Dažu kvantu spēļu analīze

Madars Virza

Vadītājs: profesors Andris Ambainis

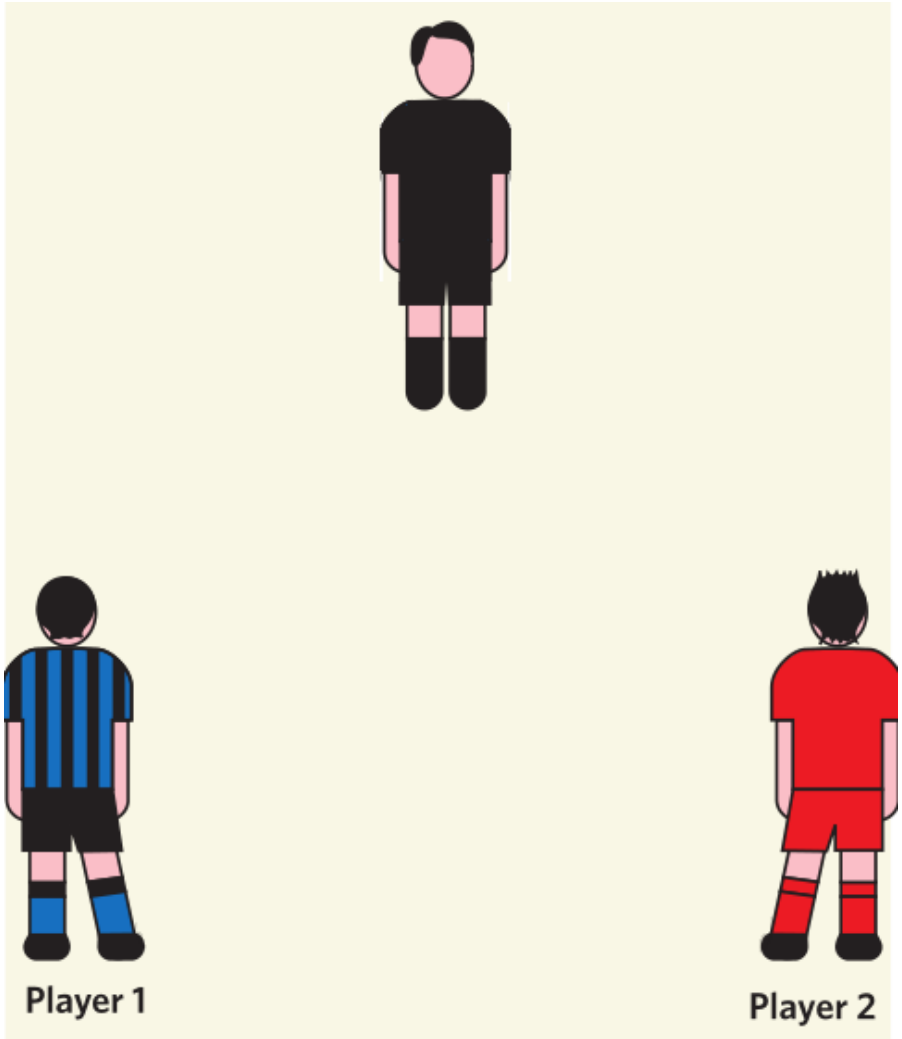
Latvijas Universitāte

2011. gada 6. jūnijā

Kvantu spēles

Nelokāla kvantu spēle

- (S, T, A, B, π, V)

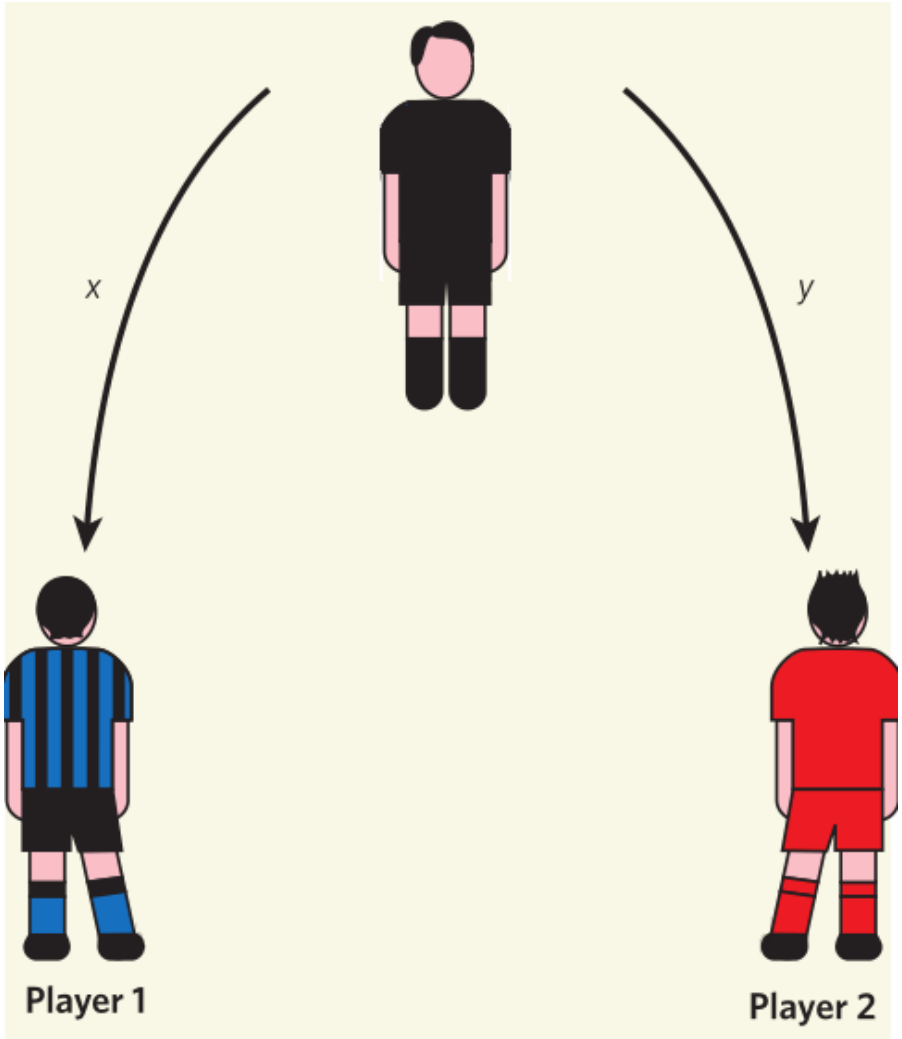


(adaptēts no “Nature”)

Kvantu spēles

Nelokāla kvantu spēle

- (S, T, A, B, π, V)
- $x \in S$, $y \in T$

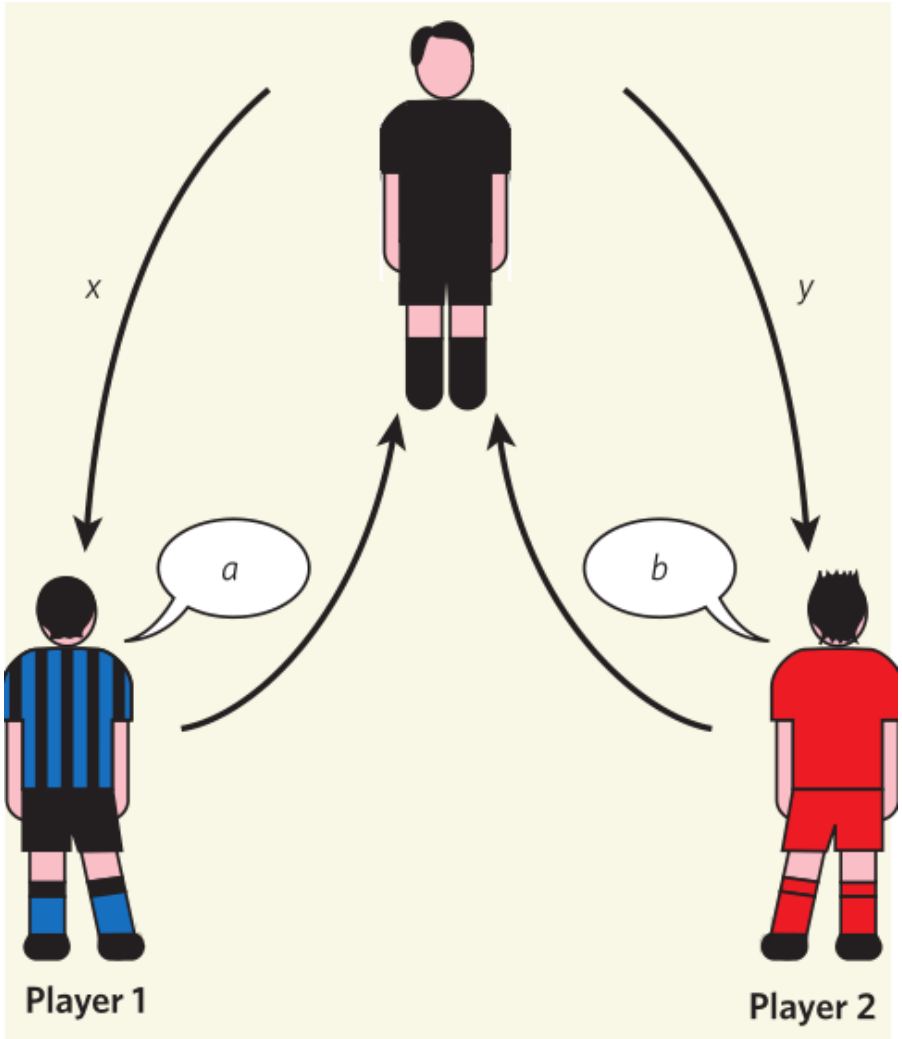


(adaptēts no “Nature”)

Kvantu spēles

Nelokāla kvantu spēle

- (S, T, A, B, π, V)
- $x \in S$, $y \in T$
- $a \in A$, $b \in B$

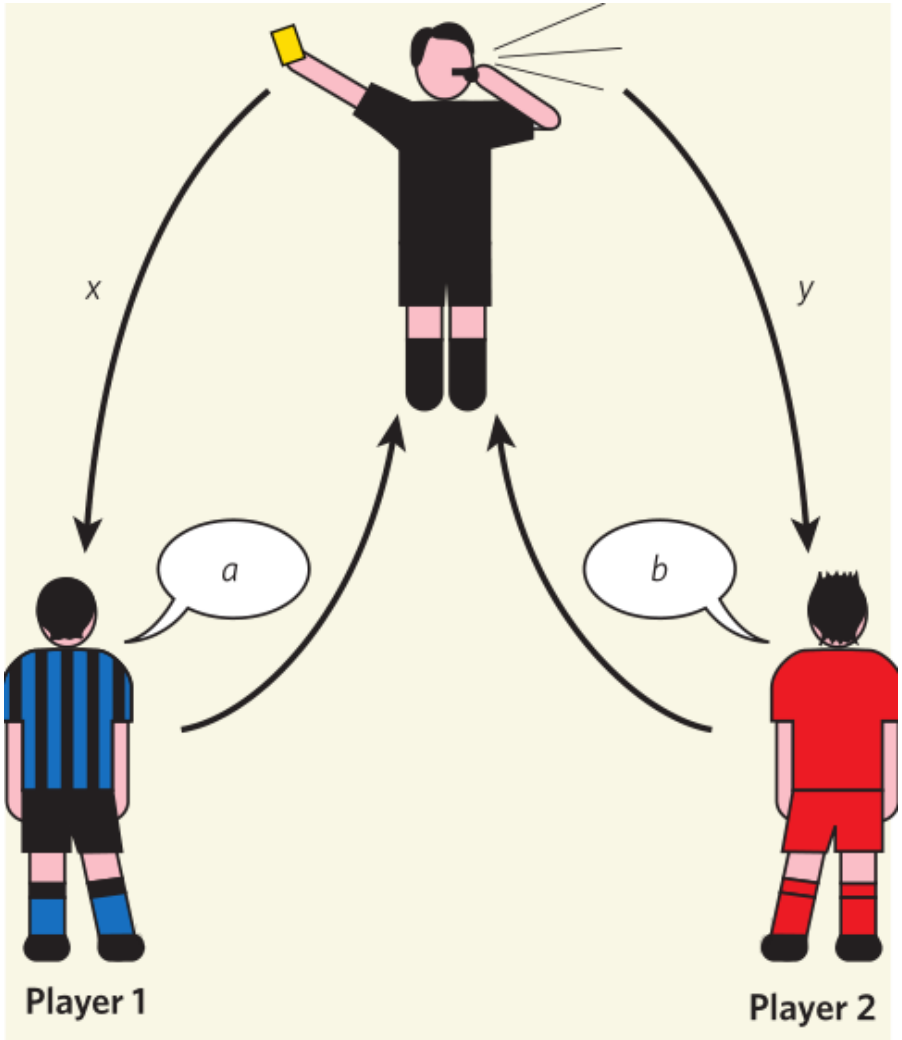


(adaptēts no “Nature”)

Kvantu spēles

Nelokāla kvantu spēle

- (S, T, A, B, π, V)
- $x \in S,\ y \in T$
- $a \in A,\ b \in B$
- spēlētāji uzvar, ja izpildās predikāts $V(x, y, a, b)$

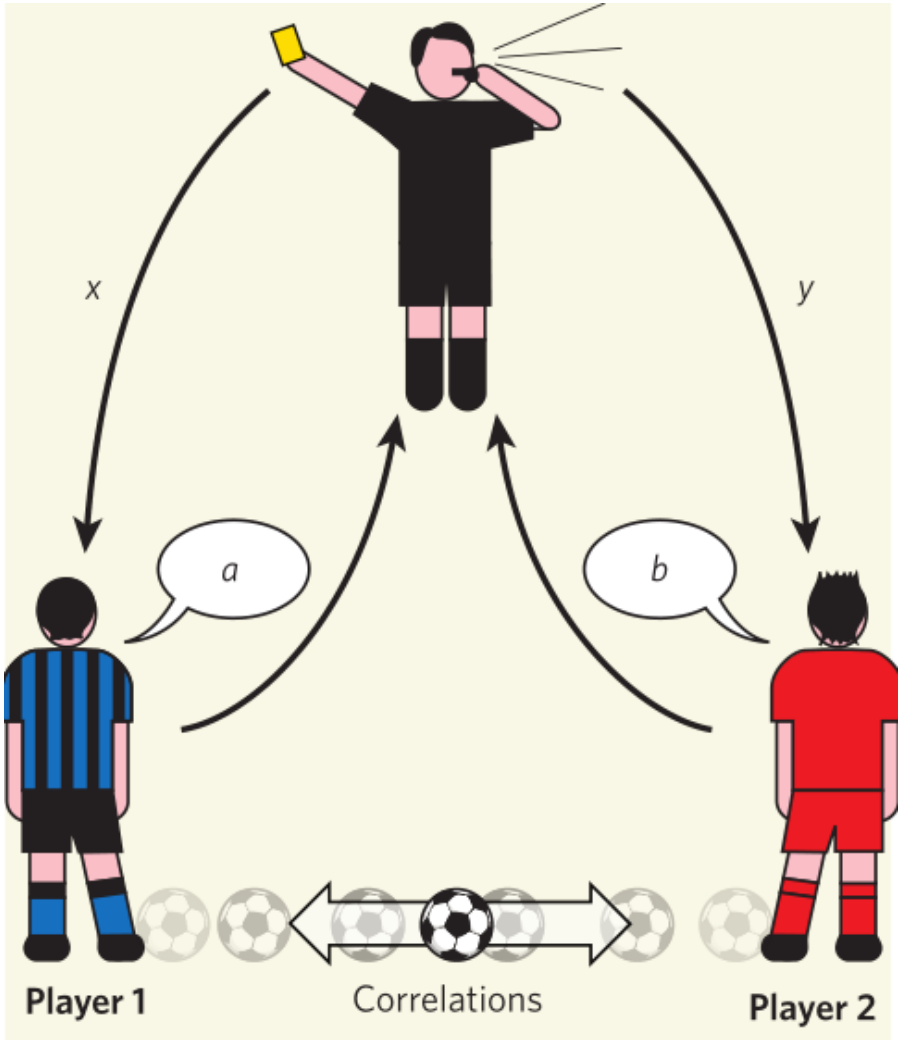


(adaptēts no "Nature")

Kvantu spēles

Nelokāla kvantu spēle

- (S, T, A, B, π, V)
- $x \in S,\ y \in T$
- $a \in A,\ b \in B$
- spēlētāji uzvar, ja izpildās predikāts $V(x, y, a, b)$
- kvantu stratēģija var izmantot kopīgu kvantu stāvokli, klasiskā – kopīgus nejaušus bitus

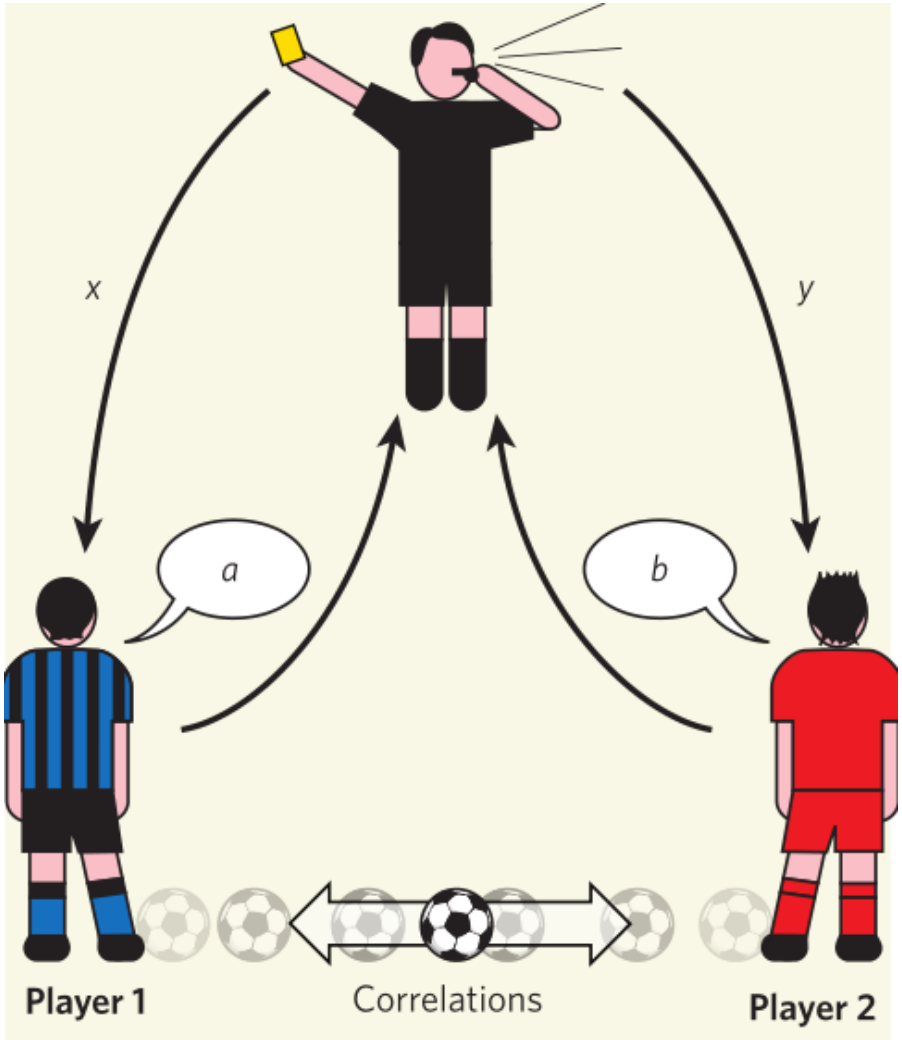


(adaptēts no "Nature")

Kvantu spēles

Nelokāla kvantu spēle

- (S, T, A, B, π, V)
- $x \in S,\ y \in T$
- $a \in A,\ b \in B$
- spēlētāji uzvar, ja izpildās predikāts $V(x, y, a, b)$
- kvantu stratēģija var izmantot kopīgu kvantu stāvokli, klasiskā – kopīgus nejaušus bitus
- spēlētāji var vienoties par stratēģiju, bet ne sazināties

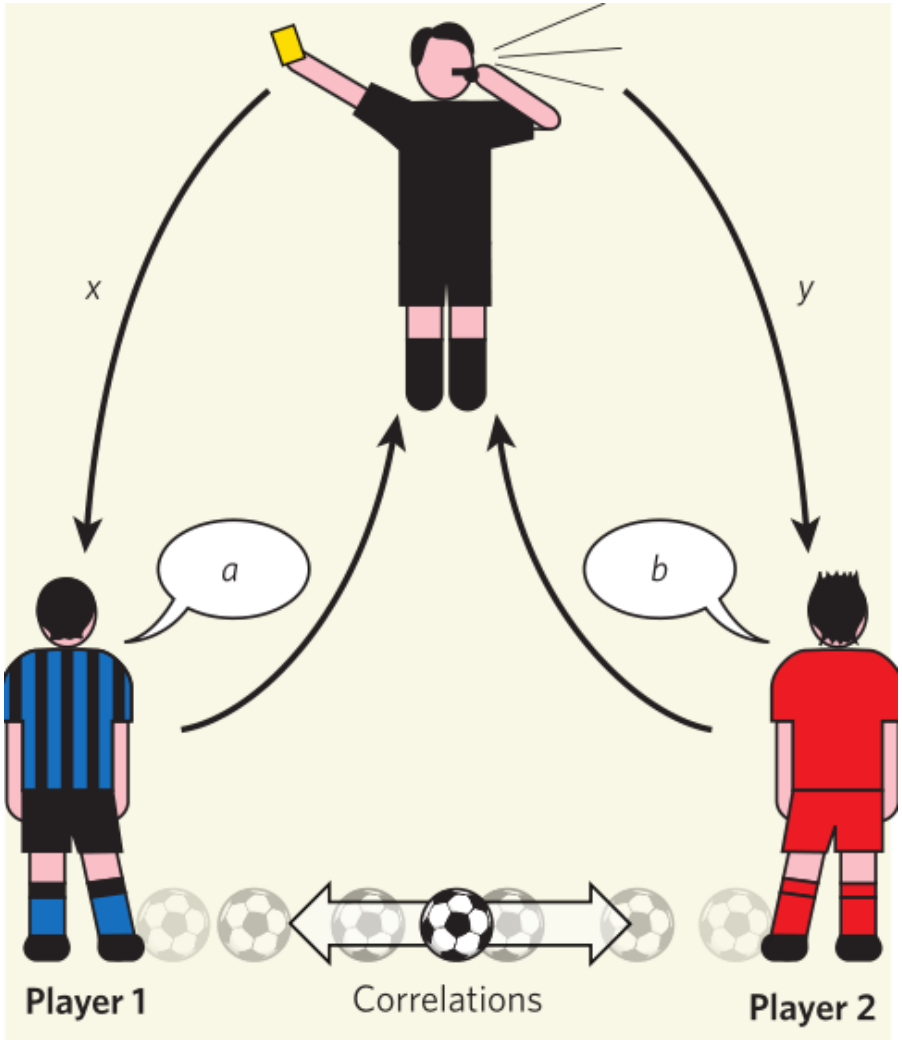


(adaptēts no "Nature")

Kvantu spēles

Nelokāla kvantu spēle

- (S, T, A, B, π, V)
- $x \in S,\ y \in T$
- $a \in A,\ b \in B$
- spēlētāji uzvar, ja izpildās predikāts $V(x, y, a, b)$
- kvantu stratēģija var izmantot kopīgu kvantu stāvokli, klasiskā – kopīgus nejaušus bitus
- spēlētāji var vienoties par stratēģiju, bet ne sazināties



(adaptēts no "Nature")

Problēma un motivācija

Problēma

- atrast kvantu spēles ar interesantām īpašībām,
- atrast metodes kvantu spēļu analīzei un izmantot tās

Problēma un motivācija

Problēma

- atrast kvantu spēles ar interesantām īpašībām,
- atrast metodes kvantu spēļu analīzei un izmantot tās

Pielietojumi

- efektīvi parādīt kvantu pasaules atšķirību no klasiskās,
- kā "būvakmens" citiem rezultātiem. Piemērs: PCP teorēma algoritmu sarežģītības teorijā,
- lai izveidotu kvantu kriptosistēmas, kuras ir drošas pret *side-channel attacks* (*device independent cryptography*)
- godīgu izsoļu nodrošināšana (izstrādes stadijā)

Piemērs

CHSH spēle

Par **CHSH**[a] **spēli** sauksim šādu divu spēlētāju spēli:

- katrs no spēlētājiem saņem vienu bitu, 0 vai 1, pie tam katru no xy komplektiem $00, 01, 10, 11$ tiesnesis izvēlas ar vienādu varbūtību,

[a] no autoru vārdiem – Clauser–Horne–Shimony–Holt

Piemērs

CHSH spēle

Par **CHSH**[a] **spēli** sauksim šādu divu spēlētāju spēli:

- katrs no spēlētājiem saņem vienu bitu, 0 vai 1, pie tam katru no xy komplektiem $00, 01, 10, 11$ tiesnesis izvēlas ar vienādu varbūtību,
- katrs no spēlētājiem atbildē dod vienu bitu, 0 vai 1,

[a] no autoru vārdiem – Clauser–Horne–Shimony–Holt

Piemērs

CHSH spēle

Par **CHSH**[a] **spēli** sauksim šādu divu spēlētāju spēli:

- katrs no spēlētājiem saņem vienu bitu, 0 vai 1, pie tam katru no xy komplektiem $00, 01, 10, 11$ tiesnesis izvēlas ar vienādu varbūtību,
- katrs no spēlētājiem atbildē dod vienu bitu, 0 vai 1,
- spēlētāji uzvar, ja spēlētāju ievadiem x, y un izvadiem a, b izpildās šāda īpašība:

$$f(x, y, a, b) \stackrel{\text{def}}{\equiv} (x \wedge y) = (a \oplus b)$$

[a] no autoru vārdiem – Clauser–Horne–Shimony–Holt

CHSH spēles analīze

Klasisko stratēģiju analīze

Klasiski nevar uzvarēt ar varbūtību > 0.75.
Varbūtību 0.75 var sasniegt.

x	y	pareizās ab
0	0	00 vai 11
0	1	00 vai 11
1	0	00 vai 11
1	1	01 vai 10

$$f(x, y, a, b) \stackrel{\text{def}}{\equiv} (x \wedge y) = (a \oplus b)$$

CHSH spēles analīze

Klasisko stratēģiju analīze

Klasiski nevar uzvarēt ar varbūtību > 0.75.
Varbūtību 0.75 var sasniegt.

Kvantu stratēģiju analīze

Kvantiski var uzvarēt ar varbūtību ≈ 0.85

Ideja: sagatavot kopīgu sapītu stāvokli un mērīt savu stāvokļa daļu citā bāzē atkarībā no ievada.

x	y	pareizās ab
0	0	00 vai 11
0	1	00 vai 11
1	0	00 vai 11
1	1	01 vai 10

$$f(x, y, a, b) \stackrel{\text{def}}{\equiv} (x \wedge y) = (a \oplus b)$$

Par šo darbu

Darbā pētītās problēmas

- Ardehali spēles klasisko stratēģiju analīze
- jaunas kvantu spēles pilnīga analīze novitārā modelī
- pētījumi par nejaušo simetrisko spēļu klasi

Ardehali spēle

XOR spēles

Par **XOR spēli** sauc tādu n spēlētāju spēli ar bināriem izvadiem, kurai spēlētāju uzvaras predikāts katram spēlētāju ievadu kortežam $(a_1, a_2, \ldots, a_n)$ pieļauj tieši vienu spēlētāju izvadu $x_1, x_2, \ldots, x_n$ XOR vērtību $v_{(a_1,a_2,\ldots,a_n)}$.

Ardehali spēle

XOR spēles

Par **XOR spēli** sauc tādu n spēlētāju spēli ar bināriem izvadiem, kurai spēlētāju uzvaras predikāts katram spēlētāju ievadu kortežam $(a_1, a_2, \ldots, a_n)$ pieļauj tieši vienu spēlētāju izvadu $x_1, x_2, \ldots, x_n$ XOR vērtību $v_{(a_1,a_2,\ldots,a_n)}$.

Ardehali spēle

Par **Ardehali spēli** sauksim n spēlētāju XOR spēli, kurai uzvaras predikāts ir šāds:

$$V(a_1, \ldots, a_n, x_1, \ldots, x_n) \stackrel{\text{def}}{\equiv} \begin{cases} \oplus_{i=1}^{n} x_i = 0 & \text{ja } a_1 + \ldots + a_n \equiv 0, 1 \pmod 4 \\ \oplus_{i=1}^{n} x_i = 1 & \text{ja } a_1 + \ldots + a_n \equiv 2, 3 \pmod 4 \end{cases}$$

Motivācija un fons

Ardehali spēles analīze

- pirmo reizi izdarīta Ardehali 1992. gada rakstā, dodot pirmo piemēru, kur kvantiskā uzvaras varbūtība ir eksponenciāli labāka par klasisko

Motivācija un fons

Ardehali spēles analīze

- pirmo reizi izdarīta Ardehali 1992. gada rakstā, dodot pirmo piemēru, kur kvantiskā uzvaras varbūtība ir eksponenciāli labāka par klasisko
- pierādījuma metodes: viennozīmīgi piemērotas Ardehali spēlei

Motivācija un fons

Ardehali spēles analīze

- pirmo reizi izdarīta Ardehali 1992. gada rakstā, dodot pirmo piemēru, kur kvantiskā uzvaras varbūtība ir eksponenciāli labāka par klasisko
- pierādījuma metodes: viennozīmīgi piemērotas Ardehali spēlei
- mūsu metodes: piemērojamas daudzām citām XOR spēlēm, tādējādi vispārinot Ardehali rezultātus

Mūsu rezultāti Ardehali spēles analīzei

Klasisko stratēģiju analīze

Teorēma. Ardehali spēlei ar n spēlētājiem optimālā klasiskā stratēģija sasniedz uzvaras varbūtību $\frac{1}{2} + 2^{-\lceil \frac{n+1}{2} \rceil}$.

Mūsu rezultāti Ardehali spēles analīzei

Klasisko stratēģiju analīze

Teorēma. Ardehali spēlei ar n spēlētājiem optimālā klasiskā stratēģija sasniedz uzvaras varbūtību $\frac{1}{2} + 2^{-\lceil \frac{n+1}{2} \rceil}$.

Kvantu stratēģiju analīze

Teorēma. (Ambainis et. al) Ardehali spēlei ar n spēlētājiem optimālā kvantu stratēģija sasniedz uzvaras varbūtību $\frac{1}{2} + \frac{1}{2\sqrt{2}}$.

Rezultāts iesniegts publicēšanai žurnālā "Theoretical Computer Science".

Apsvērumi par varbūtību sadalījumu π

"Average-case" modelis

- rāda tiesneša neitralitāti pret spēlētājiem – katrs ievads ir vienlīdz varbūtisks,
- praktiski visas publicētās analīzes ir šajā modelī

Apsvērumi par varbūtību sadalījumu π

"Average-case" modelis

- rāda tiesneša neitralitāti pret spēlētājiem – katrs ievads ir vienlīdz varbūtisks,
- praktiski visas publicētās analīzes ir šajā modelī

"Worst-case" modelis

- tiesnesis nav spēlētājiem draudzīgs – varbūtību sadalījums ir maksimāli nelabvēlīgs,
- modeļa ideja: profesors Rūsiņš Freivalds

EQUAL-EQUAL spēle

Fons

Visām publicētajām analīzēm "average-case" sakrīt ar "worst-case". EQUAL-EQUAL spēle ir radusies, mēģinot izdomāt nesamākslotu piemēru, kur tā nav.

EQUAL-EQUAL spēle

Par **EQUAL-EQUAL spēli** sauksim divu spēlētāju spēli ar n ievadiem un bināriem izvadiem katram spēlētājam (t.i. $S, T = \{1, 2, \ldots, n\}$ un $A, B = \{0, 1\}$, iepriekš dotās definīcijas apzīmējumos), kurai spēlētāju uzvaras predikāts V ir šāds:

$$V(s, t, a, b) \stackrel{\text{def}}{\equiv} (s = t) \Leftrightarrow (a = b)$$

EQUAL-EQUAL spēles analīze

Galvenā teorēma

Teorēma. EQUAL-EQUAL spēlei ar n spēlētājiem izpildās šādas īpašības:

1. eksistē fiksētas kvantu un klasiskās stratēģijas, kas jebkuram varbūtību sadalījumam dod uzvaras varbūtību $\approx \frac{2}{3}$,

EQUAL-EQUAL spēles analīze

Galvenā teorēma

Teorēma. EQUAL-EQUAL spēlei ar n spēlētājiem izpildās šādas īpašības:

1. eksistē fiksētas kvantu un klasiskās stratēģijas, kas jebkuram varbūtību sadalījumam dod uzvaras varbūtību $\approx \frac{2}{3}$,
2. eksistē varbūtību sadalījums, kuram jebkura kvantu un jebkura klasiskā stratēģija nevar dot labāku uzvaras varbūtību par $\approx \frac{2}{3}$,

EQUAL-EQUAL spēles analīze

Galvenā teorēma

Teorēma. EQUAL-EQUAL spēlei ar n spēlētājiem izpildās šādas īpašības:

1. eksistē fiksētas kvantu un klasiskās stratēģijas, kas jebkuram varbūtību sadalījumam dod uzvaras varbūtību $\approx \frac{2}{3}$,
2. eksistē varbūtību sadalījums, kuram jebkura kvantu un jebkura klasiskā stratēģija nevar dot labāku uzvaras varbūtību par $\approx \frac{2}{3}$,
3. nevienam no (α, β) vienmērīgiem ievaddatu varbūtību sadalījumiem nav kvantu priekšrocības,

EQUAL-EQUAL spēles analīze

Galvenā teorēma

Teorēma. EQUAL-EQUAL spēlei ar n spēlētājiem izpildās šādas īpašības:

1. eksistē fiksētas kvantu un klasiskās stratēģijas, kas jebkuram varbūtību sadalījumam dod uzvaras varbūtību $\approx \frac{2}{3}$,
2. eksistē varbūtību sadalījums, kuram jebkura kvantu un jebkura klasiskā stratēģija nevar dot labāku uzvaras varbūtību par $\approx \frac{2}{3}$,
3. nevienam no (α, β) vienmērīgiem ievaddatu varbūtību sadalījumiem nav kvantu priekšrocības,
4. eksistē varbūtību sadalījums ar kvantu priekšrocību

Secinājumi par EQUAL-EQUAL spēli

Secinājumi

Iegūts pārsteidzošs rezultāts: "worst-case" atšķiras no "average-case", bet lielai dabiskai varbūtību sadalījumu grupai nav kvantu priekšrocības.
Neatrisināta problēma: vai tā ir vienmēr?

Simetrisko spēļu klase

Simetriskās spēles

Par **simetrisku spēli** sauc tādu n spēlētāju XOR spēli ar bināriem ievadiem $a_1, \ldots, a_n$, kurai spēlētāju atbilžu paritātei ir jābūt atkarīgi tikai no a_i summas:

$$V(a_1, a_2, \ldots, a_n, x_1, x_2, \ldots, x_n) \stackrel{\text{def}}{=} \oplus_{i=1}^{n} x_i = v_{a_1+a_2+\ldots+a_n}$$

Šie v_0, ..., v_n arī unikāli raksturo n spēlētāju simetrisku spēli.

Simetrisko spēļu klase

Simetriskās spēles

Par **simetrisku spēli** sauc tādu n spēlētāju XOR spēli ar bināriem ievadiem $a_1, \ldots, a_n$, kurai spēlētāju atbilžu paritātei ir jābūt atkarīgi tikai no a_i summas:

$$V(a_1, a_2, \ldots, a_n, x_1, x_2, \ldots, x_n) \stackrel{\text{def}}{=} \oplus_{i=1}^{n} x_i = v_{a_1+a_2+\ldots+a_n}$$

Šie v_0, ..., v_n arī unikāli raksturo n spēlētāju simetrisku spēli.

Simetrisko spēļu piemēri

- Ardehali spēle,
- "n biti pa apli" spēle

Nejaušas simetriskas spēles

Simetriskās spēles

Par **simetrisku spēli** sauc tādu n spēlētāju XOR spēli ar bināriem ievadiem $a_1, \ldots, a_n$, kurai spēlētāju atbilžu paritātei ir jābūt atkarīgi tikai no a_i summas:

$$V(a_1, a_2, \ldots, a_n, x_1, x_2, \ldots, x_n) \stackrel{\text{def}}{\equiv} \oplus_{i=1}^{n} x_i = v_{a_1+a_2+\ldots+a_n}$$

Šie v_0, ..., v_n arī unikāli raksturo n spēlētāju simetrisku spēli.

Nejauša simetriska spēle

Par **nejaušu simetrisku spēli** sauc tādu n spēlētāju simetrisku spēli, kurai v_0, ..., v_n ir izvēlēti nejauši, neatkarīgi, 0 un 1 izvēlēm esot vienlīdz varbūtiskām.

Nejaušu simetrisku spēļu analīze

Klasiskās stratēģijas

Sagaidāmā vislabākās klasiskās stratēģijas uzvaras varbūtība ir vismaz

$$\frac{1}{2}(1+\sqrt[4]{\frac{4}{\pi^3 n}}) \approx \frac{1}{2} + 0.2996\sqrt[4]{1/n}$$

.

Nejaušu simetrisku spēļu analīze

Klasiskās stratēģijas

Sagaidāmā vislabākās klasiskās stratēģijas uzvaras varbūtība ir vismaz

$$\frac{1}{2}(1+\sqrt[4]{\frac{4}{\pi^3 n}}) \approx \frac{1}{2} + 0.2996\sqrt[4]{1/n}$$

.

Kvantu stratēģijas

Sagaidāmā vislabākās kvantu stratēģijas uzvaras varbūtība ir vismaz

$$\frac{1}{2}(1+\sqrt[4]{\frac{1}{\pi n}}) \approx \frac{1}{2} + 0.3761\sqrt[4]{1/n}$$

.

Nejaušu simetrisku spēļu analīze – vēlāk sasniegtais

Klasiskās stratēģijas

Sagaidāmā vislabākās klasiskās stratēģijas uzvaras varbūtība ir vismaz

$$\frac{1}{2}(1+\sqrt[4]{\frac{16}{\pi^3 n}}) \approx \frac{1}{2} + 0.4237\sqrt[4]{1/n}$$

.

Kvantu stratēģijas

Sagaidāmā vislabākās kvantu stratēģijas uzvaras varbūtība ir vismaz

$$\frac{1}{2}(1+\sqrt[4]{\frac{16}{\pi^3 n}}) \approx \frac{1}{2} + 0.4237\sqrt[4]{1/n}$$

.

Nejaušu simetrisku spēļu analīze

Secinājumi

- datoreksperimentu rezultāti rāda, ka kvantu stratēģiju uzvaras varbūtībai vēl papildus nāk klāt logaritmisks loceklis, tāpat klasiskām stratēģiju jaunais apakšējais novērtējums ir diezgan precīzs,
- rezultāti ir pietiekami, lai pierādītu, ka Ardehali spēle nav tipiska simetriska spēle,
- trūkst labu augšējo novērtējumu un nepieciešami turpmāki pētījumi

Rezultāti

Galvenie autora rezultāti

- jauna, vispārīgāka Ardehali spēles klasisko stratēģiju analīze,
- `EQUAL-EQUAL` spēles pilnīga analīze, pamatojot oriģinālas un interesantas kvantu spēles eksistenci,
- apakšējie novērtējumi nejaušo simetrisko spēļu klasei

Rezultāti

Galvenie autora rezultāti

- jauna, vispārīgāka Ardehali spēles klasisko stratēģiju analīze,
- `EQUAL-EQUAL` spēles pilnīga analīze, pamatojot oriģinālas un interesantas kvantu spēles eksistenci,
- apakšējie novērtējumi nejaušo simetrisko spēļu klasei

Rezultātus plānots publicēt kā nodaļas trim dažādiem rakstiem. Ardehali analīze ir iesniegta "Theoretical Computer Science".

Jautājumi?

http://madars.org/qgames/