Būla funkciju jūtīgums un bloku jūtīgums

Andrejs Vihrovs, av07006 Andris Ambainis, Dr. dat.

Latvijas Universitāte
Datorikas fakultāte

2014. gada 26. martā

Būla funkcijas

Par Būla funkcijām sauc funkcijas

$$f\colon \{0,1\}^n \mapsto \{0,1\},$$

kur $n \geqslant 0$.

Būla funkcijas

Par Būla funkcijām sauc funkcijas

$$f\colon \{0,1\}^n \mapsto \{0,1\},$$

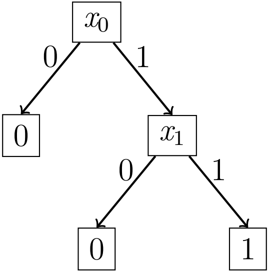
kur $n \geqslant 0$.

Būla funkcijas piemērs: $\mathrm{AND}_2(x)$

$$\mathrm{AND}_2(00) = 0 \qquad \mathrm{AND}_2(01) = 0$$
$$\mathrm{AND}_2(10) = 0 \qquad \mathrm{AND}_2(11) = 1$$

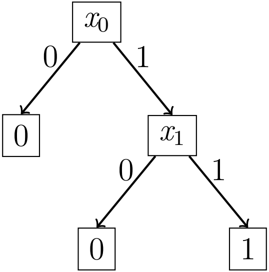
Determinēta izvēles koka sarežģītība

Determinēts izvēles koks ir binārais koks ar sakni, kur katra virsotne atbilst kādam funkcijas ievada bitam, un no tās izejošie zari atbilst šī bita vērtībām.



Determinēta izvēles koka sarežģītība

Determinēts izvēles koks ir binārais koks ar sakni, kur katra virsotne atbilst kādam funkcijas ievada bitam, un no tās izejošie zari atbilst šī bita vērtībām.



Funkcijas f determinēta izvēles koka sarežģītība $D(f)$ ir mazākā determinēta izvēles koka, kas aprēķina f, dziļums.

Būla funkcijas jūtīgums

Ja ir vārds $x \in \{0,1\}^n$, tad ar $x^{(i)}$ $(1 \leqslant i \leqslant n)$ apzīmē vārdu x, kuram i-tā bita vērtība ir nomainīta uz pretēju.

Būla funkcijas jūtīgums

Ja ir vārds $x \in \{0,1\}^n$, tad ar $x^{(i)}$ $(1 \leqslant i \leqslant n)$ apzīmē vārdu x, kuram i-tā bita vērtība ir nomainīta uz pretēju.

Ja Būla funkcijai f, ievadam x un kādam ievada bitam i izpildās

$$f(x) \neq f(x^{(i)}),$$

tad bitu i sauc par jūtīgu uz ievada x.

Būla funkcijas jūtīgums

Ja ir vārds $x \in \{0,1\}^n$, tad ar $x^{(i)}$ $(1 \leqslant i \leqslant n)$ apzīmē vārdu x, kuram i-tā bita vērtība ir nomainīta uz pretēju.

Ja Būla funkcijai f, ievadam x un kādam ievada bitam i izpildās

$$f(x) \neq f(x^{(i)}),$$

tad bitu i sauc par jūtīgu uz ievada x.

Funkcijas f jūtīgums uz ievada x $s(f,x)$ ir jūtīgu bitu skaits uz x.

Būla funkcijas jūtīgums

Ja ir vārds $x \in \{0,1\}^n$, tad ar $x^{(i)}$ $(1 \leqslant i \leqslant n)$ apzīmē vārdu x, kuram i-tā bita vērtība ir nomainīta uz pretēju.

Ja Būla funkcijai f, ievadam x un kādam ievada bitam i izpildās

$$f(x) \neq f(x^{(i)}),$$

tad bitu i sauc par jūtīgu uz ievada x.

Funkcijas f jūtīgums uz ievada x $s(f,x)$ ir jūtīgu bitu skaits uz x.

Funkcijas f jūtīgums $s(f)$ ir maksimālā $s(f,x)$ vērtība starp visiem x.

Būla funkcijas bloku jūtīgums

Ja ir bloks $B \subseteq \{1, 2, \ldots, n\}$, tad $x^{(B)}$ ir vārds x, kurā visu B ietilpstošo bitu vērtības ir nomainītas uz pretējām.

Būla funkcijas bloku jūtīgums

Ja ir bloks $B \subseteq \{1, 2, \ldots, n\}$, tad $x^{(B)}$ ir vārds x, kurā visu B ietilpstošo bitu vērtības ir nomainītas uz pretējām.

Ja Būla funkcijai f un tās ievadam x izpildās

$$f(x) \neq f(x^{(B)}),$$

tad bloku B sauc par jūtīgu funkcijai f iz ievada x.

Būla funkcijas bloku jūtīgums

Ja ir bloks $B \subseteq \{1, 2, \ldots, n\}$, tad $x^{(B)}$ ir vārds x, kurā visu B ietilpstošo bitu vērtības ir nomainītas uz pretējām.

Ja Būla funkcijai f un tās ievadam x izpildās

$$f(x) \neq f(x^{(B)}),$$

tad bloku B sauc par jūtīgu funkcijai f iz ievada x.

Funkcijas f bloku jūtīgums uz ievada x $bs(f, x)$ ir lielākais neatkarīgu jūtīgu bloku skaits uz x.

Būla funkcijas bloku jūtīgums

Ja ir bloks $B \subseteq \{1, 2, \ldots, n\}$, tad $x^{(B)}$ ir vārds x, kurā visu B ietilpstošo bitu vērtības ir nomainītas uz pretējām.

Ja Būla funkcijai f un tās ievadam x izpildās

$$f(x) \neq f(x^{(B)}),$$

tad bloku B sauc par jūtīgu funkcijai f iz ievada x.

Funkcijas f bloku jūtīgums uz ievada x $bs(f, x)$ ir lielākais neatkarīgu jūtīgu bloku skaits uz x.

Funkcijas f bloku jūtīgums $bs(f)$ ir maksimālā $bs(f, x)$ vērtība starp visiem x.

Būla funkcijas sertifikātu sarežģītība

Funkcijas f ievada x bitu apakškopu S sauc par sertifikātu, ja visiem ievadiem y, kas atbilst S, izpildās $f(y) = f(x)$.

Būla funkcijas sertifikātu sarežģītība

Funkcijas f ievada x bitu apakškopu S sauc par sertifikātu, ja visiem ievadiem y, kas atbilst S, izpildās $f(y) = f(x)$.

Funkcijas f sertifikātu sarežģītība uz ievada x $C(f, x)$ ir mazākā sertifikāta garums, kas apliecina $f(x)$ vērtību.

Būla funkcijas sertifikātu sarežģītība

Funkcijas f ievada x bitu apakškopu S sauc par sertifikātu, ja visiem ievadiem y, kas atbilst S, izpildās $f(y) = f(x)$.

Funkcijas f sertifikātu sarežģītība uz ievada x $C(f, x)$ ir mazākā sertifikāta garums, kas apliecina $f(x)$ vērtību.

Funkcijas f sertifikātu sarežģītība $C(f)$ ir maksimālā $C(f, x)$ vērtība starp visiem x.

0- un 1-sarežģītība

Daudzreiz ir ērti apskatīt tos ievaddatus, uz kuriem Būla funkcija izdod tikai vērtību 0 vai arī tikai vērtību 1. Atbilstoši tam var definēt sarežģītības mērus:

0- un 1-sarežģītība

Daudzreiz ir ērti apskatīt tos ievaddatus, uz kuriem Būla funkcija izdod tikai vērtību 0 vai arī tikai vērtību 1. Atbilstoši tam var definēt sarežģītības mērus:

Funkcijas f 0-jūtīgums $s_0(f)$ un 1-jūtīgums $s_1(f)$ — maksimālais jūtīgums uz visiem ievadiem, kur f izdod, attiecīgi, 0 vai 1.

0- un 1-sarežģītība

Daudzreiz ir ērti apskatīt tos ievaddatus, uz kuriem Būla funkcija izdod tikai vērtību 0 vai arī tikai vērtību 1. Atbilstoši tam var definēt sarežģītības mērus:

Funkcijas f 0-jūtīgums $s_0(f)$ un 1-jūtīgums $s_1(f)$ — maksimālais jūtīgums uz visiem ievadiem, kur f izdod, attiecīgi, 0 vai 1.

Līdzīgi definē funkcijas f 0-bloku jūtīgumu $bs_0(f)$ un 1-bloku jūtīgumu $bs_1(f)$, kā arī 0-sertifikātu sarežģītību $C_0(f)$ un 1-sertifikātu sarežģītību $C_1(f)$.

Dažas sarežģītības mēru saistības

	$D(f)$	$s(f)$	$bs(f)$	$C(f)$
$D(f)$	—	$s(f) \leqslant D(f)$	$bs(f) \leqslant D(f)$	$C(f) \leqslant D(f) \leqslant (C(f))^2$
$s(f)$		—	$s(f) \leqslant bs(f)$	$s(f) \leqslant C(f)$
$bs(f)$			—	$bs(f) \leqslant C(f) \leqslant (bs(f))^2$
$C(f)$				—

Dažas sarežģītības mēru saistības

	$D(f)$	$s(f)$	$bs(f)$	$C(f)$
$D(f)$	—	$s(f) \leqslant D(f)$	$bs(f) \leqslant D(f)$	$C(f) \leqslant D(f) \leqslant (C(f))^2$
$s(f)$		—	$s(f) \leqslant bs(f)$	$s(f) \leqslant C(f)$
$bs(f)$			—	$bs(f) \leqslant C(f) \leqslant (bs(f))^2$
$C(f)$				—

Var pierādīt arī stiprāku faktu: visi trīs no $D(f)$, $bs(f)$ un $C(f)$ ir polinomiāli saistīti:

$$A(f) \leqslant p(B(f)) \quad \text{un} \quad B(f) \leqslant q(A(f))$$

«Jūtīguma hipotēze» (Sensitivity Conjecture)

Kā $bs(f)$ ir saistīts ar $s(f)$? Tagad zinām

$$s(f) \leqslant bs(f) \leqslant ???$$

«Jūtīguma hipotēze» (Sensitivity Conjecture)

Kā $bs(f)$ ir saistīts ar $s(f)$? Tagad zinām

$$s(f) \leqslant bs(f) \leqslant ???$$

«Jūtīguma hipotēze» (Nisan, Szegedy): $s(f)$ un $bs(f)$ ir polinomiāli saistīti.

Precīzāk, tiek lēsts, ka

$$bs(f) \leqslant O((s(f))^2)$$

Esošie rezultāti

Novērtējumi no augšas

- $bs(f) \leqslant s(f) \cdot 4^{s(f)}$ (H.-U. Simon)
- $bs(f) \leqslant \left(\frac{e}{\sqrt{2\pi}}\right) e^{s(f)} \sqrt{s(f)}$ (Kenyon and Kutin)
- $bs(f) \leqslant 2^{s(f)-1} s(f)$ (Ambainis and Sun)

Esošie rezultāti

Novērtējumi no augšas

- $bs(f) \leqslant s(f) \cdot 4^{s(f)}$ (H.-U. Simon)
- $bs(f) \leqslant \left(\frac{e}{\sqrt{2\pi}}\right) e^{s(f)} \sqrt{s(f)}$ (Kenyon and Kutin)
- $bs(f) \leqslant 2^{s(f)-1} s(f)$ (Ambainis and Sun)

Novērtējumi no lejas

- $bs(f) = \Omega(\frac{1}{2} s(f)^2)$ (Rubinstein)
- $bs(f) = \Omega(\frac{1}{2} s(f)^2 + \frac{1}{2} s(f))$ (Virza)
- $bs(f) = \Omega(\frac{2}{3} s(f)^2 - \frac{1}{3} s(f))$ (Ambainis and Sun)

Rubinšteina funkcija

Apskatām ievadvirkni garumā $n = 2k$. Funkcija g ir 1 tad un tikai tad, ja ievadā ir tieši viens vieninieku pāris pozīcijās $2i$ un $2i+1$:

$$\left.\begin{array}{l} x = 11\ 00\ 00\ 00\ 00 \\ x = 00\ 11\ 00\ 00\ 00 \\ x = 00\ 00\ 11\ 00\ 00 \\ x = 00\ 00\ 00\ 11\ 00 \\ x = \underbrace{00\ 00\ 00\ 00\ 11}_{n = 2k \text{ biti}} \end{array}\right\} \implies g(x) = 1$$

Rubinšteina funkcija

Apskatām ievadvirkni garumā $n = 2k$. Funkcija g ir 1 tad un tikai tad, ja ievadā ir tieši viens vieninieku pāris pozīcijās $2i$ un $2i+1$:

$$\left.\begin{array}{l} x = 11\ 00\ 00\ 00\ 00 \\ x = 00\ 11\ 00\ 00\ 00 \\ x = 00\ 00\ 11\ 00\ 00 \\ x = 00\ 00\ 00\ 11\ 00 \\ x = \underbrace{00\ 00\ 00\ 00\ 11}_{n = 2k \text{ biti}} \end{array}\right\} \implies g(x) = 1$$

- $s_0(g) = 1$

Rubinšteina funkcija

Apskatām ievadvirkni garumā $n = 2k$. Funkcija g ir 1 tad un tikai tad, ja ievadā ir tieši viens vieninieku pāris pozīcijās $2i$ un $2i+1$:

$$\left.\begin{array}{l} x = 11\ 00\ 00\ 00\ 00 \\ x = 00\ 11\ 00\ 00\ 00 \\ x = 00\ 00\ 11\ 00\ 00 \\ x = 00\ 00\ 00\ 11\ 00 \\ x = \underbrace{00\ 00\ 00\ 00\ 11}_{n = 2k \text{ biti}} \end{array}\right\} \implies g(x) = 1$$

- $s_0(g) = 1$
- $bs_0(g) = k = \frac{n}{2}$

Rubinšteina funkcija

Apskatām ievadvirkni garumā $n = 2k$. Funkcija g ir 1 tad un tikai tad, ja ievadā ir tieši viens vieninieku pāris pozīcijās $2i$ un $2i + 1$:

$$\left.\begin{aligned} x &= 11\ 00\ 00\ 00\ 00 \\ x &= 00\ 11\ 00\ 00\ 00 \\ x &= 00\ 00\ 11\ 00\ 00 \\ x &= 00\ 00\ 00\ 11\ 00 \\ x &= \underbrace{00\ 00\ 00\ 00\ 11}_{n = 2k \text{ biti}} \end{aligned}\right\} \implies g(x) = 1$$

- $s_0(g) = 1$
- $bs_0(g) = k = \frac{n}{2}$
- $s_1(g) = 2k = n$

Rubinšteina funkcija

Apskatām ievadvirkni garumā $n = 2k$. Funkcija g ir 1 tad un tikai tad, ja ievadā ir tieši viens vieninieku pāris pozīcijās $2i$ un $2i+1$:

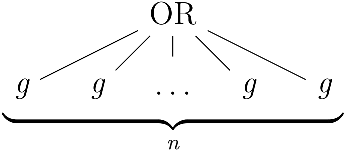
$$\left.\begin{aligned} x &= 11\ 00\ 00\ 00\ 00 \\ x &= 00\ 11\ 00\ 00\ 00 \\ x &= 00\ 00\ 11\ 00\ 00 \\ x &= 00\ 00\ 00\ 11\ 00 \\ x &= \underbrace{00\ 00\ 00\ 00\ 11}_{n=2k \text{ biti}} \end{aligned}\right\} \implies g(x) = 1$$

- $s_0(g) = 1$
- $bs_0(g) = k = \frac{n}{2}$
- $s_1(g) = 2k = n$
- $bs_1(g) = 2k = n$

Rubinšteina funkcija (2)

Ņem $f(x_1, \ldots, x_n) = \mathrm{OR}_l(g(x_1), \ldots, g(x_n))$:

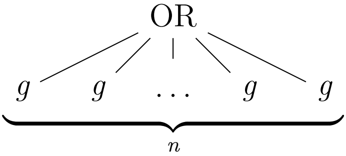
$f =$



Rubinšteina funkcija (2)

Ņem $f(x_1, \ldots, x_n) = \mathrm{OR}_l(g(x_1), \ldots, g(x_n))$:

$f =$



- $s_0(g) = 1$
- $bs_0(g) = \frac{n}{2}$
- $s_1(g) = n$
- $bs_1(g) = n$

Rubinšteina funkcija (2)

Ņem $f(x_1, \ldots, x_n) = \mathrm{OR}_l(g(x_1), \ldots, g(x_n))$:

$$f = \begin{array}{c} \mathrm{OR} \\ \underbrace{g \quad g \quad \ldots \quad g \quad g}_{n} \end{array}$$

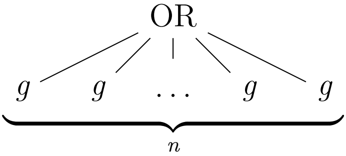
- $s_0(g) = 1$
- $bs_0(g) = \frac{n}{2}$
- $s_1(g) = n$
- $bs_1(g) = n$

- $s_0(f) = n$

Rubinšteina funkcija (2)

Ņem $f(x_1, \dots, x_n) = \mathrm{OR}_l(g(x_1), \dots, g(x_n))$:

$f =$



- $s_0(g) = 1$
- $bs_0(g) = \frac{n}{2}$
- $s_1(g) = n$
- $bs_1(g) = n$

- $s_0(f) = n$
- $bs_0(f) = \frac{n}{2} \cdot n = \frac{1}{2}n^2$

Rubinšteina funkcija (2)

Ņem $f(x_1, \dots, x_n) = \mathrm{OR}_l(g(x_1), \dots, g(x_n))$:

$$f = \underbrace{\overset{\mathrm{OR}}{g \quad g \quad \dots \quad g \quad g}}_{n}$$

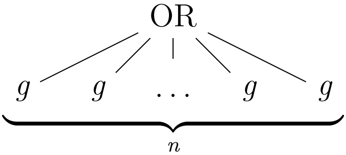
- $s_0(g) = 1$
- $bs_0(g) = \frac{n}{2}$
- $s_1(g) = n$
- $bs_1(g) = n$

- $s_0(f) = n$
- $bs_0(f) = \frac{n}{2} \cdot n = \frac{1}{2} n^2$
- $s_1(f) = n$

Rubinšteina funkcija (2)

Ņem $f(x_1, \ldots, x_n) = \mathrm{OR}_l(g(x_1), \ldots, g(x_n))$:

$f =$



- $s_0(g) = 1$
- $bs_0(g) = \frac{n}{2}$
- $s_1(g) = n$
- $bs_1(g) = n$

- $s_0(f) = n$
- $bs_0(f) = \frac{n}{2} \cdot n = \frac{1}{2} n^2$
- $s_1(f) = n$
- $bs_1(f) = n$

Rubinšteina funkcija (3)

- $s_0(g) = 1$
- $bs_0(g) = \frac{n}{2}$
- $s_1(g) = n$
- $bs_1(g) = n$

Rubinšteina funkcija (3)

- $s_0(g) = 1$
- $bs_0(g) = \frac{n}{2}$
- $s_1(g) = n$
- $bs_1(g) = n$

- $s_0(f) = n$
- $bs_0(f) = \frac{n}{2} \cdot n = \frac{1}{2}n^2$
- $s_1(f) = n$
- $bs_1(f) = n$

Rubinšteina funkcija (3)

- $s_0(g) = 1$
- $bs_0(g) = \frac{n}{2}$
- $s_1(g) = n$
- $bs_1(g) = n$

- $s_0(f) = n$
- $bs_0(f) = \frac{n}{2} \cdot n = \frac{1}{2}n^2$
- $s_1(f) = n$
- $bs_1(f) = n$

Sekas

$$s(f) = \max(s_0(f), s_1(f)) = s_1(f) = n$$

$$bs(f) = \max(bs_0(f), bs_1(f)) = bs_0(f) = \frac{1}{2}n^2$$

Rubinšteina funkcija (3)

- $s_0(g) = 1$
- $bs_0(g) = \frac{n}{2}$
- $s_1(g) = n$
- $bs_1(g) = n$

- $s_0(f) = n$
- $bs_0(f) = \frac{n}{2} \cdot n = \frac{1}{2}n^2$
- $s_1(f) = n$
- $bs_1(f) = n$

Sekas

$$s(f) = \max(s_0(f), s_1(f)) = s_1(f) = n$$

$$bs(f) = \max(bs_0(f), bs_1(f)) = bs_0(f) = \frac{1}{2}n^2$$

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

Monotonas funkcijas

Funkcija f ir monotona, ja, kādu ievada x bitu x_i nomainot no 0 uz 1, $f(x)$ vai nu nemainās, vai nu mainās no 0 uz 1 (bet ne no 1 uz 0).

Monotonas funkcijas

Funkcija f ir monotona, ja, kādu ievada x bitu x_i nomainot no 0 uz 1, $f(x)$ vai nu nemainās, vai nu mainās no 0 uz 1 (bet ne no 1 uz 0).

Monotonas funkcijas piemērs: OR_n. Ir spēkā

$$\mathrm{OR}_n(000\ldots000) = 0$$

Nomainot jebkuru bitu uz 1, $\mathrm{OR}_n(x)$ mainās uz 1. Tālāk mainot atlikušos bitus no 0 uz 1, funkcijas vērtība nemainās (paliek 1).

Monotonas funkcijas

Funkcija f ir monotona, ja, kādu ievada x bitu x_i nomainot no 0 uz 1, $f(x)$ vai nu nemainās, vai nu mainās no 0 uz 1 (bet ne no 1 uz 0).

Monotonas funkcijas piemērs: OR_n. Ir spēkā

$$\mathrm{OR}_n(000\ldots000) = 0$$

Nomainot jebkuru bitu uz 1, $\mathrm{OR}_n(x)$ mainās uz 1. Tālāk mainot atlikušos bitus no 0 uz 1, funkcijas vērtība nemainās (paliek 1).

Cits piemērs — $\mathrm{MAJORITY}_{2k+1}$ funkcija.

Sarežģ́ītības mēri monotonām funkcijām (1)

Apgalvojums: monotonām funkcijām

$$s(f) = bs(f) = C(f)$$

Tā kā mēs jau zinām, ka $s(f) \leqslant bs(f)$ un $bs(f) \leqslant C(f)$, atliek pierādīt $C(f) \leqslant s(f)$.

Sarežģītības mēri monotonām funkcijām (1)

Apgalvojums: monotonām funkcijām

$$s(f) = bs(f) = C(f)$$

Tā kā mēs jau zinām, ka $s(f) \leqslant bs(f)$ un $bs(f) \leqslant C(f)$, atliek pierādīt $C(f) \leqslant s(f)$.

Apskatām 1-sertifikātu S ($|S| = C_1(f)$):

$$S = \underbrace{111\ldots111}_{C_1(f)} *** \ldots ***$$

Jebkuram $x \in S$ izpildās $f(x) = 1$.

Sarežģītības mēri monotonām funkcijām (2)

$$S = \underbrace{111\ldots111}_{C_1(f)} *** \ldots ***$$

Ņemsim vārdu $y = \underbrace{111\ldots111}_{C_1(f)} 000\ldots000$. $f(y) = 1$, jo $y \in S$.

Pieņemsim, ka, nomainot kādu no y 1 bitiem uz 0, f vērtība paliek 1:

$$f(\underbrace{101\ldots111}_{C_1(f)} 000\ldots000) \stackrel{?}{=} 1$$

Bet tad arī $f(\underbrace{101\ldots111}_{C_1(f)} *** \ldots ***) = 1$, un nomainītais bits nepieder y sertifikātam — pretruna. Jāsecina, ka $C_1(f)$ biti ir jūtīgi.

Sekas: $C_1(f) \leqslant s_1(f)$ un $C_0(f) \leqslant s_0(f)$, tātad, $C(f) \leqslant s(f)$.

Plānotie darbi

Gala mērķis

Uzlabot zināmus novērtējumus priekš $bs(f) ? s(f)$ (gan samazinot novērtējumu no augšas, gan palielinot novērtējumu no lejas).

«Reālāki» mērķi

Izskatīt dažādus apakšgadījumus, piemēram:

- $s_0(f) = 1, 2, \ldots$
- $s_1(f) = 1, 2, \ldots$
- dažādi Būla funkciju apakšveidi

Beigas