PCP-satsen på kombinatoriskt manér

Per Austrin
austrin@kth.se

Teorigruppen
Skolan för Datavetenskap och Kommunikation

2005-10-24

Agenda

1. Bakgrund
   - Vad är ett bevis?
   - Vad är ett PCP?
   - PCP-satsen
2. PCP-satsen ur en kombinatorisk synvinkel
   - Vad, hur och varför?
   - Lite definitioner
   - Huvudresultatet
3. Glapputvidgningslemmat
   - Ännu mer definitioner
   - Bevisskiss
   - Lösa trådar

Vad är ett bevis?

bevi´s subst. ∼*et*, plur. ∼, best. plur. ∼*en*
ORDLED: *be-vis-et*

1. ngt som används för att fastställa riktigheten hos ett påstående.
2. ngt som måste tydas som omisskännligt tecken på ett visst förhållande.

(Nationalencyklopedin)

Vad är ett bevis? (forts.)

Specifikt, i dagens seminarium:

- Vi har en verifierare V (poly-tids Turing-maskin).
- Vi vill övertyga V om att strängar x tillhör ett språk L.
- V bör varken vara oresonlig eller lättlurad.
- Exempel:
  - Låt $L = 3\text{-SAT}$.
  - Givet formel Φ övertygas V om att $\Phi \in 3\text{-SAT}$ genom att vi ger en satisfierande tilldelning för Φ.

När är ett bevis verkligen ett bevis?

Vi säger att V har fullständighet $c(n)$ och sundhet $s(n)$, om:

- För varje $x \in L$ existerar ett bevis π sådant att V accepterar π med sannolikhet minst $c(|x|)$.
- För varje $x \notin L$ gäller för *alla* bevis π att V accepterar med sannolikhet *högst* $s(|x|)$.

- Vår verifierare för 3-SAT har perfekt fullständighet och sundhet, $c = 1$, $s = 0$.
- Vi antar den något grovkorniga inställningen att V är en bra verifierare så länge $s < c$ och bägge är konstanter oberoende av indatastorlek.

PCP – Probabilistically Checkable Proof

- PCP är en generalisering av vanliga bevis.
- Vi håller förutom fullständighet och sundhet noga reda på:
  - Hur många bitar av beviset vi läser, q.
  - Hur många bitar slump verifieraren använder, r.
  - Hur långt beviset är, l.
- Observation: längd begränsad av slump:
  - $l \leq q2^r$.

  Vi kommer därför ignorera längden och bara titta på mängden slump som används.

Naiv PCP för 3-SAT

Vi minskar frågekomplexiteten för vår 3-SAT-verifierare:

- Låt bevis vara variabeltilldelningar, som förut.
- Verifierare:
  - Välj en slumpvis klausul.
  - Kolla värdet på de tre variabler som ingår.
  - Acceptera om klausulen var satisfierad.
- Parametrar:
  - Fullständighet $c = 1$.
  - Sundhet $s = 1 - 1/\#\text{klausuler}$.
  - Frågekomplexitet $q = 3$.
  - Slumpkomplexitet $r = \log_2 \#\text{klausuler}$.
- Bra sånär som på sundheten, som är riktigt usel.

Hur kraftfulla är PCP?

Definition

$PCP_{s,c}[r(n), q(n)]$ är mängden av alla språk som har en PCP-verifierare med fullständighet c, sundhet s, slumpkomplexitet $r(n)$ och frågekomplexitet $q(n)$.

- Vår naiva PCP visar att 3-SAT $\in PCP_{1-1/n,1}[\log n, 3]$.
- Eftersom 3-SAT är NP-fullständigt har vi visat at $NP \subseteq PCP_{1-1/\operatorname{poly} n,1}[\mathcal{O}(\log n), 3]$.

PCP-satsen

Theorem (PCP-satsen)

$NP \subseteq PCP_{1/2,1}[\mathcal{O}(\log n), \mathcal{O}(1)]$.

Med andra ord:

- varje språk i NP har en PCP-verifierare som bara behöver läsa ett konstant antal bitar av ett polynomiellt långt bevis. Denna verifierare förkastar felaktiga bevis med sannolikhet 1/2, och accepterar alltid korrekta bevis.

Koppling till icke-approximerbarhet

En alternativ formulering av PCP-satsen:

Theorem (PCP-satsen på nytt)

Det existerar en konstant $\delta < 1$ så att det är NP-svårt att avgöra huruvida en 3-SAT*-instans är satisfierbar, eller huruvida en andel högst δ av klausulerna är satisfierbara.*

Detta implicerar att det är NP-svårt att approximera MAX-3-SAT inom en faktor δ.

Vad dagens seminarium handlar om

- Dinur, 2005:
  “The PCP Theorem by Gap Amplification”
- (google: “pcp theorem”)

Varför bevisa en redan bevisad sats?

- Tidigare bevis byggde alla på algebraiska metoder.
  - Nya typer av bevis ger ofta ökad förståelse.
  - Icke-approximerbarhets-formuleringen rent kombinatorisk.
- Mycket arbete har fokuserats på att optimera konstruktionerna. Dinurs resultat (kombinerat med resultat av Ben-Sasson och Sudan) förbättrar bästa kända.
- Kombinatoriska bevis vackrare. ☺

Grundtankar

- Istället för synsättet med verifierare väljer vi synsättet med en uppsättning villkor utav vilka man antingen kan satisfiera alla eller högst en andel δ.
- Grundklossen kommer att bli en operation som minskar δ, utan att instansen blir speciellt mycket större.
- Genom att utföra denna operation ett logaritmiskt antal gånger får vi ner δ till en konstant < 1.

Villkorsgrafer

Definition

En *villkorsgraf* är en tupel $G = (V, E, \Sigma, \mathcal{C})$ där:

1. (V, E) är en oriktad graf.
2. V är en mängd variabler som antar värden i Σ.
3. $\mathcal{C} = \{c(e)\}_{e \in E}$, där $c(e) \subseteq \Sigma^2$ är ett villkor på kanten e. Vi säger att $c(e)$ satisfieras av (a, b) omm $(a, b) \in c(e)$.

Egenskaper för villkorsgrafer

- Vi betecknar storleken av beskrivningen av en villkorsgraf G med $\text{size}(G) = \mathcal{O}(|V|^2 + |E||\Sigma|^2)$.
- För en tilldelning $\sigma : V \to \Sigma$ definierar vi *missnöjdheten*

$$\textsc{Unsat}_\sigma(G) = \frac{1}{|E|} \left|\{ e = (u, v) \in E \mid (\sigma(u), \sigma(v)) \notin c(e) \}\right|,$$

(d.v.s. andelen kanter som inte är satisfierade.)

- Missnöjdheten för en villkorsgraf är

$$\textsc{Unsat}(G) = \min_{\sigma : V \to \Sigma} \textsc{Unsat}_\sigma(G).$$

Dinurs sats

Theorem

Det existerar Σ' (av konstant storlek), sådant att det för alla Σ (av konstant storlek) finns konstanter $C > 0$ och $\alpha > 0$ sådana att varje villkorsgraf $G = (V, E, \Sigma, \mathcal{C})$ i polynomiell tid kan byggas om till en villkorsgraf $G' = (V', E', \Sigma', \mathcal{C}')$ som uppfyller

- $\text{size}(G') \leq C \cdot \text{size}(G)$.
- $\textsc{Unsat}(G) = 0 \Rightarrow \textsc{Unsat}(G') = 0$.
- $\textsc{Unsat}(G') \geq \min(2 \cdot \textsc{Unsat}(G), \alpha)$.

Från Dinurs sats till PCP-satsen

- Låt $G = (V, E, \Sigma, \mathcal{C})$ vara en villkorsgraf med $|\Sigma| = 3$.
- Obs 1: Det är NP-svårt att avgöra om $\textsc{Unsat}(G) = 0$.
- Obs 2: Om $\textsc{Unsat}(G) \neq 0$ så gäller $\textsc{Unsat}(G) \geq 1/|E|$.
- Sätt $G_0 = G$, låt G_{i+1} vara resultatet av att applicera Dinurs sats på G_i. Enkel induktion ger:
  - $\text{size}(G_i) \leq C^i \, \text{size}(G)$
  - $\textsc{Unsat}(G) = 0 \Rightarrow \textsc{Unsat}(G_i) = 0$
  - $\textsc{Unsat}(G_i) \geq \min(2^i \, \textsc{Unsat}(G), \alpha)$

Från huvudsatsen till PCP-satsen (forts.)

- Låt $k = \lceil \log_2 |E| \rceil = \mathcal{O}(\log(\text{size}(G)))$. Betrakta G_k:
  - $\text{size}(G_k) \leq C^k \, \text{size}(G) = \text{poly}(\text{size}(G))$
  - $\textsc{Unsat}(G) \neq 0 \Rightarrow \textsc{Unsat}(G_k) \geq \alpha$
- Antal bitfrågor för att kolla ett villkor: $2 \log_2 |\Sigma'| = \mathcal{O}(1)$.
- Med andra ord: $NP \subseteq PCP_{1-\alpha,1}[\mathcal{O}(\log n), \mathcal{O}(1)]$!
- För att trycka ner sundheten till $1 - \alpha' = 1/2$, bygg nya villkor som är konjunktioner av alla u-tupler av gamla villkor, där $u = \log(1 - \alpha')/\log(1 - \alpha) = \mathcal{O}(1)$.

Bevis av Dinurs sats?

- Det huvudsakliga nya inslaget i beviset av Dinurs sats är det s.k. *glapputvidgningslemmat* som ger ett sätt att pumpa upp UNSAT-värdet för en villkorsgraf.
- Detta är vad vi kommer ägna resten av seminariet åt.

Definitioner

- Vi låter $\lambda(G)$ beteckna storleken på det näst största egenvärdet till grafen G:s grannmatris.

Jag kommer också att missbruka två vanliga termer:

- Med en *stig* i en graf menar vi egentligen en väg. (Med andra ord: man får besöka samma nod flera gånger)
- Vi säger att två noder i en graf är på avstånd d från varandra om det existerar en stig på d steg mellan dem.

Exponentiering av villkorsgrafer

Definition

Låt $G = (V, E, \Sigma, \mathcal{C})$ vara en d-reguljär villkorsgraf, och $t \in \mathbb{N}$. Vi definierar $G^t = (V, E', \Sigma^r, \mathcal{C}')$ som:

- Hörn: G^t har samma hörnmängd som G.
- Kanter: Antalet kanter mellan u och v i G^t är antalet stigar av längd exakt t mellan u och v i G.
- Alfabet: alfabetet är Σ^r, där $r \approx d^{t/2}$. Intuition: varje hörn har "åsikter" om alla hörn på avstånd $t/2$.
- Villkor: villkoret på en kant $e = (u, v) \in E'$ är satisfierat om och endast om tilldelningarna på u och v är konsistenta med en tilldelning som satisfierar alla villkor från $\mathcal{C}$ på noder på avstånd $t/2$ från u eller v.

Glapputvidgningslemmat

Lätt att se att $\textsc{Unsat}(G) = 0 \Rightarrow \textsc{Unsat}(G^t) = 0$. Det kluriga steget för dagen är följande lemma:

Lemma

Låt $\lambda < d$ och $|\Sigma|$ vara godtyckliga konstanter. Det finns en konstant $\beta(\lambda, d, |\Sigma|) > 0$ sådan att för varje $t \in \mathbb{N}$ och varje d-reguljär villkorsgraf $G = (V, E, \Sigma, \mathcal{C})$ med $\lambda(G) \leq \lambda$ gäller

$$\textsc{Unsat}(G^t) \geq \beta\sqrt{t} \cdot \min\left(\textsc{Unsat}(G), 1/t\right).$$

Bevisskiss (1/4)

- Tag en bästa tilldelning $\overline{\sigma} : V \to \Sigma^r$ för G^t.
- $\overline{\sigma}(u)$ innehåller "åsikter" om alla noder som kan nås genom att ta $t/2$ steg från u.
- Låt $\overline{\sigma}(u)_v \in \Sigma$ vara u:s åsikt om v.
- Låt $P_{u,v}$ vara antalet stigar av längd $t/2$ mellan u och v.

Bevisskiss (2/4)

- Vi definierar en tilldelning $\sigma : V \to \Sigma$ för G: Låt $\sigma(u) = a$, där a är ett värde som maximerar

$$\sum_{\overline{\sigma}(v)_u = a} P_{u,v}$$

- Låt $F \subseteq E$ vara en mängd kanter i G som förkastar σ, sådan att

$$\frac{|F|}{|E|} = \min\left(\textsc{Unsat}_\sigma(G), \frac{1}{t}\right).$$

- Mål: vi vill visa $\textsc{Unsat}_{\overline{\sigma}}(G^t) \geq \Omega(\sqrt{t})\frac{|F|}{|E|}$

Bevisskiss (3/4)

- Vi säger att en stig $P = (v_0, v_1, \ldots, v_t)$ i G *träffas* av sin i:te kant om
  - $(v_{i-1}, v_i) \in F$
  - $\overline{\sigma}(v_0)_{v_{i-1}} = \sigma(v_{i-1})$
  - $\overline{\sigma}(v_t)_{v_i} = \sigma(v_i)$
- Låt $I = \{t/2 - \sqrt{t} < i \leq t/2 + \sqrt{t}\}$ vara mängden index i "mitten" på en stig.
- För en stig P, definiera

$$N(P) = \#\{\, i \in I \mid i \text{ träffar } P \,\}$$

Bevisskiss (4/4)

- Observation: $N(P) > 0 \Rightarrow P$ förkastar $\overline{\sigma}$, så:

$$\Pr_P[N(P) > 0] \leq \Pr_P[P \text{ förkastar } \overline{\sigma}] = \textsc{Unsat}(G^t)$$

- Så räcker att visa $\Pr[N(P) > 0] \geq \Omega(\sqrt{t})\frac{|F|}{|E|}$.
  - Uppskatta $\mathbb{E}_P[N(P)]$ och $\mathbb{E}_P\left[N(P)^2\right]$.
  - Använd $\Pr[X > 0] \geq \mathbb{E}^2[X] / \mathbb{E}\left[X^2\right]$
    (för icke-negativ stokastisk variabel X).

Skattning av $\mathbb{E}[N(P)]$

- Låt $Z(P)$ vara antalet "mittkanter" som ligger i F.

$$\mathbb{E}[Z(P)] = |I| \cdot \frac{|F|}{|E|} = \Theta(\sqrt{t})\frac{|F|}{|E|}.$$

- Vi söker andelen av dessa kanter vars hörn dessutom fått precis de värden som ändpunkterna i P anser att de ska ha.
- Sannolikheten att ett hörn v på avstånd $t/2$ från u har $\overline{\sigma}(v)_u = \sigma(u)$ är minst $\frac{1}{|\Sigma|}$.
- Ändpunkterna i P ligger på ungefär avstånd $t/2$ från "mitthörnen".
- Självlooparna i G och att vi är nära $t/2$ gör att det funkar, får $\mathbb{E}[N(P)] = \Omega(\sqrt{t})\frac{|F|}{|E|}$.

Skattning av $\mathbb{E}\left[N(P)^2\right]$

- Vi har $N(P) \leq Z(P)$, så $\mathbb{E}\left[N(P)^2\right] \leq \mathbb{E}\left[Z(P)^2\right]$.
- Låt $Z_i(P)$ vara en indikator för huruvida den i:te kanten i P ligger i F.

$$Z(P) = \sum_{i \in I} Z_i(P)$$

- $$\mathbb{E}\left[Z^2\right] = |I| \cdot \frac{|F|}{|E|} + 2 \sum_{i<j} \mathbb{E}\left[Z_i Z_j\right]$$
- Utnyttja expansionen hos G för att visa

$$\mathbb{E}\left[Z_i Z_j\right] \leq \frac{|F|}{|E|} \left(\frac{|F|}{|E|} + \left(\frac{\lambda}{d} \right)^{j-i} \right)$$

- Ger $\mathbb{E}\left[N(P)^2\right] \leq \mathbb{E}\left[Z(P)^2\right] \leq \mathcal{O}\left(\sqrt{t}\right) \frac{|F|}{|E|}$.

Vi knyter ihop säcken

- Till slut har vi alltså fått:

$$\begin{aligned}
\textsc{Unsat}(G^t) &\geq \Pr_P[N(P) > 0] \\
&\geq \frac{\mathbb{E}^2[N(P)]}{\mathbb{E}\left[N(P)^2\right]} \\
&\geq \frac{\left(\Omega(\sqrt{t})|F|/|E|\right)^2}{\mathcal{O}\left(\sqrt{t}\right)|F|/|E|} \\
&= \Omega(\sqrt{t})\frac{|F|}{|E|} \\
&= \Omega(\sqrt{t})\min(\textsc{Unsat}(G), 1/t)
\end{aligned}$$

Godtycklig graf är inte snäll

Glapputvidningslemmat behöver en d-reguljär expander.

Lemma

Det finns konstanter $0 < \lambda < d$ *och* $\beta > 0$ *så att varje villkorsgraf* G *kan byggas om till en villkorsgraf* G' *med samma alfabet som* G*, och*

- G' *är* d*-reguljär*
- $\text{size}(G') = \mathcal{O}(\text{size}(G))$
- $\lambda(G') \leq \lambda$
- $\beta \, \textsc{Unsat}(G) \leq \textsc{Unsat}(G') \leq \textsc{Unsat}(G)$

Alfabetsexplosionen

Resulterande villkorsgraf efter användning av glapputvidgningslemmat har alfabetstorlek $\approx |\Sigma|^{d^{t/2}}$.

Lemma

Det finns konstanter $|\Sigma_0|$ *och* $\beta > 0$ *sådana att varje villkorsgraf* $G = (V, E, \Sigma, \mathcal{C})$ *kan byggas om till en villkorsgraf* $G' = (V', E', \Sigma_0, \mathcal{C}')$, *sådan att*

- $\text{size}(G') = M(|\Sigma|)\,\text{size}(G)$
- $\beta\,\textsc{Unsat}(G) \leq \textsc{Unsat}(G') \leq \textsc{Unsat}(G)$

Tack för mig!