Būla funkciju sarežģītības mēri

Autors: Krišjānis Prūsis, kp08074

Darba vadītājs: Andris Ambainis, prof., Dr. dat.

Latvijas Universitāte
Datorikas fakultāte

2016. gada 27. janvārī

Būla funkcijas

- Būla funkcijas:

$$f(x_1, x_2, \ldots, x_n) : \{0,1\}^n \to \{0,1\}.$$

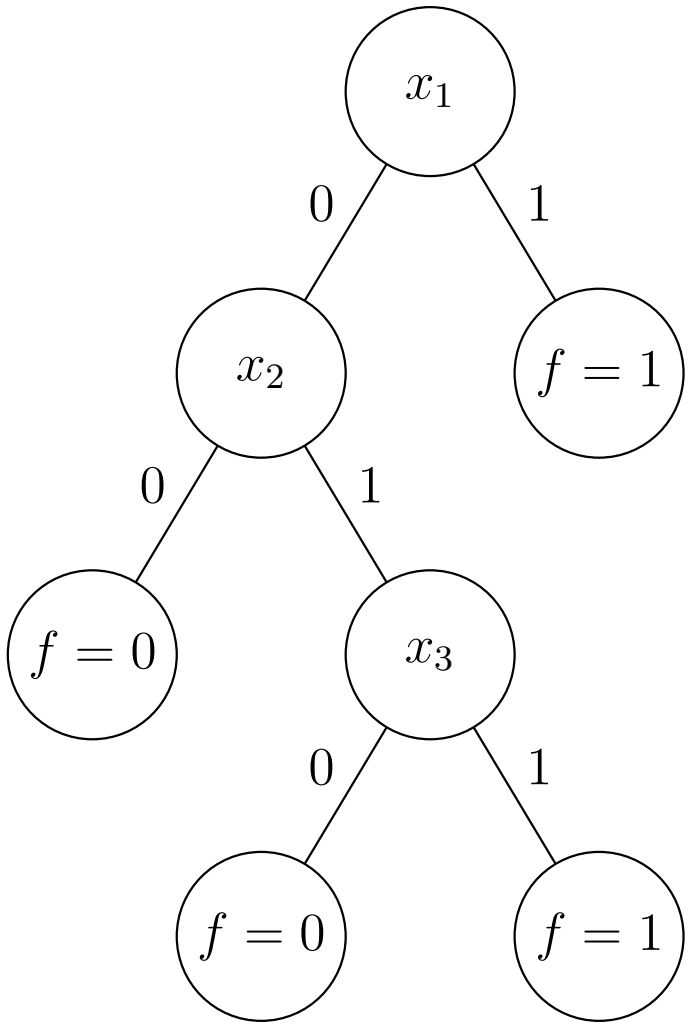
- Piemēri:

$$\textsc{Or}_2 = x_1 \vee x_2 \qquad \textsc{And}_3 = x_1 \wedge x_2 \wedge x_3.$$

Saturs

Lēmumkoku sarežģītība

- Lēmumkoku sarežģītība $D(f)$ ir augstums īsākajam lēmumkokam, kas rēķina funkciju f.
- Piemēram, koks, kas rēķina $f(x) = x_1 \vee (x_2 \wedge x_3)$.
- Ar diviem jautājumiem šo funkciju izrēķināt nevar, tādēļ šis koks ir optimāls un šajā gadījumā $D(f) = 3$.

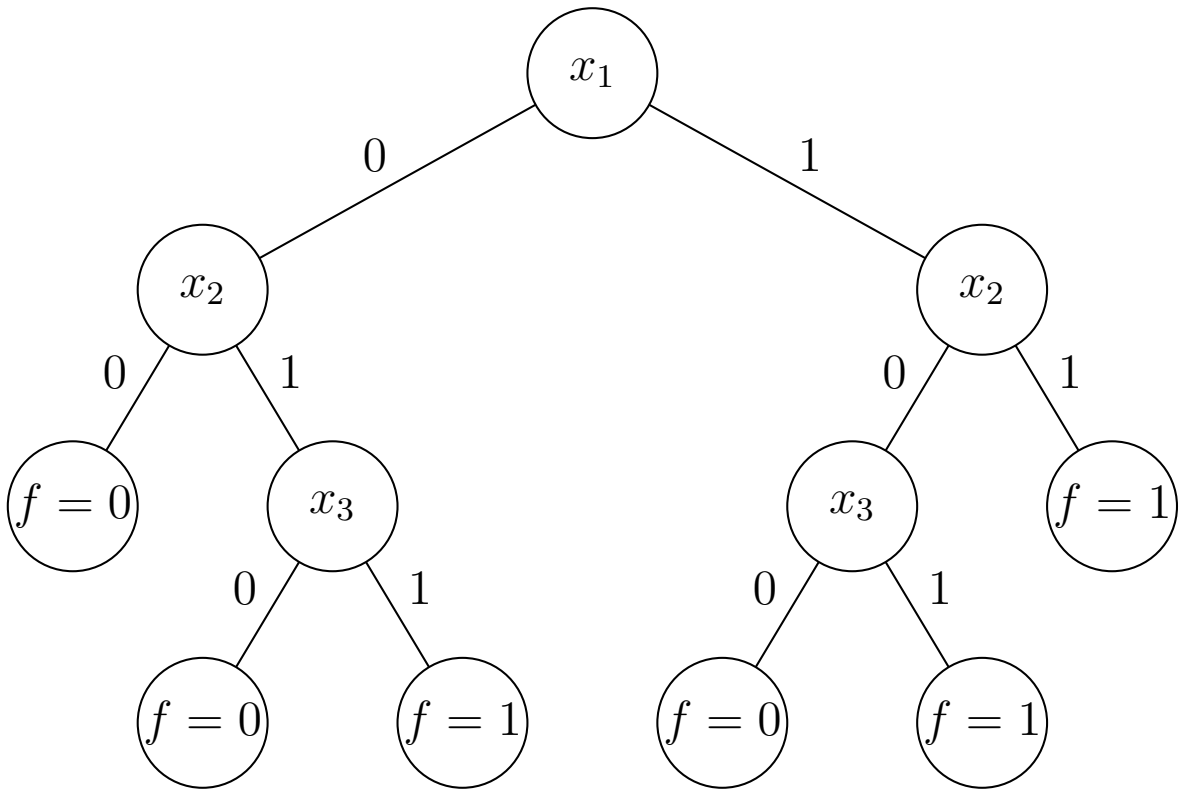


Varbūtisko lēmumkoku sarežģītība

- Varbūtisks lēmumkoks pieļauj veikt varbūtiskas izvēles.
- Koka augstuma vietā tiek minimizēts maksimālais sagaidāmais jautājumu skaits pār visiem ievadvārdiem.
- Varbūtiskā lēmumkoku sarežģītība $R(f)$ ir šis skaits labākajam varbūtiskajam lēmumkokam, kas rēķina f.

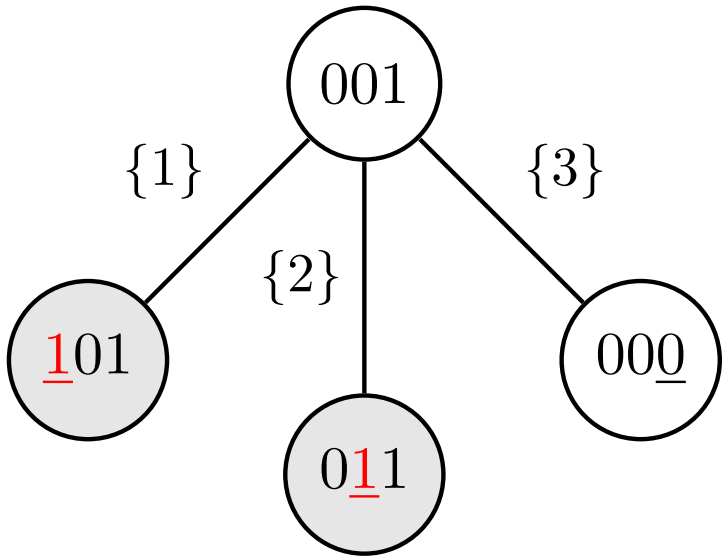
3-bitu vairākuma funkcijas lēmumkoku sarežģītība

- $\textsc{Maj}_3(001) = \textsc{Maj}_3(000) = 0.$
- $\textsc{Maj}_3(101) = \textsc{Maj}_3(111) = 1.$
- $D(\textsc{Maj}_3) = 3,$
- $R(\textsc{Maj}_3) = 2\frac{2}{3}.$



Funkcijas jutīgums

- Funkcijas jutīgums uz ievadvārdu $s(f, x)$ ir bitu skaits vārdā x, kurus nomainot, mainās funkcijas vērtība: $f(x) \neq f(x^{\{i\}})$.
- Piemēram, 3 bitu vairākuma funkcijai $\textsc{Maj}_3$:
  - $s(\textsc{Maj}_3, 000) = 0$,
  - $s(\textsc{Maj}_3, 001) = 2$,
  - $s(\textsc{Maj}_3, 101) = 2$.



Funkcijas jutīgums

- Funkcijas jutīgums ir maksimālais tās jutīgums pār visiem ievadvārdiem:

$$s(f) = \max\{s(f,x) \mid x \in \{0,1\}^n\}.$$

- Funkcijas 0 un 1 jutīgumi ir maksimālie pār ievadvārdiem ar atbilstošo vērtību:

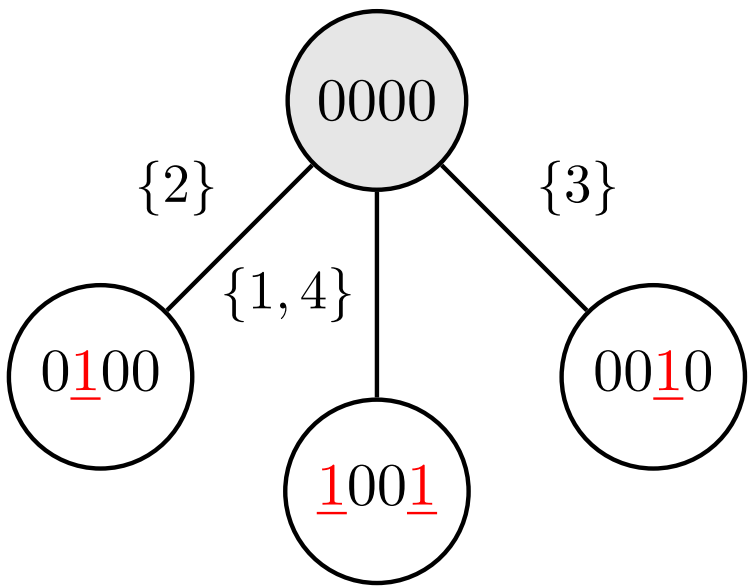
$$s_z(f) = \max\{s(f,x) \mid x \in \{0,1\}^n, f(x) = z\}.$$

- Piemēram, 3 bitu vairākuma funkcijai $\textsc{Maj}_3$
  $s_0(\textsc{Maj}_3) = s_1(\textsc{Maj}_3) = s(\textsc{Maj}_3) = 2.$

- Savukārt, 3 bitu $\textsc{And}$:
  - $s_0(\textsc{And}_3) = 1$;
  - $s_1(\textsc{And}_3) = s(\textsc{And}_3) = 3.$

Funkcijas bloku jutīgums

- f ir jutīga uz ievades pozīciju kopu jeb **bloku**, ja, nomainot visas šo bitu vērtības, mainās arī f vērtība.
- Funkcijas bloku jutīgums uz vārdu $bs(f, x)$ ir maksimālais nešķeļošos jutīgu bloku skaits.
- Aplūkojam 4 bitu sakārtotības funkciju $\textsc{Sort}_4$.
- $\textsc{Sort}_4(x) = 1 \Leftrightarrow$ $x_1 \leqslant x_2 \leqslant x_3 \leqslant x_4$ vai $x_1 \geqslant x_2 \geqslant x_3 \geqslant x_4$.
- $bs(\textsc{Sort}_4, 0000) = 3$.



Funkcijas bloku jutīgums

- Formāli, funkcijas bloku jutīgums uz ievadvārdu $bs(f, x)$ ir lielākais tāds skaitlis b, ka eksistē b nešķeļošas indeksu kopas $B_1, \ldots, B_b \in [n]$, kurām $f(x) \neq f(x^{B_i})$.
- $bs(f) = \max\{bs(f, x) \mid x \in \{0, 1\}^n\}$.
- $bs_z(f) = \max\{bs(f, x) \mid x \in \{0, 1\}^n, f(x) = z\}$.

Sertifikātu sarežģītība

- Sertifikāts c ir tāds daļējs vērtību piekārtojums ievades pozīcijām $c : S \to \{0, 1\}, S \subseteq [n]$, ka tas nosaka funkcijas vērtību.
- z-sertifikāts nosaka funkcijas vērtību z.
- 4 bitu sakārtotības funkcijai $\textsc{Sort}_4$
  - 0-sertifikāti ir, piemēram, $010*$, $1*01$, 1001;
  - 1-sertifikāti ir, piemēram, $*111$, $00*1$, 1100;
  - sertifikāti nav, piemēram, $0***$, $*10*$.

Sertifikātu sarežģītība

- Sertifikātu sarežģītība uz ievadvārdu $C(f, x)$ ir garums īsākajam sertifikātam, kuram x atbilst.
- Ekvivalenti $C(f, x)$ ir mazākais x bitu skaits, kuru vērtība jāzina, lai varētu viennozīmīgi pateikt funkcijas vērtību.
- $C(f) = \max\{C(f, x) \mid x \in \{0, 1\}^n\}$.
- $C_z(f) = \max\{C(f, x) \mid x \in \{0, 1\}^n, f(x) = z\}$.

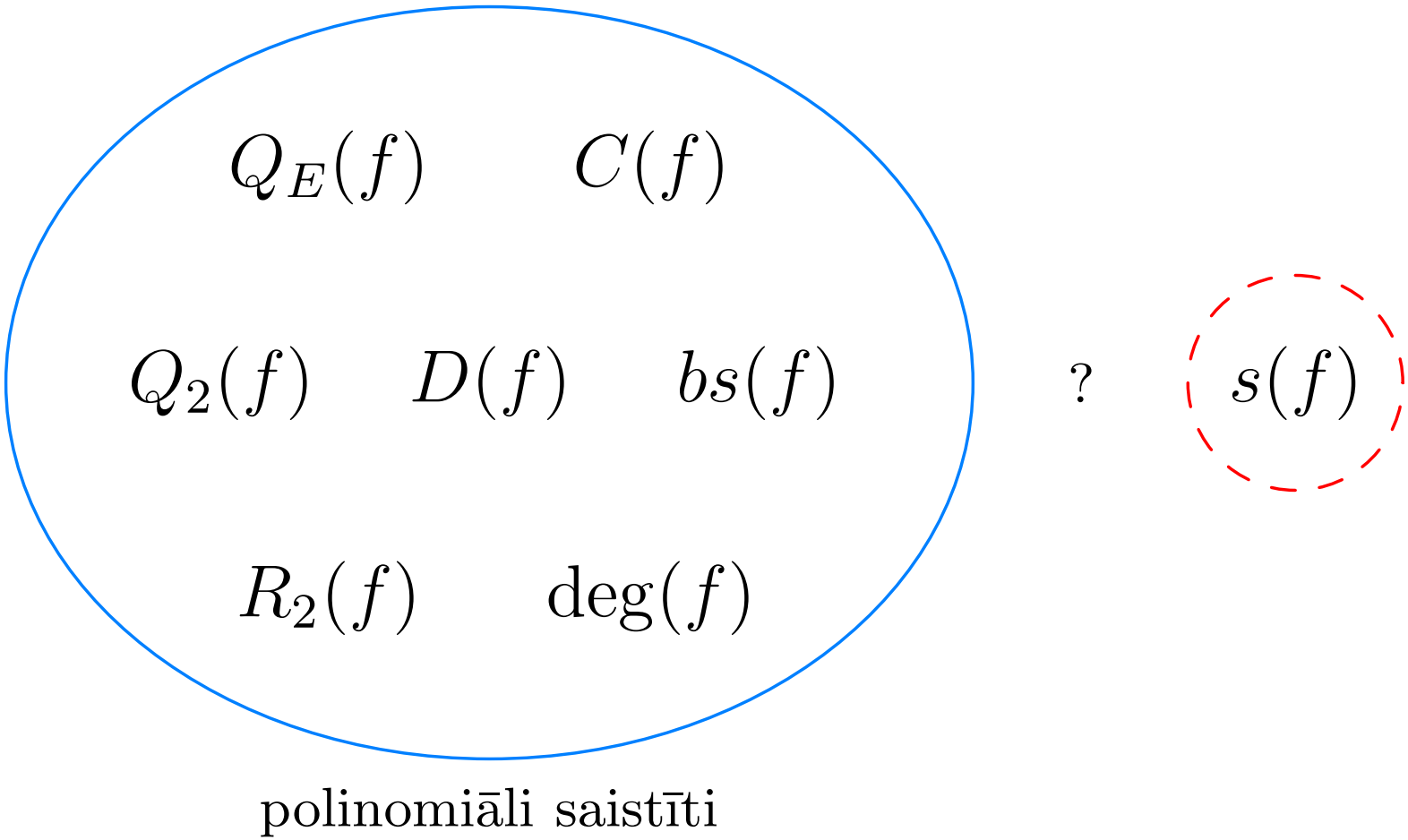
Saturs

Zināmās sakarības

- Bloku jutīgums ir polinomiāli saistīts ar lēmumkoku sarežģītību:
$$bs(f) \leqslant D(f) \leqslant bs(f)^3.$$

- Caur bloku jutīgumu tiek iegūtas arī saistības ar daudziem citiem sarežģītības mēriem, piemēram:
  - $D(f) \leqslant bs(f)^3 \leqslant 27R_2(f)^3$;
  - $D(f) \leqslant \deg(f)bs(f) \leqslant 2\deg(f)^3$. (polinoma pakāpe)

Zināmās sakarības



Jutīguma hipotēze

- Vai $s(f)$ arī polinomiāli saistīts ar šiem mēriem?
- Zināms, ka $s(f) \leqslant bs(f)$.
- **Jutīguma hipotēze**:

$$\boxed{bs(f) = \mathcal{O}(s(f)^c) \text{ kādai konstantei } c.}$$

- Problēma atklāta jau vairāk nekā 25 gadus.

Labākās konstrukcijas

- Ilgu laiku labākā bija Rubinstein 1995. gada konstrukcija:

$$bs(f) = \frac{1}{2}s(f)^2.$$

- Virza to nedaudz uzlaboja:

$$bs(f) = \frac{1}{2}s(f)^2 + \frac{1}{2}s(f).$$

- Ambainis un Sun to uzlaboja vairāk:

$$\boxed{bs(f) = \frac{2}{3}s(f)^2 - \frac{1}{3}s(f).}$$

Labākie ierobežojumi

- Pirmo netriviālo robežu deva Simon:

$$bs(f) \leqslant 4^{s(f)} s(f).$$

- Ilgu laiku labākais bija Kenyon un Kutin 2004. gada rezultāts:

$$bs(f) \leqslant \frac{e}{\sqrt{2\pi}} e^{s(f)} \sqrt{s(f)}.$$

- Ambainis, Bavarian, Gao, Mao, Sun un Zuo to nesen uzlaboja:

$$\boxed{bs(f) \leqslant 2^{s(f)-1} s(f) - s(f) + 1.}$$

Funkcijas, kurām hipotēze izpildās

- Monotonām funkcijām $s(f) = bs(f)$.
- Grafu īpašībām $s(f) = \Omega(|V|) = \Omega(\sqrt{n})$.
- Funkcijām ar $s_1(f) = C_1(f)$ izpildās

$$bs(f) \leqslant \left(\frac{2}{3} + o(1)\right) s_0(f) s_1(f).$$

Rezultāts

- Iegūts jauns labākais novērtējums bloku jutīguma un jutīguma attiecībai:

$$\boxed{bs(\hat{f}) \leqslant C(\hat{f}) \leqslant \max\left(2^{s(\hat{f})-1}\left(s(\hat{f}) - \frac{1}{3}\right), s(\hat{f})\right).}$$

- Iepriekšējais rezultāts:

$$bs(\hat{f}) \leqslant C(\hat{f}) \leqslant 2^{s(\hat{f})-1} s(\hat{f}) - s(\hat{f}) + 1.$$

Gadījums $s_1(f) = 2$

- Iegūtais rezultāts šajā gadījumā dod šādu novertējumu:

$$C_0(f) \leqslant 2s_0(f) - \frac{2}{3}.$$

- Pierādīts šāds novērtējums:

$$C_0(f) \leqslant \frac{9}{5}s_0(f).$$

- Ierobežojot arī $s_0(f) \leqslant 6$, pierādīts

$$C_0(f) \leqslant \frac{3}{2}s_0(f),$$

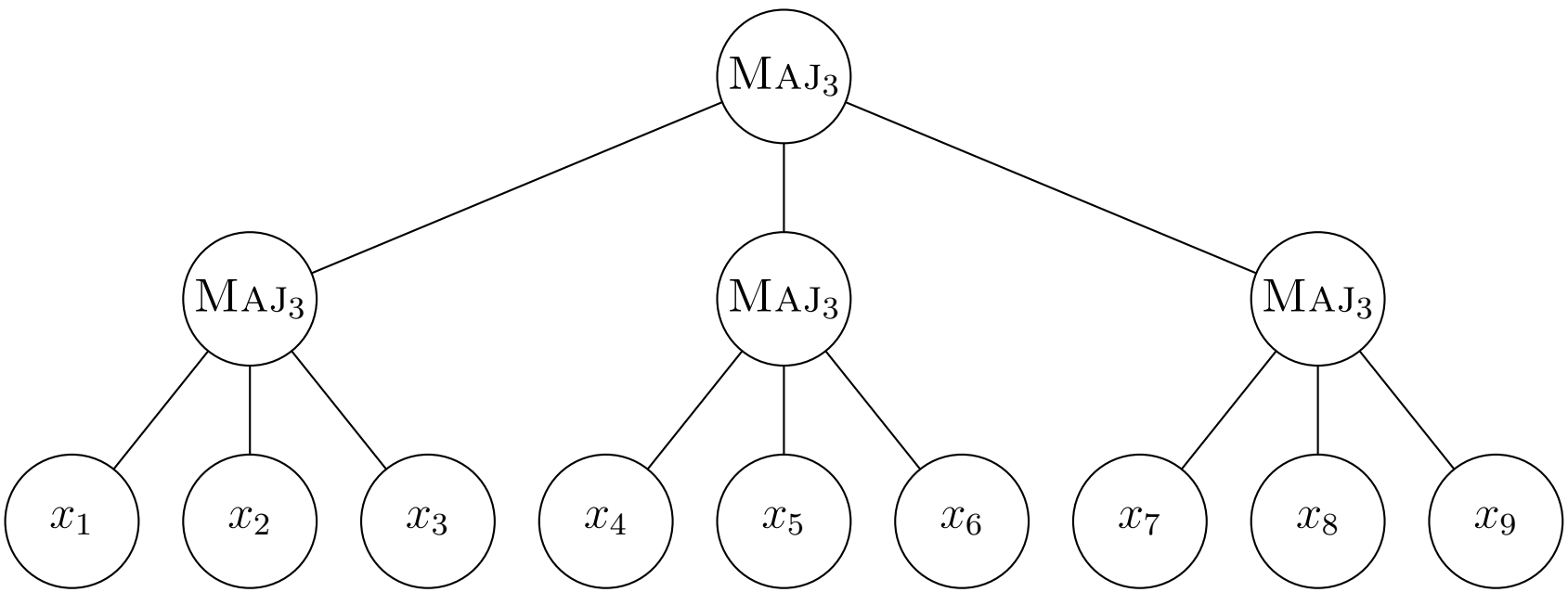
kas sakrīt ar labākām zināmajām konstrukcijām.

Saturs

Rekursīvā $\textsc{Maj}_3$ funkcija

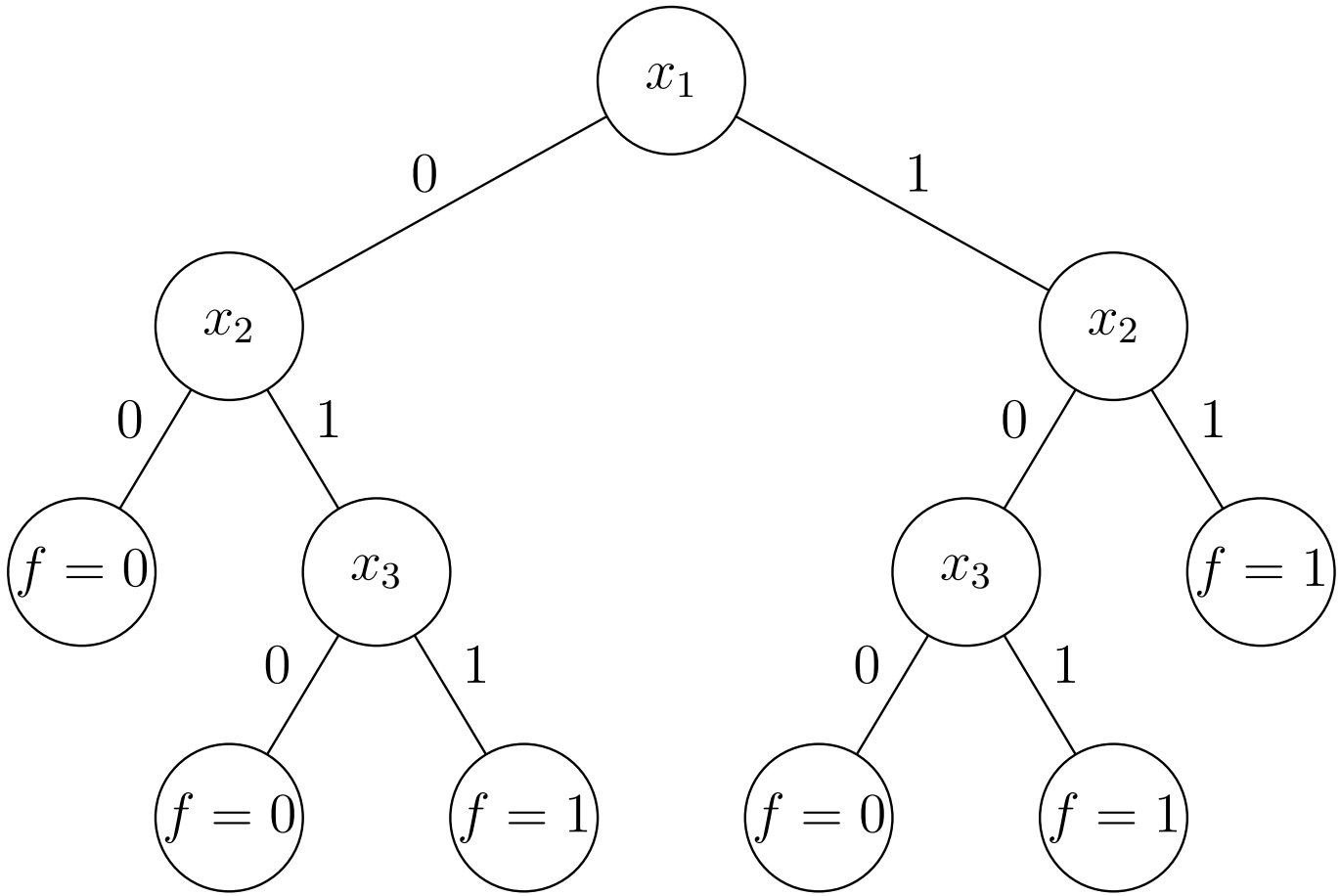
- $\textsc{Maj}_{3,h}$ — funkcija no 3^h mainīgajiem. Ja $h = 0$, atgriež vienīgo mainīgo. Citādi sadala ievadi trīs daļās, katrai rekursīvi izrēķina $\textsc{Maj}_{3,h-1}$ un pēc tam izrēķina rezultātu $\textsc{Maj}_3$.

- Piemēram, $\textsc{Maj}_{3,2}$:



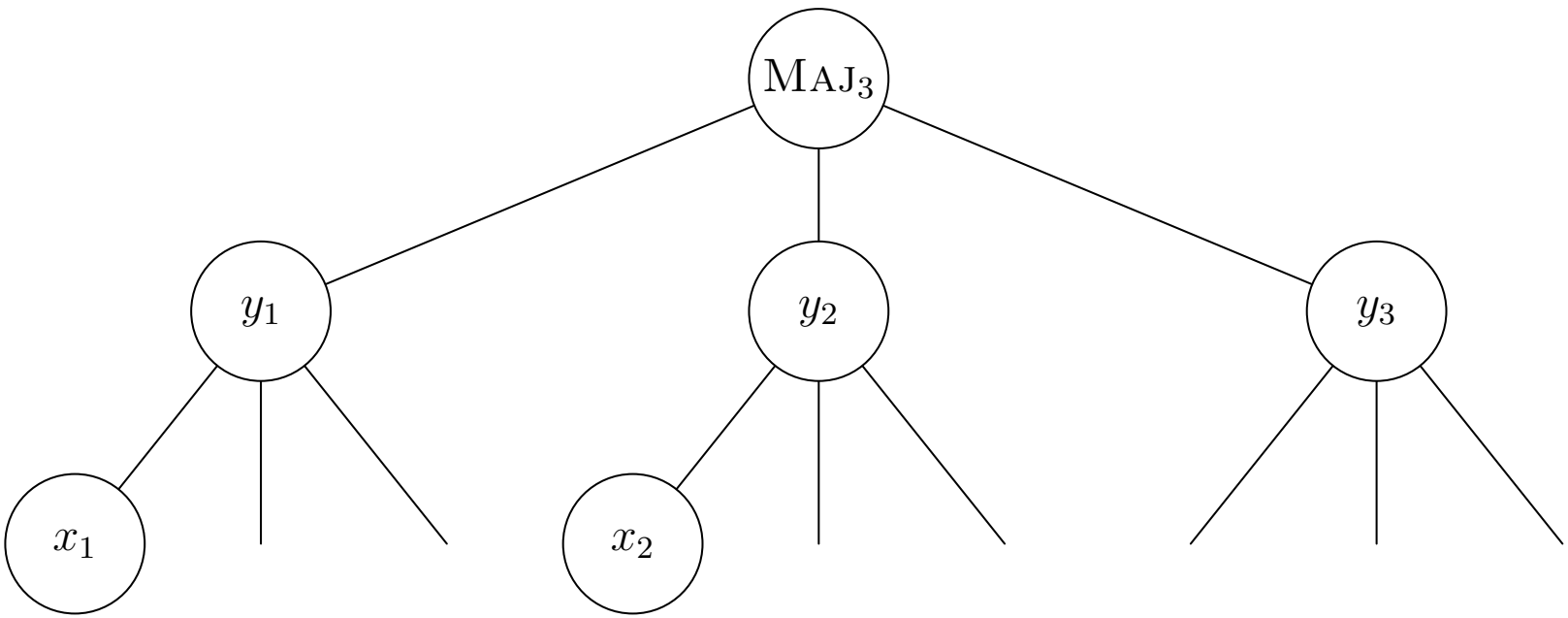
Aplūkotā problēma

- Kāds ir $R(\mathrm{MAJ}_{3,h})$?
- Rekursīvi izmantojot iepriekš aplūkoto varbūtisko lēmumkoku, varam iegūt $\left(2\frac{2}{3}\right)^h = (2.666...)^h$.



Šobrītējie rezultāti

- Apakšējā robeža (Göös un Jayram): $R(\mathrm{MAJ}_{3,h}) \geqslant 2.59^h$.
- Labākais algoritms (Magniez, Nayak, Santha, Sherman, Tardos, Xiao) sasniedz $(1.007) \cdot 2.64944^h$.
- Algoritma ideja: veikt rekursīvus izsaukumus 2 līmeņus zemāk (x_1 un x_2) un atkarībā no to rezultātiem izvēlēties, kuru y jautāt pirmo.



Mūsu pieeja

- Vai eksistē labāks algoritms, kas izmanto zemākus rekursīvos izsaukumus?
- Aplūkojam visus algoritmus, kas veic rekursīvus izsaukumus ne vairāk kā 3 līmeņus zemāk.
- Izmantojot optimizētu datorpārlasi, iegūstam, ka šobrītējais algoritms ir labākais iespējamais starp šādiem.

Saturs

Problēmas nostādne

- Dota nešķeļošos sertifikātu kopa, kas noklāj visu ievades vārdu telpu, turklāt katra sertifikāta garums ir $\leqslant m$.
- Piemēram, viena šāda kopa pie $m = 2$:

C_1	0	0	*
C_2	0	1	*
C_3	1	*	0
C_4	1	*	1

- Šoreiz ne gluži Būla funkcija — $f(x)$ atrod, kuram no šiem sertifikātiem x atbilst.
- Gribam noskaidrot $D(f)$ — cik x bitu jāpajautā, lai noteikti uzzinātu sertifikātu, kuram x pieder.

Algoritms

- $k(m)$ — jautājumu skaits, kāds nepieciešams, lai paprasītu vismaz vienu nofiksētu bitu no katra sertifikāta.
  - Paprasam šos $k(m)$ bitus.
  - Pēc tam sertifikāti būs garumā $\leqslant m-1$, tādēļ varam jautāt $k(m-1)$ bitus, lai samazinātu garumu vēl par viens.
  - Kad visi sertifikāta biti pajautāti, zinām, vai x tam atbilst.
- Kopā $k(m)+k(m-1)+\ldots+k(1)$ jautājumi.
- $k(m)\leqslant m$, tādēļ $k(m)+k(m-1)+\ldots+k(1)\leqslant m^2/2$.

Apakšējā robeža

- Cik liels var būt $k(m)$?
- Iegūta konstrukcija, kas parāda, ka $k(m) \geqslant \frac{m}{2}$.
- Konstrukcijas pamatā — izveidojam komplektu no m sertifikātiem garumā $m-1$ kuriem katram ar katru ir pretruna, katra pretruna ir citā pozīcijā, un sertifikāti citur neškeļas. Piemēram, pie $m = 4$:

C_1	0	0	0	*	*	*
C_2	1	*	*	0	0	*
C_3	*	1	*	1	*	0
C_4	*	*	1	*	1	1

- Skaidrs, ka viens jautājums var pārklāt tikai 2 no šiem sertifikātiem, tādēļ tiem nepieciešami $m/2$ jautājumi.

Papildinājuma piemērs

- Tālāk pierādam, ka šos sertifikātus var papildināt tā, lai noklātu visu ievades telpu ar sertifikātiem ne garākiem par m.

- Piemērs šim papildinājumam pie $m = 4$:

C_1	0	0	0	*	*	*
C_2	1	*	*	0	0	*
C_3	*	1	*	1	*	0
C_4	*	*	1	*	1	1
	0	0	1	*	*	0
	1	*	*	0	1	0
	0	1	0	*	*	1
	1	*	*	1	0	1
	0	1	*	0	*	0
	1	0	*	1	*	0
	0	*	1	*	0	1
	1	*	0	*	1	1

Paldies par uzmanību