dudić, Veljko Mohar, Don

Kovač, Matej Mlinarič, Rene Štuhec, Žan

April 3, 2024

Contents

1 Introduction

64th IEEE Symposium on Foundations of Computer Science (FOCS) 2023 je uradno ime konference ki je potekala od 6. do 9. novembra 2023 v mestu Santa Cruz (Kalifornija, Združene države Amerike). Njene teme so bile: algoritmi in podatkovne strukture, kriptografija, računska kompleksnost, teorija računalniškega učenja, iskanje informacij in baze podatkov. Oddanih prispevkov je bilo 421, a so jih sprejeli le 142. Vseh 142 je bilo tudi predstavljeno.

2 A Randomized Algorithm for Single-Source Shortest Path on Undirected Real-Weighted Graphs

Problem najkrajše poti je eden izmed najbolj znanih problemov v teoriji grafov. Cilj je, da najdemo najkrajšo pot med dvema vozliščema na podlagi uteženih grafov. Za reševanje tovrstnih problemov se je v preteklosti najbolj uveljavil Dijkstrin algoritem, ki deluje s časovno zahtevnostjo $O(n^2)$, kjer je n število vozlišč. To mejo so kasneje izboljšali s Fibonaccijevo kopico na $O(n \log n + m)$, kjer je m število povezav. V tem članku so se avtorji osredotočili na problem najkrajše poti iz enega vira (SSSP) na uteženih grafih. Zasnovali so nov algoritem, ki deluje s časovno zahtevnostjo $O(m\sqrt{\log n * \log\log n})$, vendar je pogojen z verjetnostjo. To pomeni, da je časovna zahtevnost algoritma pričakovana in ne zahtevnost v najslabšem primeru.

Do nedavnega je bilo ozko grlo pri iskanju SSSP vrsta s prednostjo. Ideja izboljšave je, da v vrsto vnesemo manjše število vozlišč. To dosežemo s tehniko *Bundle Construction*, ki deluje na sledeč način:

- Iz prvotne množice vozlišč V naključno izberemo podmnožico $R_1 \subseteq V$, pri čemer je vsako vozlišče vsebovano v R_1 z verjetnostjo $\frac{1}{k}$. V množici R_1 se nahaja tudi vir s.
- Na vsakem vozlišču $v \notin R_1$ poženemo Dijkstrin algoritem z začetkom v v. Vsako vozlišče, ki izločimo iz kopice dodamo v urejeno množico $V^{(v)}_{extract}$. Ko naletimo na vozlišče $u \in R_1$, oziroma je moč množice $|V^{(v)}_{extract}| > k \log k$, se Dijkstrin algoritem z začetkom v v zaključi.
- Če je bila moč množice $|V^{(v)}_{extract}| > k \log k$, potem dodamo vozlišče v v množico R_2.
- Nastavimo $R := R_1 \cup R_2$ in prvo vozlišče v $V^{(v)}_{extract} \cap R := b(v)$
- Z zgornjim rezultatom izračunamo sledeče: $Bundle(u)$ za vsak $u \in R$, $Ball(v)$ za vsak $v \in V \backslash R$ in $dist(v, u)$ za vsak $u \in Ball(v) \cup \{b(v)\}$.

Ker je pričakovana moč množice $|R_1| = O(\frac{m}{k})$, algoritem terja časovno zahtevnost $O(mk \log k)$.

Sledi algoritem *Bundle Dijkstra*, ki na osnovi pridobljene množice paketov posodablja razdalje vseh vozlišč do vira. Gre za relaksacijo vozlišč $v \in V \backslash R$.

Bundle Dijkstra - Ustvarimo tabelo, kjer bomo hranili razdalje vozlišč v do vozlišča s, in v Fibonaccijevo kopico vstavimo vsa vozlišča iz R.

1. Ko iz kopice izločimo vozlišče u, posodobimo tabelo tako, da za vsako vozlišče v, ki je zapakirano vozlišču u najdemo točno razdaljo. To storimo tako, da posodobimo $d(v)$ glede na $d(u)$, vozlišča v $Ball(v)$ in sosednja vozlišča vozlišču v in $Ball(v)$.
2. Ko je vsako vozlišče $x \in Bundle(u)$ posodobimo še sosednja vozlišča $y \in N(x)$ in vozlišča, ki so znotraj $Ball(y)$.
3. Ko posodobimo vozlišče, ki ni v množici R, posodobimo še njegovo zapakirano vozlišče $b(v)$ z $d(v) + dist(v, b(v))$.

Ker smo v algoritem vstavili le $|R|$ vozlišč, je časovna kompleksnost izločanja elementov iz kopice enaka $O(|R| \log n)$. Poleg izločanja elementov iz kopice nam k časovni kompleksnosti pripomore še zanka skozi vsa vozlišča $v \in V \backslash R$, vendar ker v algoritmu preverjamo tudi vozlišča znotraj $Ball(v)$ dobimo končno časovno zahtevnost *Bundle Dijkstra* $O(\frac{m}{k} \log n + mk)$.

Tako je skupna časovna zahtevnost celotnega zasnovanega algoritma enaka $O(\frac{m}{k} \log n + mk \log k)$, ki jo lahko minimiziramo z izbranim $k = \frac{\log n}{\log \log n}$.

3 Polynomial-Time Pseudodeterministic Construction of Primes

Gat in Goldwasser sta postavila vprašanje ali je mogoče izračunati praštevila psevdodeterministično v polinomskem času. Naključnostni algoritem je psevdodeterminističen, če izračuna fiksno kanonično rešitev za iskalni problem z visoko verjetnostjo. Članek predstavlja rešitev na ta problem v neskončno-pogostem režimu. Predstavlja brezpogojni polinomski naključnostni algoritem B, tako da za neskončno mnogo vrednosti n, $B(1^n)$ izračuna kanonično n-bitno praštevilo p_n z visoko verjetnostjo. Splošneje za vsako gosto lastnost Q nizov, ki jo je mogoče določiti v polinomskem času, obstaja neskončno-pogosta psevdodeterministična polinomska konstrukcija nizov, ki zadovoljijo Q. Pristop presega subeksponentno časovno konstrukcijo, predlagano s strani Oliveire in Santhanama. Vključuje različne inovativne koncepte, kot je nova tehnika zagona za psevdodeterministične konstrukcije, ter kvalitativno izboljšanje okvira enakomerne trdnosti-naključnosti, ki sta ga predstavila Chen in Tell, s pomočjo variante generatorja Shaltiel-Umans.

3.1 Rezultati

Glavni izrek določa pogoje, pod katerimi probabilistični algoritem s polinomskim časom, skupaj s sekvenco nizov iz določenega jezika, zagotavlja specifične verjetnostne izide. Z uporabo tega izreka na jeziku praštevil članek predstavi naključni algoritem s polinomskim časom, ki z visoko verjetnostjo zanesljivo proizvaja praštevila za neskončno mnogo vhodnih dolžin, prekašajoč prejšnje metode subexponentne časovne zahtevnosti.

Izrek 1 (Neskončno pogosto polinomski čas Psevdodeterminističnih konstrukcij). Naj bo $Q \subseteq \{0,1\}^*$ jezik z naslednjimi lastnostmi:

- **(Gostota.)** obstaja konstanta $\rho \geq 1$ tako, da za vsak $n \in \mathbb{N}_{\geq 1}$, $Q_n \triangleq Q \cap \{0,1\}^n$ ustreza $|Q_n| \geq n^{-\rho} \cdot 2^n$; in
- **(Preprostost.)** obstaja deterministično polinomski čas algoritem A_Q, ki odloča, ali vhod $x \in \{0,1\}^*$ pripada Q.

Nato obstaja verjetnostni polinomski čas algoritem B in zaporedje $\{x_n\}_{n \in \mathbb{N}_{\geq 1}}$ nizov n-bitnih nizov v Q tako, da veljajo naslednji pogoji:

1. Pri vsaki vhodni dolžini $n \in \mathbb{N}_{\geq 1}$, $\Pr[B(1^n) \notin \{x_n, \perp\}] \leq 2^{-n}$.
2. Na neskončno mnogih vhodnih dolžinah $n \in \mathbb{N}_{\geq 1}$, $\Pr[B(1^n) = x_n] \geq 1 - 2^{-n}$.

Posledice

- Obstaja verjetnostni polinomski algoritem B, ki za neskončno mnogo vrednosti n izpiše kanonično n-bitno praštevilo p_n z visoko verjetnostjo. To je dokaz moči teorije kompleksnosti v reševanju problemov, ki se zdijo biti o številski teoriji.
- Obstaja konstanta $c \geq 1$, tako da za $t(n) = n^c$ velja naslednje: Za vsak $m \geq 1$ obstaja $n > m$ in n-bitno praštevilo p_n, pri čemer je $rK^t(p_n) \leq \log(n) + O(1)$. Drugače povedano, obstaja neskončno mnogo praštevil, ki imajo zelo kratke učinkovite opise.

4 Proof of the Clustered Hadwiger Conjecture

Preden avtorji dokažejo gručasto Hadwigerjevo domnevo, opišejo naslednje pojme.

Polni grafi so grafi, v katerih je vsako vozlišče povezano z vsakim drugim vozliščem. Poln graf z n vozlišči označimo K_n.
Minorji grafa G so podgrafi, ki jih dobimo z brisanjem povezav in vozlišč ter krčenjem povezav G.
Barvanje grafa je preslikava, ki vsakemu vozlišču dodeli barvo.
Graf je k-obarvljiv, ko za njegovo obarvanje porabimo največ k barv.
Graf je pravilno obarvan, ko ima vsak sosednji par vozlišč med seboj različno barvo.
Kromatično število grafa G je najmanjše tako število k, da je G pravilno obarvan in k-obarvljiv.

Hadwigerjeva domneva:
Naj bo K_h poln graf na h vozliščih.
Hadwiger je domneval, da je vsak graf brez minorja K_h pravilno $(h-1)$-obarvljiv.

Monokromatična komponenta obarvanega grafa G so med seboj povezana vozlišča enake barve.
Gručevje je število vozlišč največje monokromatične komponente obarvanega grafa G.
Gručasto monokromatično število množice grafov je najmanjše tako število k, za katerega obstaja število c, da je vsak graf iz množice k-obarvljiv z gručevjem c.

Gručasta Hadwigerjeva domneva(v nadaljevanju izrek 1) trdi, da je vsak graf brez minorja K_h $(h-1)$-obarvljiv z gručevjem največ neke funkcije $f(h)$.

Avtorji nadaljujejo z gručastim kromatičnim številom množice grafov brez minorja K_s, t, kjer je K_s, t poln bipartitni graf z deli velikosti $t >= s >= 1$.
Izrek2:
Vsak graf brez minorja K_s, t je $(s+1)$-obarvljiv s gručevjem največ neke funkcije $f(s,t)$.
S pomočjo izreka 2 dokažejo, da je omenjeno gručasto kromatično število $s+1$.

Avtorji nato izreka 1 in 2 posplošijo na izrek 4:
Vsak graf brez minorja J_s, t je $(s+1)$-obarvljiv z gručevjem največ $f(s,t)$.

Temu iz dokazanih izrekov Liu-a in Wood-a ter definicije za 'apex' graf, ki ob odvzemu največ 1 vozlišča postane planarni graf, sledi izrek 7:
Za katerikoli celi števili $t >= s >= 3$ in katerokoli temeljišče grafa X, vsak graf $K_{s,t}$ brez podgrafov in minorjev v X je $(s+1)$-obarvljiv s clusteringom največ $f(s,t,X)$.

Dokazna metoda za izreka 4 in 7 uporablja napredne tehnike teorije grafov za reševanje kompleksnih problemov. Ključna sestavina teh dokazov je uporaba 'teorije strukture produkta grafov' skupaj z izrekom Robertsona in Seymourja, ki obravnava strukturo grafovskih minorjev. To omogoča preoblikovanje planarnih grafov v enostavnejše grafe z omejeno drevesno širino, kar olajša analizo in manipulacijo z njimi.

Pristop je sicer omejen na družine grafov, ki omogočajo močan produkt grafa. Zato se zanašamo na izrek Robertsona in Seymourja, ki razčleni grafe brez določenega vzorca na manjše dele, imenovane "torzi". Te "torzi" so sestavljene iz vdelanega podgrafa na površini, dopolnjenega z vrtinci in temeljišči s prosto okolico, podobno kot drevo kličnih vsot.

Pri barvanju določenih vrst grafov sledimo strategiji barvanja "torzij" enega za drugim, pri čemer pazimo, da ne prekrijemo že obarvanih delov y novo barvo. Teorem 4 nam zagotavlja, da lahko uporabimo največ s+1 barv, vendar to ni vedno izvedljivo, zato moramo "torze", ki jih ni mogoče pobarvati v s+1 barvah, združiti v zavese. Za barvanje celotnega

grafa preprosto pobarvamo vsako zaveso zaporedno, začevši s tisto, ki vsebuje koreninski "torzo". Pri tem posvečamo pozornost določenim vrstam točk v grafu, imenovanim "temeljišča".

Za dodatno poenostavitev grafa uporabljamo tudi metode, kot sta particioniranje in plastenje, da ohranimo omejenost velikosti presečišč vsakega dela in vsake plasti. Namesto ustvarjanja omejenega grafa količnika drevesne širine, povzdignemo zaveso, da oblikujemo manjši G↑ (G minor) z omejeno drevesno širino. S tem zagotovimo, da G↑ ostane minor od G, s čimer dopolnimo dokazno strategijo za izrek 4.

Naši rezultati ponujajo konstruktivne dokaze in algoritme polinomskega časa $O(n^c)$, neodvisne od izključenega minorja ali podgrafa, kar omogoča učinkovito obvladovanje K2,t-podgrafov. Izreka 1 in 2 zagotavljata optimalne meje za gručasto kromatsko število neminornih grafov Kh in Ks,t, poleg ključno razvitih definicij in orodij, kot so dekompozicije zavese, dvignjene zavese in kontrakcije. Pričakuje se, da bodo ta orodja uporabna v različnih kontekstih zaradi njihove učinkovitosti pri nadzoru K2,t-podgrafov.