

**Informatika**

# BE KOMPIUTERIO **D**

## Turininga informatikos mokymosi medžiaga mokiniam

Parašė Timas Bellas, Ianas H. Wittenas ir Mike'as Fellowas

Darbui klasėje pritaikė Robynas Adamsas ir Jane McKenzie

Iliustravo Mattas Powellas

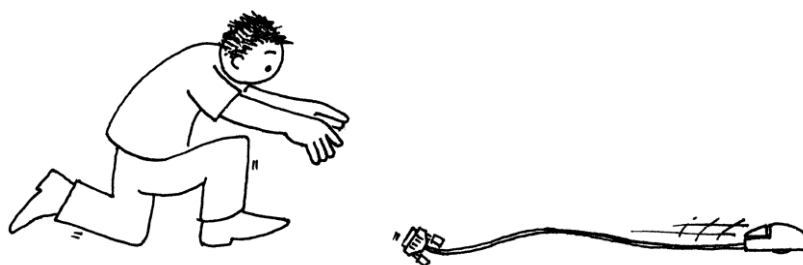
Atnaujino Samas Jarmanas

Į lietuvių kalbą išvertė Valentina Dagienė ir Eglė Jasutė

Peržiūrėjo ir papildė Alvida Lozdienė

Redagavo Audra Ivanauskienė

Viršelį kūrė Vaidotas Kinčius



<http://csunplugged.org/>



Licensed under Creative Commons

© 2015 Computer Science Unplugged (csunplugged.org)

# Turinys

Įvadas .....	4
Padėka .....	6
I dalis Duomenys Informacijos atvaizdavimas .....	7
Duomenys. Pradžią pradžia .....	8
Taškų skaičiavimas. Dvejetainiai skaičiai .....	9
Spalvinimas skaičiais. Paveikslai kompiuteryje .....	29
Pakartok tai dar kartą! Teksto suspaudimas .....	38
Kortelių keitimo magija. Klaidų radimas ir taisymas .....	47
Dvidešimt spėjimų. Informacijos teorija .....	55
II dalis Kaip veikia kompiuteris? Algoritmai .....	61
Laivų mūšis. Paieškos algoritmai .....	63
Lengviausias ir sunkiausias. Rikiavimo algoritmai .....	82
Dar sparčiau! Tinklinis rikiavimas .....	89
Purvinas miestas. Minimalūs jungiantieji medžiai .....	94
Apelsinų žaidimas. Maršruto parinkimas ir tinklo aklavietė .....	100
Akmeninės plokštelės. Tinklo komunikacijų protokolas.....	103
Linijų braižymas .....	110
III dalis Kaip pasakyti kompiuteriui, ką jis turi daryti? Algoritmų užrašymas .....	124
Kaip pasakyti kompiuteriui, ką jis turi daryti? .....	125
Lobio ieškojimas. Baigtiniai automatai .....	126
Nurodymų eilė. Programavimo kalbos .....	143
IV dalis Ko kompiuteris negali? Sunkiai sprendžiami uždaviniai .....	148
Vargšas kartografas. Grafo spalvinimas .....	150



Turistų miestas. Dominuojančios sekos .....	162
Ledo kelias. Šteinerio medžiai .....	168
V dalis Informacijos šifravimas Kriptografija.....	177
Informacijos šifravimas .....	178
Dalijimasis paslaptimis. Informacijos slėpimo protokolai.....	181
Monetos metimas. Kriptografijos protokolai .....	185
Vaikai šnipai. Viešojo rakto kriptografija.....	196
Simetrinio rakto kriptografija.....	208
VI dalis Žmogiškasis kompiuterio veidas Bendravimas su kompiuteriu ....	214
Šokolado fabrikas. Žmogaus sąsajos su kompiuteriu projektavimas.....	217
Dialogas su kompiuteriu. Tiuringo testas.....	228
Protingas popieriaus lapas.....	239



# Įvadas

---

Kompiuteriai mus supa visur. Visiems reikia mokytis jais naudotis, o dauguma iš mūsų be jų neapsieiname nė dienos. Kaipgi veikia kompiuteriai? Kaip jie „mąsto“? Kaip žmonės sukuria greitai veikiančias ir lengvai naudojamas kompiuterių programas? Informatika – vienas iš patrauklių šiandienos mokslų, atsakantis į klausimus, kaip veikia kompiuteris, kaip gerinti jo darbą, kaip sukurti dar patogesnius žmogui įrenginius. Šioje knygoje aprašomos įdomios ir smagios įvairaus amžiaus mokiniams skirtos užduotys, vadinamos veiklomis, supažindinama su kompiuterio veikimo pagrindais. Svarbiausia, kad visa tai pateikiama net nesiliečiant prie paties kompiuterio!

Ši didaktinė medžiaga pravers ne tik informatikos užklasinėse veiklose, būreliuose, bet ir įprastose pamokose. Net ir ne informatikai gali smagiai susipažinti su kai kuriais informatikos pagrindais atlikdami kai kurias veiklas drauge su mokiniais. Knygoje lengva ir suprantama kalba aprašoma daug veiklų iš įvairių informatikos temų. Pateikiami visų užduočių atsakymai, kiekviena veikla baigiama skyreliu „Apie ką visa tai?“, kuriame aiškinama atliktos veiklos teorija.

Daugelis veiklų grindžiamos matematika, pavyzdžiui, dvejetainiai skaičiai, žemėlapiai ir grafai, modeliai ar struktūros, rikiavimo užduotys ir, žinoma, kriptografija. Kitos veiklos labiau siejamos su informacinėmis technologijomis, kompiuterių veikimo pagrindais. Pateikiamas prasmingas kontekstas skatina mokinius aktyviai bendrauti, kartu spręsti problemas, atlikti kūrybinį darbą ir mąstyti. Šios veiklos ypač lavina mokinių informatinį mąstymą, kurį skatinti siekiama moderniomis mokyklų programomis.

Daugiau papildomos ir laisvai prieinamos medžiagos, įskaitant vaizdo įrašus ir paveikslus, pateikiama projekto *Unplugged* svetainėje [csunplugged.org](https://csunplugged.org). Svetainėje pateikta daug atvirosios medžiagos, pamokų, rekomendacijų siejant su informatika ir informatiniu mąstymu mokykloje, aprašoma ugdymo programos struktūra. 2023 m. lietuviška knygos versija peržiūrėta ir papildyta naujomis veiklomis.

Šią knygą parašė trys informatikos dėstytojai ir du mokytojai remdamiesi didele patirtimi mokykloje ir atsižvelgdami į šimtus pastabų bei pasiūlymų, gautų per porą dešimtmečių iš šią medžiagą naudojančių mokytojų. Įsitikinta, kad dauguma svarbių informatikos konceptų gali būti mokoma be kompiuterio. Iš tiesų kartais kompiuteris pernelyg atitraukia mokinių dėmesį nuo mokymosi. Dažnai informatikos pamokos pradedamos programavimo mokymu, tačiau tai motyvuoja ne visus mokinius, todėl tokia pradžia gali tapti reikšminga kliūtimi norint sudominti mokinius šiuolaikiniais informatikos principais. Taigi išjunkite kompiuterius ir pasiruoškite mokytis tikrosios informatikos!

Šią knygą galima laisvai parsisiųsti ir ja naudotis – tokią galimybę suteikia *Google Inc.* parama. Knyga platinama pagal kūrybinių bendrijų licenciją (<https://xn--ratija->



ckb.lt/?s=k%C5%ABry%CC%81bini%C5%B3+bendri%CC%87%CC%80j%C5%B3+licen%C5%83cija&custom\_action=custom\_search). Tai reiškia, kad knyga galima laisvai dalytis: ją kopijuoti, platinti ar persiųsti. Taip pat leidžiama knygą atnaujinti. Visa tai galima daryti laikantis šių sąlygų: būtina nurodyti knygos autorius, nenaudoti jos komerciniais tikslais, pakeista ar pertvarkyta knyga arba šios medžiagos pagrindu sukurta nauja knyga turi būti platinama pagal panašią arba tą pačią licenciją. Daugiau informacijos apie šią licenciją galite rasti internete, ieškokite CC BY–NC–SA 3.0.

Siūlome šią medžiagą naudoti klasėje ar užklausinėje veikloje: galite išspausdinti knygos kopiją ir dauginti darbo lapus mokiniams. Klauskite vertėkų ir teikite jiems siūlymų (žr. [csunplugged.org](http://csunplugged.org)).

Knyga išversta į daugelį kalbų. Apie vertimus į kitas kalbas galite sužinoti svetainėje [csunplugged.org](http://csunplugged.org).

Į lietuvių kalbą šią knygą išvertė Vilniaus universiteto mokslininkės prof. dr. Valentina Dagienė ir doc. dr. Eglė Jasutė, peržiūrėjo ir papildė Alvida Lozdienė. Redagavo Audra Ivanauskienė. Viršelį sukūrė Vaidotas Kinčius.



## Padėka

---

Daug mokinių ir mokytojų padėjo tobulinti šią knygą. Pirmieji išbandžiusieji čia aprašytas veiklas buvo mokiniai ir jų mokytojai iš Kanados Britų Kolumbijos provincijos sostinės Viktorijos *South Park* mokyklos, Naujosios Zelandijos Kraistčerčo *Shirley, Ilam* ir *Westburn* pradinė mokyklų. Nuoširdžiai dėkojame mokytojams Lindai Picciotto, Karen Able, Bryonui Porteousui, Paului Cathro, Tracy Harrold, Simone Tanoa, Lorraine Woodfield ir Lynn Atkinson, kad įsileido į savo pamokas ir teikė vertingų pasiūlymų, kaip tobulinti veiklas. Gwenda Bensemman specialiai mums parengė keleto veiklų pamokų ir pasiūlė, kaip ir ką keisti. Richardas Lyndersas ir Sumantas Murugeshas taip pat padėjo išbandyti veiklas pamokose. Dalį kriptografijos veiklų sukūrė Kenas Noblitzas. Kai kurias veiklas praktiškai atliko Viktorijos „Mathmania“ grupė, padedama Kathy Beveridge. Pradinius paveikslus kūrė Malcolmas Robinsonas ir Gail Williams. Gavome patarimų iš Hanso Knutsono. Prie šio projekto daug prisidėjo Mattas Powellas. Esame dėkingi Braino Masono mokslo ir technikos koncernui (angl. *Brian Mason Scientific and Technical Trust*) už dosnų šios knygos pradinės versijos finansavimą.

Ypač dėkojame Paului ir Ruth Ellen Howardams, kurie testavo daugelį šios knygos veiklų ir pateikė daugybę vertingų pasiūlymų. Peteris Hendersonas, Bruce'as McKenzie, Joan Mitchell, Nancy Walker-Mitchell, Gwen Stark, Tony Smithas, Timas A. H. Bellas<sup>1</sup>, Mike'as Hallettas ir Haroldas Thimbleby taip pat pasidalijo savo mintimis.

Esame dėkingi savo šeimų nariams: Bruce'ui, Fran, Grantui, Judith ir Pam už paramą ir Andrew, Annai, Hannah'i, Maxui, Michaelui ir Nikki, kurie buvo šio darbo įkvėpėjai ir pirmieji vaikai, testuodavę naują veiklą.

Ypač dėkojame *Google Inc.* už projekto *Unplugged* finansavimą ir galimybę laisvai platinti šią knygą.

Laukiame atsiliepimų ir siūlymų apie veiklas. Autoriams galite rašyti svetainėje [csunplugged.org](http://csunplugged.org).

*Autoriai*

---

<sup>1</sup> Nesusijęs su pirmuoju autoriumi.



# I dalis

## Duomenys

### Informacijos atvaizdavimas



# Duomenys. Pradžių pradžia

---

## Kaip informacija laikoma kompiuteryje?

Žodis „kompiuteris“ kilęs iš lotynų kalbos žodžio „computare“, reiškiančio „skaičiuoti“ arba „sudėti“. Šiuolaikiniai kompiuteriai gali daug daugiau, nei tik skaičiuoti. Juose gali būti kaupiama ir laikoma visa biblioteka, jie gali padėti rašyti tekstus, ieškoti informacijos, groti muziką ar rodyti vaizdo įrašus. Kaipgi juose laikoma visa ši informacija? Neįtikėtina, bet kompiuteriui reikia tik dviejų ženklų: nulio ir vieneto!

## Kuo skiriasi duomenys ir informacija?

Duomenys yra žaliava – skaičiai, kuriais operuoja kompiuteris. Kompiuteris duomenis paverčia informacija (žodžiais, skaičiais ir paveikslais), kurią gali suprasti žmogus.

## Kaip skaičiai, raidės, žodžiai ir paveikslai paverčiami nuliais ir vienetais?

Šiame skyriuje supažindinama su dvejetainiais skaičiais, aiškinama, kaip kompiuteriai vaizduoja paveikslus, kaip veikia fakso aparatai, kaip geriausia laikyti didelius informacijos kiekius, kaip išvengti klaidų ir kaip matuojama kompiuteryje laikoma informacija.





# 1 veikla

## Taškų skaičiavimas. Dvejetainiai skaičiai

---

### Santrauka

Kompiuteryje laikomus duomenis, pavyzdžiui: žodžius ir skaičius galime pavaizduoti skaitmenų 0 ir 1 sekomis.

### Ryšiai su ugdymo programomis

- ✓ Matematika: skaičiai, skaičių vaizdavimas dvejetainėje sistemoje
- ✓ Matematika: algebra, begalinė seka, sekos taisyklės, dvejetainiai laipsniai

### Gebėjimai

- ✓ Skaičiavimo
- ✓ Atitikčių nustatymo
- ✓ Sekos sudarymo

### Amžius

- ✓ Nuo 6 metų

### Priemonės

- ✓ Penkios dvejetainių skaičių kortelės. Rekomenduojama padaryti abipusių A4 formato kortelių: šypsienėlės vienoje pusėje, taškai – kitoje pusėje.

Kiekvienam mokiniui reikia:

- ✓ 5 kortelių
- ✓ Darbo lapo su dvejetainiais laipsniais

Kitų veiklų priemonės kiekvienam mokiniui:

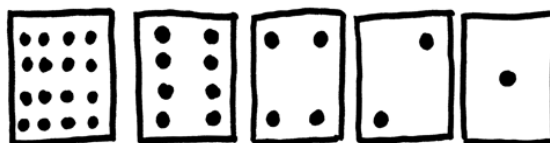
- ✓ Darbo lapas „Dvejetainiai skaičiai“
- ✓ Darbo lapas „Slapta žinutė“
- ✓ Darbo lapas „Elektroninis paštas ir modemai“
- ✓ Darbo lapas „Didesnių už 31 skaičių vaizdavimas“
- ✓ Darbo lapas „Gimtadienio torto žvakutės“
- ✓ Darbo lapas „Raidžių kodavimas“
- ✓ Darbo lapas „Daugiau apie dvejetainius skaičius“



# Dvejetainiai skaičiai

## Įvadas

Veikla visai klasei. Šiai veiklai reikia penkių kortelių (gali būti A4 formato), kurių vienoje pusėje surašyti taškai, o kita pusė – tuščia. Parenkami penki mokiniai, jie atsistoja prieš klasę ir laiko šias korteles. Kortelės rodomos tokia tvarka:



Žaidimo pavyzdį ir galimybes galima pažiūrėti vaizdo įrašė:

<https://www.teachertube.com/videos/computer-science-unplugged-binary-english-27642>

## Diskusija

Iš pradžių kortelės rodomos tuščiaja puse. Atverčiama pirmoji kortelė iš dešinės stebinčių mokinių atžvilgiu. Mokinių prašoma spėti, kiek taškų yra kortelėje, esančioje atverstosios kortelės dešinėje. Atspėjus atverčiama antroji kortelė. Mokiniai turi pastebėti ryšį tarp gretimų kortelių taškų skaičiaus. (Kiekvienoje tolesnėje kortelėje yra dvigubai daugiau taškų, nei buvo prieš tai atverstoje.)

Kiek taškų turėtų būti šeštoje kortelėje? (32) Septintoje? (64)

Stovintys mokiniai korteles vėl atverčia tuščiomis pusėmis į priekį. Prašoma kortelėmis pavaizduoti įvairius skaičius: 6 (atverčiamos 4 ir 2 taškų kortelės), 15 (atverčiamos 8, 4, 2 ir 1 taško kortelės).

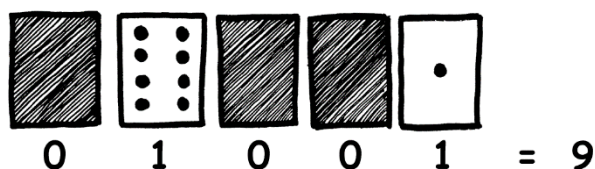
Taisyklė: nereikalingos kortelės turi būti užverstos, o reikalingos – atverstos.

Koks galimas mažiausias taškų skaičius kortelėje? (0)

Toliau verčiant korteles vaizduojami skaičiai iš eilės nuo nulio.

Klasės mokiniai gali prieiti arčiau pažiūrėti, kaip verčiamos kortelės rodant įvairius skaičius. Galima keisti korteles laikančius mokinius.

Užversta taškų kortelė atitinka 0. Atversta kortelė atitinka 1. Taip gaunama dvejetainė skaičiaus išraiška.



Mokinių prašoma parodyti 01001.

Koks dešimtainis skaičius atitinka šį dvejetainį skaičių? (9)

Koks dvejetainis skaičius atitinka dešimtainį skaičių 17? (10001)

Tokiu būdu skirtingi skaičiai vaizduojami keletą kartų, kol mokiniai perpranta sistemą. Siūloma atlikti ir kitokias dvejetainių skaičių veiklas..



# Darbo lapas. Dvejetainiai skaičiai

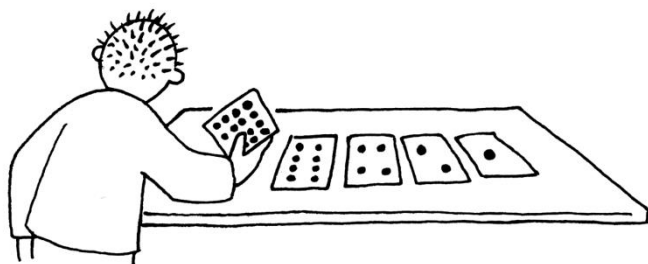
## Mokytiis skaičiuoti

Jūs tikrai mokate skaičiuoti, juk taip? O dabar išbandykite naują skaičiavimo būdą!

Ar žinote, kad kompiuteriai naudoja tik 0 ir 1? Viskas, ką girdite ir matote kompiuteryje (žodžiai, paveikslai, vaizdo įrašai ir net garsai), užrašyta tik dviejų skaitmenų sekomis! Tolesnių veiklų tikslas – išmokyti siųsti koduotas žinutes draugams taip, kaip daro kompiuteris.

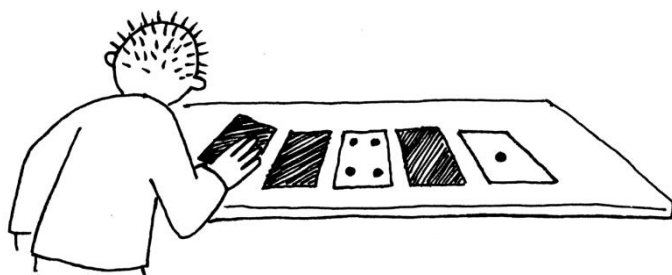
## Įvadas

Sukarpykite taškų korteles (tolesnis lapas).



Išdėliokite korteles iš eilės nuo 1, 2, 4, ... atversdami tuščia puse į viršų.

Atverskite korteles, kurių taškų suma būtų 5. Kortelių tvarkos nekeiskite!



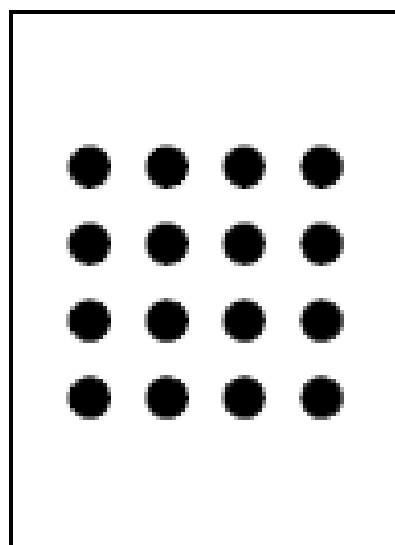
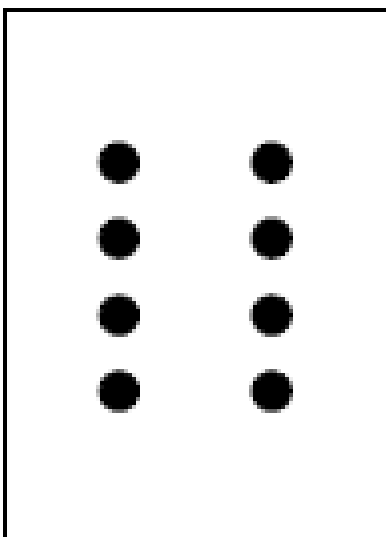
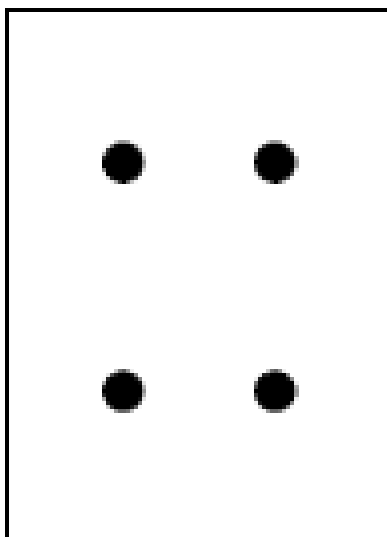
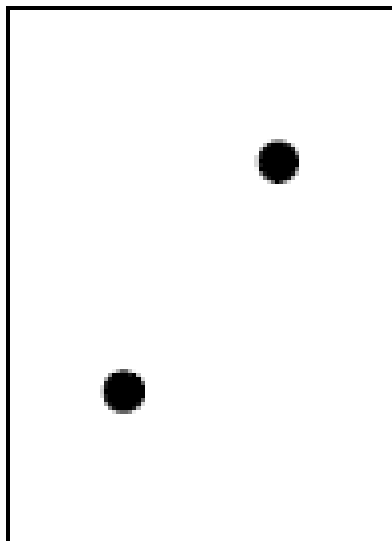
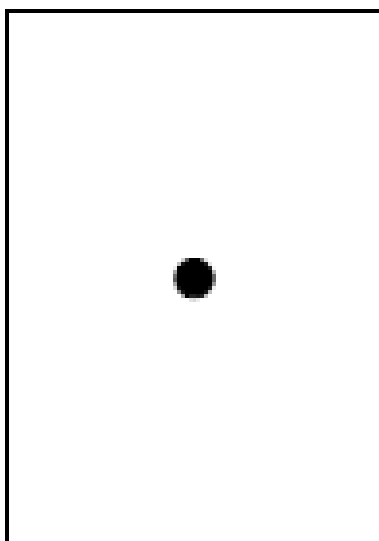
Atverskite korteles, kurių taškų suma būtų 3, 12, 19. Ar galite daugiau nei vienu būdu atversti korteles, kad gautumėte tą patį skaičių? Kokį didžiausią taškų skaičių galite atversti? Kokį mažiausią skaičių galite atversti? Ar tarp mažiausio ir didžiausio taškų skaičiaus yra skaičius, kurio negalima atversti kortelėmis?

**Gudručiams. Pabandykite kortelėmis pavaizduoti skaičius iš eilės 1, 2, 3, 4, ... Gal galite sugalvoti logišką ir praktišką kortelių atvertimo metodą, kad verčiant korteles skaičiai didėtų vienetu?**



# Dvejetainiai skaičiai

---









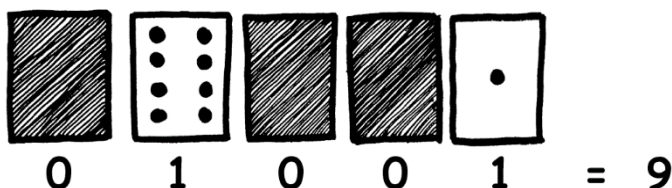






## Darbo lapas. Dvejetainiai skaičiai

Dvejetainė sistema turi tik du skaitmenis: **nulį** ir **vienetą**. Jei kortelė užversta, tai reiškia **0**, jei atversta – **1**. Pavyzdžiui:

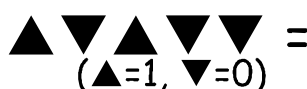
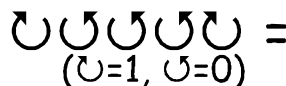
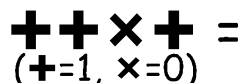
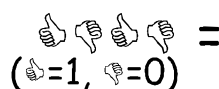
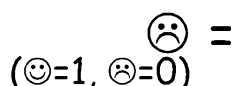
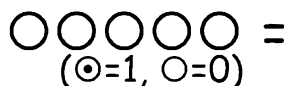
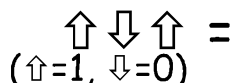
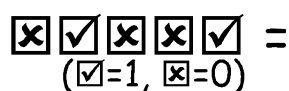


Kokį dešimtainį skaičių atitinka **10101**?

Kokį dešimtainį skaičių atitinka **11111**?

Kurią mėnesio dieną gimėte? Užrašykite tą dieną dvejetainė sistema. Nustatykite, kuris dvejetainis skaičius yra draugo gimimo dienos skaičius.

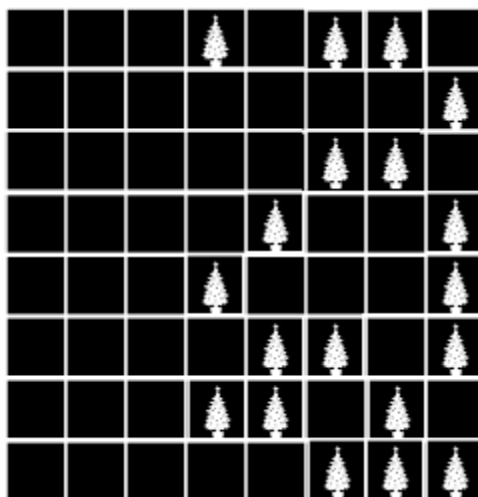
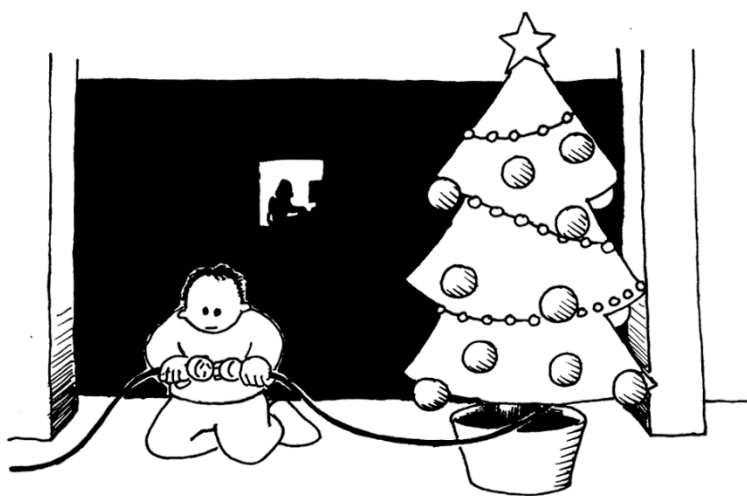
**Užrašykite, kuriuos dvejetainius skaičius atitinka šie ženklai:**



**Gudručiams. Juostelėmis, kurių ilgis 1, 2, 4, 8 ir 16 matavimo vienetų, parodykite, kaip suduriamos bet kokio ilgio iki 31 matavimo vieneto juostelės. Be to, galite nustebinti draugus parodydami, kad turėdami tik penkis skirtingus svarelius galite pasverti gana sunkius daiktus!**

## Darbo lapas. Slaptų žinučių siuntimas

Prieš pat Kalėdas Tomą atsitiktinai užrakino vienos parduotuvės viršutiniame aukšte. Aišku, jis norėjo kuo greičiau grįžti namo su dovanomis. Taigi ką daryti? Tomas bandė skambinti, rėkti, tačiau niekas jo negirdėjo. Pro langą pamatė žmogų, dirbantį kompiuteriu pastate kitoje gatvės pusėje. Kaip atkreipti jo dėmesį? Tomas apsidairė ieškodamas, kuo galėtų pasinaudoti. Jam šovė mintis perduoti žinutę Kalėdų eglutės lemputėmis, todėl šias lemputes sujungė taip, kad galėtų kiekvieną išjungti ir vėl įjungti. Tomas nusprendė perduoti savo žinutę dvejetainiu kodu, kurį turėtų suprasti žmogus, dirbantis kompiuteriu. Ką užkodavo Tomas? Ar jūs galėtumėte taip padaryti?

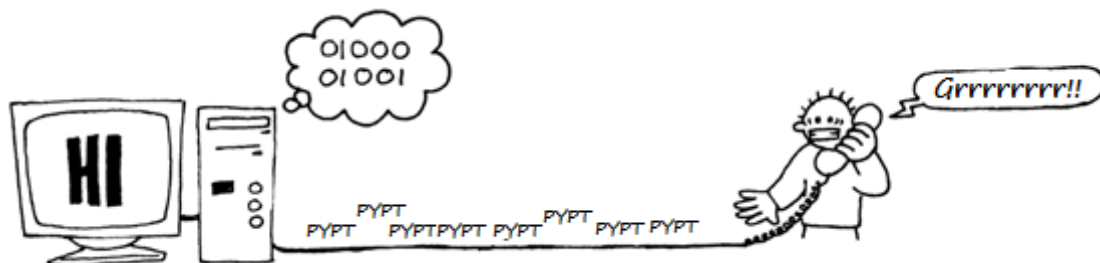


1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
a	ą	b	c	č	d	e	ę	ė	f	g	h	i	į	y	j
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
k	l	m	n	o	p	r	s	š	t	u	ų	ū	v	z	ž

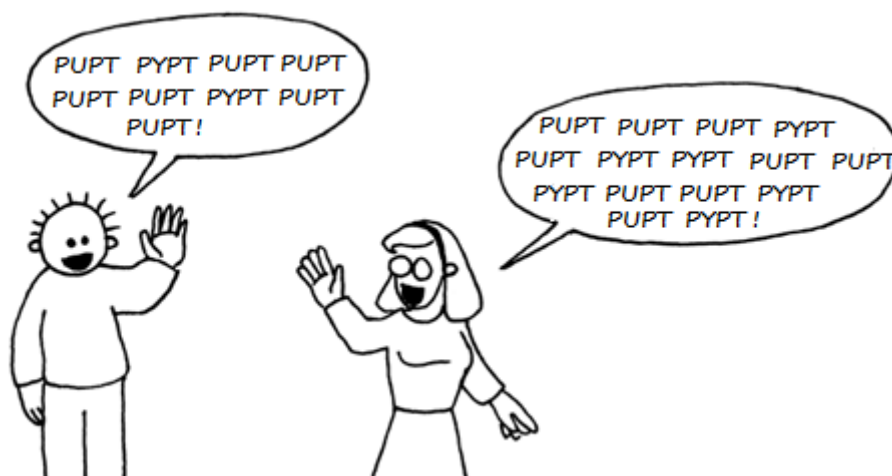


## Darbo lapas. Elektroninis paštas ir modemai

Kadise kompiuteriai buvo jungiami prie interneto naudojant modemą. Informacija buvo siunčiama dvejetainiu kodu naudojant pyptelėjimus. Aukšto tono pyptelėjimas reiškia 1, žemo tono – 0. Pyptelėjimai sklinda labai greitai. Taip greitai, kad girdėdavome ištisą cypimą.



Tuo pačiu dvejetainiu kodu, kurį Tomas taikė slaptų žinučių siuntimo užduotyje, parašykite el. laišką. Darykite atidžiai, kad nekiltų sunkumų skaitančiajam – jums nereikia būti tokiems spartiems kaip modemui 😊



# Darbo lapas. Didesnių už 31 skaičių vaizdavimas

Paimkite anksčiau naudotas dvejetaines korteles su taškais. Kiek taškų reikėtų nupiešti septintoje iš eilės kortelėje? Kiek aštuntoje? Pagal kokią taisyklę galima suskaičiuoti, kiek taškų reikia nupiešti kiekvienoje naujoje kortelėje? Jau įsitikinote, kad skaičiams nuo 1 iki 31 pavaizduoti užtenka penkių kortelių.

Įsižiūrėkite į seką. Ar galite nusakyti sekos narių ryšį?

**1, 2, 4, 8, 16...**

Sudėkite:  $1 + 2 + 4 = ?$  Kiek gaunate?

Dabar sudėkite:  $1 + 2 + 4 + 8 = ?$

Kiek gaunate sudėję visus skaičius nuo pirmosios iki penktosios kortelės?

Ar teko kada girdėti apie skaičiavimą „pirštais“? Išmėginkite šį būdą, kai skaičiai didesni kaip 10. Naudodami dvejetainę sistemą įsivaizduokite, kad vienas vienos rankos pirštas yra kortelė. Šitaip galite gauti 32 skaičius. Nepamirškite, kad 0 – taip pat skaičius!

Pabandykite skaičiuoti iš eilės. Pakeltas pirštas reiškia 1, nuleistas – 0.

Abiejų rankų pirštais galite suskaičiuoti nuo 0 iki 1023. Tai 1024 skaičiai!

Jei vienos rankos pirštais galite pavaizduoti 32 skaičius, o abiejų rankų –  $32 \times 32 = 1024$  skaičius, kiek skaičių galėtų pavaizduoti keturrankis pabaisiukas?



## Darbo lapas. Gimtadienio torto žvakutės

---

Ant gimtadienio torto paprastai uždegama po vieną žvakę kiekvieniems gyvenimo metams.

Kadangi kiekviena žvakė gali degti arba ne, galėtume jas panaudoti, kad parodytume dvejetainį jūsų amžiaus vaizdą. Pavyzdžiui, 14 metų dvejetainis yra 1110, todėl galite jį pavaizduoti keturiomis žvakėmis.

Gimtadienio tortas, ant kurios kuriame dega 13 metų atitinkantis dvejetainis žvakučių skaičius:



Kokie yra dvejetainių žvakių naudojimo pranašumai?

Kodėl dvejetainės žvakės senstant tampa prasmingesnės?

Ar yra dvejetainių žvakių naudojimo trūkumų ir kaip jas įveiktumėte?

(Beje, įprasta žvakučių ant torto naudojimo sistema vadinama unarine (sistemos pagrindas yra vienas), nes kiekvienos paskesnės žvakės vertė yra lygiai vienetu didesnė nei ankstesnės!)



## Darbo lapas. Dar daugiau apie dvejetainius skaičius

---

1. Kaip manote, kas nutiktų, jei dvejetainio skaičiaus pabaigoje prirašytumėte nulį? Jei nulį prirašytumėte dešimtainio skaičiaus pabaigoje, gautumėte 10 kartų didesnį skaičių už pradinį. Pavyzdžiui, prie 9 prirašę nulį gautumėte 90, kuris yra 10 kartų didesnis už 9.

Taigi kas nutiktų, jei nulį prirašytumėte dvejetainio skaičiaus pabaigoje? Pabandykite:

1001 → 10010

(9) (?)

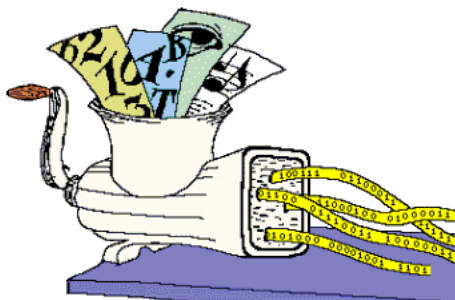
Sugalvokite hipotezę, pritaikykite ją keliems pavyzdžiams. Suformuluokite taisyklę. Kaip manote, kodėl taip atsitinka?





## Apie ką visa tai?

Kompiuterio kalba – tai dvejetainių skaičių kalba, kurios abėcėlę sudaro tik du skaitmenys – 0 ir 1.



Visos informacijos rūšys – duomenys – kompiuteryje virsta dviejų būsenų signalais - nulių ir vienetų sekomis.

Mokytojams rekomenduojama pasižiūrėti įvadinį vaizdo įrašą apie dvejetainius skaičius:

<https://youtu.be/GUqle9RE3Y8>

Atlikdami užduotis naudojome korteles su taškais. Kiekviena kortelė atitinka bitą kompiuteryje. Žodis „bitas“ kilęs iš anglų k. frazės „binary digit“ (liet. *dvejetainis skaitmuo*). Lietuvių kalbos abėcėlės raidėms (32 didžiosioms ir antra tiek mažosioms) koduoti pakaktų 6 kortelių arba, kitaip sakant, bitų. Tačiau kompiuteris turi ne tik atpažinti raides, bet skirti didžiąsias ir mažąsias raides, skaitmenis, aritmetinių operacijų ženklus, skyrybos ženklus, specialiuosius ženklus ir pan.

Pažvelgę į kompiuterio klaviatūrą matome daug ženklų. Kaip manote, kiek bitų kompiuteriui reikia visiems šiems ženklams užkoduoti?

Kompiuteriuose teksto ženklai dažniausiai koduojami 8 bitais. Dėl to ir kompiuterio atmintis skirstoma į 8 bitų grupes, vadinamas baitais. Vieno baito pakanka kelių kalbų abėcėlėms ir dar daugeliui kitų reikalingų ženklų užkoduoti.

Suskaičiuokite, kiek ženklų telpa į vieną baitą.



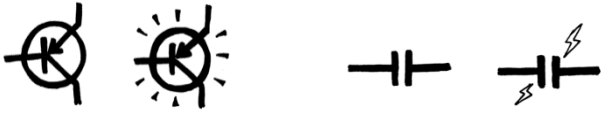
Daugiau apie ženklų kodavimą galite paskaityti knygoje:

V. Dagienė, G. Grigas, T. Jevsikova „Programinės įrangos lokalizavimas“.



Kompiuteriai ir kiti kompiuteriniai įrenginiai naudoja dvejetainę sistemą informacijai kaupti ir apdoroti. Dvejetainė sistema vadinama todėl, kad vartojami tik du skaitmenys.

Dvejetainis skaitmuo, bitas kompiuterio atmintyje reiškia tranzistorių, kuris tam tikru momentu yra įjungtas arba išjungtas, arba kondensatorių, kuris yra įkrautas arba ne.



Magnetinėse laikmenose bitai reiškiami ant jų paviršiaus išsidėsčiusiomis magnetinio lauko kryptimis: šiaurė → pietūs arba pietūs → šiaurė.



Optiniuose diskuose bitai įrašomi optiniu būdu ir juos nuskaitant diskų paviršiaus dalys atspindi šviesą arba jos neatspindi.



Kodėl kompiuteriuose naudojama dvejetainė skaičiavimo sistema? Kai yra tik dvi reikšmės, daug paprasčiau kurti prietaisus informacijai apdoroti. Jei būtų naudojama dešimtainė sistema, kompaktinis diskas turėtų turėti 10 būdų skaitmenims nuo 0 iki 9 išreikšti. Sukurti tokį prietaisą būtų brangu ir sudėtinga. Nors sakoma, kad kompiuteris duomenis vaizduoja nuliais ir vienetais, bet iš tiesų jame yra tik aukštoji ir žemoji įtampa arba į šiaurę ar į pietus nukreipta magnetinio lauko kryptis ar pan. Visa tai žymima 0 ir 1, kad būtų lengviau suprantama žmonėms. Šiais bitais kompiuteryje atvaizduojami tekstai, paveikslai, dainos, skaičiai, programos.

Vienu bitu atvaizduojama labai mažai informacijos, todėl bitai jungiami po 8 į sekas, kurios gali išreikšti skaičius nuo 0 iki 255. Aštuonių bitų grupė vadinama baitu. Kompiuterio sparta priklauso nuo to, kiek bitų vienu metu jis gali apdoroti. Pavyzdžiui, 32 bitų kompiuteris vienos operacijos metu gali apdoroti 32 bitų skaičius, o 16 bitų kompiuteris pirmiausia turėtų 32 bitų skaičių padalyti į dalis. Tai, žinoma, lėtina kompiuterio darbą. Taigi skaičiams, tekstui ir kitokiai informacijai laikyti ir apdoroti kompiuteris naudoja tik bitus ir baitus.

Norėdami užkoduoti bet kurios abėcėlės vieną ženklą dvejetainiu kodu, turime laikytis šių taisyklių:

Kiekvieno koduojamo ženklo dvejetainis kodas turi būti sudarytas iš to paties skaičiaus ženklų;

Kiekvienam koduojamos abėcėlės ženklui turi būti atitinkamas dvejetainis kodas;

Skirtingų ženklų dvejetainiai kodai turi būti skirtingi.

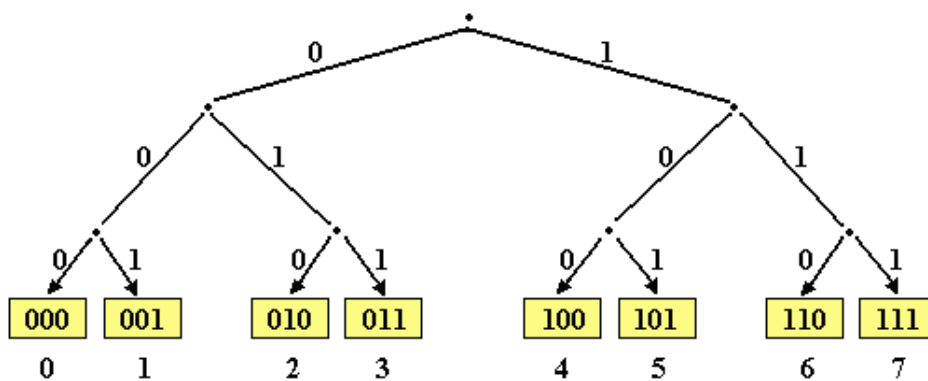
Laikantis šių taisyklių iš dvejetainio kodo visuomet galima sužinoti pradinį simbolį, kitaip sakant, galimas vienareikšmis iškodavimas.



**1 pavyzdys.** Tarkime, turime abėcėlę, sudarytą iš simbolių: {0, 1, 2, 3, 4, 5, 6, 7}. Reikia kiekvieną simbolį užkoduoti dvejetainine abėcėle: (0, 1 ).

Jau žinome, kaip tai padaryti: išrašome visas simbolių kombinacijas, sudarytas iš vieno, dviejų, trijų simbolių ir t. t., kol gausime ne mažiau kaip 8 skirtingas. Akivaizdu, kad vieno simbolio nepakaks – jų tik du. Dviejų simbolių kombinacijų keturios: 00, 01, 10, 11. Trijų simbolių kombinacijos kaip tik 8: jas galime rasti nuosekliai perstumdami vienetų ir nulių padėtis.

Skaičių vaizduoti dvejetainiu kodu patogu braižant schemą. Pradedame iš viršaus nubrėžę dvi atkarpas: atitinkančias nulį ir vienetą. Šių atkarpų galuose vėl brėžiame dvi atkarpas: vėl nuliui ir vienetui. Taip darome tol, kol paskutinių atkarpų skaičius tampa lygus arba didesnis koduojamos abėcėlės simbolių skaičiui. Tuomet belieka peržiūrėti nuo viršaus iki paskutinės atkarpos ir užrašyti kiekvieno simbolio kodą.



Skaičių vaizdavimas dvejetainiu medžiu.

Šitokia schema vadinama **dvejetainiu medžiu**, kadangi iš kiekvieno taško išeina dvi atkarpos, atitinkančios dvejetainės abėcėlės simbolius. Atkarpos vadinamos šakomis.

# Sprendimai ir užuominos

---

## Dvejetainiai skaičiai

3 pavaizduoti reikia kortelių su 2 ir 1 tašku.

12 pavaizduoti reikia kortelių su 8 ir 4 taškais.

19 pavaizduoti reikia kortelių su 16, 2 ir 1 tašku.

Tik vieninteliu būdu galima pavaizduoti kiekvieną iš šių skaičių.

Didžiausias skaičius, kurį galima pavaizduoti, yra 31. Mažiausias yra 0. Galima pavaizduoti visus skaičius nuo 0 iki 31. Kiekvieną iš jų galima pavaizduoti tik vienu būdu.

**Gudručiams.** Didinant skaičių vienetu, iš eilės apverčiamos taškais į viršų visos kortelės iš dešinės į kairę.

## Dvejetainiai skaičiai

10101 = 21, 11111 = 31

## Slaptų žinučių siuntimas

Užkoduota žinutė: PADĖKITE

## Didesnių už 31 skaičių vaizdavimas

Jei sudedami visi skaičiai nuo pirmojo, tai jų suma visada bus vienetu mažesnė už kitą sekos skaičių.

Keturrankis pabaisiukas gali pavaizduoti  $1024 \times 1024 = 1\,048\,576$  skaičių — nuo 0 iki 1 048 575!

## Raidžių kodavimas

Lietuvių abėcėlės raidžių kodai:

a	00000	h	01011	r	10110
ą	00001	i	01100	s	10111
b	00010	j	01101	š	11000
c	00011	y	01110	t	11001
č	00100	j	01111	u	11010
d	00101	k	10000	ų	11011
e	00110	l	10001	ū	11100
ę	00111	m	10010	v	11101
ė	01000	n	10011	z	11110
f	01001	o	10100	ž	11111
g	01010	p	10101		

## Dar daugiau apie dvejetainius skaičius

Parašius nulį dvejetainio skaičiaus dešinėje, šis skaičius padidėja dvigubai. Kiekvienas vienetas dvejetainiame skaičiuje padvigubėja, todėl ir galutinis skaičius padvigubėja. (Dešimtainės sistemos skaičiaus dešinėje prirašius nulį, šis skaičius padidėja 10 kartų.)



## 2 veikla

# Spalvinimas skaičiais. Paveikslai kompiuteryje

---

### Santrauka

Piešiniai, paveikslai, nuotraukos ir kitokie vaizdai kompiuteryje koduojami bitais. Čia aiškinama, kaip tai daroma.

### Ryšiai su ugdymo programomis

- ✓ Matematika: geometrija – formos ir erdvės
- ✓ Informatika: įvairių duomenų atvaizdavimas skaičiais; atminties taupymas – pasikartojančių duomenų taupesnis kodavimas

### Gebėjimai

- ✓ Skaičiavimo
- ✓ Vaizdavimo

### Amžius

- ✓ Nuo 7 metų

### Priemonės

- ✓ Pateiktis „Spalvinimas skaičiais“

Kiekvienam mokiniui reikia:

- ✓ Darbo lapo „Vaikiškas faksas“
- ✓ Darbo lapo „Nupiešk savo paveikslą“



# Spalvinimas skaičiais

---

## Įvadas

### Diskusiniai klausimai

1. Ką daro fakso aparatai?
2. Kuriose iš šių situacijų kompiuteriai turi įrašyti paveikslus?  
(Dirbant piešimo programa, žaidžiant interaktyviusius žaidimus ar rengiant skaidres pateikčių programa.)
3. Kaip kompiuteriai gali koduoti paveikslus vien skaičiais?

### Išsamus paaiškinimas



Kompiuterio ekranas yra tarsi tinklelis, sudarytas iš mažų taškelių, vadinamų pikseliais (angl. *pixels*).

Kiekvienas juodai balto paveikslu pikselis yra arba juodas, arba baltas.

Aukščiau pateikta raidė „a“ padidinta tam, kad įsivaizduotume pikselius. Kompiuteriui įrašant paveikslą reikalinga tik informacija, kurie taškeliai yra juodi, o kurie – balti.

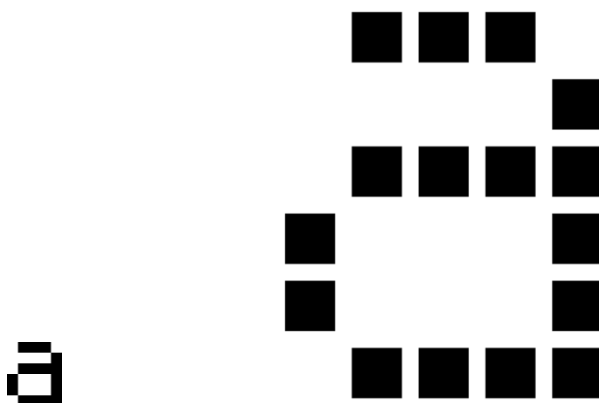
	■	■	■		1, 3, 1
				■	4, 1
	■	■	■	■	1, 4
■				■	0, 1, 3, 1
■				■	0, 1, 3, 1
	■	■	■	■	1, 4

Šis piešinys rodo, kaip galima koduoti paveikslus skaičiais. Pirmoje eilutėje yra vienas baltas pikselis, trys juodi ir vėl vienas baltas, todėl pirmoji eilutė užrašoma skaičių 1, 3, 1 seka.

Pirmasis skaičius visada nusako baltųjų pikselių skaičių. Jei pirmasis pikselis yra juodas, tada skaičių seka turi prasidėti nuliu. Darbo lape pateikiama keletas paveikslų, kuriuos siūloma mokiniams užkoduoti aprašytu metodu.



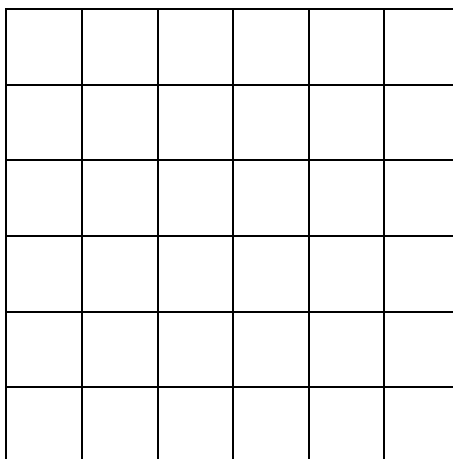
# Spalvinimas skaičiais



▲ Raidė „2“, matoma kompiuterio ekrane, ir ta pati tik padidinta raidė, kai matomi ją sudarantys pikseliai.

	■	■	■		1, 3, 1
				■	4, 1
	■	■	■	■	1, 4
■				■	0, 1, 3, 1
■				■	0, 1, 3, 1
	■	■	■	■	1, 4

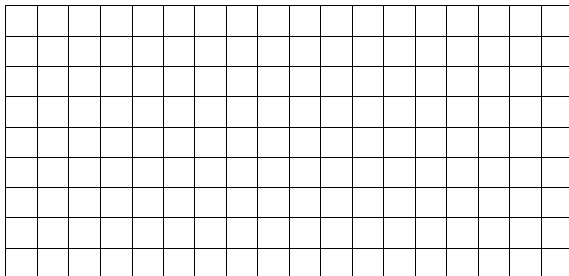
▲ Tas pats paveikslas, užkoduotas skaičiais.



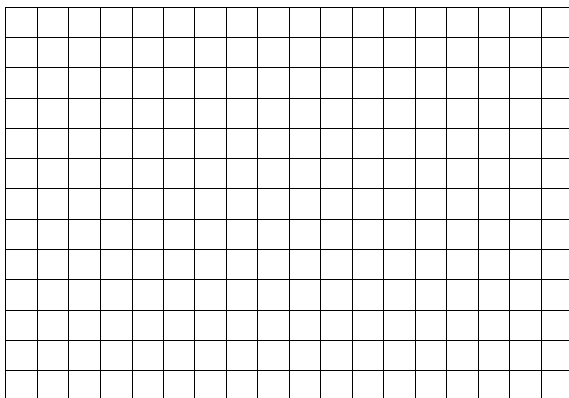
▲ Tuščias tinklėlis (naudojamas mokytis)

# Darbo lapas. Vaikiškas faksas

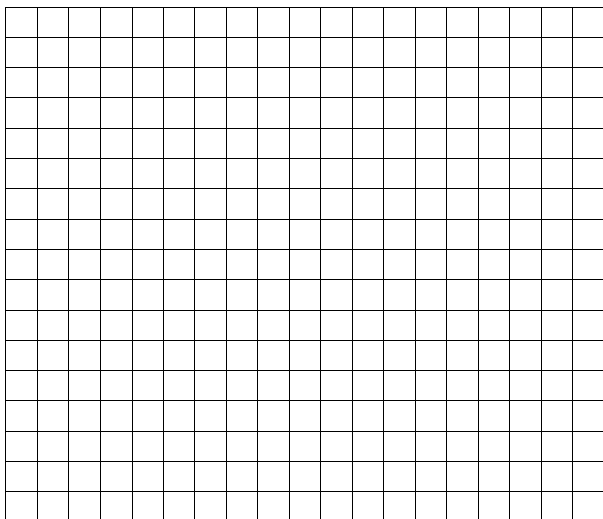
Pirmasis paveikslas yra paprasčiausias, paskutinis – sudėtingiausias. Atliekant užduotį lengva padaryti klaidų, tad patariama piešti pieštuku ir po ranka turėti trintuką!



4, 11  
4, 9, 2, 1  
4, 9, 2, 1  
4, 11  
4, 9  
4, 9  
5, 7  
0, 17  
1, 15



6, 5, 2, 3  
4, 2, 5, 2, 3, 1  
3, 1, 9, 1, 2, 1  
3, 1, 9, 1, 1, 1  
2, 1, 11, 1  
2, 1, 10, 2  
2, 1, 9, 1, 1, 1  
2, 1, 8, 1, 2, 1  
2, 1, 7, 1, 3, 1  
1, 1, 1, 1, 4, 2, 3, 1  
0, 1, 2, 1, 2, 2, 5, 1  
0, 1, 3, 2, 5, 2  
1, 3, 2, 5



6, 2, 2, 2  
5, 1, 2, 2, 2, 1  
6, 6  
4, 2, 6, 2  
3, 1, 10, 1  
2, 1, 12, 1  
2, 1, 3, 1, 4, 1, 3, 1  
1, 2, 12, 2  
0, 1, 16, 1  
0, 1, 6, 1, 2, 1, 6, 1  
0, 1, 7, 2, 7, 1  
1, 1, 14, 1  
2, 1, 12, 1  
2, 1, 5, 2, 5, 1  
3, 1, 10, 1  
4, 2, 6, 2  
6, 6

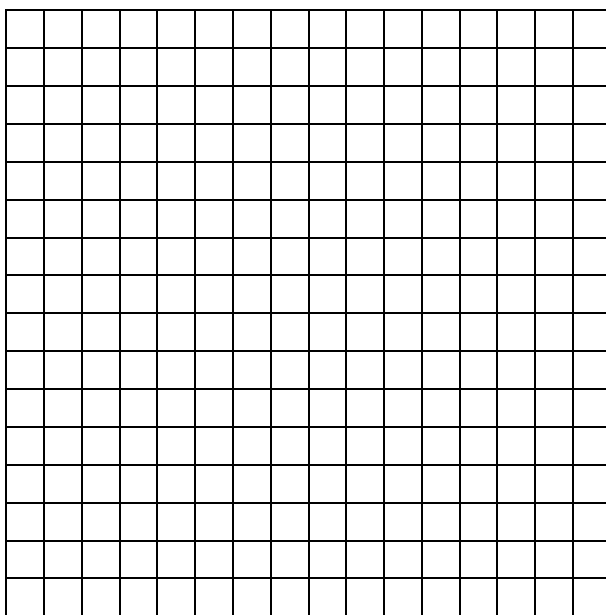




## Darbo lapas. Nupiešk savo paveikslą

---

**Gudručiams.** Jei norite nupiešti spalvotą paveikslą, spalvoms turite suteikti kodus (pavyzdžiui, galima sutarti, kad 0 žymi juodą spalvą, 1 – raudoną, 2 – žalią ir t. t.). Kaip ir anksčiau pikselius atvaizduosime dviem skaičiais: pirmasis nusakys vienodų pikselių (langelių) skaičių, antrasis – reikiamą spalvą. Nupieškite spalvotą paveikslą ir duokite jį draugui iškoduoti. Nepamirškite pasakyti, kuris skaičius atitinka kurią spalvą.



---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

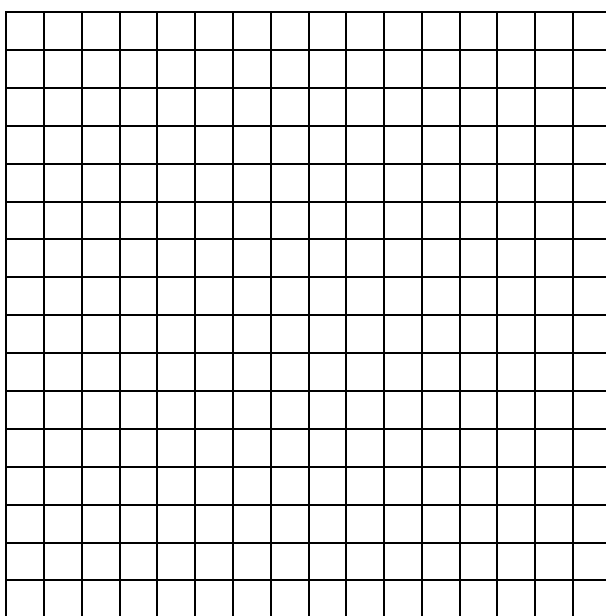
---

---

---

---

---



---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

## Užuominos ir galimi pakeitimai

1. Pabandykite piešti užsidėję kopijavimo popierių ant tinklelio viršaus taip, kad galutinis paveikslas būtų matomas be tinklelio. Tada paveikslas bus matomas aiškiau.
2. Užuoat spalvinę tinklelio langelius, mokiniai ant didesnio tinklelio gali klijuoti ar dėti lipnius kvadratinus lapelius ar kartono kvadratėlius.

## Diskusija

Paprastai pikselių skaičius eilutėje yra ribojamas ir užrašomas dvejetainiu skaičiumi. Kaip užrašytumėte dvylikos juodų pikselių eilę skaičiais tik iki 7? (Vienas iš būdų užkoduoti dvylikos juodų pikselių eilę yra pirmiausia nurodyti 7 juodus pikselius, tada nulį baltųjų ir galų gale likusius penkis juodus pikselius.)



## Apie ką visa tai?

---

Fakso aparatai yra paprasčiausi kompiuteriai, kurie nuskenuoja nespaltotą popieriaus lapą į maždaug  $1000 \times 2000$  pikselių tinklėlį. Tada tą nuskenotą tinklėlį fakso aparatas per modemą siunčia į kitą fakso aparatą, kuris išspausdina pikselius ant popieriaus lapo. Dažnai faksu siunčiamuose paveiksluose yra didelių baltų (pavyzdžiui, paraščių) ir juodų pikselių blokų (pavyzdžiui, linijų). Spalvoti paveikslai dažniausiai turi labai daug pasikartojančių dalių. Įvairiais suspaudimo metodais programuotojai siekia sutaupyti atminties tokiems paveikslams laikyti. Metodas, aprašomas šiame skyriuje, vadinamas *vienodų eilėje kodavimu*. Tai labai efektyvus būdas paveikslams glaudinti.

Kodėl reikia vaizdus glaudinti ir kodėl mums rūpi taupyti vietą? Suglaudinti vaizdai užima žymiai mažiau vietos standžiajame diske, tačiau šiais laikais kompiuterių standieji diskai yra gana dideli.

O kaip dėl vaizdo įrašų, filmų? Filmai ir vaizdo įrašai sudaryti iš daugybės statinių vaizdų, rodomų labai greitai vienas po kito. Tarkime, mūsų filmą sudaro 120 statinių vaizdų, kurie sudaro judančio vaizdo įspūdį.

Jei vienam nesuglaudintam vaizdai atsisiųsti reikia 10 sekundžių, kiek sekundžių užtruktų atsisiųsti visą nesuglaudintą filmą?

(Atsakymas:  $120 \times 10 = 1200$  sekundžių. O tai yra 1200/60 arba 20 minučių.)

Akivaizdu, kad tai nėra tikslus skaičius (vienam vaizdai nebūtinai reikia 10 sekundžių atsisiųsti, o daugumoje filmų yra daug daugiau nei 120 vaizdų), tačiau visi žinome, kiek kartų mums yra tekę laukti, kol bus įkrautas vaizdo įrašas.

Nuotraukos dažniausiai suglaudamos iki dešimties ar net iki šimto kartų (panašiais metodais, pavyzdžiui, JPEG, GIF ir PNG). Tokių nuotraukų diske galima laikyti daugiau, o jų peržiūra tinklalapyje trunka tik dalį sekundės.

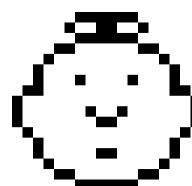
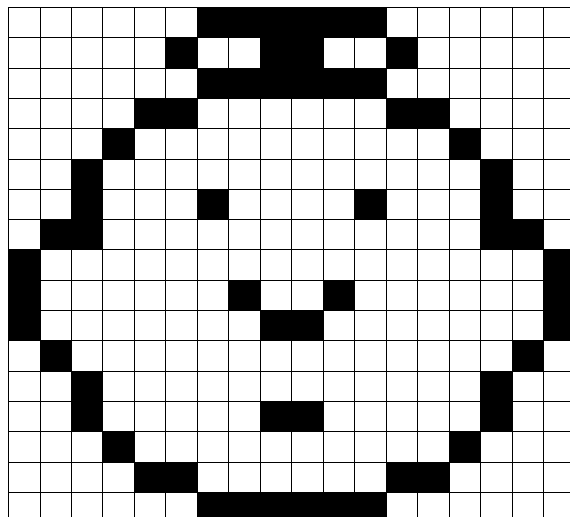
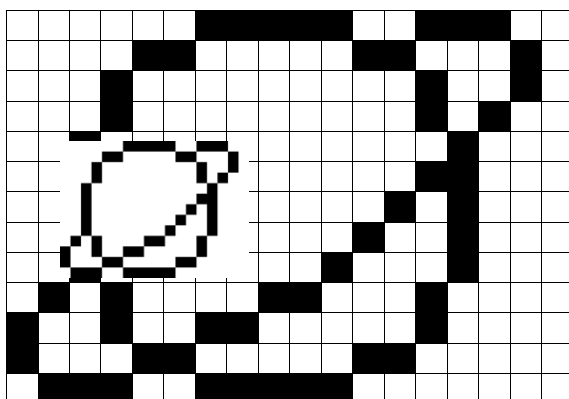
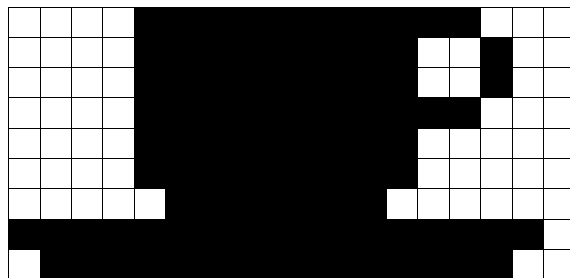
Paprastai programuotojas nusprendžia, kuris iš glaudinimo metodų labiausiai tinka paveikslams siųsti.



# Sprendimai ir užuominos

---

Atsakymai. Darbo lapas „Vaikiškas faksas“



## 3 veikla

# Pakartok tai dar kartą! Teksto suspaudimas

---

### Santrauka

Kompiuterių atmintis, kurioje laikoma informacija, yra ribota, todėl ta informacija turi būti vaizduojama kuo efektyviau. Šiuo tikslu informaciją reikia suglaudinti. Užkoduotų (t. y. suglaudintų) norimų saugoti duomenų, kurie išskleidžiami, kai prireikia, kompiuteris gali laikyti daugiau arba tokius suglaudintus duomenis kur kas sparčiau persiųsti internetu.

### Ryšiai su ugdymo programomis

- ✓ Lietuvių kalba: atpažinti pasikartojimus žodžiuose ir tekste
- ✓ Informatika: atminties taupymas nesaugant pasikartojančių duomenų

### Gebėjimai

- ✓ Teksto kopijavimo

### Amžius

- ✓ Nuo 9 metų

### Priemonės

- ✓ Pateiktis „Pakartok tai dar kartą!“

Kiekvienam mokiniui būtinas:

- ✓ Darbo lapas „Pakartok tai dar kartą!“
- ✓ Darbo lapas „Gudručiams“
- ✓ Darbo lapas „Trumpas ir saldus“
- ✓ Darbo lapas „Tikriems gudručiams“



# Pakartok tai dar kartą!

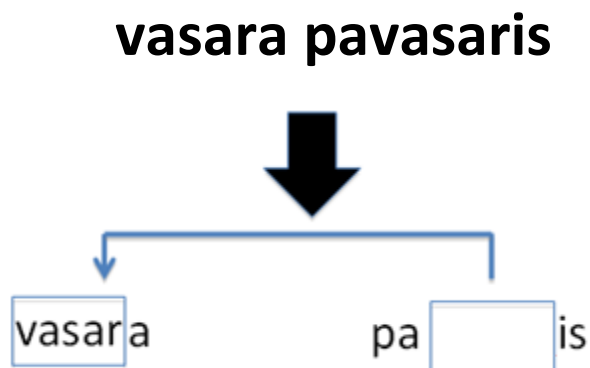
---

## Įvadas

Kompiuteriai laiko ir persiunčia daugybę duomenų. Kad jiems nereikėtų labai daug atminties arba kad pernelyg ilgai neužtruktų informacijos siuntimas, kompiuteriai suglaudina tekstą panašiai, kaip aprašoma šioje veikloje.

## Diskusija ir pavyzdžiai

Parodoma skaidrė „Saulė“. Ieškoma pasikartojančių raidžių eiliuotame tekste, pateiktame skaidrėje. Ar galima rasti pasikartojančių raidžių po dvi ar daugiau grupelių? O gal kartojasi net visas žodis ar frazė? (Pakeiskite juos kvadratėliais, kaip parodyta diagramoje toliau.)



**Pakartok tai dar kartą!**

---

**Saulė**

**Vasara pavasaris**

**Vasara pavasaris**

**Saulė šypsosi**

**Vasara pavasaris**

**Vasara pavasaris**

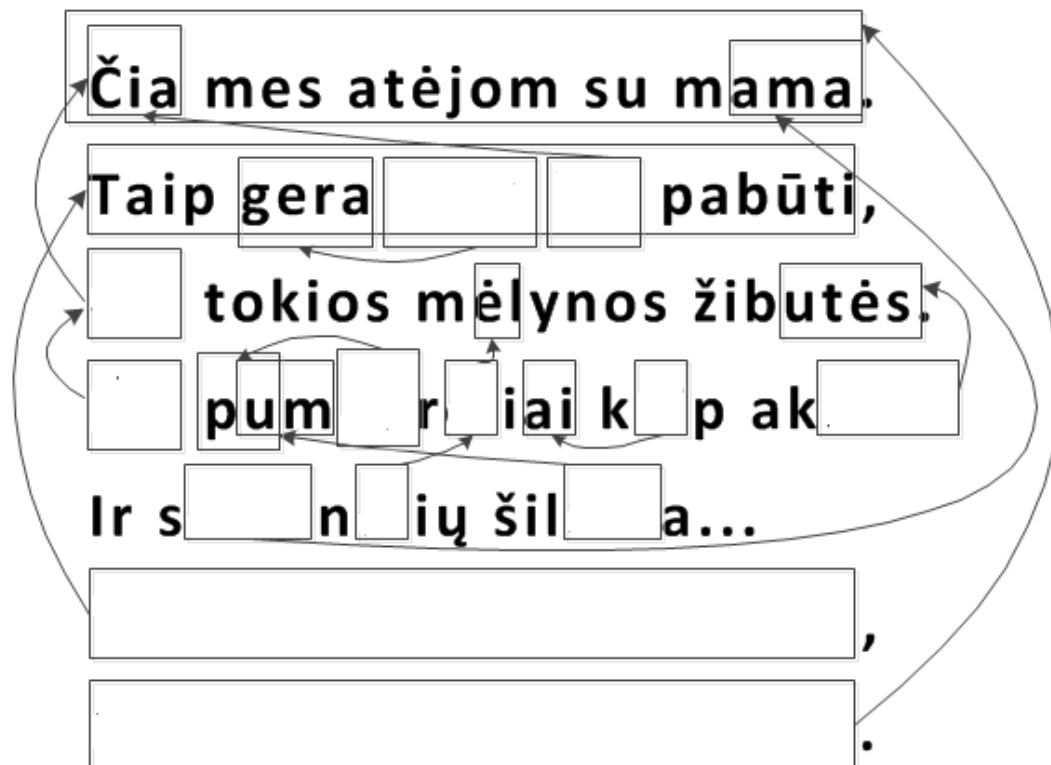
**Į laukelį kviečia**





## Darbo lapas. Pakartok tai dar kartą!

Šiame eilėraštyje trūksta daug raidžių ir žodžių. Ar galite užpildyti tuščius stačiakampius raidėmis ir žodžiais, kad eilėraštis būtų baigtas? Trūkstamas raides ir žodžius galite atsekti pagal rodykles.



Dabar patys pasirinkite kokį norite eilėraštį ar ketureilį ir suglaudinkite jo tekstą. Atkreipkite dėmesį, kad rodyklės turi rodyti į ankstesnes teksto dalis. Užkoduotas eilėraštis iškoduojamas tokia tvarka, kokia įprastai skaitome tekstą: iš kairės į dešinę ir iš viršaus į apačią.

**Iššūkis:** atkreipkite dėmesį, kiek nedaug pirminio teksto žodžių reikia palikti!

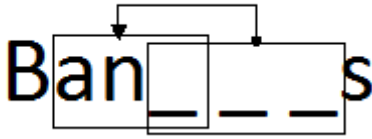
**Užomina:** stenkitės neapkrauti teksto rodyklėmis. Rašydami eilėraštį palikite daugiau laisvos vietos aplink žodžius ir tarp raidžių, kad galėtumėte piešti stačiakampius ir rodykles.

Suglaudintą tekstą lengviau užkoduoti, kai pasirašote atskirai sau visą eilėraštį ir tada nupiešiate kvadratėlius ir rodykles.

## Darbo lapas. Gudručiams

---

Kaip išspręstumėte šį galvosūkį?



Kartais trūkstamos teksto dalys rodo pačios į save. Šiuo atveju žodis gali būti iškoduotas teisingai, jeigu kopijuojame raides iš kairės į dešinę. Tada kiekviena raidė gali būti kopijuojama prieš tai, kai įrašoma. Toks kopijavimo būdas labai naudingas kompiuteriams, kai yra daug pasikartojimų.

Pabandykite nupiešti patys.

Kompiuteryje stačiakampiai ir rodyklės vaizduojami skaičiais. Pavyzdžiui,

## Pasas

gali būti užrašytas kaip **Pas(2,2)**. Pirmasis skaičius **2** rodo antrą vietą nuo galo – kopijavimo vietos pradžią

**Pas—**

Antrasis skaičius **2** reiškia, kad kopijuosime dvi iš eilės einančias raides.

**Pasa—**

**Pasas**



Kadangi žodžiui užkoduoti naudojami du skaičiai, verta suglaudinti dviejų ar daugiau raidžių grupes, kitaip nebus sutaupoma vietos. Iš tiesų failo dydis gali padidėti, jeigu dviem skaičiais koduosime vieną raidę.

Sugalvokite žodžių ir suspauskite juos taip, kaip darytų kompiuteris. Ar jūsų draugai galėtų juos iškoduoti?

## Darbo lapas. Trumpas ir saldus

---

Kiek žodžių čia reikia iš tiesų?

Tarkime, jūs esate kompiuteris, kuris nori sutalpinti savo diske kuo daugiau informacijos. Išbraukite visas grupes po dvi ar daugiau pasikartojančių raidžių. Jos nebereikalingos, nes keičiamos rodyklėmis. Jūsų tikslas – išbraukti kuo daugiau raidžių.

**Apvali, saldi gražuolė...**

**Šmurkšt, po suolu jau nupuolė.**

**„Kurgi bėgi? Grįžk į puodą...“**

**Bet, pakėlus savo kuodą,**

**Bulvė lekia per laukus:**

**„Nebegrįšiu pas vaikus.“**



## Darbo lapas. Tikriems gudručiams

---

### Ar pasiruošę tikrai „kietai“ suglaudinti?

Toliau pateikta istorija buvo apdorota kompiuterio programa, kuri šioje istorijoje aptiko mažiausiai 1000 galimų išbraukti raidžių. Kiek galite rasti jūs? Prisiminkite, gali būti išbraukiamos tik grupės po dvi ar daugiau pasikartojančių raidžių. Sėkmės!

*„Vieną kartą, labai labai seniai, trys maži paršiukai nusprendė pasistatyti sau namus. Pirmasis paršiukas nebuvo labai protingas ir nusprendė pasistatyti namą iš šiaudy, nes taip būsią pigiau. Antrasis paršiukas irgi nebuvo labai protingas, todėl nusprendė pasistatyti namą iš šakų, esą siekdamas ekologiško, nes tai buvo madinga net tais laikais. Trečiasis paršiukas buvo protingesnis negu jo broliai ir nusipirko krūvą plytų iš gretimo miesto, kad pasistatytų tvirtą ir patogų namelį.*

*Tuo pat po įkurtuvių vakarėlio pirmasis paršiukas suposi kėdėje ir skaitė knygą. Staiga kažkas pabeldė į duris. Tai buvo didelis piktas vilkas.*

*– Paršiuk, paršiuk, įleisk mane! – prašė vilkas.*

*– Ne, nė per nago juodymą! – sužviogė pirmasis paršiukas.*

*– Tada aš supyksiu, giliai įkvėpsiu ir nupūsiu tavo namą! – užriaumojo vilkas ir, labai supykęs, giliai įkvėpė, stipriai papūtė ir suniokojo namą. Išsigandęs pirmasis paršiukas kiek įkabindamas nubėgo pas savo brolių į iš šakų pastatytą namą. Vos tik pasijuto saugus, vilkas vėl buvo prie antrojo paršiuko slenksčio.*

*– Paršiuk, paršiuk, įleisk mane! – prašė vilkas.*

*– Ne, nė per nago juodymą! – sužviogė antrasis paršiukas.*

*– Tada aš supyksiu, giliai įkvėpsiu ir nupūsiu tavo namą! – užriaumojo vilkas ir, labai supykęs, giliai įkvėpė, stipriai papūtė ir suniokojo šakų namą. Abu išsigandę paršiukai nubėgo pas trečiąjį brolių į plytų namą, bet vilkas lipo jiems ant kulnų ir tuoj pat jau buvo prie durų slenksčio.*

*– Paršiuk, paršiuk, įleisk mane! – prašė vilkas.*

*– Ne, nė per nago juodymą! – sužviogė trečiasis paršiukas.*

*– Tada aš supyksiu, giliai įkvėpsiu ir nupūsiu tavo namą! – užriaumojo vilkas ir, labai supykęs, giliai įkvėpė, stipriai papūtė... Bet namas buvo pastatytas iš plytų! Vilkas bepūsdamas užduso, o namas liko stovėti. Tada vilkui šovė nauja mintis. Kaminas! Jis užlipo šakotu qžuolu ant stogo ir tik tada pamatė, kad namas – be kamino, nes trečiasis paršiukas rūpinosi aplinka ir įrengė elektrinį šildymą. Labai įniršęs vilkas paslydo ir nukrito nuo stogo. Jis susilaužė kairę koją, bet dar blogiau, kad prarado savo orumą. Paršiukai juokėsi, kai vilkas nušlubavo atgal. Jie suprato, kaip protinga gyventi mieste, kur vilkai yra tik zoologijos sode. Paršiukai persikraustė į miestą ir ten gyveno ilgai ir laimingai.“*



## Apie ką visa tai?

---

Kompiuterio atminties talpa didėja kasdien – per paskutinius metus standartinių kompiuterių ji padidėjo net milijonus kartų, bet, matyt, tai dar ne pabaiga. Kompiuteriuose gali būti laikoma knygų ar net ištisa biblioteka, muzikos įrašų ir filmų, jei tik yra laisvos vietos. Didelės apimties dokumentai internete yra labai didelė problema, nes ilgai užtrunka juos atsisiųsti. Dabar stengiamasi sumažinti kompiuterius – net telefonai ir rankiniai laikrodžiai gali laikyti labai daug informacijos.

Vienas šios problemos sprendimų štai toks: užuot pirkę kompiuterius, turinčius daugiau atminties, ar įsigiję spartesnį interneto ryšį, galime duomenis taip suglaudinti, kad jie užimtų mažiau vietos. Dažniausiai duomenys koduojami ir iškoduojami kompiuteriu automatiškai. Mes to proceso beveik nepastebime. Nors iš tiesų kompiuteris atlieka daugiau veiksmų, matome tik tai, kad diske telpa daugiau informacijos ar sparčiau atsiunčiamas tinklalapis.

Sugalvota daug duomenų suglaudavimo metodų. Atliekant šią veiklą, buvo naudojamas metodas, kai nuorodomis rodoma į prieš tai buvusius pasikartojančius simbolių tekste. Šis metodas vadinamas tiesiog „Lempel–Ziv–Welch“ (LZW), jį 1970 m. sugalvojo Izraelio mokslininkai.

Metodas tinka bet kuriai kalbai, juo lengvai suglaudunami ir perpus sumažinami duomenys. Todėl šis metodas dažnai naudojamas asmeniniuose kompiuteriuose bei sparčiuosiuose modemuose, juo suglaudunami GIF ir PNG paveikslai, sumažinamas siunčiamų duomenų kiekis, tad jų siuntimas kur kas spartesnis.



# Sprendimai ir užuominos

---

Pakartok tai dar kartą!

Čia mes atėjom su mama.

Taip gera gera čia pabūti,

Čia tokios mėlynos žibutės.

Čia pumpurėliai kaip akutės

Ir samanėlių šiluma...

Taip gera gera čia pabūti,

Čia mes atėjom su mama.



## 4 veikla

# Kortelių keitimo magija. Klaidų radimas ir taisymas

---

### Santrauka

Saugant duomenis laikmenoje ar siunčiant iš vieno kompiuterio į kitą įprasta manyti, kad jie nesikeičia. Tačiau kartais įvyksta kas nors nenumatyta ir duomenys pasikeičia. Šioje veikloje mokiniams magišku triuku parodoma, kaip nustatyti, kada duomenys yra sugadinti, ir kaip tai ištaisyti. Žaidimo metu mokiniai išsiaiškina, kaip tikrinti gautus duomenis naudojant lyginimo tikrinimo metodą.

### Ryšiai su ugdymo programomis

- ✓ Matematika: skaičiavimas ir įvertinimas
- ✓ Matematika: pavyzdžių aiškinimas ir ryšių nustatymas, nežinomos reikšmės paieška
- ✓ Matematika: koordinatės
- ✓ Informatika: duomenų pagrindimas

### Gebėjimai

- ✓ Skaičiavimo
- ✓ Lyginių ir nelyginių skaičių atpažinimo

### Amžius

- ✓ Nuo 7 metų

### Priemonės

- ✓ 36 kortelės (geriausia magnetinės), kurių viena pusė nuspalvinta
- ✓ Stalas (arba metalinė lenta) demonstracijai

Kiekvienai mokinių porai reikia:

- ✓ 36 vienodų kortelių, kurių viena pusė nuspalvinta

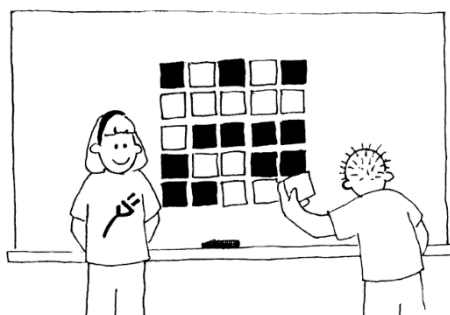


# Magiškas triukas

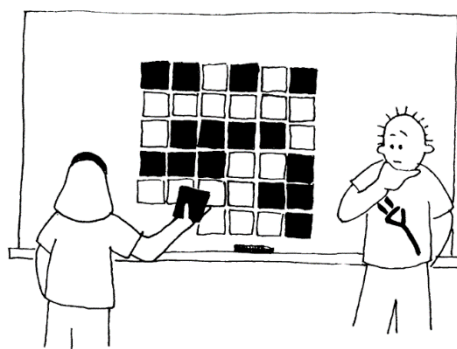
## Demonstracija

Reikia 36 vienodų kortelių, kurių abi pusės yra skirtingų spalvų. (Galima iškirpti iš spalvoto popieriaus lapo, kurio viena pusė yra spalvota, o kita – balta, galima naudoti bet kokias žaidybines kortas, atminties žaidimo korteles ir pan. – svarbu, kad visų kortelių viena pusė būtų vienoda.) Demonstracijai patogiu naudoti korteles su magnetais iš abiejų pusių, tik reikia, kad abi jų pusės dar būtų ir skirtingų spalvų. (Dažniausiai tokios kortelės turi magnetus iš vienos pusės. Dvi korteles galima suklijuoti ta puse, kurioje nėra magneto, tada ant vienos iš „magnetinių“ naujos kortelės pusių nupiešti baltą tašką ar tą pusę nuspalvinti.)

1. Mokinio paprašoma išdėlioti korteles kvadratu  $5 \times 5$  (kuri kortelės pusė bus viršuje nesvarbu).



Mokytojas išdėlioja dar vieną eilutę ir stulpelį, kad šiek tiek pasunkintų užduotį.



Papildomos kortelės ir yra šio uždavinio – triuko pagrindas. Papildomas korteles reikia sudėti taip, kad kiekvienoje eilutėje ir stulpelyje būtų lyginis nuspalvintų kortelių skaičius.

2. Tegul mokinys vieną kortelę apverčia, kai mokytojas nežiūri. Apverstos kortelės eilutėje ir stulpelyje bus nelyginis nuspalvintų kortelių skaičius. Taip nesunkiai nustatoma, kuri kortelė buvo apversta. Ar mokiniai galėtų atspėti, kaip atliekamas šis triukas?

## Mokiniai mokomi šio triuko:

1. Mokiniai susiskirsto poromis ir išdėlioja savo korteles ant stalo kvadratu  $5 \times 5$ .





2. Atkreipiamas dėmesys, po kiek nuspalvintų kortelių yra kiekvienoje eilutėje ir stulpelyje. Ar jų skaičius yra lyginis, ar nelyginis? Primenama, kad nulį šiame žaidime laikome lyginiu skaičiumi.
3. Pridedama po vieną papildomą kortelę prie kiekvienos eilutės ir įsitikinama, kad kiekvienoje eilutėje nuspalvintų kortelių yra nelyginis skaičius. Papildoma kortelė vadinama lyginumo kortele.
4. Taip pat pridedama dar viena kortelių eilutė, kad kiekviename stulpelyje būtų po nelyginį skaičių spalvotų kortelių.
5. Dabar viena kortelė apverčiama. Ką galima pastebėti apverstos kortelės stulpelyje ir eilutėje? (Nuspalvintų kortelių skaičius – nelyginis.) Lyginumo kortelė parodo, kur buvo pakeista.
6. Kortelės kaitaliojamos toliau – šis triukas atliekamas iš naujo.

### **Papildomos veiklos:**

1. Šį triuką galima išbandyti ir su kitais objektais. Pavyzdžiui, su loginio žaidimo kortelėmis (balta – juoda), monetomis (herbas ir skaičius) arba kortelėmis su 0 ir 1 skirtingose pusėse (siejama su dvejetainė sistema).
2. Kas nutiktų, jei būtų apverstos dvi ar daugiau kortelių? (Negalima visada tiksliai pasakyti, kurios dvi kortelės buvo apverstos, tačiau visada galima pasakyti, kad kai kas buvo pakeista. Galima aptarti, kas įvyksta, jei apverčiamos viena ar daugiau kortelių porų. Įmanoma, kad apvertus 4 korteles lyginumo kortelės neparodys klaidos.)
3. Galima išbandyti triuką su daugiau kortelių, pavyzdžiui, išdėstyti iš jų didelį kvadratą  $9 \times 9$ . (Šis triukas gali būti daromas su bet kiek kortelių, be to, jų nebūtina išdėstyti kvadratu.)
4. Kitas įdomus pratimas – nagrinėti apatinę dešiniąją kortelę. Jei ši lyginimo kortelė bus teisinga stulpeliui virš jos, tai ar ši kortelė bus teisinga ir eilutei iš kairės? (Taip, visada, jei naudojamas nelyginis lyginumas.)
5. Šiame pratime lyginumas yra nelyginis – nelyginis nuspalvintų kortelių skaičius eilutėse ir stulpeliuose. Ar galima tą patį padaryti su lyginiu lyginumu? (Tai įmanoma. Tačiau apatinės dešinėsios lyginumo kortelės pratimas tinka tik tada, kai yra lyginis (arba nelyginis) ir eilučių, ir stulpelių skaičius išdėstyname plote. Pavyzdžiui, korteles išdėsčius  $5 \times 9$  arba  $4 \times 6$  pratimą galima atlikti, o išdėsčius  $4 \times 7$  pratimas netinka.)



# Realaus gyvenimo pavyzdys gudručiams

Remiantis panašia metodika, tikrinami knygų ir kitų prekių brūkšniniai kodai. Apžiūrėkite ant užpakalinio knygos viršelio išspausdintą 10 arba 13 skaitmenų kodą. Paskutinis skaitmuo yra kontrolinis skaitmuo, panašiai kaip anksčiau žaidžiant lyginumo kortelė.

## Knygos ISBN numerio tikrinimas

Vadinasi, jei knygai suteiktas *tarptautinis standartinis knygos numeris* ISBN (angl. *International Standard Book Number*), galima patikrinti, ar nepadaryta klaida. Paprastai tikrinama kontrolinė suma.

Toliau aptariama, kaip tikrinama kontrolinė 10 skaitmenų suma. Pirmasis skaitmuo dauginamas iš 10, antrasis – iš 9, trečiasis – iš 8 ir t. t., devintasis dauginamas iš 2. Visos gautos sandaugos sudedamos. Pavyzdžiui, kodo ISBN 0–13–911991–4 suma yra

$$(0 \times 10) + (1 \times 9) + (3 \times 8) + (9 \times 7) + (1 \times 6) \\ + (1 \times 5) + (9 \times 4) + (9 \times 3) + (1 \times 2) = 172.$$

Gautas skaičius padalijamas iš 11. Kokia liekana?

$$172 : 11 = 15 \text{ liekana } 7$$

Jei liekana yra 0, tai kontrolinė suma yra 0. Kitu atveju iš 11 atimama liekana ir gaunama kontrolinė suma

$$11 - 7 = 4$$

Ar skaitmuo 4 yra ISBN knygos kodo paskutinis skaitmuo? Taip.

Tai reiškia, kad numeruojant knygas naudojamas ISBN.

Jei paskutinis skaitmuo būtų ne 4, būtų aišku, kad padaryta klaida.

Galima apskaičiuoti 10 skaitmenų kodo kontrolinę sumą, kuriai reikia daugiau kaip vieno skaitmens (iš 11 atėmus liekaną gaunama 10). Kai taip atsitinka, kontrolinio skaičiaus vietoje rašomas ženklas X.

## Brūkšninio kodo tikrinimas

Kitas kontrolinio skaitmens pavyzdys yra gaminio brūkšninis kodas. Jis nustatomas kita formule (tokia pat formule tikrinami ir 13 skaitmenų knygų kodai).

Brūkšninis kodas (angl. barcode) – įvairaus pločio nevienodu atstumu išdėstytų lygiagrečių brūkšnelių seka. Tai vizualus, įrenginiams įskaitomos informacijos pateikimo būdas. Kiekvienas skaitmuo žymimas dviem skirtingo pločio brūkšniais ir dviem tarpais.

Brūkšninius kodus nuskaito brūkšninių kodų skaitytuvai (dar vadinami optiniais skeneriais). Brūkšninį kodą sudaro: šalies kodas, gamintojo kodas, prekės kodas, kontrolinis skaičius.

Jei brūkšninis kodas nuskaitomas neteisingai, tai paskutinis (kontrolinis) skaitmuo skiriasi nuo jo apskaičiuotos reikšmės. Kai taip nutinka, kasininkas dar kartą nuskaito



kodą. Kontrolinis skaitmuo naudojamas banko sąskaitų, mokesčių, traukinių numeriuose ir kitur, kur žmonėms reikia įsitikinti, kad naudojamas numeris yra teisingas.



Traškos duonos riekelių „Jorė“ dėžutės brūkšninis kodas

Labiausiai paplitę yra 13 eilučių europietiški kodai EAN-13 (angl. *European Article Numbering*) ir suderinamas su jais 13 eilučių kodas UPC, naudojamas Kanadoje ir JAV.

### **Kontrolinės sumos skaičiavimas**

1. Sudedami antras, ketvirtas, šeštas, aštuntas, dešimtas ir dvyliktas skaitmenys ir gauta suma patrigubinama.
2. Prie gauto rezultato pridedami visi kiti kodo skaitmenys, išskyrus kontrolinį.
3. Paskutinis gautos sumos skaitmuo atimamas iš 10.

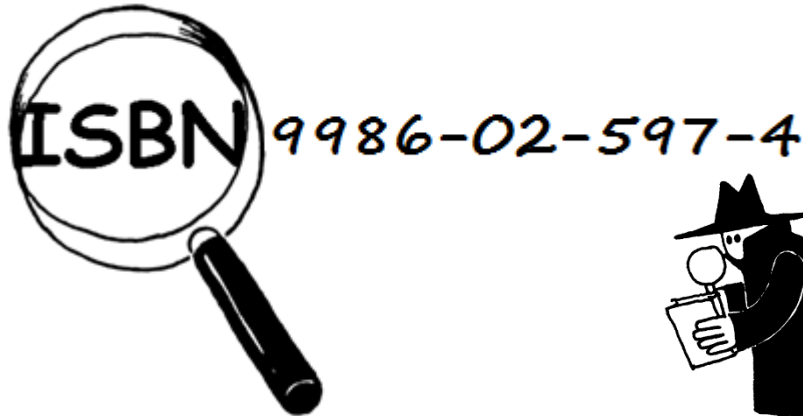
Jei skirtumas nesutampa su kontroliniu skaičiumi, kodas netikras, prekė padirbta.

Apskaičiuokite „Jorės“ dėžutės brūkšninio kodo kontrolinį skaičių. Ar jis tikras?

# Patikrink šią knygą!

Detektyvai

Knygų tikrinimo paslaugos



Randame ir patikriname ISBN kontrolines sumas už nedidelį mokestį.

Prisijunk prie mūsų. Savo klasėje arba bibliotekoje suraskite knygų ir patikrinkite jų ISBN kodus.

## Ar jų kontrolinės sumos teisingos?

Kartais būna klaidų.

Dažnai pasitaikančios klaidos:

- ✗ pakeista skaitmens reikšmė;
- ✗ du skaitmenys sukeisti vietomis;
- ✗ skaitmuo įterptas į numerį;
- ✗ skaitmuo praleistas numeryje.

Ar galėtumėte surasti knygą su X kontrolinei sumai 10? Neturėtų būti labai sunku, nes kiekviena 11 knyga jį turi.

Kokios klaidos nebūtų galima nustatyti? Ar galima pakeisti skaitmenį ir gauti teisingą kontrolinę sumą?

Kas nutiks, jei du skaitmenys bus sukeisti vietomis (dažna skaitmenų rinkimo klaida)?



## Apie ką visa tai?

---

Tarkime, reikia įnešti 10 € į banko sąskaitą. Banko kasininkas įveda sumą ir siunčia duomenis į centrinį kompiuterį. Tačiau atsiranda trikdžių ir į centrinį kompiuterį vietoj kodo 10 € nusiunčiamas kodas 1000 €. Nors klientui tai džiaugsmas, bet bankui – tai didelė problema!

Svarbu nustatyti siunčiamų duomenų klaidas. Priimančias duomenis kompiuteris turi patikrinti, ar jie siunčiant nebuvo sugadinti kokių elektros trikdžių. Kartais klaidingai perduodamų duomenų siuntimas pakartojamas, tačiau kai kada tai neįmanoma, pavyzdžiui, kai diską sugadina magnetinė ar elektrinė spinduliuotė, karštis ar jis pažeidžiamas fiziškai arba kai duomenys gaunami iš kosmoso, labai ilgai reikia laukti retransliacijos, jei įvyksta klaida. Pavyzdžiui, signalas eina pusę valandos nuo Jupiterio iki Žemės, kai jis nuo Žemės būna mažiausiai nutolęs.

Reikia mokėti atpažinti sugadintus duomenis (*klaidos radimas*) ir atkurti originalius duomenis (*klaidos ištaisymas*).

„Magiško triuko“ žaidimo metodika naudojama ir kompiuteriuose. Bitai surašomi į įsivaizduojamus stulpelius ir eilutes, į kiekvieną eilutę ir stulpelį prirašomi papildomi lyginumo bitai. Tokiu būdu galima ne tik nustatyti klaidą, bet ir pasakyti, kur ji yra. Pažeistas bitas atkuriamas. Klaida ištaisoma.

Kompiuteriuose naudojamos daug sudėtingesnės klaidų kontroliavimo sistemos, kurios gali nustatyti ir ištaisyti sudėtingesnius klaidas. Dalis kompiuterio standžiojo disko yra skirta klaidoms taisyti, todėl diskas gali patikimai veikti net tada, jei dalis jo yra pažeista. Tam naudojama klaidų kontrolė pagrįsta lyginumu.

## Sprendimai ir užuominos

---

ISBN 10 skaitmenų kodo kontrolinės sumos klaida yra nenustatoma, kai vienas skaitmuo padidėja, o kitas sumažėja. Tada sumos yra vienodos, o kodai skirtingi. Naudojant aprašytą skaičiavimo metodą, vargu ar tai kada nutiks. 13 skaitmenų ISBN sistemoje yra kitokio tipo nenustatomų klaidų: trys iš eilės einantys skaitmenys apverčiami. Tačiau dauguma klaidų (vienas neteisingai surinktas skaitmuo arba vietomis sukeisti du skaitmenys) dažniausiai aptinkama.



## 5 veikla

### Dvidešimt spėjimų. Informacijos teorija

---

#### Santrauka

Kiek informacijos yra 1000 puslapių knygoje? Kur informacijos daugiau: 1000 puslapių telefonų knygoje, 1000 tuščių puslapių ar J. R. R. Tolkinio (J. R. R. Tolkien) knygoje „Žiedų valdovas“? Jei galima išmatuoti informaciją, galima ir įvertinti, kiek vietos reikia šiai informacijai laikyti. Pavyzdžiui, ar galite perskaityti toliau esantį sakinį?

Šis skersinis nra bus.

Tikriausiai galite, nes balsės šiame sakinyje neturi daug informacijos. Ši veikla supažindina su informacijos turinio matavimo būdu.

#### Ryšiai su ugdymo programomis

- ✓ Matematika: skaičiai, skaičių palyginimas, rikiavimas
- ✓ Matematika: algebra, modeliai ir sekos
- ✓ Lietuvių kalba: rašyba, teksto elementų atpažinimas

#### Gebėjimai

- ✓ Skaičių lyginimo ir skaičių intervalų naudojimo
- ✓ Dedukcijos
- ✓ Klausinėjimo

#### Amžius

- ✓ Nuo 10 metų

#### Priemonės

- ✓ Pirmai veiklai atlikti papildomos priemonės nereikalingos

Papildomai veiklai atlikti kiekvienam mokiniui reikia:

- ✓ Darbo lapo „Sprendimų medžiai“

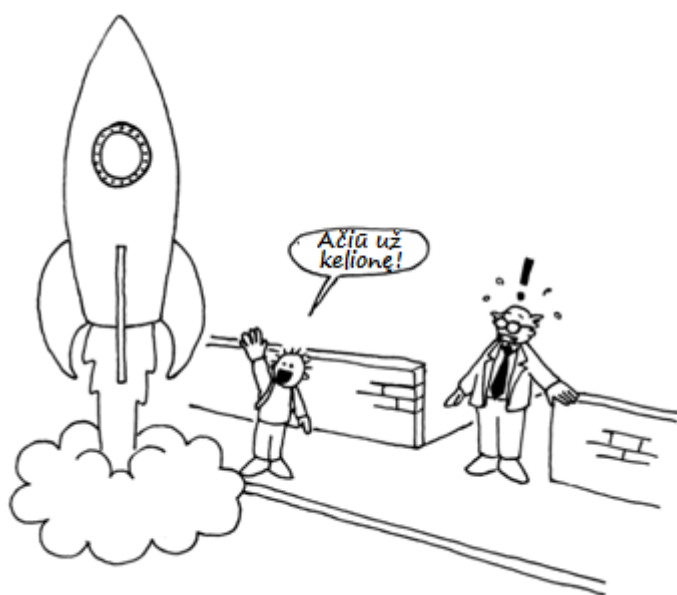


# Dvidešimt spėjimų

---

## Diskusija

1. Su mokiniais diskutuojama, kaip jie supranta, kas yra informacija.
2. Kaip galima pamatuoti, kiek informacijos yra knygoje? Ar puslapių, žodžių skaičius yra svarbus? Ar viena knyga gali turėti daugiau informacijos už kitą? Ar nuobodžiai knyga turi mažiau informacijos negu įdomi? Ar 400 puslapių knygoje, kurioje parašyta tik „cha, cha, cha...“, yra daugiau (mažiau) informacijos nei, pavyzdžiui, telefonų knygoje?
3. Paaiškinama, kad informacija informatikoje matuojama pagal pranešimo ar knygos netikėtumą. Sakykime, jūsų draugas, kuris kiekvieną dieną eina į mokyklą pėsčiomis, sako: „Aš atėjau į mokyklą pėsčiomis“. Jo pasakymas nesuteikia jums informacijos, nes jis nėra netikėtas. Tačiau, jei jis pasakytų: „Aš atskridau į mokyklą sraigtasparniu“, tai būtų netikėta ir jūs informacijos gautumėte daugiau.
4. Kaip įvertinti informacijos netikėtumą?
5. Vienas iš būdų yra parodyti, kaip sunku atspėti informaciją. Jei jūsų draugas pasakytų: „Atspėk, kaip aš šiandien atvykau į mokyklą“, tai pirmasis spėjimas tikriausiai būtų, kad jis atėjo pėsčiomis. Tačiau reikėtų dar kelių spėjimų, jei jis atskrido sraigtasparniu, ar dar daugiau spėjimų, jei atskrido erdvėlaiviu.
6. Informacijos kiekis, kurį turi žinia, priklauso nuo to, kaip lengva ar sunku ją atspėti. Toliau aprašytas žaidimas padės tai išsiaiškinti.



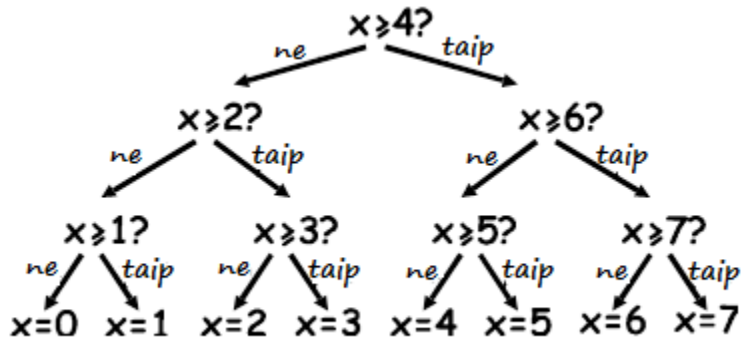




## Darbo lapas. Sprendimų medžiai

Išsiaiškinome klausinėjimo strategiją, todėl esame pasiruošę perduoti žinią neklausinėdami.

Pateikta diagrama „Sprendimų medis“ vaizduoja skaičiaus nuo 0 iki 7 spėjimą.



Nurodykite atsakymų „taip“ ir „ne“ kelią, kai spėjate skaičių 5.

Kiek pasirinkčių „taip“ ir „ne“ reikia norint atspėti bet kurį skaičių?

Atkreipiame dėmesį į kai ką įdomaus. Aukščiau pavyzdyje po skaičiais 0, 1, 2, 3, ... paskutinėje eilėje užrašykite jų reikšmes dvejetainė sistema (žr. 1 veiklą).

Atidžiau pažvelkite į medį. Pakeiskite medyje pasirinktį „ne“ į 0, o „taip“ – į 1. Ką matote?

Žaidžiant skaičių spėjimo žaidimą klausimai parenkami taip, kad pasirinkčių seka vaizduotų spėjamą skaičių dvejetainė sistema.

Nubraižykite sprendimų medį, kuris vaizduotų skaičiaus nuo 0 iki 15 spėjimą.

**Gudručiams.** Kokį medį naudotumėte spėdami kieno nors amžių?  
Kokiu medžiu pavaizduotumėte sakinio raidžių sprendimų medį?

## Apie ką visa tai?

---

Žymus amerikiečių matematikas (buvęs fokusininkas, taip pat važinėjęs vienračiu) Klodas Šenonas (Claude Shannon) atliko daug šio žaidimo eksperimentų. Jis išmatavo informacijos kiekį bitais – kiekvienas atsakymas „taip“ arba „ne“ yra vienas bitas. K. Šenonas atrado, kad informacijos kiekis žinioje priklauso nuo to, kas žinoma. Kartais gali būti užduodamas klausimas, kuris labai sumažina toliau užduodamų klausimų skaičių. Tokiu atveju informacijos kiekis yra mažesnis. Pavyzdžiui, informacijos, kokia puse atsivers viena metama moneta, kiekis, yra vienas bitas: herbas arba skaičius. Bet jei moneta netaisyklinga (deformuota) ir herbas atsivers devynis kartus iš dešimties, tai informacijos kiekis mažesnis kaip vienas bitas. Kaip nustatyti, ar monetos atsivertusioji pusė išsiaiškina užduodant vieną klausimą, į kurį atsakoma tik „taip“ ir „ne“? Tiesiog galima klausti: „Ar metus monetą du kartus abu kartus atsivers herbas?“ Į 80 proc. tokių klausimų, jei metama netaisyklinga mo–neta, atsakymas būtų „taip“ ir tik 20 proc. klausimų atsakymas būtų „ne“. Vidutiniškai užduodamas mažiausiai vienas klausimas apie vieną monetos metimą.

K. Šenonas įvedė informacijos turinio matavimo terminą – *entropiją*. Entropija priklauso ne tik nuo galimų atsakymų skaičiaus, bet ir nuo įvykio tikimybės. Neįtikėtinam arba netikėtam įvykiui išsiaiškinti užduodama daugiau klausimų, nes tokiu būdu gaunama daugiau informacijos.

Informatikams žinios entropija yra labai svarbi. Negalima suspausti žinios, kad užimtų mažiau vietos nei jos entropija, o geriausia pakavimo programa yra kaip spėjimo žaidimas. Kadangi kompiuterio programa „spėja“, o atsakymai koduojami bitais, klausimų perskaičiavimas gali būti atliktas vėliau, atkuriant informaciją. Geriausia pakavimo programa gali sumažinti tekstinio failo dydį – tai sutaupo gana daug kompiuterio atminties!

Spėjimo metodas taikomas ir kuriant kompiuterio programų vartotojo sąsają, kai spėjama, kokius ženklus vartotojas ruošiasi toliau rinkti. Tai gali būti naudinga neįgaliesiems, kuriems sunku rinkti ženklus klaviatūra. Kompiuteris spėja, ką žmogus ruošiasi rinkti, tad šiam belieka sutikti arba atmesti siūlymus. Kompiuteriui užtenka tik vieno atsakymo „taip“ arba „ne“ kiekvienam ženklui, bet tai gali būti didelė pagalba sutrikusios koordinacijos ar judėjimo žmonėms, kuriems sunku naudotis kompiuterio klaviatūra ar pele. Ši teksto rinkimo sistema naudojama ir kai kuriuose liečiamuosiuose telefonuose.



## Sprendimai ir užuominos

---

Vieno „taip“ arba „ne“ klausimo atsakymas atitinka lygiai vieną bitą ir nepriklauso nuo klausimo sudėtingumo. Pavyzdžiui, gali būti užduodamas paprastas klausimas: „Ar skaičius yra didesnis už 50?“ arba sudėtingesnis: „Ar skaičius yra nuo 20 iki 60?“, atsakymas vis tiek yra vienas bitas.

Jei skaičiaus spėjimo žaidime klausimai pasirenkami tam tikra tvarka, atsakymų seka yra spėjamo skaičiaus reikšmė dvejetainėje sistemoje. Trys dvejetainėje sistemoje yra 110, atsakymų apie šį skaičių seka skaičiaus spėjimo žaidime yra „ne, taip, taip“ arba „0, 1, 1“, jei „ne“ žymimas 0, o „taip“ – 1.

Raidės spėjimas sakinyje gali priklausyti nuo prieš ją esančios raidės.



# **II dalis**

## **Kaip veikia kompiuteris?**

### **Algoritmai**



# Kaip veikia kompiuteris?

---

Kompiuteris gali būti puikus žmogaus pagalbininkas, kai reikia kaupti, laikyti, saugoti, apdoroti, perduoti informaciją ar jos ieškoti. Kompiuteriu apdorojamą informaciją įprasta vadinti duomenimis. Veiksmai su jais užrašomi algoritmais. Kompiuteriu apdorojama daug informacijos. Siekiant kuo didesnės spartos reikia sukurti tokių algoritmų, kurie padėtų iš informacijos gausos kuo greičiau rasti tam tikrą informaciją ir ją perduoti tinklu.

Algoritmas – tai aiškūs ir tikslūs nurodymai, kaip ir kokius veiksmus reikia atlikti siekiant užsibrėžto tikslo arba išspręsti suformuluotą uždavinį. Informatikoje algoritmo sąvoka yra esminė. Algoritmu kompiuteriui nurodoma, kaip spręsti problemą. Vieni algoritmai yra spartesni už kitus, todėl jais išspręsti problemas galima daug greičiau nei anksčiau. Pavyzdžiui, surasti skaičiaus  $\pi$  (pi) milijoną skaitmenų po kablelio, visus tinklalapius, kuriuose minimas tam tikras žodis, talpiausią dėjimo į konteinerį būdą, didžiausią pirminį skaičių ir kt.

Algoritmo sąvoka atsirado labai seniai, daugiau nei prieš tūkstantį metų. Pats žodis „algoritmas“ kilo iš IX a. arabų matematiko ir astronomo Mohamedo ibn Musos al Chorezmio lotyniškais rašmenimis parašyto vardo *Algorithmi*. Šis mokslininkas sudarė keturių aritmetikos veiksmų dešimtainiais skaičiais taisyklės, kurias Europoje imta vadinti „algorizmais“. Vėliau šis žodis buvo pakeistas „algoritmu“, jam suteikta platesnė prasmė – juo pradėtos vadinti įvairių skaičiavimų (ne tik aritmetinių) taisyklės.

## 6 veikla

# Laivų mūšis. Paieškos algoritmai

---

### Santrauka

Dažnai kompiuteris turi surasti tam tikrą informaciją iš didelio jos kiekio. Tuo tikslu turi būti sukurtas greitas ir efektyvus būdas. Čia pateikiami trys skirtingi paieškos metodai: *nuoseklioji paieška*, *dvejetainė paieška* ir *maiša* (angl. *hashing*).

### Ryšiai su ugdymo programomis

- ✓ Matematika: skaičiai ir skaičiavimai, skaičių palyginimas
- ✓ Matematika: sąryšiai ir funkcijos, koordinatės
- ✓ Informatika: algoritmai

### Gebėjimai

- ✓ Loginio argumentavimo

### Amžius

- ✓ Nuo 9 metų

### Priemonės

Kiekvienam mokiniui reikia:

- ✓ Darbo lapų laivų mūšio žaidimams
  - 1A, 1B pirmajam žaidimui
  - 2A, 2B antrajam žaidimui
  - 3A, 3B trečiajam žaidimui
- ✓ Papildomi žaidimų lapai: 1A', 1B', 2A', 2B', 3A', 3B'



# Laivų mūšis

---

## Įvadas

1. Pasirenkama 15 mokinių, kurie sustoja viena eile prieš klasę. Kiekvienam mokiniui duodama kortelė su skaičiumi (atsitiktine tvarka). Skaičiai nerodomi likusiems mokiniams. Pasakoma, į kokį intervalą patenka turimi skaičiai.
2. Kitiems mokiniams duodama po dėžutę su keturiais ar penkiais saldainiais. Mokiniai turi surasti duotą skaičių. Jie gali „sumokėti“ saldainiais ir pažiūrėti į tam tikrą kortelę. Jei jie suranda teisingą skaičių anksčiau, nei išdalija savo saldainius, tai likusius saldainius gali pasilikti.
3. Kai žaidimas baigiamas, jei reikia, jį galima sužaisti dar kartą.
4. Kortelės išmaišomos ir vėl išdalijamos mokiniams. Dabar mokiniai sustoja į eilę jų kortelėse esančių skaičių didėjimo tvarka. Kartojama paieška, aprašyta antrajame punkte.

Jei skaičiai surikiuoti, mokiniai turėtų suvokti geriausią veikimo būdą – už vieną saldainį gali atsikratyti pusės mokinių, pasirinkę atversti vidurinio mokinio kortelę. Kartodami šį veiksmą jie gali išsiaiškinti ieškomą skaičių „sumokėję“ tris saldainius. Šio metodo efektyvumas akivaizdus.

## Veikla

Mokiniai gali suvokti, kaip kompiuteris ieško informacijos, žaisdami laivų mūšio žaidimą. Žaidžiant šį žaidimą mokinių paprašoma apgalvoti metodus, kuriais galima tiksliau nustatyti laivo vietą.





# Laivų mūšis. Nuoseklioji paieška

---

## Instrukcija

1. Mokiniai susiskirsto poromis. Vienas paima 1A lapą, kitas – 1B. Savo lapų mokiniai vienas kitam nerodo!
2. Abu mokiniai apveda vieną laivą viršutinėje savo lapo kortelėje ir pasako jo numerį vienas kitam.
3. Vienas po kito abu mokiniai spėja, kur yra apibrauktas porininko laivas: sako bet kurio laivo raidę, o porininkas turi pasakyti to laivo numerį.
4. Mokiniai turi nustatyti, kiek reikia šūvių norint pataikyti į porininko pasirinktą laivą. Šūvių skaičius atitinka žaidimo taškus.

(Papildomi lapai 1A' ir 1B' skirti mokiniams, norintiems žaisti dar kartą arba iškart atspėjusiems porininko laivo vietą. Lapai 2A', 2B' ir 3A', 3B' skirti kitiems žaidimams.)

## Diskusija

1. Kokie žaidimo rezultatai?
2. Koks galimas mažiausias ir didžiausias šūvių skaičius? (Mokiniai turėtų nurodyti atitinkamai 1 ir 26. Daroma prielaida, kad mokiniai nešaus į tą patį laivą du kartus.)



# Laivų mūšis. Dvejetainė paieška

---

## Instrukcija

1. Mokiniai susiskirsto poromis. Vienas paima 1A lapą, kitas – 1B. Savo lapų mokiniai vienas kitam nerodo!
2. Abu mokiniai apveda vieną laivą viršutinėje savo lapo kortelėje ir pasako jo numerį vienas kitam.
3. Vienas po kito abu mokiniai spėja, kur yra apibrauktas porininko laivas: sako bet kurio laivo raidę, o porininkas turi pasakyti to laivo numerį.
4. Mokiniai turi nustatyti, kiek reikia šūvių norint pataikyti į partnerio pasirinktą laivą. Šūvių skaičius atitinka žaidimo taškus.

(Papildomi lapai 2A' ir 2B' skirti mokiniams, norintiems žaisti dar kartą arba iškart atspėjusiems porininko laivo vietą. Lapai 3A', 3B' skirti kitam žaidimui.)

## Diskusija

1. Kokie žaidimo rezultatai?
2. Koku metodu buvo surinkta mažiausiai taškų?
3. Į kurį laivą šaunama pirmiausia? (Šūvis į vidurinį sutrumpina paiešką perpus.) Į kurį laivą šaunama antrą kartą? (Geriausia šauti į vidurinį laivą ieškomame intervale.)
4. Jei buvo veikiama šiuo metodu, kiek prireikė šūvių pataikyti į laivą? (Daugiausia 5 šūviai.)

Šis metodas vadinamas *dvejetainė paieška*, nes intervalai visada dalijami į dvi dalis.



# Laivų mūšis. Maiša

---

## Instrukcija

1. Mokiniai susiskirsto poromis. Vienas paima 3A lapą, kitas – 3B. Abu vienas kitam pasako savo pasirinkto laivo numerį.
2. Žaidžiant šį žaidimą reikia nustatyti, kuriame iš dešimties stulpelių (nuo 0 iki 9) yra laivas. Tuo tikslu sudedami laivo numerio skaitmenys. Gautos sumos vienetų skaitmuo parodo, kuriame stulpelyje yra laivas. Pavyzdžiui, laivo numeris yra 2345, tai  $2+3+4+5$  yra 14. Vienetų skaitmuo yra 4, taigi laivas yra ketvirtajame stulpelyje. Nustačius laivo stulpelį belieka atspėti laivą. Šis metodas vadinamas *maiša*, nes skaitmenys yra „sugrūsti“ drauge.
3. Dabar galima pabandyti žaisti šiuo metodu. Žaidimą galima pakartoti pasirenkant laivą iš kito stulpelio.

(Gali būti naudojami tik papildomi lapai 3A' ir 3B', nes abiejuose lapuose laivai turi būti išdėstyti stulpeliuose vienodai.)

## Diskusija

1. Kokie žaidimo rezultatai?
2. Kokiu metodu buvo surinkta mažiausiai taškų?
3. Kuriuos laivus buvo lengviausia nušauti? (Tuos, kurie yra vieninteliai stulpelyje.) Kuriuos sunkiausia? (Tuos, kai jie yra stulpeliuose, kuriuose yra daugiau kitų laivų.)
4. Kuris iš paieškos metodų greičiausias? Kodėl?
5. Kuo vienas paieškos metodas geresnis už kitą? (Antrasis metodas yra greitesnis už pirmąjį, bet pasirinkus pirmąjį nereikia išrikiuoti laivų. Trečiasis metodas paprastai yra greičiausias, bet netinkamai pasirinkus pirmąjį laivą, paieška šiuo metodu gali būti labai lėta.)



## Papildomos veiklos

---

1. Mokiniai gali sugalvoti žaidimų patys. Žaisdami antrąjį žaidimą jie turėjo skaičius išdėlioti didėjančiai. Mokiniai galėtų pamąstyti, kaip būtų galima pasunkinti trečią laivų mūšio žaidimą. (Sunkiausia žaisti, kai visi laivai yra vienoje eilėje.) Kaip būtų galima pakeisti trečią žaidimą? (Reikėtų sudėti po vienodą skaičių laivų kiekviename stulpelyje.)
2. Kas nutiktų, jei ieškomo laivo lape nebūtų? (Atlikdami nuosekliają paiešką tuo įsitikintume padarę 26 žingsnius. Jei paieška dvejetainė, reikėtų tik 5 žingsnių. Jei naudojamos maiša, žingsnių skaičius priklauso nuo laivų skaičiaus kiekviename stulpelyje.)
3. Kiek dvejetainės paieškos žingsnių prireiktų laivo vietai nustatyti, jei būtų 100 laivų (6 žingsnių), 1000 laivų (apie 9) ar milijonas laivų (apie 19)? (Žingsnių skaičius didėja labai lėtai palyginti su laivų skaičiumi. Kai laivų skaičius padidėja dvigubai, reikalingas papildomas žingsnis.)



## Mano laivai

Šūvių skaičius:

9058	7169	3214	5891	4917	2767	4715	674	8088	1790	8949	13	3014
A	B	C	D	E	F	G	H	I	J	K	L	M
8311	7621	3542	9264	450	8562	4191	4932	9462	8423	5063	6221	2244
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

## Priešininko laivai

Šūvių skaičius:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

# 1A



## Mano laivai

Šūvių skaičius:

1630	9263	4127	405	4429	7113	3176	4015	7976	88	3465	1571	8625
A	B	C	D	E	F	G	H	I	J	K	L	M
2587	7187	5258	8020	1919	141	4414	3056	9118	717	7021	3076	3336
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

## Priešininko laivai

Šūvių skaičius:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

# 1B



## Mano laivai

Šūvių skaičius:

163	445	622	1410	1704	2169	2680	2713	2734	3972	4208	4871	5031
A	B	C	D	E	F	G	H	I	J	K	L	M
5283	5704	6025	6801	7440	7542	7956	8094	8672	9137	9224	9508	9663
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

## Priešininko laivai

Šūvių skaičius:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

2A



## Mano laivai

## Šūvių skaičius:

33	183	730	911	1927	1943	2200	2215	3451	3519	4055	5548	5655
A	B	C	D	E	F	G	H	I	J	K	L	M
5785	5897	5905	6118	6296	6625	6771	6831	7151	7806	8077	9024	9328
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

## Priešininko laivai

## Šūvių skaičius:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

2B





Mano laivai										Šūvių skaičius:																									
0	A 9047	B 1829	1	C 3080	D 9994	2	3	E 5125	F 1480	G 8212	4	H 8051	I 1481	J 4712	K 6422	5	L 7116	M 8944	N 4128	6	O 6000	P 7432	Q 4110	7	R 9891	S 1989	T 2050	U 8199	8	V 4392	9	W 1062	X 2106	Y 5842	Z 7057

Priešininko laivai										Šūvių skaičius:																									
0	A	B	C	D	1	E	F	G	2	H	I	J	3	K	4	L	M	N	5	6	O	P	Q	7	R	S	T	U	8	V	W	X	9	Y	Z

# 3A



Šūvių skaičius:																									
<b>Mano laivai</b>		0	1	2	3	4	5	6	7	8	9														
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
9308	1478	8417	9434	6519	2469	5105	1524	8112	2000	4135	9050	1265	5711	4200	7153	6028	3121	9503	1114	7019	2385	5832	1917	1990	2502

Priešininkų laivai																									
Šūvių skaičius:																									
0	1	2	3	4	5	6	7	8	9																
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

# 3B



## Mano laivai

Šūvių skaičius:

6123	1519	9024	5164	2038	2142	7156	9974	9375	7104	1004	1023	5108
A	B	C	D	E	F	G	H	I	J	K	L	M
1884	3541	5251	4840	3289	3654	2480	5602	8965	4053	2405	2304	1959
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

## Priešininko laivai

Šūvių skaičius:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

1A'

Mano laivai		Šūvių skaičius:	
A	2387	9003	3951
B	5695	1284	4761
C	7118	1196	1741
D	3791	3405	3132
E	6682	682	682
F	9493	9864	7359
G	1250	7036	2916
H	7562	9299	8910
I	6713	5173	8617
J	4222	4222	4222
K			
L			
M			
N			
O			
P			
Q			
R			
S			
T			
U			
V			
W			
X			
Y			
Z			

Priešininko laivai		Šūvių skaičius:	
A			
B			
C			
D			
E			
F			
G			
H			
I			
J			
K			
L			
M			
N			
O			
P			
Q			
R			
S			
T			
U			
V			
W			
X			
Y			
Z			

1B'



## Mano laivai

Šūvių skaičius:

28	326	943	1321	1896	2346	2430	2929	3106	3417	4128	4717	4915
A	B	C	D	E	F	G	H	I	J	K	L	M
5123	5615	6100	7015	7120	7695	7812	8103	8719	9020	9608	9713	9911
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

## Priešininko laivai

Šūvių skaičius:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

2A'

## Mano laivai

## Šūvių skaičius:

56	194	306	1024	1510	1807	2500	2812	3011	3902	4178	5902	5915
A	B	C	D	E	F	G	H	I	J	K	L	M
6102	6526	6818	7020	7155	7913	8016	8230	8599	8902	9090	9526	9812
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

## Priešininko laivai

## Šūvių skaičius

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

2B'

## Mano laivai

## Šūvių skaičius:

0	A 1982 B 7841	1	C 6113 D 1055	2		3	E 9121 F 1011 G 2984	4	H 5009 I 2651 J 1751 K 4848	5	L 1248 M 1716 N 2148	6	O 2004 P 5173 Q 2806	7	R 9369 S 1321 T 3004 U 7190	8	V 3285	9	W 9172 X 2052 Y 6012 Z 7525
---	------------------	---	------------------	---	--	---	----------------------------	---	--------------------------------------	---	----------------------------	---	----------------------------	---	--------------------------------------	---	--------	---	--------------------------------------

## Priešininko laivai

## Šūvių skaičius:

0	A B C D	1	E F G	2	H I J	3	K	4	L M N	5		6	O P Q	7	R S T U	8	V W X	9	Y Z
---	------------------	---	-------------	---	-------------	---	---	---	-------------	---	--	---	-------------	---	------------------	---	-------------	---	--------

# 3A'





## Mano laivai

## Šūvių skaičius:

0	A 8615 B 7003 C 1991 D 6211	1	E 1361 F 7644 G 5600	2	H 7726 I 9003 J 5557	3	K 3000	4	L 1814 M 2002 N 8844	5		6	O 9656 P 4002 Q 1221	7	R 6993 S 3121 T 4300 U 1907	8	V 8208 W 9423 X 4176	9	Y 2917 Z 4122
---	--------------------------------------	---	----------------------------	---	----------------------------	---	--------	---	----------------------------	---	--	---	----------------------------	---	--------------------------------------	---	----------------------------	---	------------------

## Priešininko laivai

## Šūvių skaičius:

0	A B	1	C D	2		3	E F G	4	H I J K	5	L M N	6	O P Q	7	R S T U	8	V	9	W X Y Z
---	--------	---	--------	---	--	---	-------------	---	------------------	---	-------------	---	-------------	---	------------------	---	---	---	------------------

# 3B'





## Apie ką visa tai?

---

Kompiuteriuose laikoma labai daug informacijos, ji turi būti greitai apdorojama. Daugiausia paieškos sunkumų kyla dėl būtinos didelės spartos: interneto paieškos sistemomis paieška atliekama tarp milijardo tinklalapių per sekundės dalį. Duomuo (pvz., žodis, kodas ar vardas), pagal kurį ieškoma informacijos, vadinamas reikšminiu žodžiu.

Kompiuteris apdoroja informaciją labai greitai. Galima pamanyti, kad jis paiešką pradeda nuo pirmojo elemento ir tikrina visus elementus iš eilės, kol randa ieškomą. Tokia *nuoseklioji paieška* buvo atliekama viename iš žaidimų, tačiau šis paieškos metodas yra labai lėtas – net ir kompiuteriui. Pavyzdžiui, prekybos centre yra 10000 skirtingų produktų, išdėliotų skirtingose lentynose. Kai nuskaitomas prekės kodas, kompiuteris turi patikrinti 10000 kodų, kol randa reikiamą prekę ir jos kainą. Jei vieną prekę kompiuteris tikrintų vieną tūkstantą sekundės, tai užtruktų 10 sekundžių. Kiek užtruktų surasti visas kieno nors perkamas prekes!

*Dvejetainė paieška* yra greitesnis metodas. Šiuo metodu skaičiai rikiuojami iš eilės didėjančiai. Tikrinant vidurinį sąrašo elementą nustatoma, kurioje pusėje yra ieškomas skaičius. Šis veiksmas kartojamas, kol surandamas ieškomas skaičius. Prisiminus pavyzdį apie prekybos centrą surasti prekės kainą užtruktų dvi šimtasias sekundės, o tai sunkiai pastebima.

Trečiasis duomenų paieškos metodas vadinamas *maiša*. Ši paieška remiasi raktu, sudaromu taip, kad reikiama informacija būtų surasta tiksliai iškart. Pavyzdžiui, jei paieškos raktas yra telefono numeris, galima sudėti visus skaitmenis, imti gautos sumos dalybos iš 11 liekaną. Šiuo atveju maišos raktas šiek tiek panašus į sumų skaičiavimo veiklas, kurios aprašomos 4 veiklos skyriuje – nedidelė duomenų dalis, priklausoma nuo kitų apdorotų duomenų. Maža tikimybė, kad keli maišos raktai atsidurs toje pačioje vietoje ir tada kompiuteris turės atlikti paiešką pagal kiekvieną iš jų, kol suras ieškomą skaičių.

Programuotojai naudoja maišos metodą, kai ieškant duomenų eilė negali būti saugoma ar lėta paieška nėra tikėtina.



## 7 veikla

# Lengviausias ir sunkiausias. Rikiavimo algoritmai

---

### Santrauka

Dažnai kompiuteriui reikia išrikiuoti sąrašą. Pavyzdžiui, išrikiuoti vardus pagal abėcėlę, elektroninius laiškus pagal datą ar kt. Išrikiuotame sąrašė galima greičiau pamatyti ir surasti ieškomą informaciją. Išrikiavus mokinių pažymius, aiškiai matomi patys žemiausi ir patys aukščiausi įvertinimai.

Kai kurie rikiavimo metodai yra neefektyvūs net ir atliekant juos kompiuteriu. Žinoma, yra atrasti keli greitesni rikiavimo metodai. Šiame skyriuje mokiniai sužinos apie skirtingus rikiavimo metodus, kaip pasirinktas „gudrus“ rikiavimo metodas paspartina rikiavimą.

### Ryšiai su ugdymo programomis

- ✓ Matematika: matai ir matavimai, praktinis svorio matavimas
- ✓ Informatika: algoritmai

### Gebėjimai

- ✓ Svarstyklių naudojimo
- ✓ Rikiavimo
- ✓ Lyginimo

### Amžius

- ✓ Nuo 8 metų

### Priemonės

Kiekvienai mokinių grupei reikia:

- ✓ 8 vienodo dydžio, bet skirtingo svorio pakuočių (gali būti pakuotės nuo pieno, nepermatomi plastikiniai buteliukai nuo gėrimo ar skardinės dėžutės, pripildytos smėlio ar vandens)
- ✓ Svirtinių svarstyklių
- ✓ Darbo lapo „Svorių rikiavimas“
- ✓ Darbo lapo „Skaldyk ir valdyk!“



# Lengviausias ir sunkiausias

---

## Diskusija

Kompiuteriui dažnai reikia išrikiuoti duomenis. Kas nutiktų, jei duomenys būtų neišrikiuoti?

Paprastai kompiuteris gali palyginti dvi reikšmes vienu metu. Atlikdami užduotis mokiniai supras, kaip kompiuteris tai daro.

## Veikla

1. Mokiniai suskirstomi į grupes.
2. Kiekvienai grupei duodamas Darbo lapas „Svorių rikiavimas“, sveriamų pakuočių rinkiniai ir svirtinės svarstyklės.
3. Mokiniai atlieka šią veiklą ir tada aptaria rezultatus.



# Darbo lapas. Sviurių rikiavimas

**Tikslas:** surasti geriausią nežinomų sviurių rikiavimo metodą.

**Reikia:** smėlio arba vandens, 8 vienodų pakuočių, svirtinių svarstyklių.

**Ką daryti:**

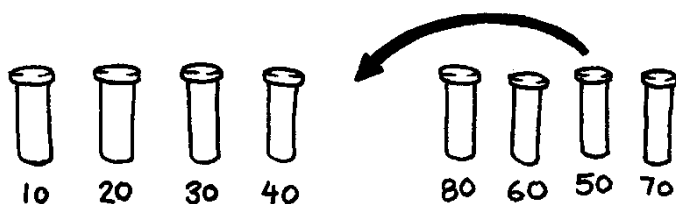
1. Į kiekvieną pakuotę įpilkite skirtingą kiekį smėlio arba vandens. Sandariai uždarykite.
2. Sumaišykite pakuotes, kad nežinotumėte, kiek juose smėlio ar vandens.
3. Suraskite lengviausią pakuotę. Koku paprasčiausiu būdu tai galima padaryti?

**Patarimai.** Naudokite svirtines svarstyklas. Vienu metu galite jomis palyginti tik du sviurus.

4. Atsitiktinai pasirinkite 3 pripildytas pakuotes. Išrikiuokite jas nuo lengviausios iki sunkiausios pasverdami svirtinėmis svarstyklėmis. Kaip tai atlikote? Kiek mažiausiai kartų reikėjo sverti? Kodėl?
5. Išrikiuokite visas 8 pripildytas pakuotes nuo lengviausios iki sunkiausios.
6. Tada patikrinkite, ar gerai išrikiavote, lygindami dviejų gretimų pakuočių sviurį svirtinėmis svarstyklėmis.

## Išrenkamojo rikiavimo algoritmas

Vienas iš kompiuterio naudojamų rikiavimo algoritmų yra *išrenkamojo rikiavimo algoritmas*. Pirma, surandamas mažiausias sviuris ir atidedamas į šoną. Antra, surandamas mažiausias sviuris iš likusiųjų ir atidedamas šalia pirmojo mažiausio. Tai kartojama, kol visi sviuriai išrikiuojami.



Suskaičiuokite, kiek kartų lyginote sviurus.

**Gudručiams.** Parodykite, kaip matematiškai galima suskaičiuoti, kiek kartų reikia atlikti palyginimą norint išrikiuoti 8 daiktus jų sviurių didėjimo (mažėjimo) tvarka. Kiek reikės palyginimų, jei bus 20 daiktų?

# Darbo lapas. Skaldyk ir valdyk!

## Greitojo rikiavimo algoritmas

*Greitojo rikiavimo algoritmas* yra daug greitesnis ir paprastesnis už *išrenkamojo rikiavimo algoritmą*, todėl yra labai dažnai naudojamas.

Ką daryti:

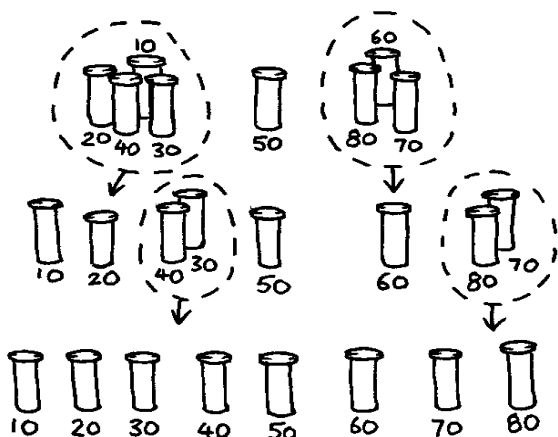
1. Į kiekvieną pakuotę įpilkite skirtingą kiekį smėlio arba vandens ir uždarykite.
2. Sumaišykite pakuotes, kad nežinotumėte, kiek jose smėlio ar vandens.

Atsitiktinai pasirinkite vieną pakuotę ir padėkite jį ant svarstyklių lėkštelės.

Visas likusias pakuotes palyginkite su atsitiktinai pasirinkta. Lengvesnias už ją padėkite kairėje svarstyklių pusėje, o sunkesnes – dešinėje. Pakuotę, su kuria lyginate kitas, padėkite viduryje tarp grupių. (Baigus sverti visas pakuotes gali būti, kad vienoje pusėje bus daug daugiau pakuočių nei kitoje.)

Pasirinkite vieną iš atrinktų pakuočių grupių ir pakartokite tą patį: atsitiktinai iš grupės pasirinkite pakuotę ir palyginkite visas likusias su ja. Tą patį padarykite ir su kita pakuočių grupe. Pakuotę, su kuria lyginate kitų svorį, padėkite viduryje tarp sudarytų naujų dviejų grupių.

Kartokite šiuos veiksmus, kol grupėse liks tik po vieną pakuotę. Kadangi visose grupėse liko tik po vieną pakuotę, vadinasi, visos pakuotės yra išrikiuotos nuo lengviausios iki sunkiausios.



Kiek kartų reikėjo lyginti pakuotes naudojant šį algoritmą?

*Greitasis rikiavimas* yra daug efektyvesnis už *išrenkamojo rikiavimo algoritmą*, jei iš pradžių pavyksta pasirinkti patį lengviausią arba patį sunkiausią daiktą. Jei pasirenkamas vidutinio svorio daiktas, užtenka 14 kartų palyginti visus daiktus ir taip juos išrikiuoti nuo lengviausio iki sunkiausio. Padaryti tą patį *išrenkamojo rikiavimo algoritmu* prireiktų 28 lyginimo kartų.

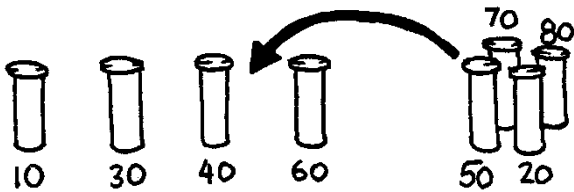
**Gudručiams. Kiek kartų greitojo rikiavimo algoritmu reikėtų lyginti daiktus, jei visada atsitiktinai pasirinktumėte lengviausią daiktą?**



## Kiti rikiavimo metodai

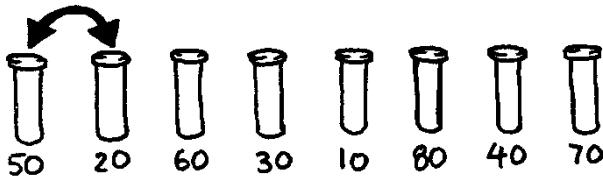
Sugalvota daug rikiavimo metodų. Pabandykite išrikiuoti savo daiktus įvairiais metodais. Rikiuoti tenka ne tik daiktus, bet žodžius (sąvokas), taip pat daiktus apibūdinančius įvairius skaičius, todėl apibendrinant daiktus, sąvokas, skaičius dažnai naudojame objekto sąvoką, o vieną iš rikiuojamų objektų įvardijame kaip elementą.

Pagrindinis *įterpiamojo rikiavimo algoritmo* principas – kiekvienas elementas imamas iš eilės ir įterpiamas į jam skirtą vietą jau surikiuotoje objektų grupėje. Kiekvieną kartą įterpus objektą, neišrikiuotoje grupėje objektų mažėja, o išrikiuotoje – daugėja.

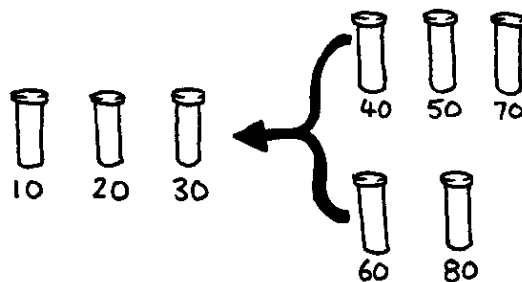


*Burbulinio rikiavimo algoritmo* principas – nuosekliai iš eilės patikrinti gretimų objektų poras, prirėkus objektus sukeisti, t. y. perkelti mažesnį arčiau pradžios. Šitaip per pirmą žingsnį lengviausias objektas perkeliamas į pirmą poziciją, vėliau tas pats principas taikomas likusiems objektams ir t. t.

Šio algoritmo veikimo principas primena virimą, kai oro burbulai kyla į paviršių, dėl to jis ir vadinamas burbulinio rikiavimo metodu. Nors nėra labai efektyvus, šis metodas mėgstamas dėl savo paprastumo.



*Sąlyginio rikiavimo algoritmas* – vienas iš „skaldyk ir valdyk“ principu grindžiamų rikiavimo algoritmų. Pirmiausia objektai atsitiktinai padalijami į dvi lygias (arba panašias, jei yra nelyginis objektų skaičius) grupes. Kiekviena grupė rikiuojama atskirai, paskui abi grupės vėl sujungiamos: lyginant skirtingų grupių objektus po du iš eilės mažiausias objektas perkeliamas į jungtinės objektų grupės pabaigą. Paveiksle 40 ir 60 gramų objektai yra kiekvienos grupės pradžioje, į jungtinę grupę dedamas mažesnio svorio objektas – 40 g ir t. t.



Kaip išrikiuoti mažai objektų? Patartinas sąlyginio rikiavimo algoritmas! Visos grupės padalijamos po vieną objektą, todėl nereikia rūpintis, kada baigti rikiuoti.



## Apie ką visa tai?

---

Išrikiuotame sąrašė daug lengviau surasti reikiamą informaciją. Telefonų knygoje, knygų kartotekoje elementai rikiuojami pagal abėcėlę. Jei jie nebūtų išrikiuoti pagal abėcėlę, būtų daug sunkiau susigaudyti informacijos gausybėje ir rasti reikiamą pavardę telefonų knygoje ar autorių kartotekoje. Išrikiuotame skaičių sąrašė lengva pamatyti didžiausią, mažiausią ar vienodus elementus.

Dažnai rikiuojant pasitelkiami kompiuteriai, todėl informatikai ieško vis greitesnio rikiavimo algoritmo. Dauguma rikiavimo algoritmų, pavyzdžiui, *išrenkamojo*, *įterpiamojo ar burbulinio rikiavimo*, yra naudingi sprendžiant tam tikras problemas. Algoritmai, tokie kaip *greitojo ar sąlajinio rikiavimo*, yra daug efektyvesni ir pritaikomi didesniam objektų skaičiui. Pavyzdžiui, 100000 objektų *greitojo rikiavimo algoritmas* išrikiuoja 2000 kartų greičiau nei *išrenkamojo rikiavimo algoritmas*, o 1000000 objektų – 20000 kartų greičiau. Kompiuteris turi apdoroti milijonus duomenų (daugybė tinklalapių turi milijonus vartotojų, vienoje nuotraukoje yra milijonai pikselių). Šiuodu algoritmai skiriasi tuo, kad pirmasis apdoroja duomenis per 1 s, o antrajam apdoroti tuos pačius duomenis reikia 5 valandų. Ne tik prireikia ilgesnio laiko, bet ir energijos sunaudojama 20000 kartų daugiau. Laiko ir energijos sąnaudos neturi įtakos programinei įrangai, tačiau yra svarbios naudojant prietaisus su baterijomis (planšetinius ar nešiojamuosius kompiuterius, mobiliuosius telefonus ir kt.).

*Greitojo rikiavimo algoritmas* veikia „skaldyk ir valdyk“ principu. Objektai padalijami į mažesnes grupes, kiekvienai iš jų pritaikomas greitojo rikiavimo algoritmas. Algoritmas kartojamas, kol grupėse lieka po vieną objektą. Paprasta rikiuoti, kai lieka tik po vieną objektą! Praktiškai šis metodas yra daug greitesnis nei kiti rikiavimo metodai. Jis realizuoja *rekursijos* idėją, pagal kurią algoritmas keletą kartų kreipiasi į save patį, kol išsprendžia problemą.



## Sprendimai ir užuominos

---

1. Geriausias būdas surasti lengviausią objektą yra tikrinti visus objektus lyginant vieną su kitu. Kitaip tariant, objektai lyginami po du, iš kiekvienos poros ant svarstyklių lėkštelės paliekamas lengvesnis objektas tol, kol perrenkami ir palyginami visi objektai.
2. Objektų svoris lyginamas svirtinėmis svarstyklėmis. Tai galima atlikti palyginus svorį triskart, o kartais ir dukart, jei mokiniai supranta, kad lyginimo operacija yra tranzityvi (t. y. jei A yra lengvesnis už B, o B yra lengvesnis už C, tai A turi būti lengvesnis už C).

### Gudručiams

Norint nustatyti mažiausio svorio objektą iš dviejų reikia vieną kartą juodu palyginti. Ieškant lengviausio iš trijų objektų reikia tuos objektus palyginti du kartus, iš keturių objektų – reikia juos palyginti tris kartus ir t. t. Rikiuojant aštuonis objektus ir norint iš jų surasti pirmą lengviausią reikia 7 kartus palyginti visus objektus, šešis kartus – norint surasti antrą lengviausią objektą ir t. t. Išeina, kad reikia palyginti

$$7 + 6 + 5 + 4 + 3 + 2 + 1 = 28 \text{ kartus.}$$

Rikiuojant  $n$  objektų reikėtų palyginti  $1 + 2 + 3 + 4 + \dots + n - 1$  kartų.

Šiuos skaičius sudėti yra paprasta, kai jie sugrupuojami.

Pavyzdžiui, sudedant skaičius  $1 + 2 + 3 + \dots + 20$ , sugrupuojama

$$(1 + 20) + (2 + 19) + (3 + 18) + (4 + 17) + (5 + 16) +$$

$$(6 + 15) + (7 + 14) + (8 + 13) + (9 + 12) + (10 + 11) = 21 \times 10 = 210$$

Bendruoju atveju gaunama  $1 + 2 + 3 + 4 + \dots + n - 1 = n(n - 1)/2$ .





## 8 veikla

# Dar sparčiau! Tinklinis rikiavimas

---

### Santrauka

Kompiuterio sparta ne visada lemia problemos sprendimo spartą. Vienas iš būdų greičiau išspręsti problemą yra padalyti ją į dalis ir sprendimui naudoti kelis kompiuterius. Šiame skyriuje aiškinamas *tinklinio rikiavimo algoritmas*, kuriuo vienu metu galima lyginti kelis rikiavimo metodus.

### Ryšiai su ugdymo programomis

- ✓ Matematika: skaičiai, skaičių palyginimas

### Gebėjimai

- ✓ Lyginimo
- ✓ Rikiavimo
- ✓ Algoritmo sudarymo
- ✓ Problemos sprendimo bendradarbiaujant

### Amžius

- ✓ Nuo 7 metų

### Priemonės

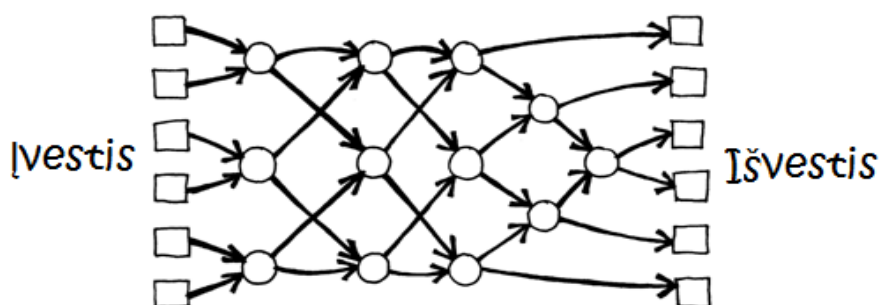
Lauko žaidimas.

- ✓ Kreida
- ✓ Du šešių kortelių rinkiniai. Paruošiamos *tinklinio rikiavimo algoritmo* kortelės
- ✓ Laikmatis



# Tinklinis rikiavimas

Pirmiausia ant žemės (grindinio) nupiešiamas tinklas, kaip parodyta paveiksle. Tinklas turi būti gana didelis, kad mokiniai galėtų po jį vaikščioti.



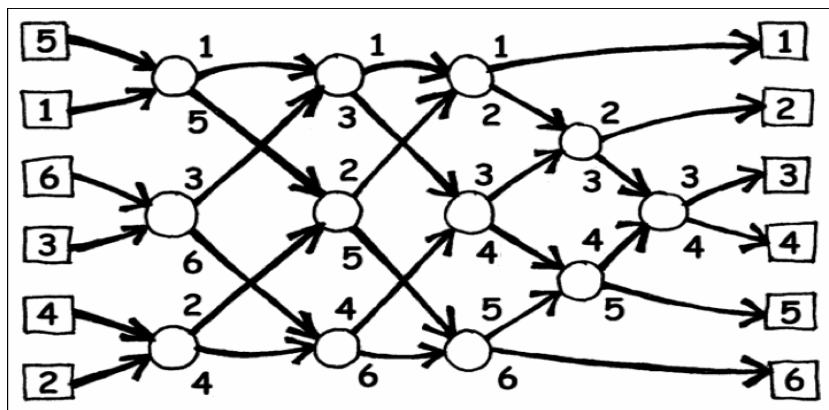
## Instrukcijos

Šiame skyriuje supažindinama, kaip kompiuteris rikiuoja atsitiktinius skaičius *tinklinio rikiavimo algoritmu*.

1. Mokiniai susiskirsto į grupes po šešis. Vienu metu tik viena grupė naudojami tinklu.
2. Kiekvienas mokinys paima kortelę su ant jos užrašytu skaičiumi.
3. Kiekvienas mokinys atsistoja ant kvadrato kairėje tinklo pusėje (ten, kur pažymėta įvestis). Mokinių turimų kortelių skaičiai neturėtų eiti iš eilės.
4. Mokinys juda nurodyta kryptimi. Atsistojęs ant apskritimo **palaukia kito mokinio**.
5. Du mokiniai susitikę apskritime palygina savo kortelių skaičius. Mokinys, kurio skaičius kortelėje yra mažesnis, eina toliau kairiosios rodyklės kryptimi, o kurio skaičius didesnis – dešinėsios rodyklės kryptimi.
6. Mokinys teisingai baigia žaidimą, kai pasiekia kvadratą tinklo dešinėje (ten, kur pažymėta išvestis).

Jei komanda suklysta, turi pradėti iš naujo. Prireikus mokiniams padedama suprasti, ką reikia daryti pasiekus apskritimą.

Rikiavimo pavyzdys parodytas toliau paveiksle.



## Tinklinis rikiavimas

---

**1**

**2**

**3**

**4**

**5**

**6**

---

**156**

**221**

**289**

**314**

**422**

**499**

## Variantai

Kiekvienos grupės tinklo perėjimo laikas gali būti išmatuojamas laikmačiu ir nustatoma greičiausiai šį rikiavimą atlikusi grupė.

Galima naudoti ir korteles su didesniais (pvz., triženkliais) skaičiais.

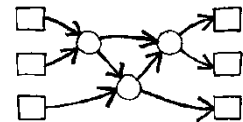
Galimos kortelės ir su labai dideliais skaičiais arba žodžiais, kuriuos galima išrikiuoti pagal abėcėlę.

## Gudručiams

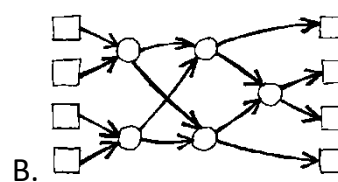
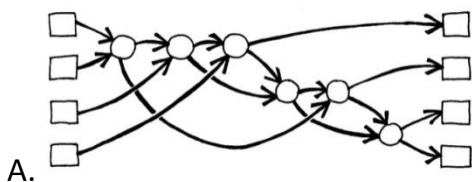
Kas atsitiktų, jei visi mokiniai, turintys kortelių su mažesniais (didesniais) skaičiais, pasuktų ne į dešinę (kairę), o į kairę (dešinę)? (Skaičiai būtų išrikiuoti atvirkščiai.)

Ar visada skaičiai išrikiuojami teisingai pasiekus išvestį, jei rikiavimo kryptys pakeičiamos priešingomis? (Ne visada. Mokiniai turėtų pateikti pavyzdį, kada išrikiuojama neteisingai.)

Mokiniam pasiūloma sukurti mažesnį ar didesnį tinklą. Pavyzdžiui, dešinėje, paveiksle, vaizduojamas tinklas, kuriuo išrikiuojami tik trys skaičiai. Mokiniai turėtų patys sukurti tokį ar panašų tinklą.



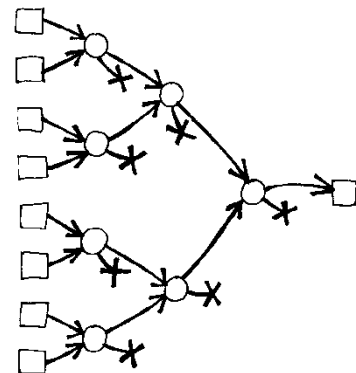
Toliau pateikiami du tinklai, kuriais išrikiuojama po keturis skaičius. Kuriuo iš jų – A ar B – tai padaroma greičiau? (B tinklu. A tinkle visi skaičiai lyginami iš eilės, o B tinkle keli skaičiai lyginami vienu metu. A tinkle naudojamas nuoseklusis palyginimas, o B – lygiagretusis.)



Mokiniam pasiūloma sukurti didesnį tinklą.

Naudojant tinklą galima surasti mažiausią arba didžiausią skaičių. Pavyzdžiui, toliau paveiksle išrenkamas mažiausias skaičius iš aštuonių. Atliekant šį algoritmą išvedamas tik mažiausias skaičius, o kiti lieka tinklo aklavietėse.

Kokie kasdieniniai darbai gali būti arba negali būti paspartinti taikant lygiagretumo principą? Pavyzdžiui, maisto ruošimas būtų daug lėtesnis, jei naudotume tik vieną kaitvietę, nes tada viskas turėtų būti verdama ar kepama paeiliui. Kurie darbai gali būti atlikti greičiau pasamdžius daugiau žmonių? Kuriuose darbuose neišeina panaudoti lygiagretumo principo?



## Apie ką visa tai?

---

Kompiuteriai tampa neatsiejami nuo žmonių gyvenimo, todėl būtina, kad jie vis sparčiau apdorotų informaciją.

Yra keletas būdų paspartinti kompiuterio darbą: problemai spręsti kurti algoritmus, kurių atlikimo laikas būtų kuo trumpesnis, arba problemą dalyti dalimis ir jai spręsti naudoti keletą kompiuterių. Pavyzdžiui, jei norima išrikiuoti šešis skaičius tinkle, reikia 12 kartų palyginti skaičių poras. Tačiau vienu metu gali būti lyginamos net trys skaičių poros, o tai daugiau nei perpus sutrumpina rikiavimo laiką.

Žinoma, ne visas problemas galima išspręsti greičiau lygiagretumo principu. Pavyzdžiui, vienas žmogus kasa 10 m griovį. Jei dešimt žmonių kastų po 1 m, užduotis būtų atlikta daug greičiau. Tačiau to paties metodo negalima taikyti kasant 10 m gylio duobę, nes antrojo metro žemių iš duobės negalima kasti, kol neiškastas metras žemių virš jo. Informatikai aktyviai darbuojasi ieškodami geriausio problemos padalijimo metodo, kad būtų galima pritaikyti lygiagretumo metodą.



## 9 veikla

# Purvinas miestas. Minimalūs jungiantieji medžiai

---

### Santrauka

Realiame gyvenime esama daug įvairių tinklų – tai telefonų tinklai, komunalinių paslaugų tinklai, kompiuterių tinklai, kelių tinklai ir kt. Kuriant paslaugų tinklus svarbu nustatyti, kur optimalu tiesti kelią, ryšio kabelius ar kt. Todėl dažnai sprendžiama efektyvaus objektų sujungimo į tinklą problema.

### Ryšiai su ugdymo programomis

- ✓ Matematika: geometrija, geometrinės figūros, trumpiausias kelias žemėlapyje

### Amžius

- ✓ Nuo 9 metų

### Gebėjimai

- ✓ Problemų sprendimo

### Priemonės

Kiekvienam mokiniui reikia:

- ✓ Darbo lapo „Purvinas miestas“



# Purvinas miestas

---

## Įvadas

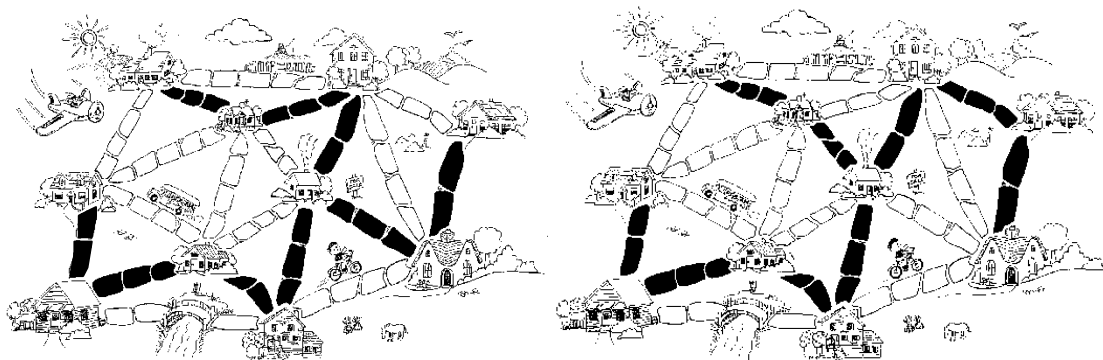
Ši veikla skiriama susipažinti, kaip kompiuteriai padeda surasti geriausią realios problemos – kaip geriausia nutiesti kelią – sprendimą. Mokiniais išdalijami darbo lapai, kuriuose paaiškinta *Purvino miesto* problema.

## Diskusija

Aptariama, kokiais būdais mokiniai galvoja ieškoti sprendimo.

Šią užduotį galima spręsti keliais būdais. Vienas būdas – pradėti nuo miesto plano, kuriame nėra sužymėta gatvių. Reikia žymėti po vieną gatvę, jungiančią du namus, prie kurių gatvė dar nenutiesta. Kitas uždavinio sprendimo būdas, kai miesto plane yra sužymėtos visos gatvės, – šalinti po vieną nereikalingą gatvę ir tikrinti, ar į visus namus galima patekti likusiomis gatvėmis.

Šios užduoties sprendiniai gali būti skirtingi – visi namai gali būti sujungti vienodo ilgio, bet skirtingomis gatvėmis. Toliau paveiksle parodyti du skirtingi šios užduoties sprendiniai.



Toliau su mokiniais galima aptarti, kur prireikia tinklų realiame gyvenime.

Informatikoje šie tinklų vaizdavimo būdai vadinami *grafais*. Grafas – tai taškai (viršūnės), sujungti linijomis (briaunomis). Realiame gyvenime tinklai gali būti vaizduojami grafais ieškant optimalaus sprendimo.

*Grafų* uždaviniams spręsti yra sukurta ir daug algoritmų, kuriais, pavyzdžiui, lengviau rasti trumpiausią atstumą tarp dviejų taškų arba trumpiausią kelią, jungiantį visus taškus.

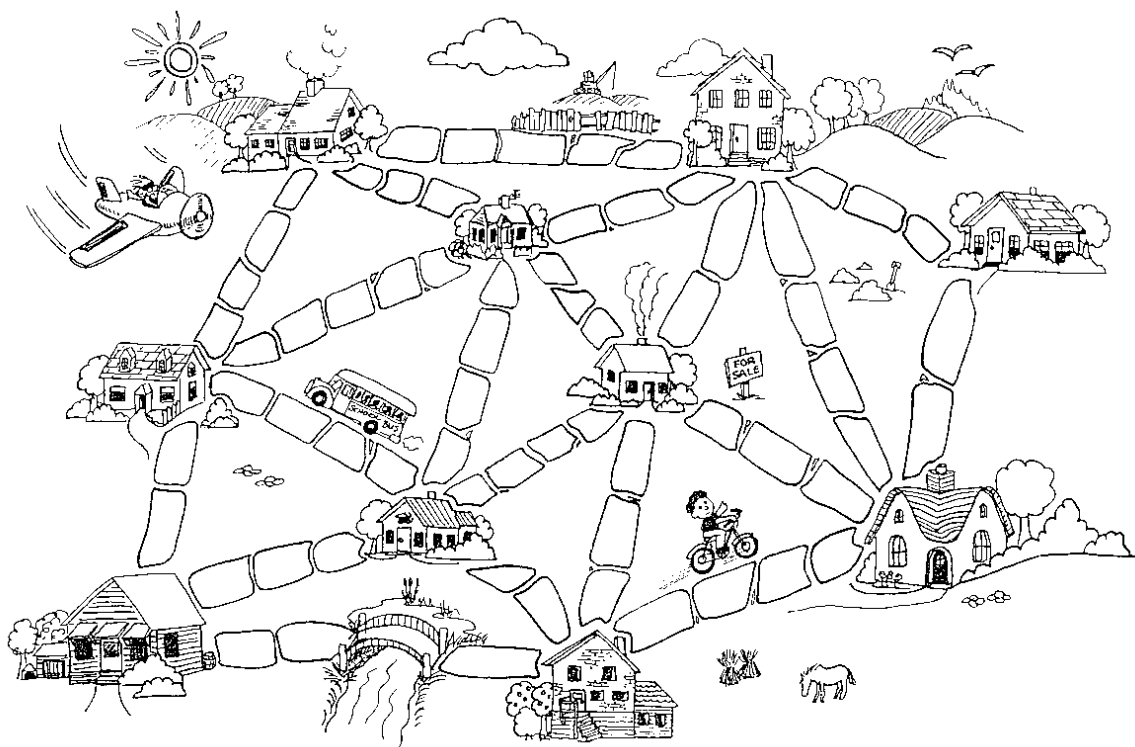
## Darbo lapas. Purvinas miestas

Vienoje šalyje yra miestas, kuriame nenuitiesta grįstų gatvių. Po lietaus žemė mieste pažliunga, automobiliai klimpsta purve, o žmonės išsipurvina. Miesto meras nusprendė išgrįsti kai kurias miesto gatves, tačiau jis nenori išleisti daugiau pinigų, nei būtina, nes mieste dar reikia pastatyti baseiną. Meras iškėlė du reikalavimus:

1. Grįstų gatvių turi būti tiek, kad jomis būtų galima nueiti į kiekvieną namą.
2. Gatvių grindimo išlaidos turi būti mažiausios.

Pateiktas miesto planas. Akmenų skaičius tarp kiekvieno namo proporcingas gatvės grindimo kainai. Suraskite geriausią gatvių grindimo variantą, kuris sujungtų visus namus ir būtų pigiausias.

Pagalvokite, koku būdu galima pradėti spręsti šią problemą?







## Apie ką visa tai?

---

Tinklo sujungimo problemos dažnos realiame gyvenime. Kuriant naują (ar plečiant jau esančią) gyvenvietę reikia suprojektuoti elektros, dujų ir vandens linijas į kiekvieną namą. Jomis tiesiami elektros laidai, dujų ar vandens vamzdžiai. Kiekvienas namas turi būti prijungtas prie reikiamo tinklo.

Problema, kai reikia suprojektuoti trumpiausią tinklą, vadinama *minimalaus jungiančiojo medžio* užduotimi.

*Minimalus jungiantysis medis* pravartus ne tik komunalinių tinklų problemai spręsti, bet ir kompiuterių tinklams, telefono ryšio, naftotiekio ar oro linijoms projektuoti. Planuojant geriausią kelionės maršrutą reikia atsižvelgti ne tik į kelionės patogumą, bet ir į kainą. Niekas nenori praleisti valandų valandas lėktuve keliaudamas į kitą šalį aplinkiniu maršrutu vien dėl to, kad tokia kelionė yra pigesnė. Planuojant kelionę „purvino miesto“ algoritmas nėra labai tinkamas, nes juo sutrumpinamas tik bendras gatvės ilgis.

*Minimalus jungiantysis medis* naudojamas sprendžiant ir kitus *grafų* uždavinius, pavyzdžiui, sprendžiant „keliaujančio pirklio“ uždavinį ieškoma trumpiausio kelio, kuriuo turi būti aplankytos visos *grafo* viršūnės.

*Minimalaus jungiančiojo medžio* uždaviniams spręsti sukurta daug efektyvių algoritmų. Galima pradėti nuo miesto plano, kuriame nesužymėtos gatvės, ir žymėti po vieną gatvę, jungiančią du, iki šiol dar neprijungtus namus. Šį algoritmą 1956 m. aprašė Jozefas Bernardas Kruskalas, todėl jis vadinamas J. B. Kruskalo algoritmu.

Informatikoje *grafų* uždaviniams, pavyzdžiui, „keliaujančio pirklio“, kuo geriau išspręsti sukurta ir tebekuriama gana efektyvių metodų.



# Sprendimai ir užuominos

---

## Variantai gudručiams

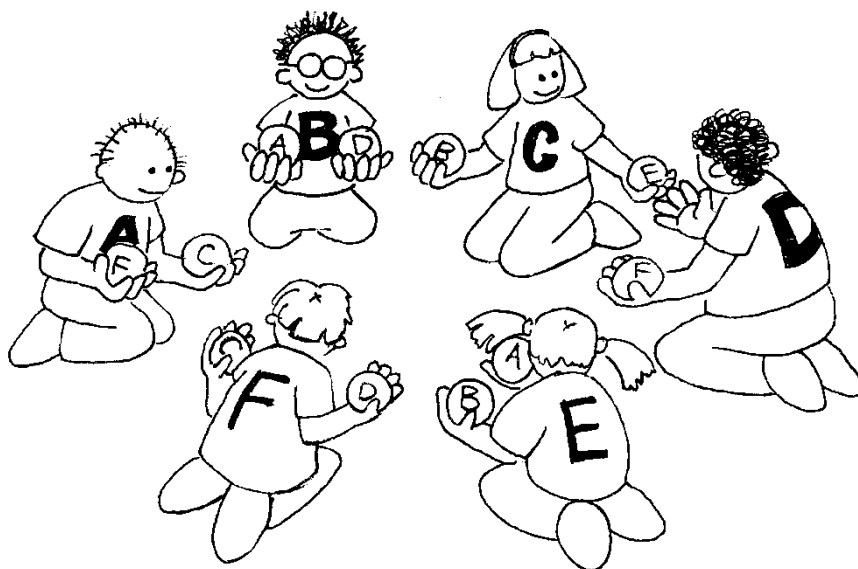
Kiek gatvių reikia norint sujungti  $n$  namų? Optimalus sprendimas – reikia  $n - 1$  gatvių.



## 10 veikla

# Apelsinų žaidimas. Maršruto parinkimas ir tinklo aklavietė

---



### Santrauka

Kai vienu metu daugeliui žmonių prireikia to paties (pavyzdžiui, daug vairuotojų pasirenka tą patį maršrutą ar vienu metu gaunama daug žinučių), gali susidaryti aklavietė. Veikiant sutartinai galima išvengti šio nemalonumo.

### Ryšiai su ugdymo programomis

- ✓ Matematika: loginės problemos

### Gebėjimai

- ✓ Problemos sprendimo bendradarbiaujant
- ✓ Loginio pagrindimo

### Amžius

- ✓ Nuo 9 metų

### Priemonės

Kiekvienam mokiniui reikia:

- ✓ Dviejų apelsinų (ar kitų vaisių) arba teniso kamuoliukų
- ✓ Priemonės raidei užrašyti ar priklijuoti ant kiekvieno mokinio ir jo apelsinų arba teniso kamuoliukų



# Apelsinų žaidimas

---

## Įvadas

Žaisdami šį žaidimą mokiniai sprendžia bendradarbiavimo problemą. Kiekvieno žaidėjo tikslas – savo rankose turėti tik žaidėjui priskirta raide pažymėtus apelsinus.

1. Penki ar daugiau mokinių susėda ratu. Kiekvienas mokinys prisiklijuoja (prisisega) lapelį su jam priskirta raide.
2. Kiekvienam mokiniui, išskyrus vieną, išdalijama po du apelsinus, po vieną į ranką. Likusiam mokiniui duodamas vienas apelsinas, kad būtų viena ranka laisva.
3. Apelsinai, kaip ir mokiniai, sužymimi raidėmis ir išdalijami taip, kad nei vienas mokinys neturėtų nei vienoje rankoje apelsino su jam priskirta raide.
4. Apelsinai siunčiami ratu pagal dvi taisykles:
  - a) Rankoje gali būti tik vienas apelsinas vienu metu.
  - b) Apelsinas gali būti perduotas tik šalia (iš kairės ar dešinės) esančiam mokiniui, jei jis turi laisvą ranką (Mokinys gali perduoti bet kurį iš savo apelsinų).
5. Apelsinai siunčiami ratu tol, kol bent vienas mokinys turi ne savo raide pažymėtą apelsiną.

Mokiniai turėtų pastebėti, kad jei jie bus „godūs“ (laikysis „savųjų“ apelsinų, kai tik juos gaus), visai grupei gali nepavykti pasiekti tikslo. Reikėtų priminti, kad šis žaidimas yra komandinis ir pavieniai mokiniai negali jo laimėti. Užduotis bus įvykdyta tik tuomet, kai visi mokiniai savo rankose turės „savuosius“ apelsinus.

## Diskusija

Kokiais būdais mokiniai sprendžia problemą?

Kokiose realaus gyvenimo situacijose pasitaiko aklaviečių? (Pavyzdžiui, eismo spūstys, žaidžiant krepšinį, žmonių spūstis tarpduryje bandant išeiti iš patalpos.)

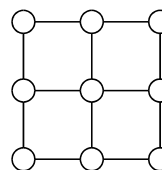
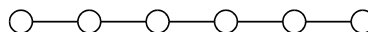
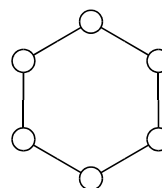
## Gudručiams

Mokiniai gali išbandyti žaidimą su daugiau (ar mažiau) mokinių.

Tegul mokiniai pasvarsto apie naujas žaidimo taisykles.

Tegul mokiniai atlieka veiklą nekalbėdami.

Tegul mokiniai išbando pakeistus žaidimus: susėsti viena linija arba turėti daugiau nei du kaimynus, kaip parodyta paveiksluose.



## Apie ką visa tai?

---

Maršruto parinkimas ir aklavietė yra dažna problema reguliuojant eismą, telefono ryšio linijas ir informacijos perdavimo kompiuteriu srautus. Inžinieriai praleidžia daug laiko ieškodami šios problemos sprendimo, bandydami suprojektuoti tinklus, kad šios problemos sprendimas būtų paprastesnis.

Maršruto parinkimas, spūstis, grūstis ir aklavietė – tai įvairių tinklų sudarymo nesėkmių išraiška. Didžiuosiuose miestuose dažnai pasitaiko eismo spūsčių. Kartais jos tampa aklavietėmis automobiliams, kai jie negali pajudėti nei pirmyn, nei atgal. Inžinieriai sprendžia sudėtingas problemas ieškodami paprastesnio ir pralaidesnio maršruto, kuriame spūsčių tikimybė būtų kuo mažesnė.

Kartais daugiau nei vienas vartotojas naudoja tuos pačius tinklo duomenis tuo pačiu metu. Jei vienas vartotojas nori atnaujinti duomenis tinkle, patartina juos „užblokuoti“. Jei vienu metu du vartotojai bando atnaujinti tuos pačius duomenis, tai duomenys gali būti įrašyti neteisingai. Tačiau, jei bandoma iš skirtingų vietų užblokuoti tuos pačius duomenis tuo pačiu metu, gali susidaryti aklavietė.

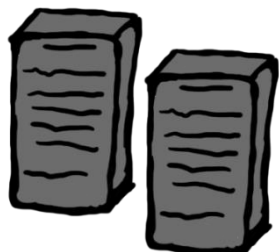
Vienas iš didžiausių informatikos pasiekimų yra lygiagretusis skaičiavimas, kai keletas kompiuterių dirba vienu metu sudarydami vieną galingą kompiuterį. Tokius žaidimus, kaip „Apelsinų“ žaidimas, su šiuo kompiuteriu galima žaisti be perstojo ir daug greičiau.



## 11 veikla

# Akmeninės plokštelės. Tinklo komunikacijų protokolas

---



### Santrauka

Kompiuteriai perduoda informaciją vieni kitiems internetu, tačiau internetas nėra patikimas ir kartais siunčiama informacija prarandama. Kai prie siunčiamos žinutės pridedama tam tikros papildomos informacijos, šios žinutės perdavimo patikimumas padidėja daug kartų. Ši papildoma informacija sudaro komunikacijų protokolą.

### Ryšiai su ugdymo programomis

- ✓ Matematika: loginės problemos
- ✓ Lietuvių kalba: komunikavimas, kito asmens klausymas

### Gebėjimai

- ✓ Problemos sprendimo bendradarbiaujant
- ✓ Loginio argumentavimo

### Amžius

- ✓ Nuo 9 metų

### Priemonės

Kiekvienam mokiniui reikia:

- ✓ Daug tuščių kortelių (apie 30), kurios atliks plokštelių vaidmenį

Kiekvienam pasiuntiniui reikia:

- ✓ Žinučių veiksmų kortelių rinkinio

Mokytojui reikia:

- ✓ Laikmačio



# Akmeninės plokštelės

---

## Ivadas

Ši veikla skiriama paaiškinti, kaip veikia skirtingi komunikavimo metodai. Pateikiamos taisyklės ir aprašomi veiksmai mokinius supažindina su komunikavimo protokolais. Mokiniai dalyvauja vaidmenų žaidime, testuoja savo protokolo veikimą nepatikimoje aplinkoje, panašioje į paketų perdavimą internetu (TCP/IP).

## Pasirengimas (30 min.)

1. Pasiruošiamos žinučių kortelės: jos atspausdinamos ir sukarpomos.
2. Suformuluojama žinutė. Nusprendžiama, kokia žinutė bus siunčiama. Žinutė turi būti beprasmė, kad nebūtų galima nuspėti jos struktūros perduodant. Pavyzdžiui, „1LHC255HD(RLLS“ arba telefono numeris.
3. Pasiruošiamos plokštelės: jos atspausdinamos ir sukarpomos. Kiekvienoje plokštelėje yra vietos 6 ženklams (vienas žinutės ženklas rašomas į vieną langelį), todėl viena žinutė netelpa į vieną plokštelę. Žinutei perduoti reikės apie 30 plokštelių kiekvienam mokiniui.

**Patarimai.** Žinučių veiksmų kortelės žymi tris veiksmus: atidėti, pristatyti ir nepristatyti. Šių veiksmų derinimas nusako perdavimo tinklo kokybę. Kuo daugiau kortelių „pristatyti“, tuo tinklas patikimesnis. Kuo daugiau kortelių „atidėti“, tuo tinklas mažiau patikimas. Šios kortelės vaizduoja kompiuterio tinklo ir komunikacijų kanalą.

## Žaidimo instrukcija

1. Mokiniai pasidalija į poras. Vienos poros nariai turi atsisėsti kuo nuošaliau, kad nematytų vienas kito ir negalėtų kalbėtis. Jie gali būti skirtinguose kambariuose ar tame pačiame kambaryje, bet nususukę vienas nuo kito.
2. Vienam poros nariui duodama suformuluota žinutė, kurią jis turi perduoti savo porininkui per pasiuntinį.
3. Žinučių veiksmų kortelės sumaišomos, pasirenkamas pasiuntinys. Juo gali būti mokytojas ar mokinys, jei mokinių skaičius nelyginis ir vienas mokinys lieka be poros. Jei klasė didelė, galima pasirinkti du pasiuntinius.
4. Mokiniui, turinčiam žinutę, duodamos plokštelės. Pirmoje plokštelėje jis parašo dalį žinutės. Virš plokštelės užrašo mokinio, kuriam siunčia žinutę, vardą ir perduoda plokštelę pasiuntiniui.
5. Pasiuntinys, paėmęs plokštelę, traukia veiksmų kortelę, ją apverčia ir perskaito, ką turi padaryti su šia plokštele.
6. Kartojami 4 ir 5 žingsniai su kiekviena plokštele.

Po 5 ar daugiau chaoso ir nesėkmių minučių mokiniai turėtų suprasti, kad protokolui tik vardo neužtenka. Sustabdomas žaidimas ir pradedama diskusija.





Su kokia problema mokiniai susidūrė pirmiausia? Ar tai plokštelių eiliškumas? Tikriausiai būtų protinga į vieną iš 6 ženklams skirtų vietų įrašyti siunčiamos žinutės plokštelės eilės numerį? Tai reikštų, kad žinutės tekstui lieka mažiau vietos. Kaip tai lemia plokštelių skaičių?

Po kurio laiko mokiniai turėtų pastebėti kitas problemas. Žaidimas sustabdomas ir padiskutuojama. Galima pastebėta problema – dingusios plokštelės, nežinoma, ar plokštelė buvo neišsiųsta, ar reikia siųsti iš naujo. Tikėtina, kad mokiniai pasiūlys sprendimą: gavęs plokštelę porininkas turi išsiųsti patvirtinimą ir tik gavus patvirtinimą išsiunčiama kita žinutės dalis. Tai reiškia, kad porininkas taip pat turi turėti tuščių plokštelių. Prieš tęsdami žaidimą mokiniai turi susitarti, kam bus naudojamos 6 ženklų vietos jų plokštelėse.

Šiam žaidimui užtenka dviejų mokinių, bet rekomenduojama žaisti su visa klase. Jei klasė didelė, gali būti ir keli pasiuntiniai. Su klase aptariama, kas atsitiktų, jei būtų daug pasiuntinių arba jei jų būtų tik vienas?



Pristatyti šią žinutę dabar	Pristatyti šią žinutę po kitos
Pristatyti šią žinutę dabar	Pristatyti šią žinutę po kitos
Pristatyti šią žinutę dabar	Pristatyti šią žinutę po kitos
Pristatyti šią žinutę dabar	Nepristatyti šios žinutės
Pristatyti šią žinutę dabar	Nepristatyti šios žinutės

<p><b>Kam:</b></p> <table border="1"> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> </table> <p><b>Nuo ko:</b></p>							<p><b>Kam:</b></p> <table border="1"> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> </table> <p><b>Nuo ko:</b></p>						
<p><b>Kam:</b></p> <table border="1"> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> </table> <p><b>Nuo ko:</b></p>							<p><b>Kam:</b></p> <table border="1"> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> </table> <p><b>Nuo ko:</b></p>						
<p><b>Kam:</b></p> <table border="1"> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> </table> <p><b>Nuo ko:</b></p>							<p><b>Kam:</b></p> <table border="1"> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> </table> <p><b>Nuo ko:</b></p>						
<p><b>Kam:</b></p> <table border="1"> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> </table> <p><b>Nuo ko:</b></p>							<p><b>Kam:</b></p> <table border="1"> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> </table> <p><b>Nuo ko:</b></p>						



## Akmeninės plokštelės

---

Antikos laikais vieną miestą valdė keletas valdytojų, kurie gyveno skirtingose to miesto vietose. Valdydami vieną miestą, jie kartu turėdavo aptarti labai svarbius klausimus.

Norėdami bendrauti nuotoliniu būdu, valdytojai turėdavo siųsti vienas kitam žinutes per visą miestą. Pasiuntiniai valdytojus skirdavo pagal jų namų numerius.

Vienintelis būdas nusiųsti žinutę – užrašyti ją ant stačiakampės akmeninės plokštelės ir nunešti ją tam, kam liepdavo siunčiantis miesto valdytojas. Akmeninės plokštelės dydis buvo nustatytas toks, kad joje tilpdavo tik 6 informacijos ženklai. Vienas informacijos ženklas galėjo būti viena raidė arba vienas skaičius. Visa žinutė galėdavo būti užrašoma ir ant kelių plokštelių, bet jos būdavo labai sunkios ir vienu metu pasiuntinys galėdavo nunešti tik vieną plokštelę.

Be to, visiškai pasitikėti pasiuntiniais nebuvo galima, nes jie buvo užmaršūs ir tingūs. Jie užmiršdavo, kam skirta žinutė arba sustodavo pailsėti ir nenunešdavo plokštelės laiku.

Miesto valdytojai norėjo rasti patikimesnį bendravimo būdą. Jie sumanė sukurti taisykles, kurios padėtų sužinoti, ar išsiųsta žinutė pasiekė adresatą, ar gauta žinutė buvo teisinga. Tačiau iš pradžių valdytojai sutarė tik dėl to, kad plokštelėje turi būti rašoma, kam žinutė skirta.

Ši veikla turėtų padėti suformuluoti taisykles, kaip miesto valdytojai turėtų rašyti žinutes.



## Apie ką visa tai?

---

Siunčiami internetu duomenys dalijami į paketus. Tačiau tų duomenų siuntimo kanalai ne visada patikimi. Vienas ar kitas paketas kartais yra sugadinamas, prarandamas arba sumaišoma jo eilė.

Akmeninių plokštelių žaidime plokštelės vaizduoja paketus, o jų turinys – duomenis. Paketuose yra ir duomenų, ir *antraštės* informacija. *Antraštės* informacijos kiekis lemia, kiek informacijos galima perduoti vienu paketu. Kadangi paketai yra nustatyto dydžio, reikia numatyti žinutės ir papildomos informacijos kiekio balansą.

Mokiniai pastebi, kad keičiantis plokštelėmis dalį žinutės vietos reikia skirti kitokiai informacijai: paketo numeriui, paketą sudarančių pakų skaičiui arba patvirtinimui, ar paketas gautas. Kuo daugiau papildomos informacijos įtraukiama į paketus, tuo daugiau reikia tokių paketų.

Interneto protokolai, pavyzdžiui, TCP ir UDP, suderina šiuos veiksnius ir užtikrina patikimą ir efektyvų duomenų perdavimą.

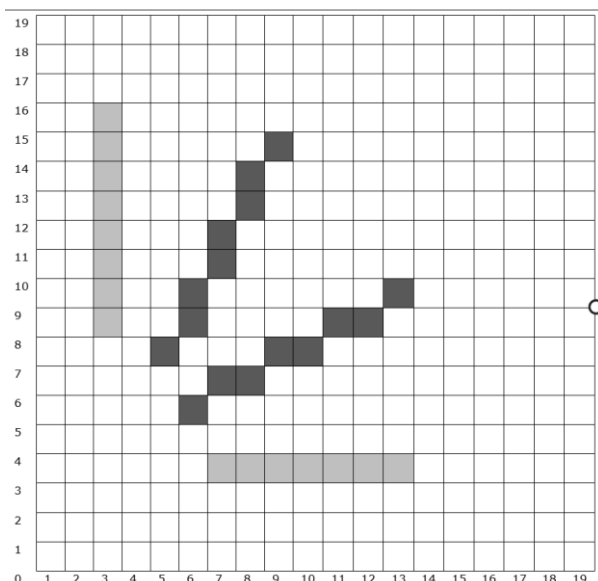
Ši veikla parengta ir aprašyta pagal skelbiamą projekto „Computing Science Inside“ medžiagą ([csi.dcs.gla.ac.uk](http://csi.dcs.gla.ac.uk)).



# 12 veikla

## Linijų braižymas

---



### Tikslas

Susipažinti su pagrindiniais kompiuterinių įrenginių darbo principais: kaip informacija, duomenys vaizduojami kompiuteriuose. Veiklą sukūrė „SC Unplugged“ bendruomenės narys Joshua Scott.

### Ryšys su ugdymo programomis

- ✓ Informatika: algoritmo taikymas
- ✓ Matematika: dvimatė koordinacių sistema, geometrija, liniuotės, skriestuvo naudojimas

### Gebėjimai

- ✓ Stačiakampė koordinacių sistema
- ✓ Algoritmas
- ✓ Matavimo ir braižymo priemonių naudojimas

### Amžius

- ✓ 5 ir aukštesnės klasės: grafinis vaizdavimas kompiuteryje, taškinė ir vektorinė grafika, koordinacių plokštuma, supažindinimas su algoritmais, naudojamais objektams braižyti kompiuterių programose.

### Priemonės

- ✓ Pieštukas
- ✓ Liniuotė, skriestuvai
- ✓ Veiklų priemonės kiekvienam mokiniui:
- ✓ Darbo lapas „Paprastoji linija“
- ✓ Darbo lapas „Sudėtingesnė linija“



- ✓ Darbo lapas „Bresenhamo linijos brėžimo algoritmas“
- ✓ Darbo lapas „Pasvirusios tiesės“
- ✓ Darbo lapas „Apskritimai“
- ✓ Darbo lapas „Apskritimo centro algoritmas“



## Darbo lapas. Paprasta linija

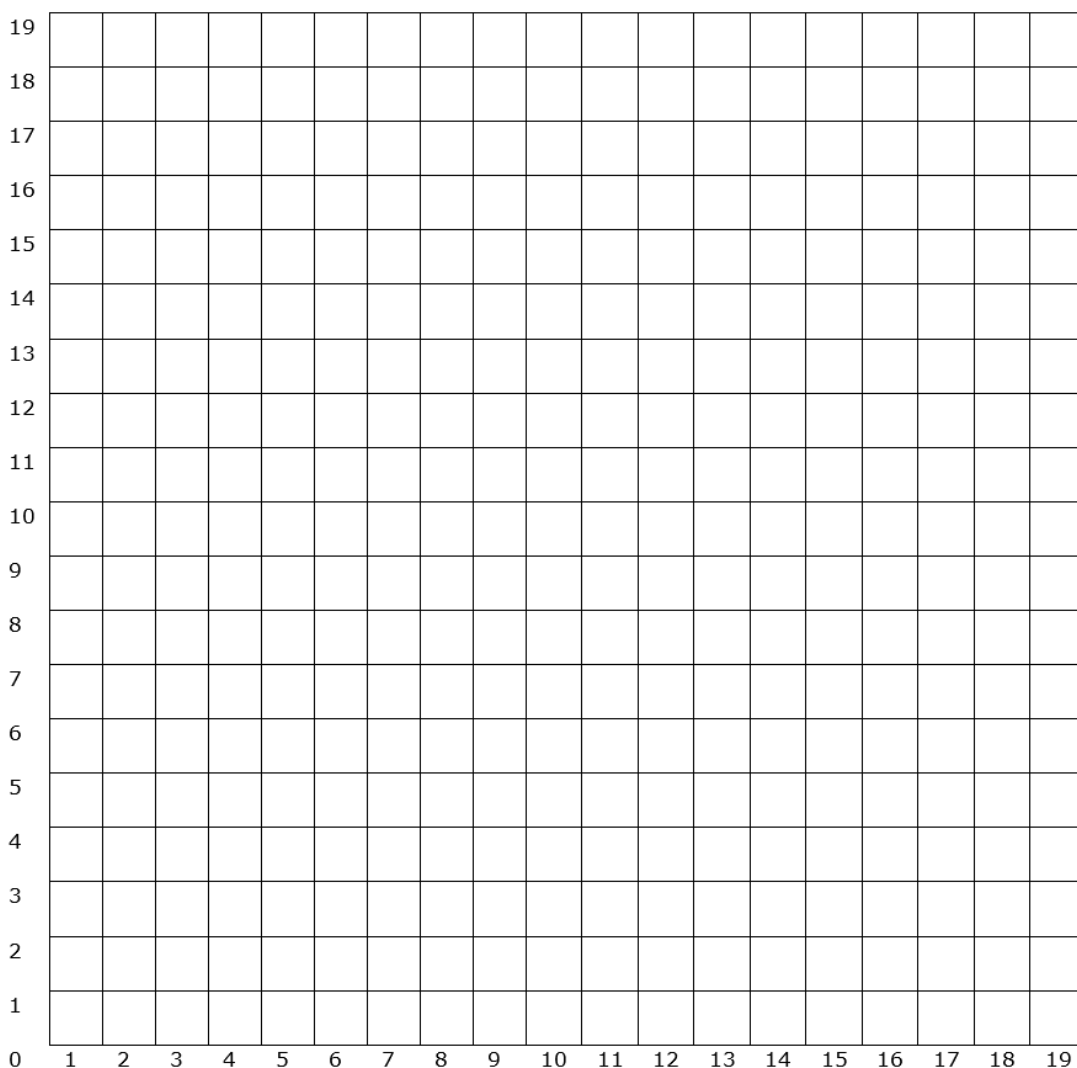
---

Kompiuteriai piešia vaizdus naudodami pikselius. Pikseliai – tai maži kvadratėliai, iš kurių sudarytas kompiuterio monitoriuje matomas vaizdas. Jei atidžiai pažvelgsite į kompiuterio ekraną su didinamuoju stiklu, pamatysite atskirus pikselius.

Kad nubrėžtų liniją, kompiuteris turi išsiaiškinti, kuriuos pikselius reikia užpildyti, kad linija atrodytų tiesi. Tai galime išbandyti spalvindami kvadratėlius tinklelyje.

Toliau esančiame tinklelyje pabandykite nubrėžti šias tiesias linijas, užpildydami pikselius tinklelyje:

- $(2, 17) \rightarrow (10, 17)$
- $(18, 2) \rightarrow (18, 14)$
- $(1, 5) \rightarrow (8, 12)$



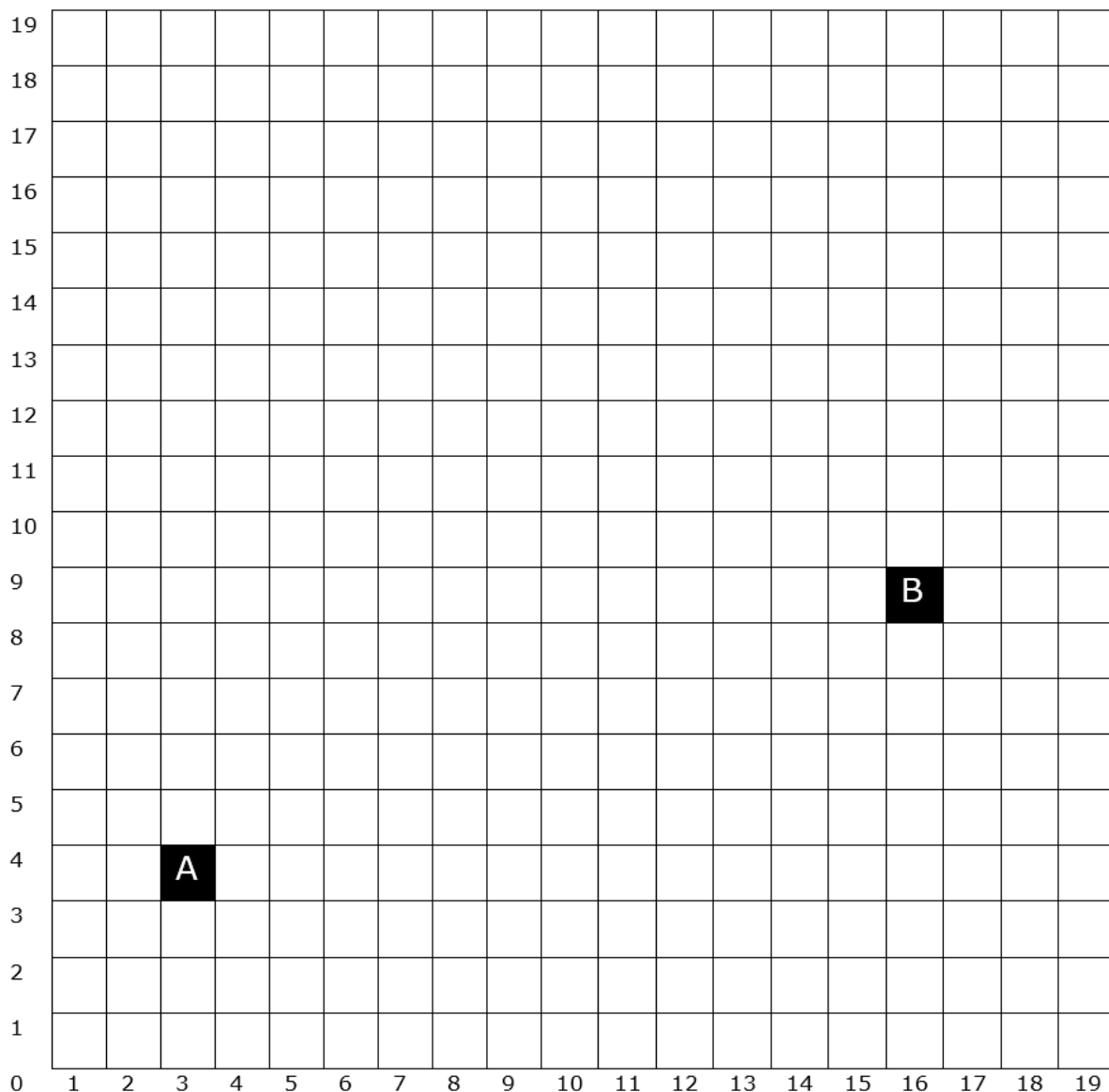
Patikrinkite su liniuote, ar jūsų linija tiesi.





## Darbo lapas. Sudėtingesnė linija

Ar galite nubrėžti tiesią liniją iš taško A į tašką B spalvindami langelius ir nenaudodami liniuotės?



Baigę brėžti liniją, pabandykite ją patikrinti liniuote. Liniuotę dėkite taip, kad ji eitų per A ir B langelių centrus. Ar liniuotė eina per visus langelius, kuriuos nuspalvinote?

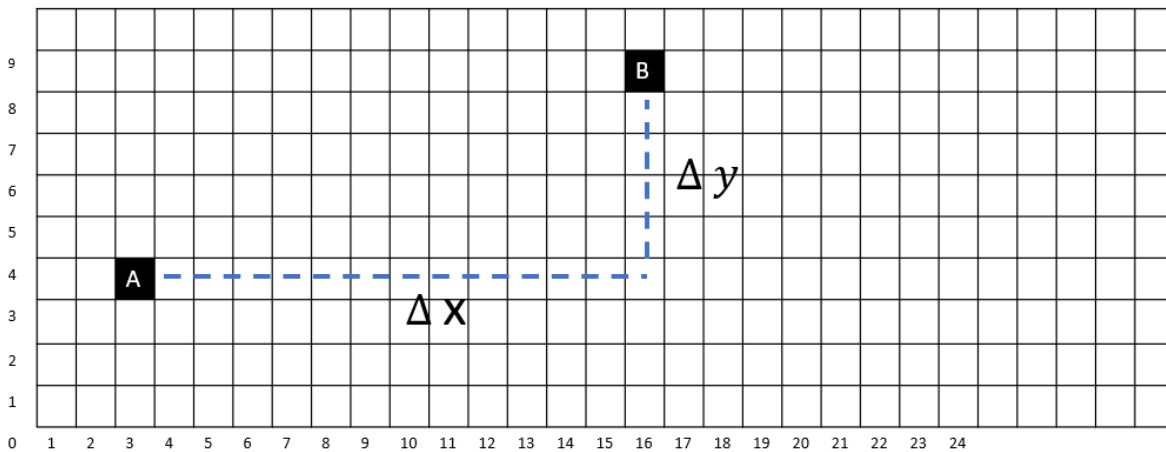


## Bresenhamo linijos brėžimo algoritmas

Bresenhamo tiesės algoritmas pavadintas Jacko Eltono Bresenhamo, kuris jį sukūrė 1962 m. IBM bendrovėje, vardu. Bresenhamo algoritmas buvo išplėstas, kad galima būtų gauti apskritimus, elipses, kubines ir kvadratinės Bezerio kreives (<http://members.chello.at/easyfilter/bresenham.html>).

Vienas iš būdų, kaip kompiuteris gali sužinoti, kuriuos pikselius nuspalvinti, yra Bresenhamo algoritmas.

Pabandykite nubrėžti tą pačią atkarpą AB taikydami Bresenhamo algoritmą. Algoritmas remiasi šiomis paprastomis taisyklėmis:



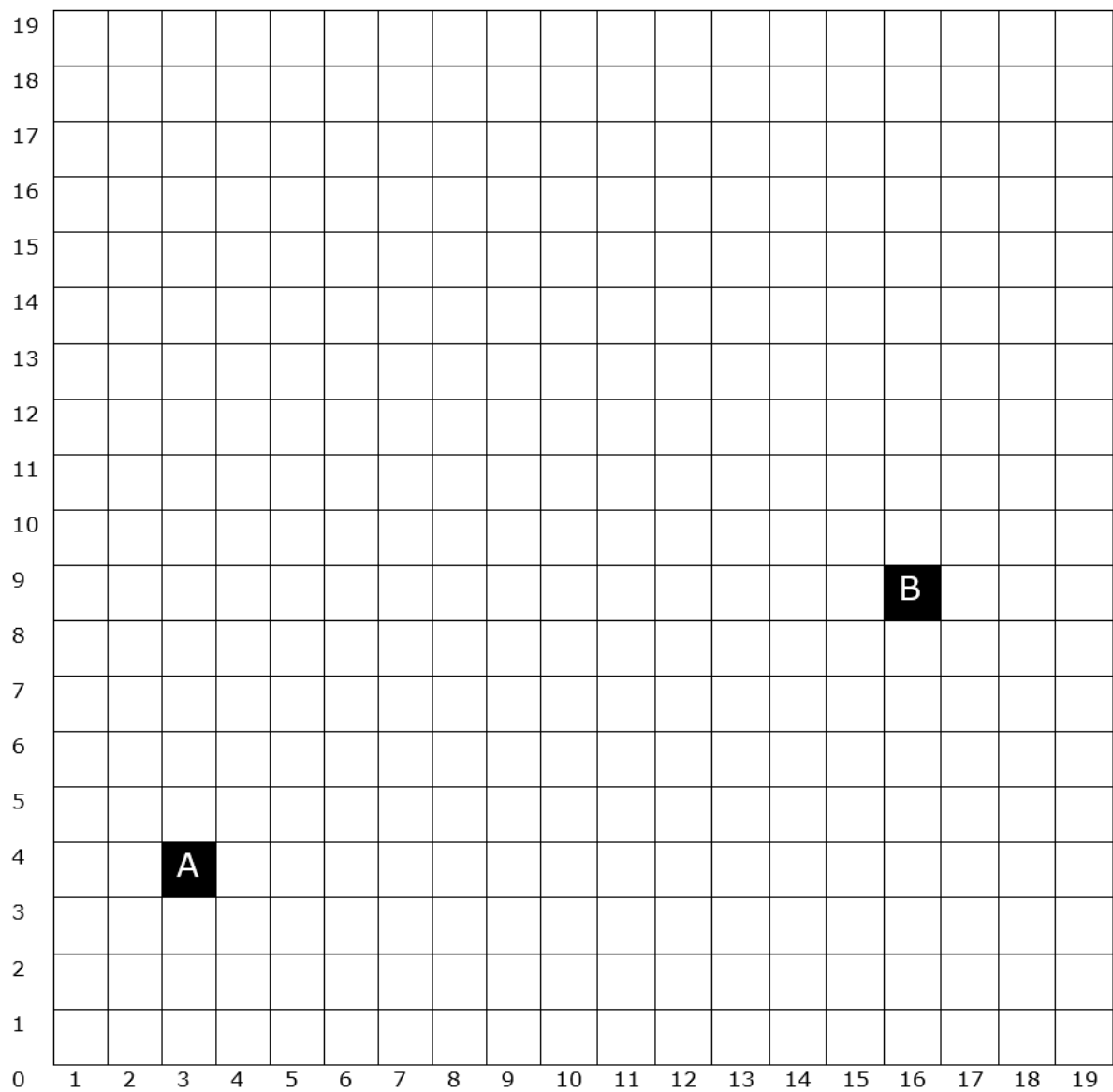
$$A(x_0; y_0) \quad B(x_1; y_1) \quad \Delta x = |x_1 - x_0|, \quad \Delta y = |y_1 - y_0|$$

- $P_0 = 2 \cdot \Delta y - \Delta x$
- Nuspalvinkite pradinį tašką. Perskaičiuokite  $\Delta y$  ir  $\Delta x$ .
- Tada kiekvienai padėčiai išilgai X ašies:
  - jei  $P < 0$ , tai langelį spalvinkite ant tos pačios linijos, kaip ir ankstesnį,
  - ir prie  $P$  pridėkite  $2 \cdot \Delta y$ ;
  - jei  $P \geq 0$ , tai langelį spalvinkite vienu aukščiau nei ankstesnį,
  - ir prie  $P$  pridėkite  $2 \cdot \Delta y - 2 \cdot \Delta x$ .

Tęskite šį procesą, kol pasieksite linijos pabaigą.



Be liniuotės, naudodami Bresenhamo linijos algoritmą, nubrėškite tiesią liniją iš A į B.



Baigę brėžti liniją, patikrinkite ją liniuote. Palyginkite su pirmuoju savo variantu.



## Pasvirusios tiesės

Iki šiol naudota Bresenhamo linijų piešimo algoritmo versija veikia tik toms linijoms, kurių pasvyrimas (nuolydis) yra nuo 0 iki 1. Tam kad algoritmas būtų bendresnis ir jį būtų galima naudoti bet kokiai linijai braižyti, reikia papildomų taisyklių:

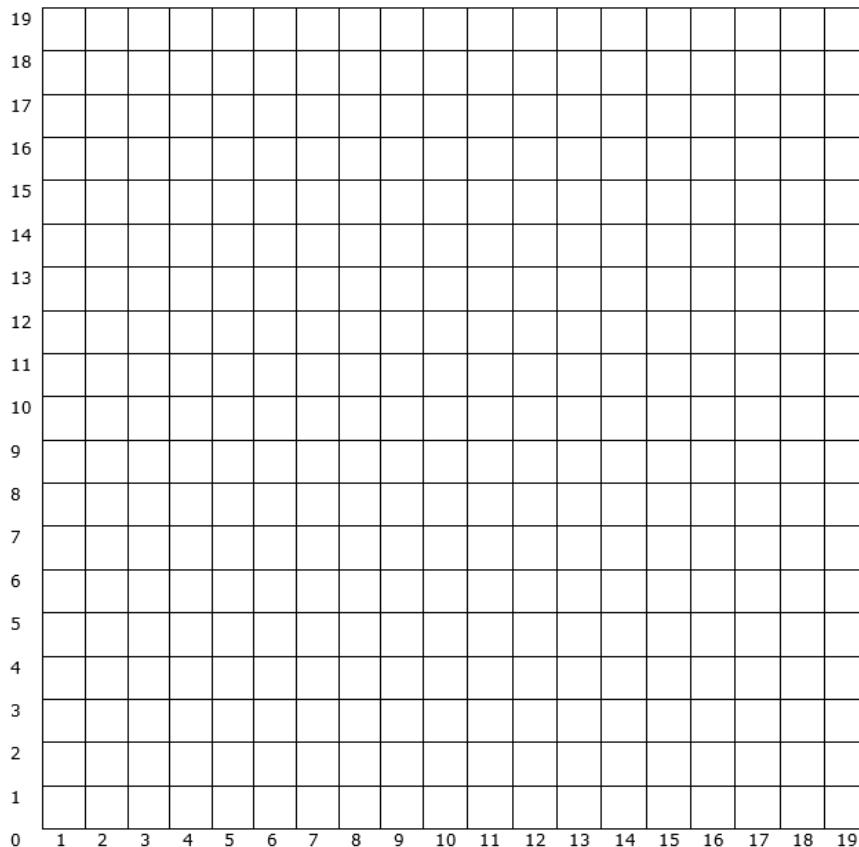
- Jei linija yra pasvirusi žemyn, o ne į viršų, tada, kai  $P$  reikšmė yra 0 arba didesnė, tai kito stulpelio langelis spalvinamas viena eilute žemiau ankstesnio langelio, o ne virš jo.
- Jei  $Y$  vertės pokytis yra didesnis už  $X$  vertės pokytį, tada  $A$ ,  $B$  ir pradinės  $P$  vertės skaičiavimus reikia keisti.

Apskaičiuodami  $A$ ,  $B$  ir pradinę  $P$  reikšmę, naudokite  $X$  ten, kur anksčiau naudojote  $Y$ , ir atvirkščiai. Spalvindami langelius, užuot ėję per kiekvieną  $X$  ašies stulpelį, eikite per kiekvieną  $Y$  ašies eilutę, kiekvienoje eilutėje spalvindami po vieną langelį.

- $P_0 = 2 \cdot \Delta x - \Delta y$ .
- Nuspalvinkite pradinį tašką. Perskaičiuokite  $\Delta y$  ir  $\Delta x$ .
- Tada kiekvienai padėčiai išilgai  $Y$  ašies:
  - jei  $P < 0$ , tai langelį spalvinkite ant tos pačios linijos, kaip ir ankstesnį,
  - ir prie  $P$  pridėkite  $2 \cdot \Delta x$ .
  - jei  $P \geq 0$ , tai langelį spalvinkite vienu aukščiau nei ankstesnį
  - ir prie  $P$  pridėkite  $2 \cdot \Delta x - 2 \cdot \Delta y$ .

Tęskite šį procesą, kol pasieksite linijos pabaigą.





Viršuje esančiame tinklelyje nubrėžkite **savo** atkarpą. Atkarpos pradiniam taškui pasirinkite X reikšmę – pirmąją savo vardo raidę, paverstą skaičiumi. (pvz., Barbora būtų 3, nes B yra trečioji abėcėlės raidė). Jei skaičius didesnis už 19, iš jo atimkite 20. Pradžios taško Y reikšmei pasirinkite skaičių, gautą iš antrosios jūsų vardo raidės.

Atkarpos pabaigos taškui naudokite pirmąją ir antrąją savo pavardės raides. Pavyzdžiui, jei Jūsų vardas ir pavardė yra Jonas Smitas, naudokite raides „Jo“, kad pasirinktumėte pradžios tašką (16, 1). Tada naudokite „Sm“ raides, kad nustatytumėte galutinį atkarpos tašką (4, 19). Jei abi x ar y koordinatės sutampa, tai atkarpos galo koordinatėse sukeiskite x ir y vietomis (kad užduotis būtų įdomesnė). Atkarpą nubrėžkite naudodami Bresenhamo algoritmą.

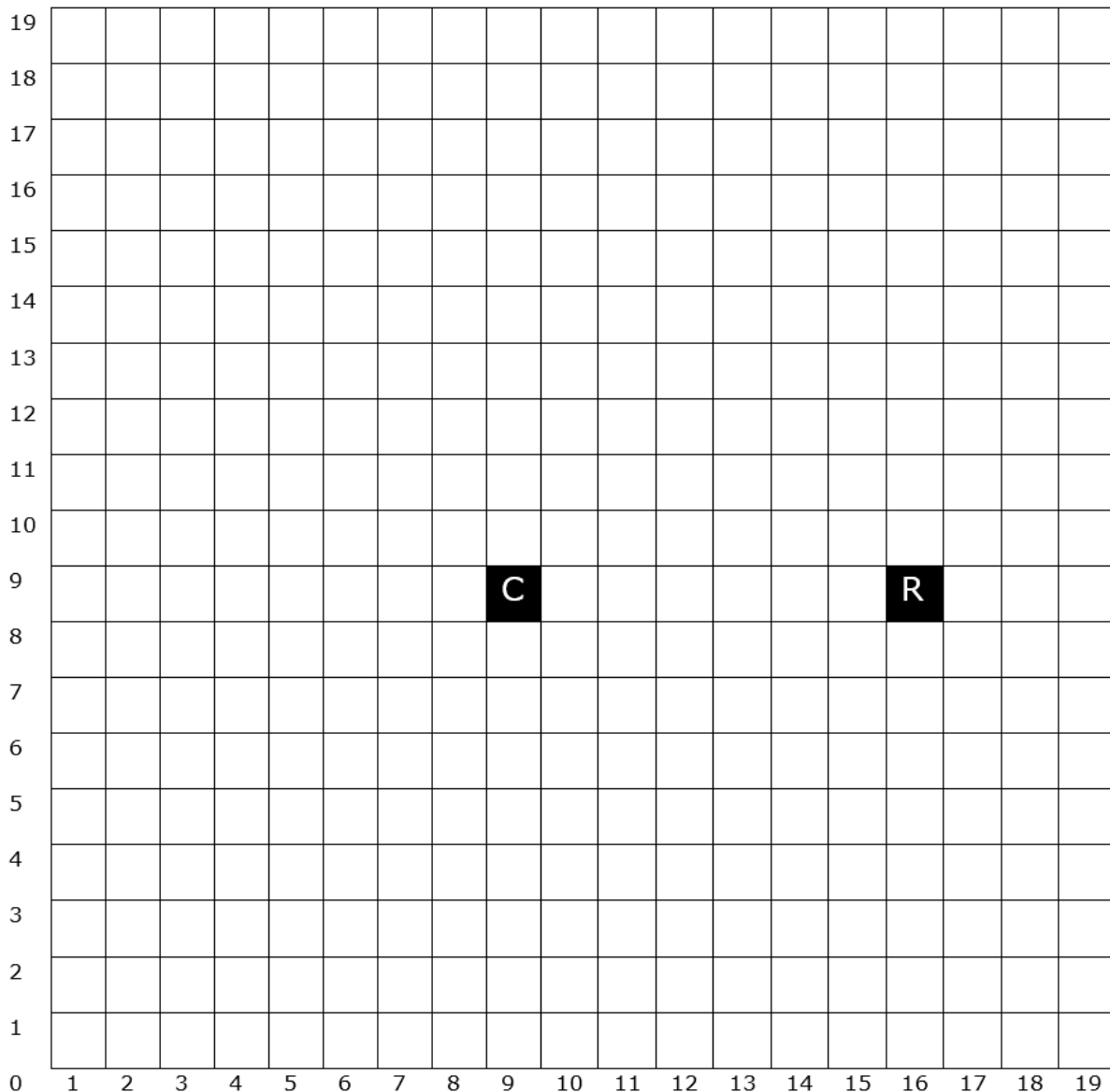
1	Aa	9	Éé	17	Kk	25	Šš
2	Ąą	10	Ff	18	Ll	26	Tt
3	Bb	11	Gg	19	Mm	27	Uu
4	Cc	12	Hh	20	Nn	28	Ųų
5	Čč	13	Ii	21	Oo	29	Ūū
6	Dd	14	Jj	22	Pp	30	Vv
7	Ee	15	Yy	23	Rr	31	Zz
8	Ęę	16	Jj	24	Ss	32	Žž



## Apskritimai

Be tiesių, kita įprasta forma, kurią dažnai reikia nubraižyti kompiuteriuose, yra apskritimai. Buvo sukurtas į Bresenhamo tiesių braižymo algoritmą panašus algoritmas, skirtas apskritimams braižyti, vadinamas apskritimo centro algoritmu (angl. *Midpoint Circle Algorithm*).

Apskritimą apibrėžia centro taškas ir spindulys. Visi apskritimo taškai yra spindulio atstumu nutolę nuo apskritimo centro. Centro taškas turi X ir Y koordinates.



Pabandykite ranka nubrėžti apskritimą užpildydami langelius (nenaudodami liniuotės ar skriestuvo). Atkreipkite dėmesį, kaip sunku tai padaryti.

## Apskritimo centro algoritmas

Pateikiame apskritimo centro algoritmą.

$E = -$  spindulys

$x =$  spindulys

$y = 0$

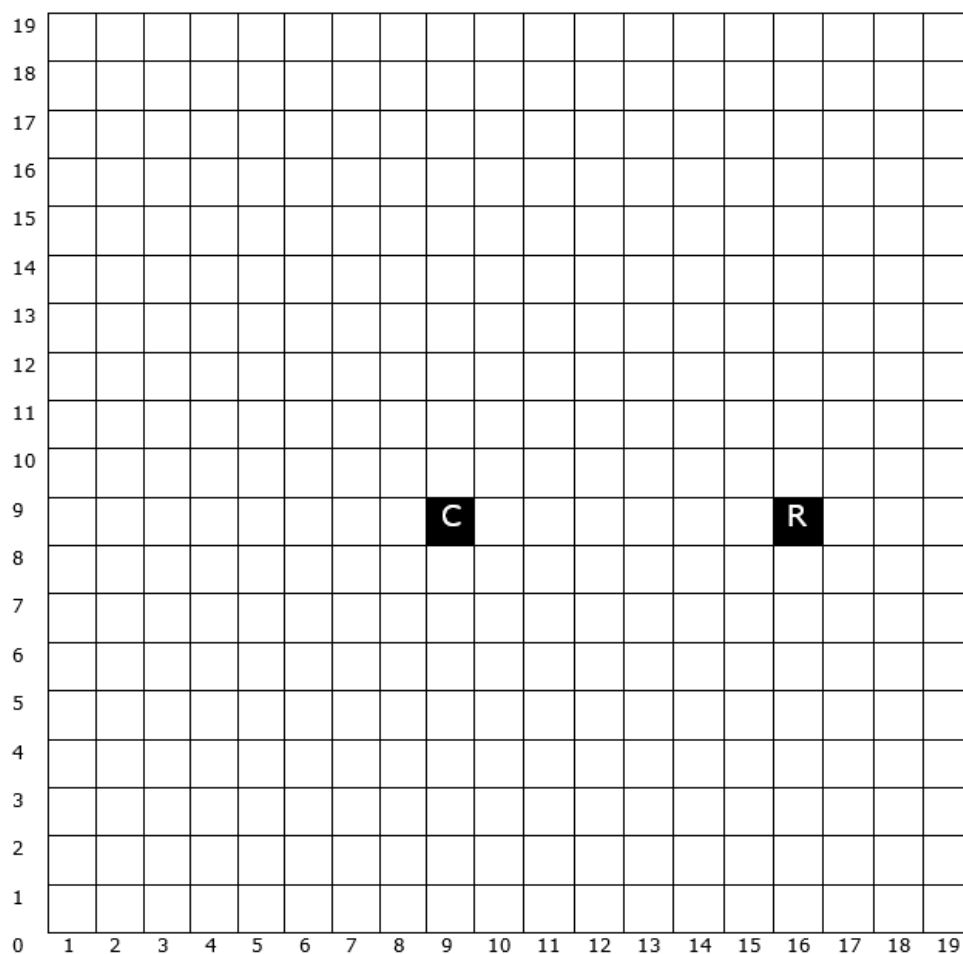
Centro  $C$  koordinatės  $(x_0; y_0)$

Tol, kol  $y$  taps didesnis už  $x$ , kartokite šiuos žingsnius iš eilės:

- dėkite (nuspalvinkite) pikselį, kurio koordinatės  $(x + x_0, y + y_0)$
- $E$  padidinkite  $2 \cdot y + 1$
- $y$  padidinkite 1
- Jei  $E$  yra didesnis arba lygus 0, tai iš  $E$  atimkite  $(2x - 1)$ , tada iš  $x$  atimkite 1.

Vadovaudamiesi taisyklėmis, nubrėžkite apskritimą, kurio centras yra  $C$ .

$C$  – apskritimo centras,  $CR$  – apskritimo spindulys



Kai  $y$  tampa didesnis už  $x$ , nuspalvinama viena aštuntoji apskritimo dalis. Likusią apskritimo dalį galima nuspalvinti simetriškai jau turimai daliai. Nuspalvinkite langelius išilgai  $OX$  ir  $OY$  ašių taip, kad simetrijos ašis kirstų apskritimo centro langelio vidurį.



Dabar nuspalvinta pusė apskritimo – kairioji ir dešinioji pusė. Norint pridėti likusią apskritimo dalį, reikia naudoti kitą simetrijos ašį. Ar galite išsiaiškinti, kuri simetrijos ašis reikalinga apskritimui užbaigti? Prieš atsiversdami puslapį ir norėdami patikrinti atsakymą, pagalvokite, kokią simetriją naudoti.

Norėdami užbaigti apskritimą, turite pamąstyti apie įstrižainę. Simetrijos ašis turėtų būti su 1 arba  $-1$  posvyriu ir kirsti apskritimo centro langelį.

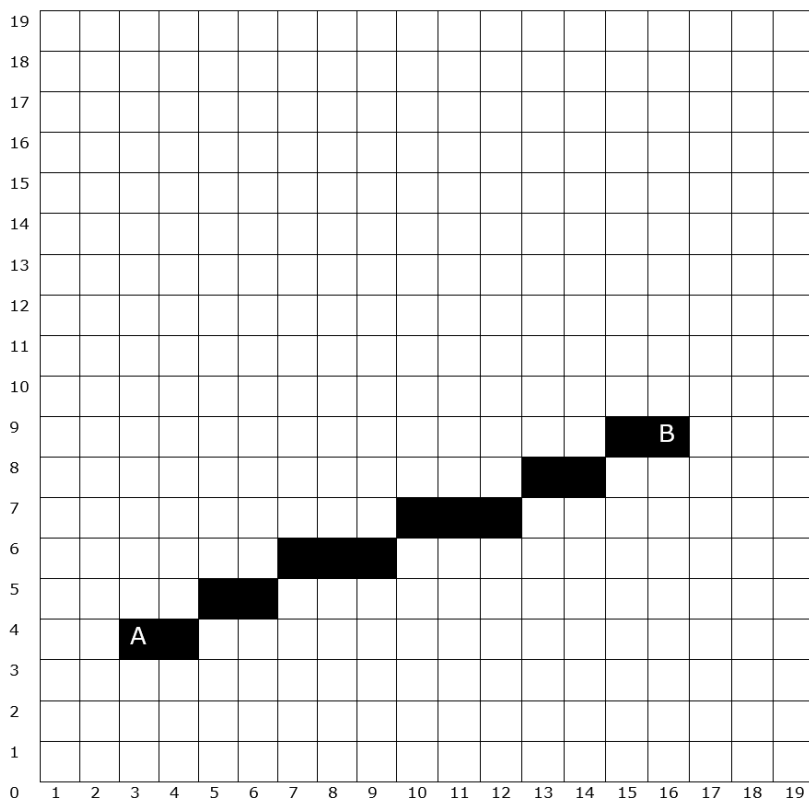
Nors aštuntadalio simetrijos ašies naudojimą lengviau suprasti žmogui, kompiuteris visus simetriškus taškus gali nubraižyti tuo pačiu metu, kai spalvina pirmojo aštuntadalio langelį.





# Sprendimai ir užuominos

## „Bresenhamo linijos brėžimo algoritmas



Atkarpa nuo A iki B

Teisingos suskaičiuotos reikšmės:

$$A = 10, B = -16$$

$P_0 = -3$ , dėti pikselį toje pačioje eilutėje kaip ir pradinis langelis.

$P_1 = 7$ , dėti pikselį virš ankstesniojo langelio.

$P_2 = -9$ , dėti pikselį toje pačioje eilutėje, kaip ir ankstesnįjį pikselį.

$P_3 = 1$ , dėti pikselį virš ankstesnio langelio.

$P_4 = -15$ , dėti pikselį toje pačioje eilutėje kaip ir ankstesnis langelis.

$P_5 = -5$ , dėti pikselį toje pačioje eilutėje kaip ir ankstesnis langelis.

$P_6 = 5$ , dėti pikselį virš ankstesnio langelio.

$P_7 = -11$ , dėti pikselį toje pačioje eilutėje kaip ir ankstesnis langelis.

$P_8 = -1$ , dėti pikselį toje pačioje eilutėje kaip ir ankstesnis langelis.

$P_9 = 9$ , dėti pikselį virš ankstesnio langelio.

$P_{10} = -7$ , dėti pikselį toje pačioje eilutėje kaip ir ankstesnis langelis.

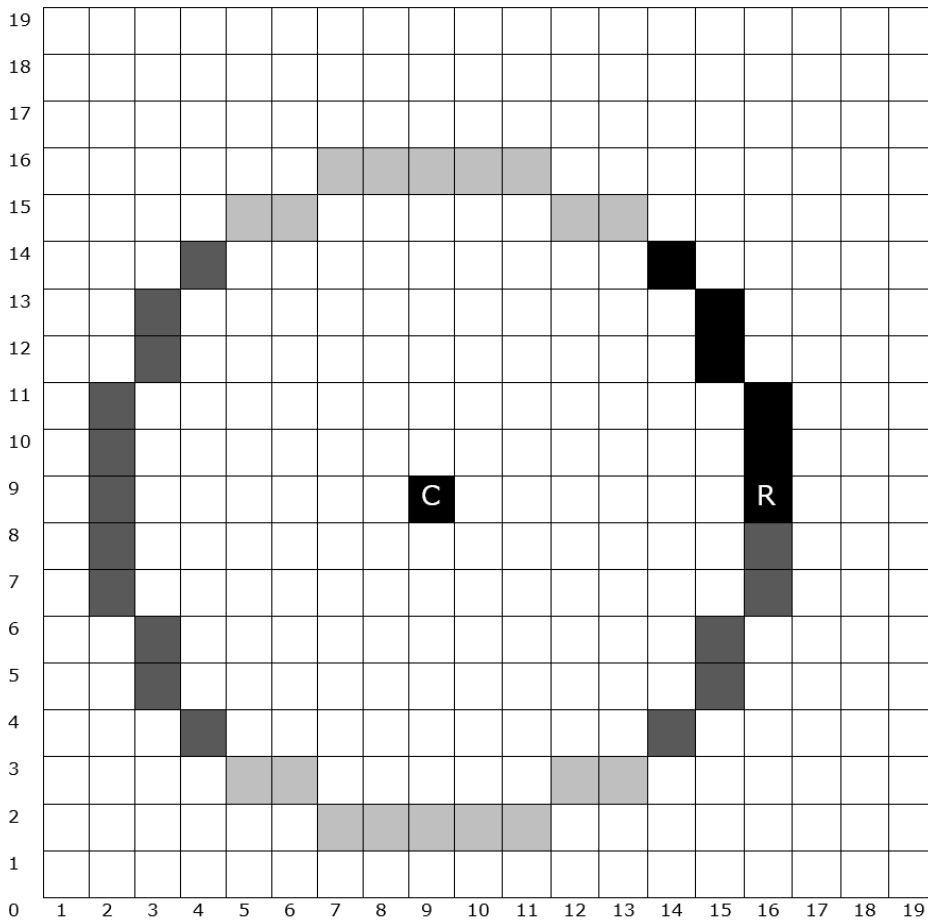
$P_{11} = 3$ , dėti pikselį virš ankstesnio langelio.

$P_{12} = -13$ , dėti pikselį toje pačioje eilutėje kaip ir ankstesnis langelis.



# „Apskritimo centro algoritmas“

Teisingai paskaičiuoti pikseliai:



Juodi langeliai rodo pradinį nubrėžto apskritimo aštuntadalį. Tamsiai pilki langeliai rodo simetriją išilgai OX ir OY ašių. Šviesiai pilki langeliai rodo simetriją įstrižos simetrijos ašies atžvilgiu

Algoritmo skaičiavimai:

$E_0 = -7, x_0 = 7, y_0 = 0$ ; dėti pikselį (16, 9).

$E_1 = -6, y_1 = 1$ ; dėti pikselį (16, 10).

$E_2 = -3, y_2 = 2$ ; dėti pikselį (16, 11).

$E_3 = 2, y_3 = 3$ ;

$E_4 = -11, x_4 = 6$ ; dėti pikselį (15, 12);

$E_5 = -4, y_5 = 4$ ; dėti pikselį (15, 13);

$E_6 = 5, y_6 = 5$ ;

$E_7 = -6, x_7 = 5$ ; dėti pikselį (14, 14);

$E_8 = 5, y_8 = 6$ ; y didesnis nei x, todėl galime atidėti simetriškai visą aštuntadalį.



## Apie ką visa tai?

---

Kompiuteris braižo linijas ir apskritimus atlikdamas nurodytas užduotis. Nuo žaidimų grafikos iki linijų braižymo ir net mažyčio apskritimo, skirto raidei nusakyti – taškui virš i raidės. Derinant linijas ir piešimą su užpildymu ir išlyginimu, kompiuteriai gali piešti tolygiai, nepriklausomai nuo kompiuterio raiškos. Kai vaizdas kompiuteryje aprašomas kaip kontūras ir užpildas, jis vadinamas vektorine grafika. Vektorinę grafiką galima perpiešti bet kokia raiška. Tai reiškia, kad, naudojant vektorinį paveikslėlį, priartinus vaizdą nebus matomi pikseliai, kurie matomi priartinus taškinės grafikos vaizdą. Kontūriniai šriftai yra vienas iš dažniausių vektorinės grafikos naudojimo būdų. Jie leidžia padidinti tekstą iki labai didelių dydžių, neprarandant kokybės.

Vektorinės grafikos programose kiekviena linija turi savo algoritmą, kuris pakeitus linijos padėtį ar jos dydį, kaskart perskaičiuojamas. Todėl vektorinės grafikos paveikslai nepriklauso nuo kompiuterio raiškos. Tačiau kompiuteryje ar spausdinant jie vis tiek turi būti atvaizduoti skaitmenine forma – pikseliais.



# **III dalis**

## **Kaip pasakyti kompiuteriui, ką jis turi daryti?**

### **Algoritmų užrašymas**



# Kaip pasakyti kompiuteriui, ką jis turi daryti?

Kompiuteris įvykdo milijonus paliepiimų per vieną sekundę. Kad kompiuteris vykdytų tuos paliepiimus, reikia teisingai surašyti jam nurodymus. Tai nėra taip lengva, kaip gali atrodyti!

Gavęs kokį nors nurodymą žmogus naudojasi savo patirtimi ir suvokia, ką turėtų daryti. Jei žmogui sakoma „eik pro šias duris“, jis supranta, kad reikia eiti pro duris, o jei jos uždarytos – pirma reikia jas atidaryti. Kompiuteris nurodymus supranta kitaip. Iš tikrųjų komandas jis supranta pažodžiui, todėl, pavyzdžiui, jei kompiuteris yra įmontuotas į judantį robotą, norint išvengti nesėkmių reikia imtis atsargumo ir saugumo priemonių. Jei kompiuteris robotui liepia eiti pro duris, tai robotas ir eina kiaurai pro duris, nekreipdamas dėmesio, ar jos uždarytos ar atidarytos.

Šioje dalyje aiškinama, kaip bendraujama su viską pažodžiui suprantančia mašina naudojant baigtinę komandų seką.

Pirmos veiklos skyriuje supažindinama su „mašina“, atpažįstančia žodžius, skaičius ir simbolių eilutes, su kuriomis kompiuteris dirba. Ši „mašina“ vadinama baigtiniu automatu.

Atliekant antrąją veiklą sužinoma, kaip susikalbėti su kompiuteriu. Programuotojas turi išmokyti nurodyti kompiuteriui, ką šis turi daryti, aiškiais komandomis, nes kompiuteris jas supranta pažodžiui. Komandų sąrašas vadinamas programa. Yra daug įvairių programavimo kalbų, kurias programuotojas gali vartoti programoms kompiuteriui rašyti. Mes pasirinkome paprastą kalbą, kuri gali būti vartojama ir be kompiuterio.



# 13 veikla

## Lobio ieškojimas. Baigtiniai automatai

---

### Santrauka

Kompiuterių programos apdoroja įvairių dokumentų arba kitų programų tekstų sekas, sudarytas, pavyzdžiui, iš raidžių arba žodžių. Informatikos mokslininkai šiuo tikslu naudoja baigtinį automatą, kuris atlieka komandas ir patikrina, ar kompiuteris atpažįsta žodžių ar simbolių eilutes. Pasitelkdami lobių žemėlapius, susipažinsime su baigtinio automato darbu.

### Ryšiai su ugdymo programomis

- ✓ Matematika: loginės užduotys
- ✓ Socialiniai mokslai: Baltijos jūros salos
- ✓ Lietuvių kalba: sakinio sudarymas

### Gebėjimai

- ✓ Žemėlapių skaitymo
- ✓ Schemos aiškinimo
- ✓ Logikinio mąstymo
- ✓ Komandų (instrukcijų) vykdymo

### Amžius

- ✓ Nuo 9 metų

### Medžiaga

Reikia:

- ✓ Salų kortelių rinkinio. (Instrukcijų neturi matyti mokiniai, braižantys maršrutus žemėlapyje!) Salų kortelės. (Salų kortelė perlenkiama per lenkimo liniją taip, kad vienoje pusėje būtų sala su pavadinimu, o kitoje – komandos.)

Kiekvienam mokiniui reikia:

- ✓ Darbo lapo „Maršrutai iki lobio Hyjumos saloje“
- ✓ Rašymo priemonės

Gudručiams siūloma atlikti papildomų veiklų. Jiems reikia:

- ✓ Darbo lapo „Lobio slėpimas“
- ✓ Darbo lapo „Paslaptingas monetos žaidimas“



# Lobių sala

---

## Įvadas

Tikslas – surasti lobių salą Baltijos jūroje. Draugiški Baltijos jūros piratai plaukioja laivais tarp salų pastoviais maršrutais. Norėdami pralobti piratai siūlo keliones turistams. Iš kiekvienos salos išplaukia du jū laivai – A ir B. Turistai gali pasirinkti, kuriuo laivu plaukti. Į kiekvieną salą galima nuvykti arba laivu A, arba laivu B, bet ne abiem. Saloje yra žmogus, kuris pasako, į kurią salą toliau plauks laivas. Tačiau piratai yra mažaraščiai, be to, neturi visų salų žemėlapių, todėl turistams duotame žemėlapyje reikia pažymėti maršrutą ir laivą, kuriuo galima keliauti toliau. Reikia surasti geriausią maršrutą į salą, kurioje paslėptas lobis.

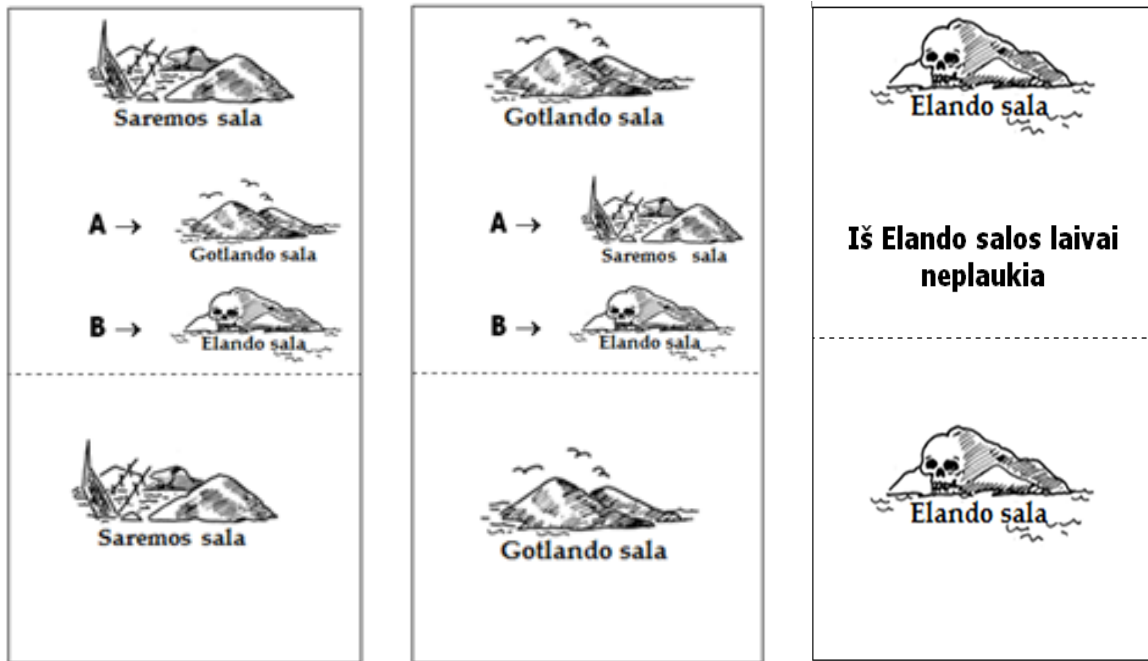
## Demonstracija

(**Patarimai.** Kiekvienai veiklai yra skirtingi salų žemėlapiai.)

Lentoje nupiešiamas trijų salų žemėlapis, kaip parodyta toliau paveiksle.

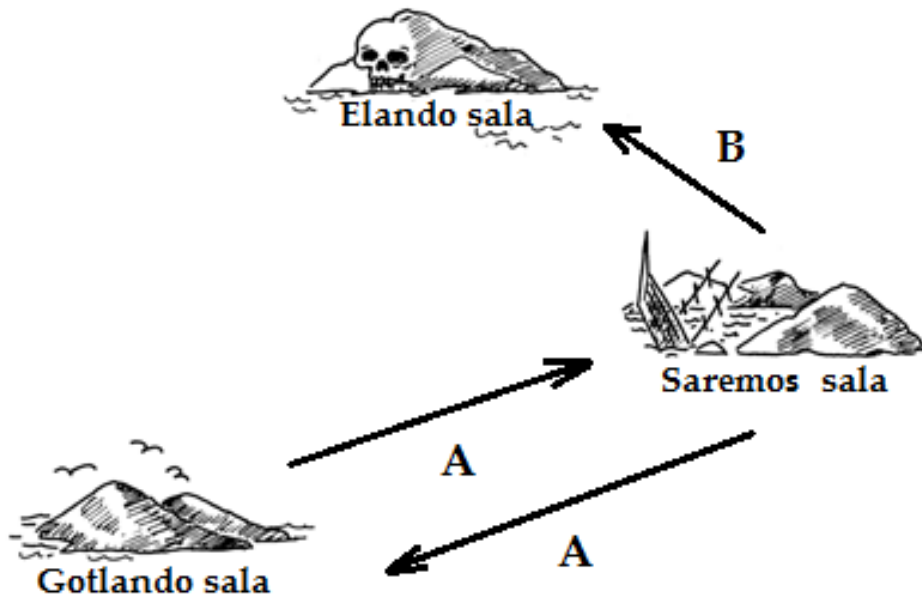


Atspausdinamos trys demonstravimo kortelės. Pakviečiami trys mokiniai ir kiekvienam padalijama salos kortelė ir instrukcija. Įspėjama, kad veikloje, kurią mokiniai atliks vėliau, bus naudojamos kitų maršrutų kortelės.




Kelionė pradedama Saremos saloje. Pasirenkamas laivas A. Mokiniai gali nukreipti laivą į Gotlando salą. Pažymimas maršrutas lentoje. Gotlando saloje vėl pasirenkamas laivas A. Grįžtama į Saremos salą. Lentoje pažymima kelionė. Dabar pasirenkamas laivas B. Šis laivas plaukia į Elando salą, kur patenkama į aklavietę.

Galutinis maršrutas atrodo taip:







# Demonstravimo kortelės





**Saremos sala**

A →   
**Gotlando sala**


B →   
**Elando sala**


---

**Saremos sala**




**Gotlando sala**

A →   
**Saremos sala**

B →   
**Elando sala**

---

**Gotlando sala**



## Demonstravimo kortelės

---



**Iš Elando salos laivai  
neplaukia**

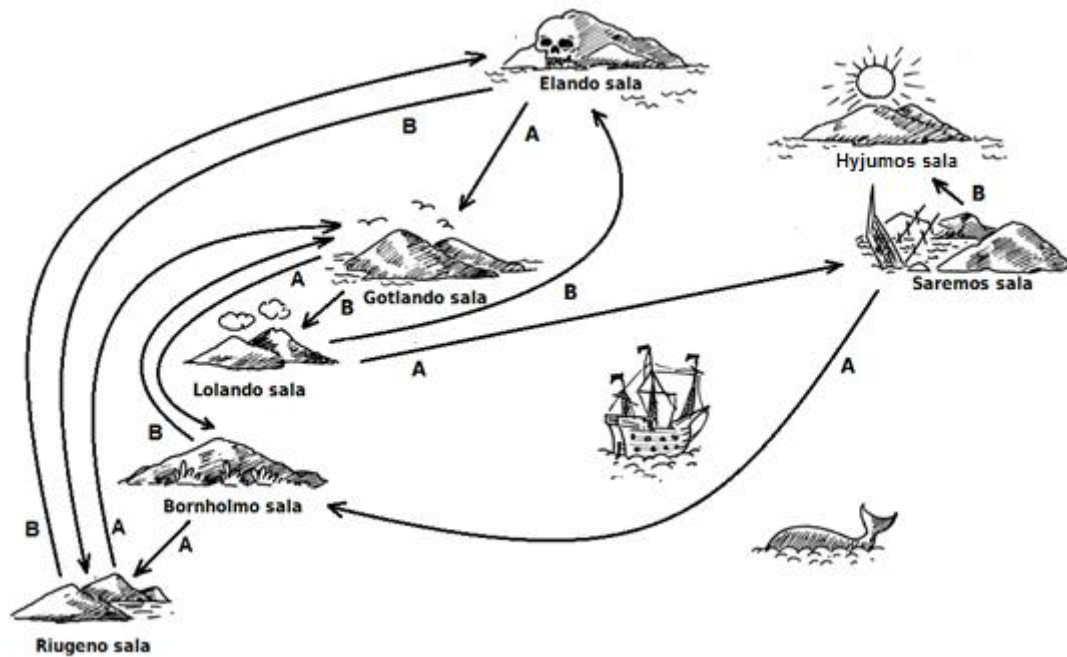


## Veikla

Parenkami 7 mokiniai, turėsiantys vaizduoti salas. Jie laiko savo salos kortelę, kurios kitoje pusėje užrašytos slaptos instrukcijos. Salas vaizduojantys mokiniai atsistoja kas sau aikštelėje ar kambaryje. Likusieji mokiniai vaizduos turistus. Kiekvienam iš jų duodamas salų žemėlapis, kuriame reikia nubraižyti maršrutą iš **Gotlando salos** į **Hyjumos salą**. Pastarojoje saloje paslėptas lobis. Kol salas vaizduojantys mokiniai renkasi korteles ir sustoja į vietas, „turistus“ geriausia išsiųsti už durų.

Jei kuris iš „turistų“ greitai nubraižo maršrutą, pasiūlykite rasti daugiau maršrutų iki lobio salos.

Visi galimi maršrutai pavaizduoti paveiksle:

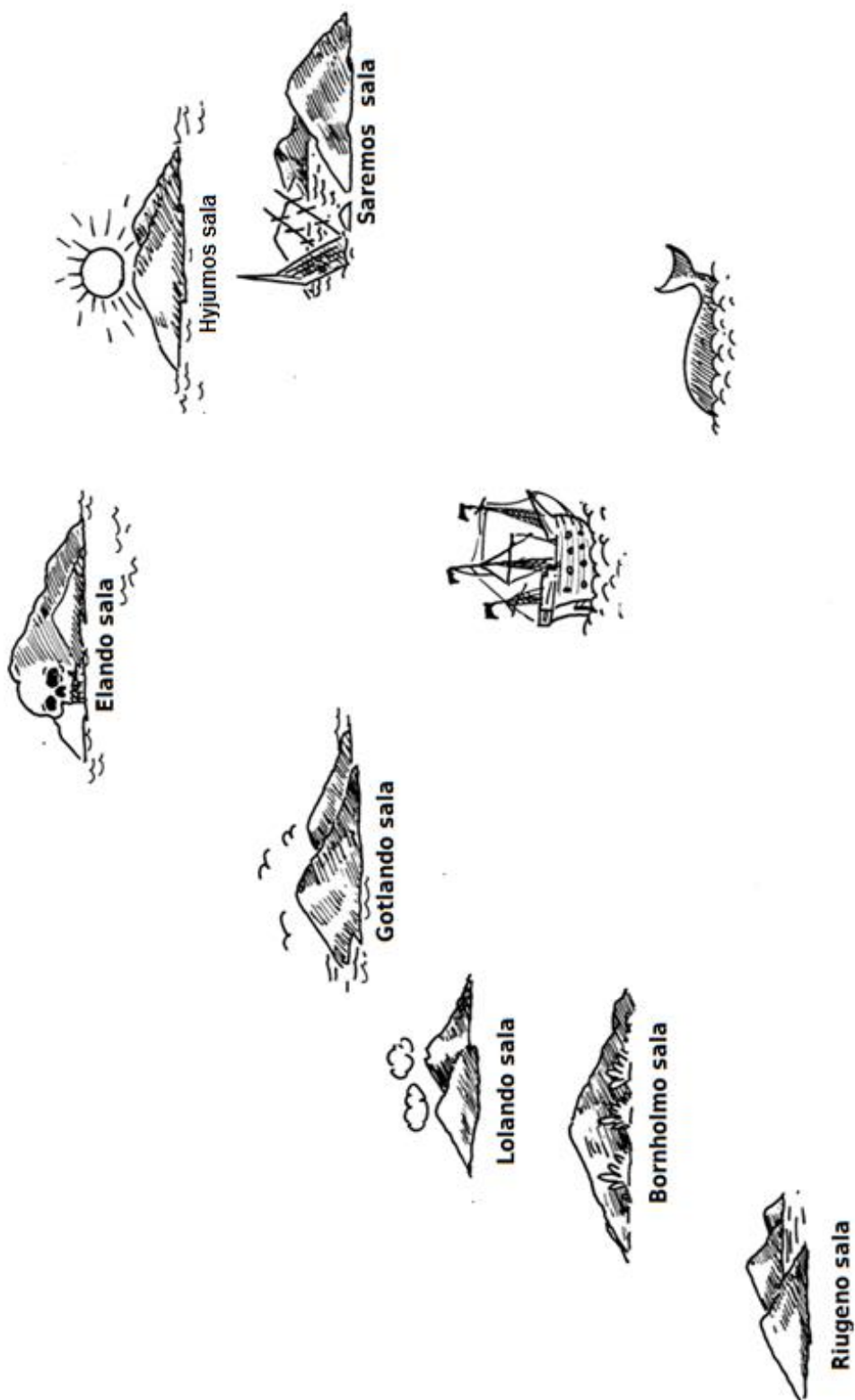


## Diskusija


Koks yra trumpiausias maršrutas? Koks galėtų būti ilgiausias maršrutas? Kai kuriuose maršrutuose gali būti ciklų. Tegul mokiniai pateikia maršrutų su ciklais pavyzdžių. (Pavyzdžiui, ir maršrutu BBBABAB, ir maršrutu BBBABBABAB pasiekama Hyjumos sala.)


# Darbo lapas. Maršrutai iki Iobio Hyjumos saloje


---



# Salų kortelės su instrukcijomis (1/4)


  
**Bornholmo sala**


A →   
**Riugeno sala**


B →   
**Gotlando sala**


---

**Bornholmo sala**




  
**Riugeno sala**

A →   
**Gotlando sala**


B →   
**Elando sala**

---


**Riugeno sala**




## Salų kortelės su instrukcijomis (2/4)




**Gotlando sala**


A →   
**Bornholmo sala**

B →   
**Lolando sala**


---




**Gotlando sala**




**Elando sala**

A →   
**Gotlando sala**


B →   
**Riugeno sala**


---





**Elando sala**


## Salų kortelės su instrukcijomis (3/4)


  
**Lolando sala**


A →   
Saremos sala


B →   
Elando sala

**Lolando sala**  


  
**Saremos sala**

A →   
Bornholmo sala

B →   
Hyjunos sala

**Saremos sala**  


## Salų kortelės su instrukcijomis (4/4)

---



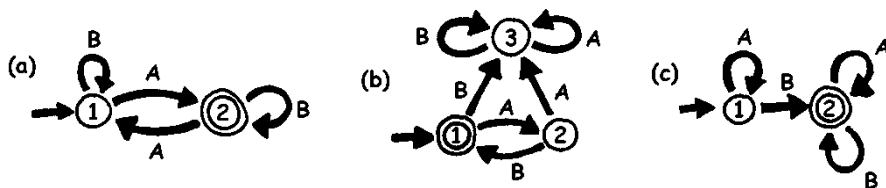
**Sveikiname!  
Pasiekėte lobio  
salą.**





# Baigtinis automatas

Žemėlapij galima braižyti ir taip:



Šiose schemose salos vaizduojamos apskritimais ir žymimos skaičiais, galutinis tikslas (lobio sala) vaizduojamas dvigubu apskritimu. Kuriais maršrutais galima nuplaukti į lobio salą?

## Patarimai

A schemoje kelionė bus baigta tik tada, jei maršrute bus nelyginis laivų A skaičius. Pavyzdžiui: AB, BABAA ar AAABABA.

B schemoje pasiekti lobio salą galima tik nuosekliai kaitaliojant laivus A ir B. Pavyzdžiui: AB, ABAB, ABABAB, ...

C schemoje pasiekti lobio salą galima tik tokiais maršrutais, kuriuose yra bent vienas laivas B. Netinkami maršrutai: A, AA, AAA, AAAA, ...

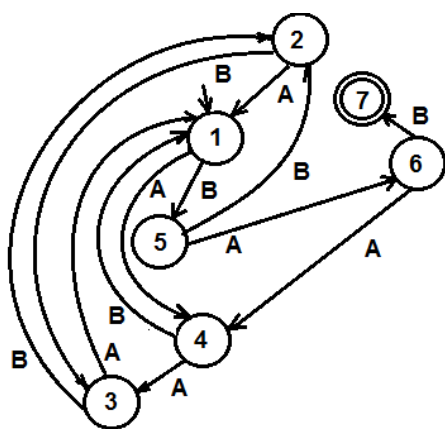
## Darbo lapas. Lobio slėpimas

Sudėtingesnė veikla su baigtiniu automatu galima, kai turime daugiau salų (būsenų) ir galima sudaryti daugiau maršrutų.

Ar galėtumėte labai gerai paslėpti lobį? Kur geriausia paslėpti lobį, kad būtų sunku jį rasti?

Pateikiame sudėtingesnių užduočių. Gerai išnagrinėkite ir apgalvokite, kurio amžiaus mokiniams siūlytumėte, gal ką modifikuotumėte ar pridėtumėte papildomų reikalavimų.

Ankstesnės veiklos lobio paieškos žemėlapis pavaizduotas baigtiniu automatu, kaip tai įprasta daryti informatikoje. Įėjimas (pradžia) žymima skaičiumi 1, o išėjimas (pabaiga) – dvigubu apskritimu



**1 užduotis.** Nupieškite savo salų žemėlapius naudodami baigtinio automato žymėjimus. Sudarykite salų korteles su savo instrukcijomis. Koks trumpiausias maršrutas, kuriuo pasiekiamas jūsų paslėptas lobis?

**2 užduotis.** Išbandykite savo salų žemėlapij ir korteles su draugais. Duokite jiems A ir B sekas ir pažiūrėkite, ar jie suras paslėptą lobį.

**3 užduotis.** Pasiūlykite kitokių žaidimų, kurie iliustruotų baigtinio automato idėją.

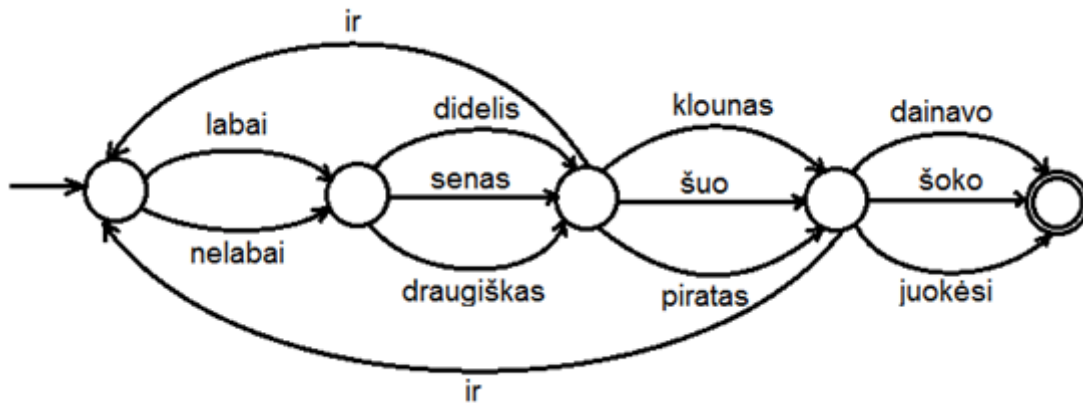
1.

## Darbo lapas. Baigtinio automato taikymas sakiniams sudaryti

---

Baigtinis automatas labai tinka sudaryti žodžiams, sekoms, sakiniams.

Toliau paveiksle pavaizduota, kaip sudaryti sakinius taikant baigtinį automatą. Sakiniai sudaromi renkantis leidžiamus kelius schemeje ir užrašant kelyje pasitaikančius žodžius.



**Užduotis.** Pateikite sakinių, sudarytų pagal šį baigtinį automatą. Ar visi sudaryti sakinių pavyzdžiai tinka semantiškai? Prisiminkite, kas yra sintaksė ir semantika, paaiškinkite pavyzdžiais.

Dabar patys nubraižykite kokį baigtinį automatą sakiniams sudaryti. Tikriausiai net linksmų istorijų galėtumėte sukurti!

## Darbo lapas. Paslaptingas monetos žaidimas

---

Draugai atsisiuntė žaidimą iš interneto. Žaidime robotas meta monetą ir reikia spėti, kuria puse – herbu ar skaičiumi – ji atsivers. Iš pradžių žaidimas pasirodė labai lengvas. Tikimybė laimėti yra 0,5. Bent jau taip manė draugai. Po kurio laiko draugai pradėjo abejoti. Jie pastebėjo, kad moneta metama pagal tam tikrą taisyklę. Ar žaidime yra kokia apgaulė? Tikriausiai ne! Jie nusprendė tai išsiaiškinti. Vienas iš jų surašė metimų rezultatus. Štai ką jis surašė (H – herbas, S – skaičius):

HSHHSHHHSSHHHHSSHSSSHHHHHSHHHSSSHHHSSSHHHHHHSSHSSSSSHSSHSSSHHH  
SSHHSHHHHHHHHSSHHHSSSSHHHHHSSSSSSS

Ar galėtumėte nuspėti, pagal kokią taisyklę metamos monetos?

Galima nubraižyti schemą, pagal kurią gaunama atitinkama metamos monetos atsivertimų seka.

**Užomina:** joje yra tik 4 „salos“!



## Apie ką visa tai?

---

Informatikoje baigtinis automatas padeda sugeneruoti ženklų ar įvykių sekas.

Vienas iš baigtinio automato pavyzdžių yra informacijos skambučiai. Kai skambinama informacijos numeriu, iš pradžių atsiliepiama įrašų: „Jei norite ..., spauskite 1, jei norite ..., spauskite 2, jei norite ..., spauskite 3“ ir t. t. Telefono mygtuko paspaudimas yra baigtinio automato kitame telefono linijos gale įvestis. Šis dialogas gali būti labai paprastas arba labai sudėtingas. Kartais galima patekti į baigtinio automato ciklą. Jei taip atsitinka, sistema parodo klaidą, o tai gali nuvilti skambintoją.

Kitas pavyzdys yra bankomatas. Bankomato programa pateikia seką įvykių, iš kurių vartotojas pasirenka reikiamą. Programoje yra visos įmanomos įvykių galimybės kaip baigtinio automato būsenos. Kiekvieno klavišo paspaudimas perkelia į kitą būseną. Kai kurios būsenos pateikia instrukcijas kompiuteriui, pavyzdžiui, „išduoti 100 Eur“, „spausdinti sąskaitą“ arba „išimti kortelę“.

Kai kurie kompiuteriai naudoja schemas, kurios padeda sudaryti anglų kalbos sakinius. Jie gali ir generuoti sakinius, ir vykdyti tai, ką vartotojas įveda. 1960 m. parašyta programa „Eliza“ (pavadinta Elizos Dolittle garbei), kuri gali bendrauti su žmogumi. Programa primena bendravimą su psichoterapeutu, nes vartoja tokias frazes, kaip „papasakokite apie savo šeimą“ ir „prašom tęsti“. Žinoma, ji nieko nesupranta, tačiau yra gana įtaigi. Kai kurie ją išbandę žmonės galvojo, kad kalba su psichoterapeutu.

Nors kompiuteriai prastai supranta gyvą kalbą, tačiau jie lengvai gali apdoroti dirbtines kalbas. Viena iš svarbiausių dirbtinių kalbų grupių yra programavimo kalbos. Naudodamas baigtinį automatą kompiuteris skaito programas ir verčia jas į elementarias instrukcijas, kurias pats gali tiesiogiai vykdyti.

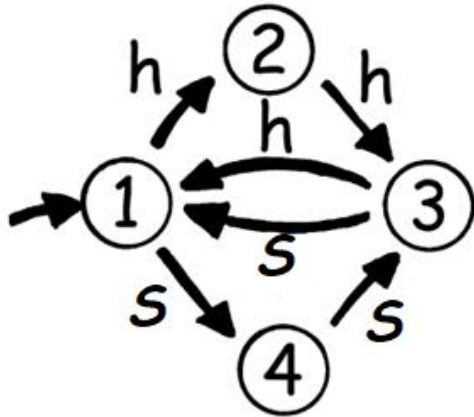


# Sprendimai ir užuominos

---

## Paslaptingas monetos žaidimas

Paslaptingas monetos žaidimas vyksta pagal tokią schemą:



# 14 veikla

## Nurodymų eilė. Programavimo kalbos

---

### Santrauka

Kompiuteris gali atlikti veiksmus tik pagal algoritmą – programą, užrašytą taikant sutartas taisykles. Programa – tai algoritmas, užrašytas programavimo kalbos žymėnėmis taip, kad jį būtų galima atlikti kompiuteriu. Kompiuteris kiekvieną komandą supranta paraidžiui. Ši veikla iliustruoja kaip tik šį programavimo aspektą.

### Ryšiai su ugdymo programomis

- ✓ Lietuvių kalba: sakomo teksto interpretacija

### Gebėjimai

- ✓ Instrukcijų kūrimo ir vykdymo

### Amžius

- ✓ Nuo 7 metų

### Priemonės

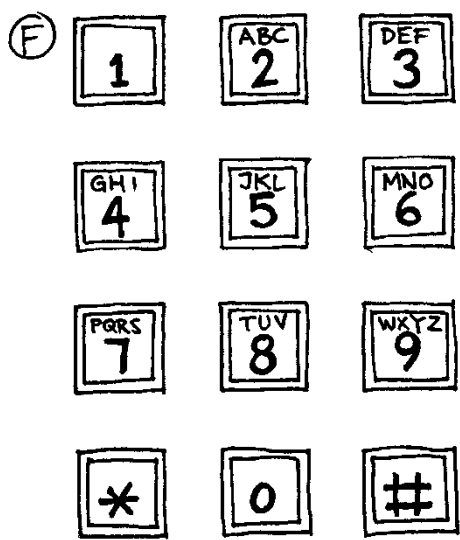
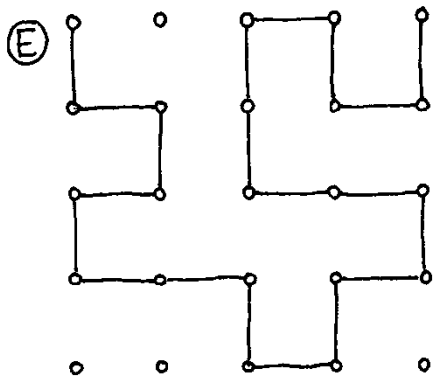
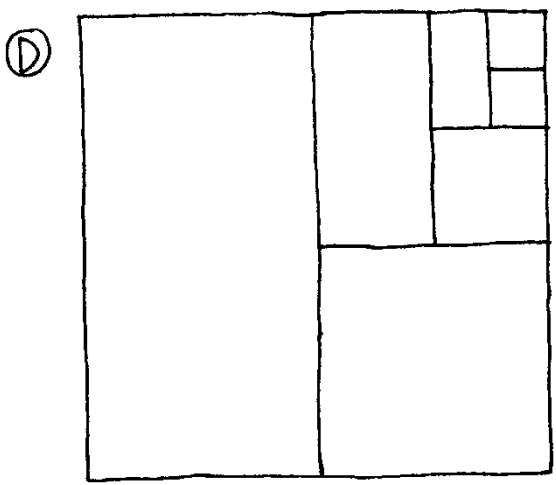
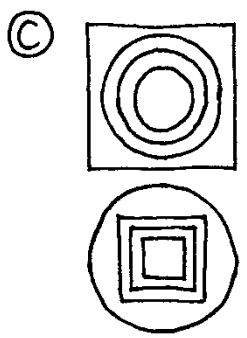
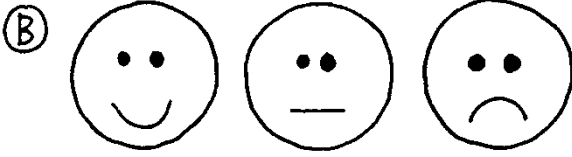
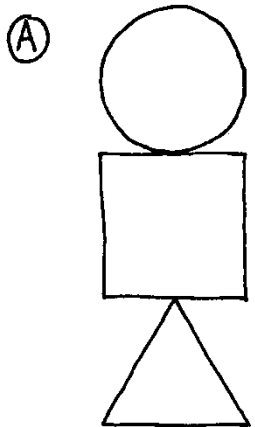
Reikia:

- ✓ Kortelių su paveikslėliais

Kiekvienam mokiniui reikia:

- ✓ Rašymo priemonės, popieriaus lapo ir liniuotės







# Nurodymų eilė

---

## Įvadas

Diskutuojama, kas būtų, jei žmonės tiksliai vykdytų nurodymus. Pavyzdžiui, kaip pasielgtų žmogus, jei paprašytume jo eiti pro uždarytas duris?

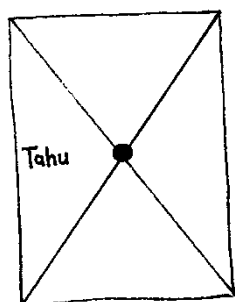
Kompiuteris tiksliai vykdo nurodytas komandas, net jei jos ir neturi jokios prasmės.

## Demonstracija

Mokiniai pabando vykdyti tikslūs nurodymus:

1. Pažymėkite tašką lapo viduryje.
2. Pradėdami nuo kairiojo viršutinio lapo kampo su liniuote brėžkite tiesią liniją per tašką centre iki apatinio dešiniojo lapo kampo.
3. Pradėdami nuo apatinio kairiojo lapo kampo su liniuote brėžkite liniją per tašką centre iki viršutinio dešiniojo lapo kampo.
4. Parašykite savo vardą viduriniame trikampyje lapo kairėje.

Mokinių rezultatas turėtų atrodyti taip:



## Veiklos

Parenkamas mokinys, kuriam duodamas vienas iš aukščiau pateiktų paveiks–lėlių. Mokinys turi sakyti žingsnius, kaip tą paveikslėlį nupiešti. Kiti mokiniai piešia pagal jo nurodymus. Jie gali klausti, jei ko nesupranta. Tikslas – padėti mokiniams suprasti, kaip vykdomi tikslūs nurodymai.

Pratimas kartojamas, tačiau mokiniams nebeleidžiama klausti. Patariama piešti paprastesnį paveikslėlį, nes mokiniai greitai pradeda klysti.

Pratimas kartojamas, bet šį kartą nurodymus duodantis mokinys pasislepia, kad piešiantys mokiniai galėtų jį tik girdėti. Mokiniai negali klausinėti.

Atkreipiamas dėmesys, kad paskutinis pratimas yra labai panašus į tai, kaip programuotojas rašo programą kompiuteriui. Jis surašo nurodymus ir rezultatą pamato tik tada, kai kompiuteris juos visus įvykdo.

Tegul mokiniai ką nors nupiešia ir parašo to piešinio nurodymus, kuriuos gali išbandyti poromis ar su visa klase.

## Variantai

Mokiniai galėtų:

1. Parašyti popierinio lėktuvėlio lankstymo nurodymus.
2. Vartodami frazes: „eik  $x$  metrų tiesiai“, „pasisuk dešinėn (90 laipsnių)“ ir „pasisuk kairėn (90 laipsnių)“, parašyti nurodymus, kaip nueiti į tam tikrą vietą mokyklos teritorijoje.

Mokiniai kartu turi tikrinti parašytas instrukcijas, jas taisyti, kol gaunamas norimas rezultatas.

3. „Akla višta“. Vienam mokiniui užrišamos akys. Kiti mokiniai nurodinėja, kur šis turi eiti, kad pasiektų tikslą.



## Apie ką visa tai?

---

Kompiuteris gali atlikti tik tiksliai užrašytą algoritmą, vadinamą programa. Programai užrašyti vartojamos programavimo kalbos, sukurtos pagal tam tikras taisykles ir turinčios ribotą skaičių kompiuteriui suprantamų komandų. Vienos kalbos yra tinkamesnės vienokiam uždaviniui spręsti, kitos – kitokiam.

Nepriklausomai nuo vartojamos programavimo kalbos, programuotojas turi tiksliai nurodyti, ką kompiuteris turi atlikti. Priešingai nei žmogus, kompiuteris įvykdo visas komandas paraižiu, net jei jos visiškai absurdiškos.

Programos turi būti parašytos teisingai, nes net maža klaida gali sukelti daug problemų. Galima tik įsivaizduoti klaidos padarinius erdvėlaivių paleidimo, branduolinės elektrinės ar traukinių valdymo kompiuterių programose. Anglų kalba šios klaidos vadinamos „bugs“ (liet. *vabalai*). Įdomu tai, kad šis angliškas pavadinimas atsirado 1940 m. dėl kandies, pašalintos (angl. *debugged*) iš elektroninės skaičiavimo mašinos elektros perjungiklio.



Kuo sudėtingesnė programa, tuo didesnė jos klaidų tikimybė.

Programos sudėtingumas tapo pagrindiniu iššūkiu, kai JAV buvo kuriama Strateginės gynybos („Žvaigždžių karų“) programos kompiuterių valdymo sistema. Ši sistema turėjo sudaryti neįveikiamą gynybą nuo branduolinės atakos. Kai kurie informatikai tvirtino, kad sistema niekada neveiks, nes programinė įranga yra labai sudėtinga ir nepatikima. Pagrindinis jų argumentas buvo tai, kad programinę įrangą reikia testuoti ir nustatyti kiek įmanoma daugiau klaidų. Esą šios sistemos ištestuoti neįmanoma, nes norint įsitikinti, kad ji veikia, reikia patikrinti visas jos galimybes, iš kurių viena – paleisti JAV branduolines raketas.

# **IV dalis**

## **Ko kompiuteris negali?**

### **Sunkiai sprendžiami uždaviniai**



# Sunkiai sprendžiami uždaviniai

Ar yra tokių uždavinių, kuriuos sunkiai sprendžia net ir kompiuteriai? Žinoma! Galima iškart pateikti pavyzdį: paprastas pokalbis kompiuteriui yra neįveikiamas, nes jis negali suprasti, mąstyti ir pateikti reikšmingų atsakymų. To kompiuteris negali padaryti tik dėl to, kad žmogus pats nežino, kaip šie procesai vyksta, ir negali jų aprašyti kompiuteriui suprantamomis komandomis. Tačiau yra ir kita grupė kompiuteriui sunkių uždavinių. Šiuos uždavinius parašyti kompiuteriui suprantama programavimo kalba yra nesunku, bet juos kompiuteris spręstų milijonus šimtmečių. Net šimtą kartų spartesnis kompiuteris juos spręstų milijonus metų, o milijoną kartų spartesnis – šimtus metų. Sunkiai kompiuterio sprendžiamas uždavinys yra toks, kurį net ir sparčiausias kompiuteris sprendžia daug ilgiau, nei trunka žmogaus gyvenimas.

Šioje dalyje pateikiama uždavinių, neturinčių efektyvių sprendimų. Kompiuteris juos spręstų milijonus šimtmečių. Taip pat supažindinama su didžiausia informatikos mokslo paslaptimi: niekas nežino, ar yra efektyvesnis uždavinio sprendimo būdas! Tai reiškia, kad nėra įrodymo, kad efektyvus sprendimo būdas egzistuoja arba kad tokio sprendimo nėra. Informatikoje yra tūkstančiai neišspręstų visiškai skirtingų, tačiau sprendžiamų vienu būdu uždavinių. Jei būtų rastas efektyvus vieno uždavinio sprendimas, tai jį būtų galima pritaikyti ir kitiems uždaviniams spręsti. Šios dalies skyriuose supažindinama su keliais sunkiai sprendžiamais uždaviniais.

## Mokytojams

Šioje dalyje aprašomos trys veiklos. Atliekant pirmą veiklą spalvinami žemėlapiai ir skaičiuojama, kiek reikia spalvų gretimoms šalims skirtingai nuspalvinti. Užsiimant antra veikla paprastame gatvių žemėlapyje tam tikrose vietose statomi ledų furgonai. Atliekant trečią veiklą virve ir kabliais jungiami taškai į tinklą.

Atliekant šias veiklas stengiamasi parodyti idėjų sudėtingumą: paprasti, aiškūs ir nesunkiai suprantami uždaviniai yra sunkiai sprendžiami. Dažniausiai šie uždaviniai kyla iš paprastų kasdieninio gyvenimo situacijų, kai reikia sudaryti žemėlapius ar tvarkaraščius, projektuoti kelius. Tokie uždaviniai vadinami NP pilnumo uždaviniais. NP pilnumo sąvoka aprašoma skyreliuose „Apie ką visa tai?“ kiekvienos šios dalies veiklos aprašo pabaigoje. Veiklos turi būti atliekamos iš eilės. Jas atlikę mokiniai jau turės supratimą apie svarbiausius atvirusius informatikos klausimus.

Ši dalis pavadinta „Sunkiai sprendžiami uždaviniai“, nes joje aptariami uždaviniai iš tiesų labai sudėtingi, jiems spręsti reikia labai daug laiko, o sprendimai mažai kam suprantami. Kai kurie uždaviniai išvis neišsprendžiami. Vienaip ar kitaip, šie uždaviniai labai svarbūs praktiniame gyvenime, jų išsprendimas būtų reikšmingas įvairioms mokslo tyrimų sritims. Pavyzdžiui, daugelis kriptografijos uždavinių remiasi sunkiai sprendžiamais uždaviniais. Pastarieji svarbūs ir dėl to, kad, tarkime, tokį uždavinį išsprendęs nusikaltėlis galėtų iškoduoti slaptus duomenis ir juos parduoti arba, pavyzdžiui, tiesiog klastoti bankų pavedimus. Apie tai plačiau rašoma V dalyje „Kriptografija“.



## 15 veikla

# Vargšas kartografas. Grafo spalvinimas

---

### Santrauka

Daugelyje optimizavimo uždavinių tam tikri įvykiai negali vykti vienu metu ar tam tikri objektai negali būti gretimi. Pavyzdžiui, kiekvienas, kam teko daryti klasės ar susitikimo tvarkaraštį, yra susidūręs su visų dalyvių sąlygų suderinimo problema. Tokio pobūdžio uždaviniai gali būti sprendžiami taikant grafo spalvinimo metodą. Spalvinant grafą siekiama, kad gretimi jo elementai būtų skirtingų spalvų. Atliekant šią veiklą grafo spalvinimo metodu sudaromas žemėlapis.

### Ryšiai su programomis

- ✓ Matematika: skaičiai, dvejetainė skaičiavimo sistema
- ✓ Matematika: algebra, begalinė skaičių seka, skaičių sekos taisyklės, dvejetainis laipsnis

### Gebėjimai

- ✓ Problemų sprendimo
- ✓ Loginio argumentavimo
- ✓ Algoritmų vykdymo
- ✓ Bendradarbiavimo ir įžvalgumo

### Amžius

- ✓ Nuo 7 metų

### Priemonės

- ✓ Lenta arba kitas rašymo paviršius ir rašymo priemonė  
Kiekvienam mokiniui reikia:
- ✓ Vieno ar kelių darbo lapo kopijų
- ✓ Spalvotų smeigtukų ar spalvotų lipniųjų lapelių
- ✓ Spalvotų pieštukų, flomasterių ar kreidelių



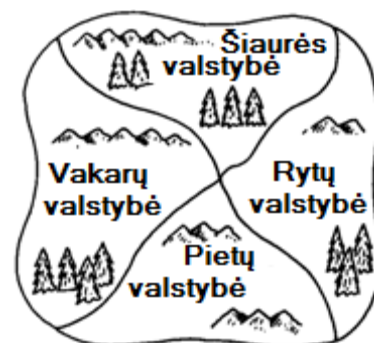
# Grafo spalvinimas



## Įvadas

Šiame skyriuje pasakojama apie kartografa, kuriam mokiniai turi padėti nuspalvinti žemėlapij taip, kad gretimos valstybės būtų skirtingų spalvų.

Pavyzdžiui, paveiksle dešinėje parodytas žemėlapis su keturiomis valstybėmis: Šiaurės, Vakarų, Rytų ir Pietų. Jei Šiaurės valstybė nuspalvinama raudonai, tai Vakarų negali būti spalvinama raudonai, nes nesimatys sienos su Šiaurės valstybe. Vakarų valstybę galima spalvinti, pavyzdžiui, žaliai. Tada ir Rytų valstybė gali būti spalvinama žaliai, nes neturi bendrų sienų su Vakarų valstybe (jei dvi valstybės liečiasi tik viename taške, laikoma, kad jos neturi bendrų sienų). Pietų valstybė gali būti spalvinama raudonai, nes neturi bendrų sienų su Šiaurės valstybe.



Šio pasakojimo kartografas gyvena labai vargingai ir negali įsigyti daug spalvotų pieštukų, todėl prašoma naudoti kuo mažiau spalvų.

## Diskusija

Šiai veiklai pateikiami keturi pavyzdžiai – darbo lapai. Jie skirti mokiniams, tačiau juos turėtų gerai išnagrinėti ir studentai, būsimi mokytojai, kad gerai suprastų sprendimo eigą, gebėtų paaiškinti kylančias problemas.

Pirmasis darbo lapas. Pirmojo darbo lapo pavyzdžiui nuspalvinti pakanka tik dviejų spalvų. Vis tik sumažinti spalvų skaičių iki dviejų daugeliui mokinių gali būti sunku. Tačiau ši užduotis yra paprasta, palyginti su žemėlapiais, kuriuose yra daugiau valstybių ir reikia daugiau spalvų.



Spalvindami žemėlapij dviem spalvomis mokiniai gali suformuluoti taisyklę: jei viena valstybė spalvinama viena spalva, tai jos kaimynė turi būti spalvinama kita spalva. Ši taisyklė kartojama, kol nuspalvinamas visas žemėlapis. Geriausia siekti, kad šią taisyklę mokiniai sugalvotų ir pateiktų patys.

Padiskutuokite, kodėl šiam pavyzdžiui nuspalvinti užtenka dviejų spalvų? Kokie Jūsų argumentai?

Antrasis darbo lapas. Tai jau sunkesnė užduotis. Pasiūlykite mokiniams pasitarti, kokiomis priemonėmis geriau spręsti grafo spalvinimo uždavinius. Galbūt mokiniai, užuot spalvinę, sugalvos naudoti spalvotus smeigtukus arba lipniousius lapelius. Šis būdas leidžia apsigalvoti ir prireikus valstybę pažymėti kita spalva.

Ar galite paaiškinti, koku būdu spalvinant žemėlapij prireikia mažiausiai spalvų? Vienas iš mąstymo būdų, kodėl šiam žemėlapiui reikia bent trijų spalvų, galėtų būti toks: daugiausiai trys valstybės turi bendrų sienų.

Tolesni darbo lapų pavyzdžiai (trečiasis ir ketvirtasis) sudėtingesni, prireiks daugiau spalvų. Atsakymai pateikiami šios medžiagos pabaigoje. Būtinai skatinkite mokinius diskutuoti, argumentuoti, ieškoti geresnių sprendimo kelių. Mokiniai turi patys atrasti, kiek mažiausiai reikia spalvų spalvinant vieną ar kitą grafą.

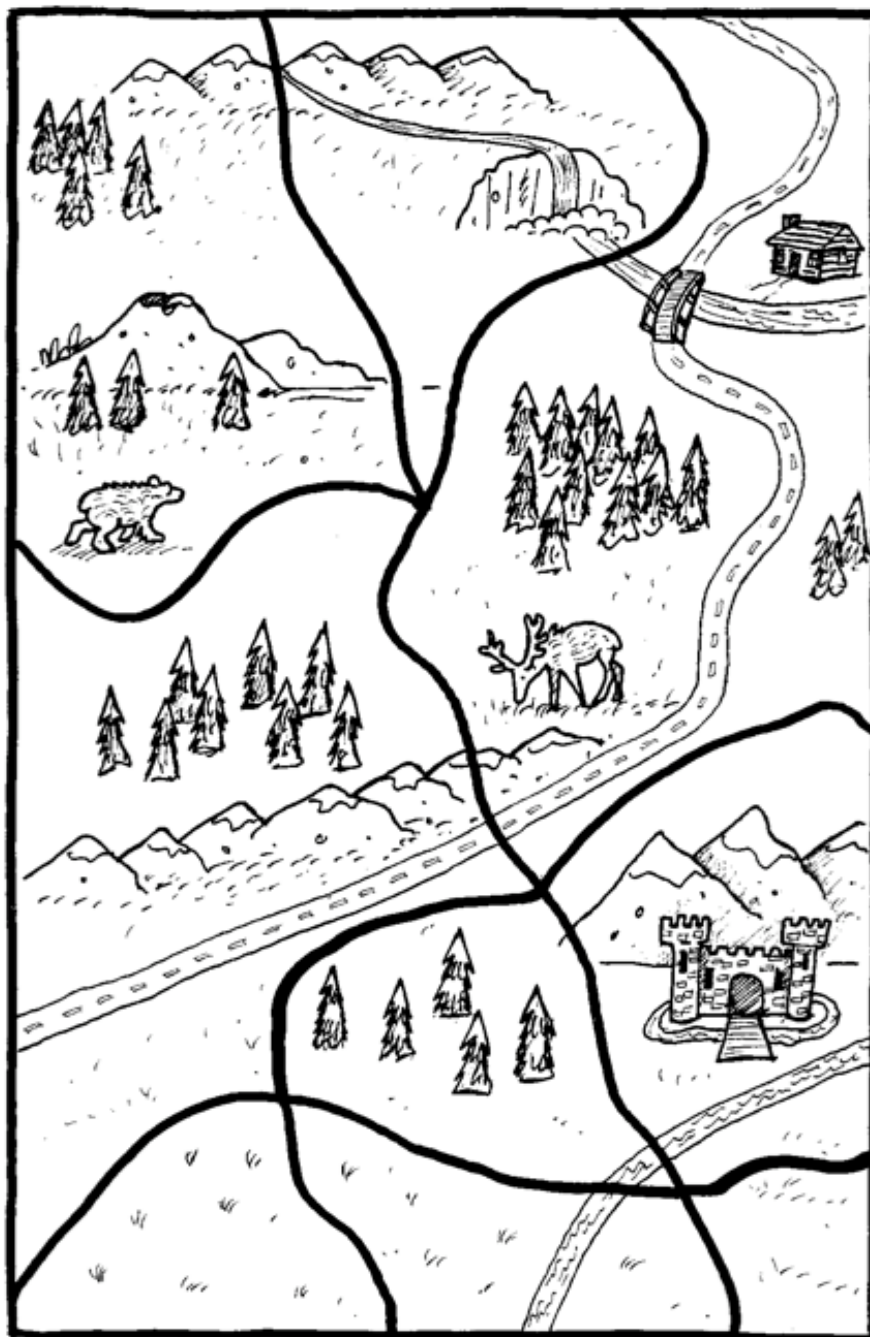
Kai mokiniai nuspalvina visus žemėlapius, galima paprašyti, kad sukurtų ir savo žemėlapių, kuriems nuspalvinti reikėtų mažiausiai penkių spalvų, arba kad įrodytų, kad bet kuriam žemėlapiui nuspalvinti pakanka keturių spalvų. Tokiai užduočiai atlikti mokiniams turėtų prireikti daugiau laiko. Mokiniai gali greitai nubraižyti žemėlapij, kuriam nuspalvinti reikia penkių spalvų, bet daugeliu atvejų galima parodyti, kad jį galima nuspalvinti ir keturiomis spalvomis. Kaip manote, kodėl taip yra?





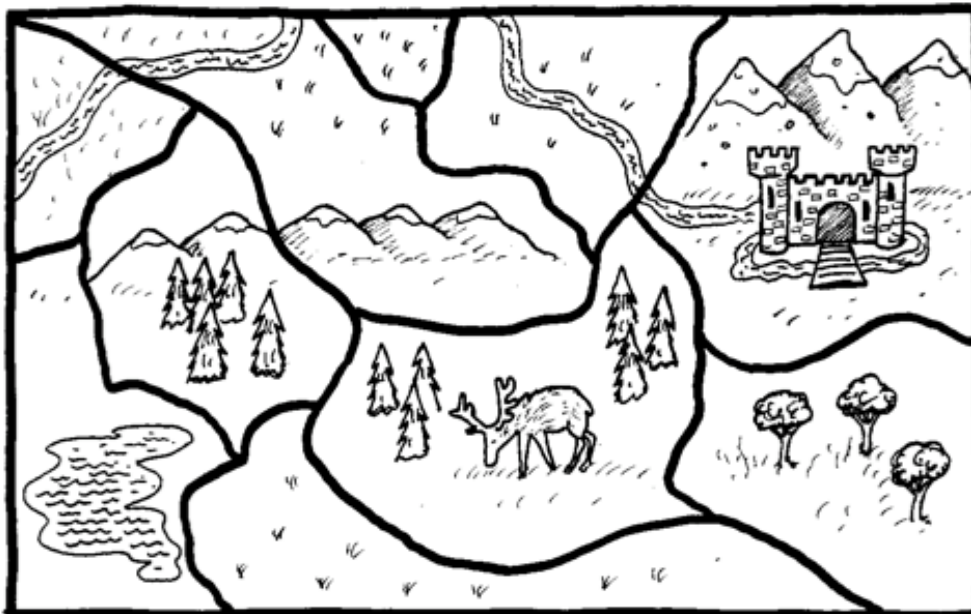
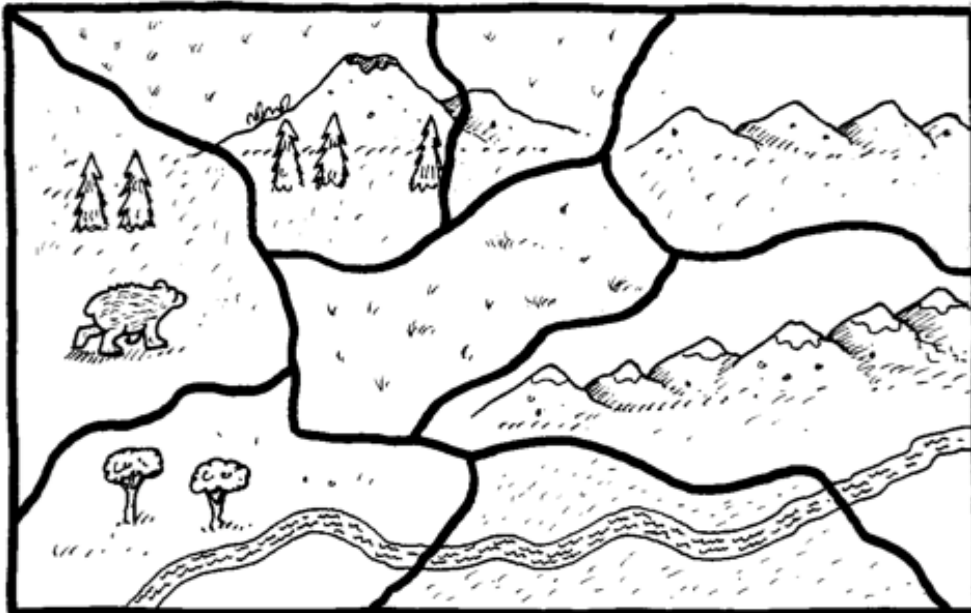
## Darbo lapas. Grafo spalvinimas (1)

Nuspalvinkite valstybes šiame žemėlapyje naudodami kuo mažiau spalvų. Valstybės, turinčios bendrą sieną, negali būti spalvinamos tokia pat spalva.



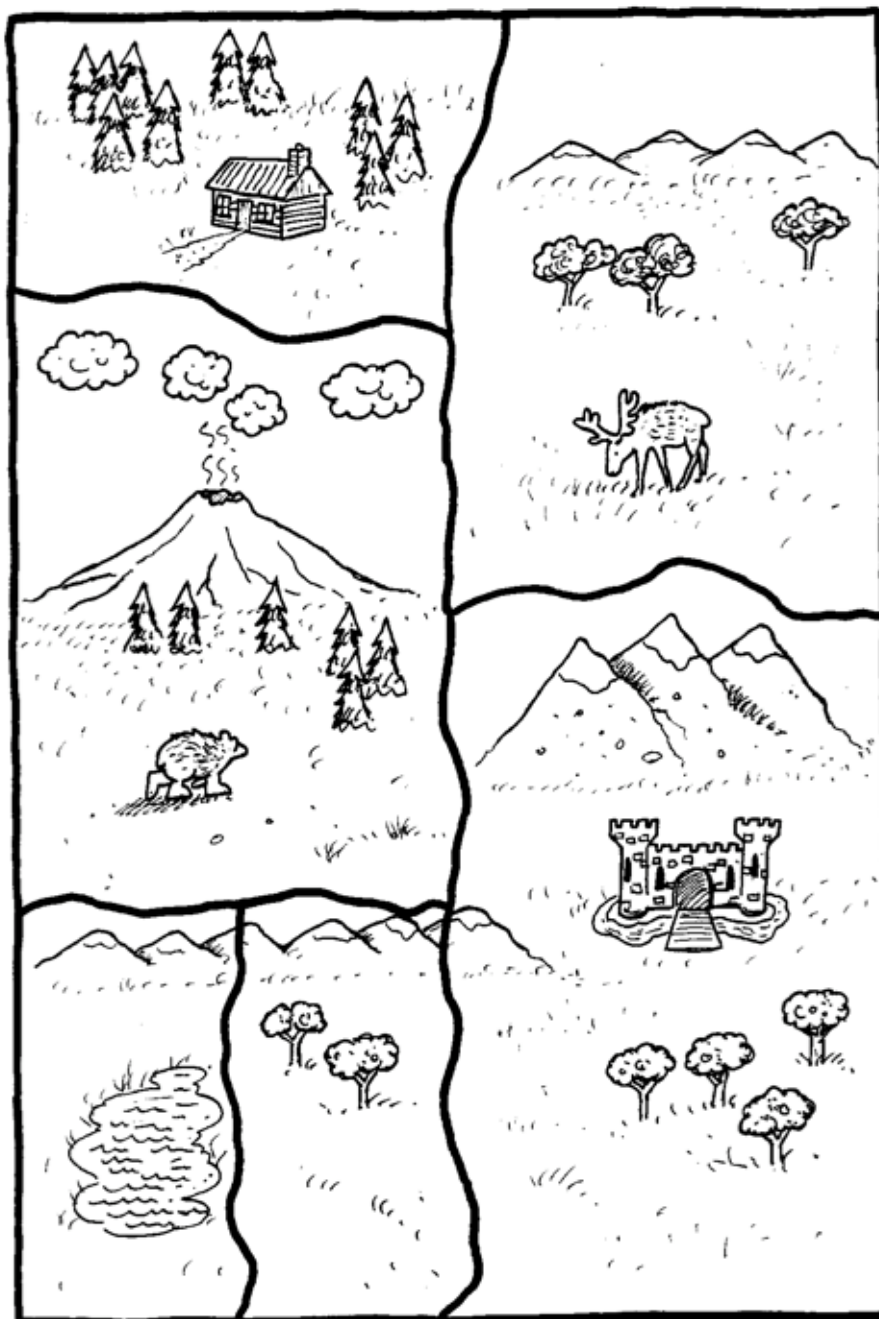
## Darbo lapas. Grafo spalvinimas (2)

Nuspalvinkite valstybes šiuose žemėlapiuose naudodami kuo mažiau spalvų. Valstybės, turinčios bendrą sieną, negali būti spalvinamos tokia pat spalva.



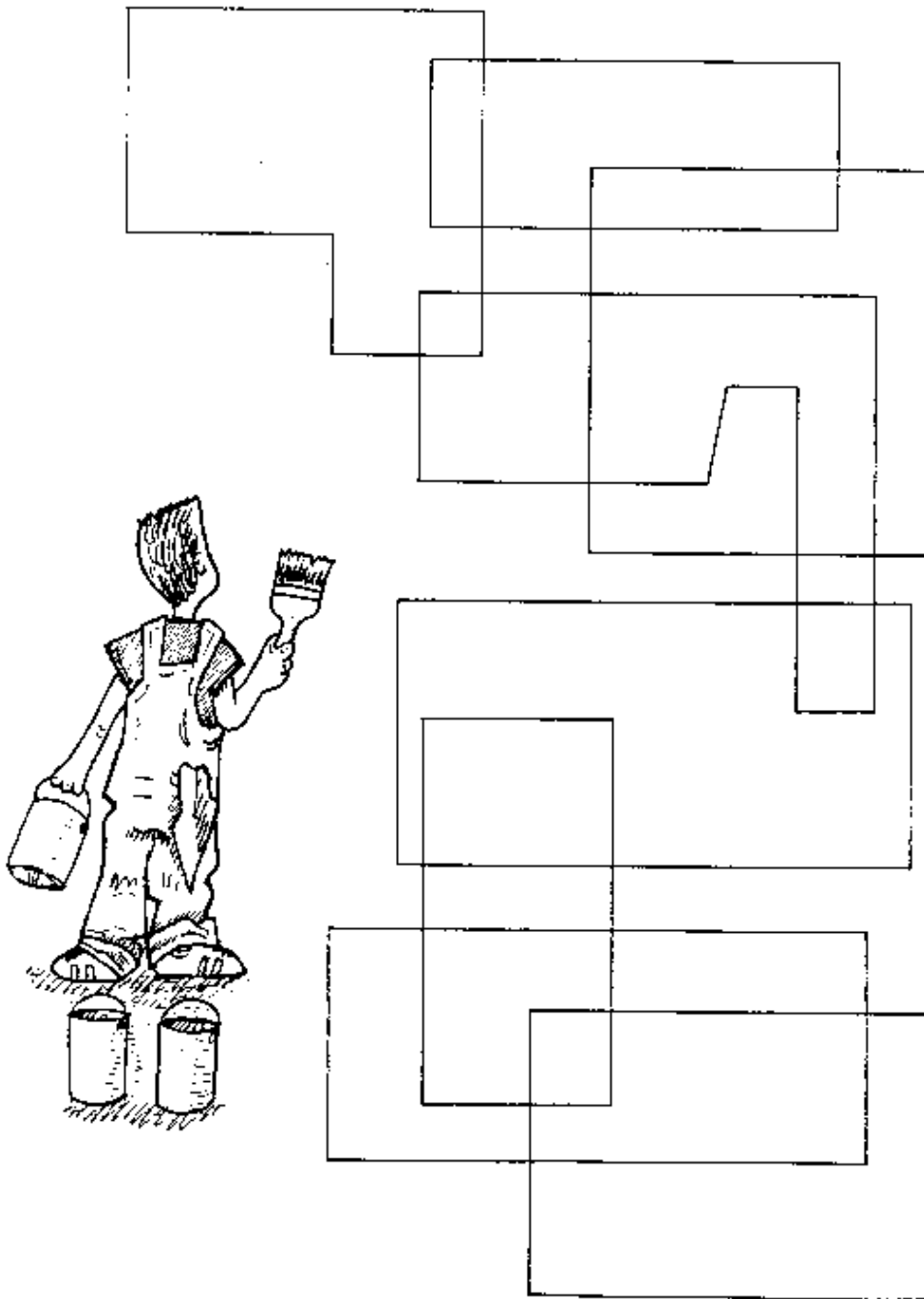
## Darbo lapas. Grafo spalvinimas (3)

Nuspalvinkite valstybes šiame žemėlapyje naudodami kuo mažiau spalvų. Valstybės, turinčios bendrą sieną, negali būti spalvinamos tokia pat spalva.



## Darbo lapas. Grafo spalvinimas (4)

Nuspalvinkite sritis šioje schemoje naudodami kuo mažiau spalvų. Sritys, turinčios bendrą ribą, negali būti spalvinamos tokia pat spalva.



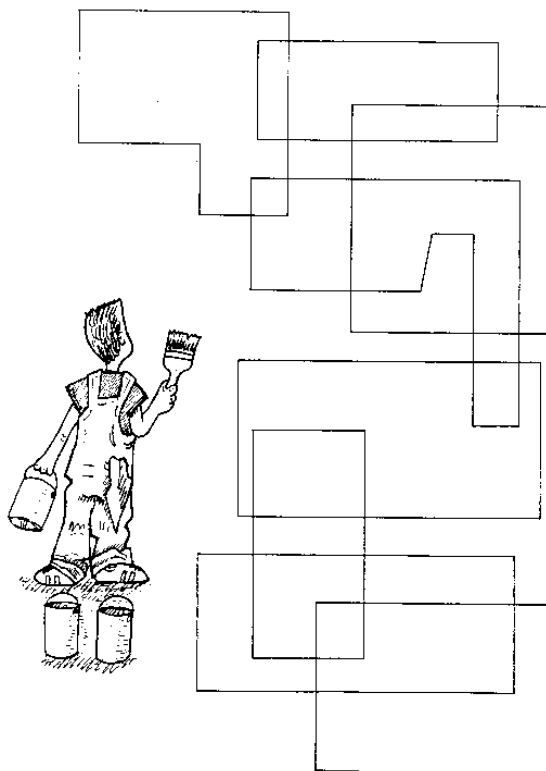
## Gudručiams

Paprasta sukurti žemėlapij, kuriam nuspalvinti tereikia dviejų spalvų. Toks pavyzdys parodytas ketvirtame darbo lape, kur schema yra sudėliota iš persidengiančių uždarytų geometrinių figūrų. Taip sudėliotą schemą ar žemėlapij visada bus galima nuspalvinti naudojant tik dvi spalvas. Užduotis mokiniams būtų sukurti ir patikrinti keletą tokių žemėlapių. Tada reikėtų klausti, kodėl taip yra, kokiomis savybėmis turi pasižymėti žemėlapis (grafas), kad būtų galima nuspalvinti naudojant tik dvi spalvas. Būtina išklaustyti kiekvieną mokinį. Mokiniai patys turi spręsti, ar pateikti argumentai yra įtikinantys, ar jų pakanka.

Žemėlapiui, nupieštam ant lapo ar rutulio (gaublio), visada užtenka keturių spalvų. Mokslininkams įdomu, kiek spalvų reikia žemėlapiui, kuris nupieštas ant kitokio paviršiaus, pavyzdžiui, toro. Šiuo atveju visada pakanka penkių spalvų. Mokiniai galėtų tai išbandyti.

Grafų teorijoje yra įvairių grafo spalvinimo uždavinių interpretacijų. Pavyzdžiui, jei vienas žmogus spalvina žemėlapij, nubraižytą ant lapo, tai tikrai žino, kad protingai spalvinant užtenka keturių spalvų. O jei tas žmogus spalvintų valstybes paeiliui ne vienas, o su priešiška nusiteikusi ar grafų spalvinimo teorijos nežinančiu partneriu? Vienas spalvina viską gerai apgalvodamas, o kitas neapdairiai spalvina valstybes paeiliui. Kiek mažiausiai skirtingų spalvų reikėtų žemėlapiui nuspalvinti? Didžiausias skaičius nėra žinomas. 1992 m. buvo įrodyta, kad 33 skirtingų spalvų visada pakaktų. 2008 m. buvo įrodyta, kad visada pakaktų 17 skirtingų spalvų. Ekspertai spėja, kad turėtų užtekti 10 skirtingų spalvų, bet tai nėra įrodyta. Mokiniai galėtų išbandyti šį uždavinį poromis spalvindami žemėlapius.

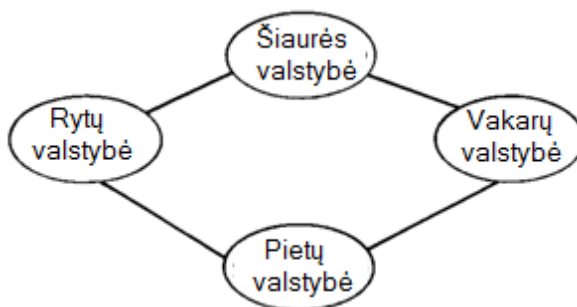
Kita grafo spalvinimo uždavinio interpretacija yra *imperijos spalvinimas*. Šiai interpretacijai reikia dviejų skirtingų, bet vienodą skaičių valstybių turinčių žemėlapių. Kiekviena valstybė viename žemėlapyje (Žemės) turi atitikti valstybę kitame žemėlapyje (Žemės valstybės koloniją Marse). Spalvinant šiuos žemėlapius keliamos dvi sąlygos: valstybės, turinčios bendrą sieną, negali būti tokios pat spalvos ir kiekviena valstybė viename žemėlapyje turi būti nuspalvinta tokia pat spalva kaip ją atitinkanti valstybė kitame žemėlapyje. Kiek mažiausiai skirtingų spalvų reikia šiems žemėlapiams nuspalvinti? Atsakymas dar nežinomas.



## Apie ką visa tai?

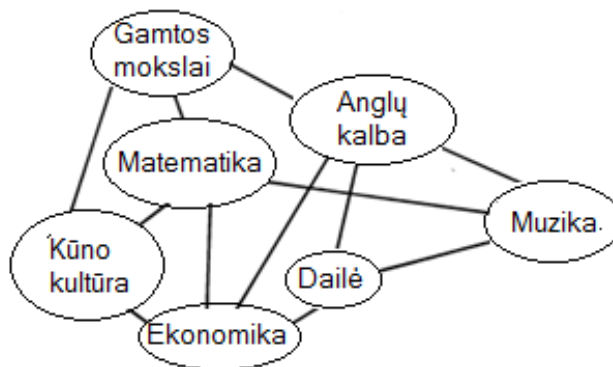
„Žemėlapių spalvinimo“ uždavinyje, spręstame atliekant šią veiklą, reikėjo surasti mažiausią skaičių skirtingų spalvų (dvi, trys, keturios spalvos), kuriomis būtų galima nuspalvinti vieną ar kitą žemėlapi. 1852 m. buvo suformuluotas teiginys, kad bet kokį žemėlapi galima nuspalvinti mažiausiai keturiomis skirtingomis spalvomis, bet iki 1976 m. jis nebuvo įrodytas. Ši keturių spalvų teorema buvo įrodyta tik po 120 metų, nes informatikos mokslas turėjo ir turi daugybę neatsakytų klausimų.

Žemėlapių spalvinimas priklauso grafo spalvinimo uždavinių grupei. Informatikoje grafas yra abstrakti objektų ryšių sistema, ji parodyta paveiksle.



Informatikoje grafai vaizduojami apskritimais arba taškais (vadinamais viršūnėmis), sujungtais briaunomis arba lankais, kurie rodo tam tikrus ryšius tarp vaizduojamų objektų. Paveiksle pateikiamas demonstracijos žemėlapi vaizduojantis grafas. Viršūnės vaizduoja valstybes, o linijos – valstybių sienas. Grafe spalvinimo uždavinys formuluojamas taip: viršūnės turi būti sujungtos skirtingų spalvų linijomis. Spalvinant grafą neribojamas skirtingų spalvų skaičius, nes grafo viršūnės gali būti jungiamos daugeliu būdų. Dvimatis vaizdas sumažina jungimo būdų skaičių. Grafo spalvinimo uždavinys yra surasti mažiausią skaičių skirtingų spalvų tam tikram grafui nuspalvinti.

Paveiksle dešinėje viršūnės atitinka mokykloje mokomus dalykus. Linija, jungianti dvi viršūnes, reiškia, kad mažiausiai vienas mokinys mokosi tų dviejų dalykų, todėl tvarkaraštyje abiejų dalykų pamokos negali būti įrašytos kaip vykstančios vienu metu. Optimalaus pamokų tvarkaraščio sudarymas yra grafo spalvinimo uždavinys, kai kiekviena spalva reiškia kitą pamokos laiką.



Informatikos grafų spalvinimo algoritmas dažnai naudojamas realaus gyvenimo problemoms spręsti, bet veikiausiai netaikomas žemėlapiams spalvinti. Vargšo kartografo veikla tik fikcija. Tokie uždaviniai sprendžiami praktiškai, nes realiame gyvenime galime naudotis gal ir neoptimaliu, bet vis tiek labai geru rezultatu.

Kompiuterio sugaištas laikas grafų spalvinimo uždaviniui spręsti ilgėja eksponentiškai didėjant grafo dydžiui. Žemėlapių spalvinimo uždavinys gali būti sprendžiamas perrenkant visus įmanomus spalvinimo variantus. Žinoma, kad pakanka mažiausiai keturių skirtingų spalvų. Vadinasi, reikia patikrinti visas žemėlapių spalvinimo keturiomis spalvomis galimybes. Jei žemėlapyje yra  $n$  valstybių, tai galimybių yra  $4^n$ . Šis





skaičius auga labai greitai: kiekviena šalis padidina galimybių skaičių 4 kartais ir tokiu būdu keturgubina sprendimo laiką. Net jei būtų toks kompiuteris, kuris galėtų rasti 50 valstybių spalvinimo sprendimą per valandą, tai 51 šaliai nuspalvinti reikėtų jau 4 valandų. Tokie uždaviniai išlieka aktualūs, nes išrandami vis spartesni kompiuteriai.

Grafo spalvinimas yra geras pavyzdys uždavinio, kurio sprendimo laikas ilgėja eksponentiškai. Paprastu atveju, kai mažai valstybių, surasti optimalų sprendimą yra gana paprasta ir be kompiuterio, bet daugėjant valstybių uždavinys tampa nebeišsprendžiamas net ir kompiuteriu.

Realiame gyvenime dažnai tenka spręsti tokius uždavinius. Nors jie ir sunkiai sprendžiami, realiame gyvenime reikia gauti rezultatą. Informatikos metodai pateikia gana gerų, bet ne puikių sprendimų. Šie heuristinių metodų rezultatai yra labai artimi optimaliems, greitai apdorojami kompiuteriu ir tinkami praktiniams tikslams. Pavyzdžiui, mokyklose gali prireikti vieno kabineto daugiau, nei būtina, dėl mažos pamokų tvarkaraščio paklaidos, taip pat ir žemėlapyje gali būti viena spalva daugiau, nei būtina.

Niekas neįrodė, kad nėra efektyvaus būdo šiems uždaviniams spręsti, bet taip pat niekas neįrodė, kad jis yra. Informatikos mokslininkai lieka skeptiški, kad kada nors bus rastas efektyvus metodas. Kitų veiklų skyriuose daugiau pasakojama apie sunkiai sprendžiamus uždavinius.

### **Daugiau informacijos**

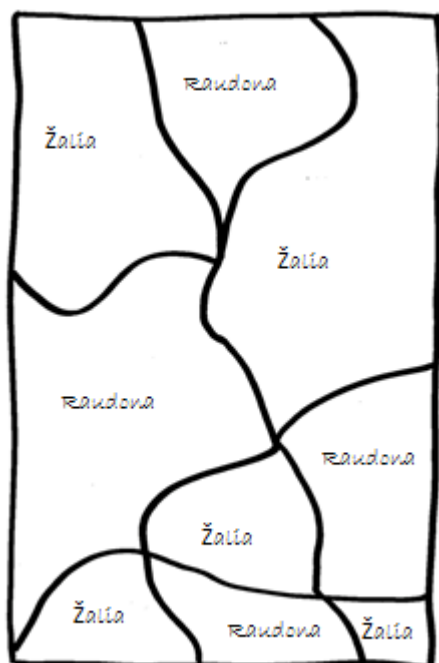
Davido Harel'o knygoje „Algorithmics“ nagrinėjama keturių spalvų teorema, pateikiama jos istorija. Daugiau žemėlapių spalvinimo aspektų aptariama knygoje „The Spirit of Computing“ (Addison–Wesley, Reading, MA, 1st edition, 1987; 2nd edition, 1992; 3rd edition (with Y. Feldman), 2004).

Nancy Casey ir Mike'o Fellowso knygoje „This is MEGA–Mathematics!“ (Los Alamos National Labs, 1992).

Mareko Kubale knygoje „Graph Colorings“ aprašoma grafo spalvinimo uždavinių istorija. Šia tema galima rasti daug tinklalapių. (American Mathematical Society, Providence, Rhode Island, 2004).



## Sprendimai ir užuominos



A.



B.

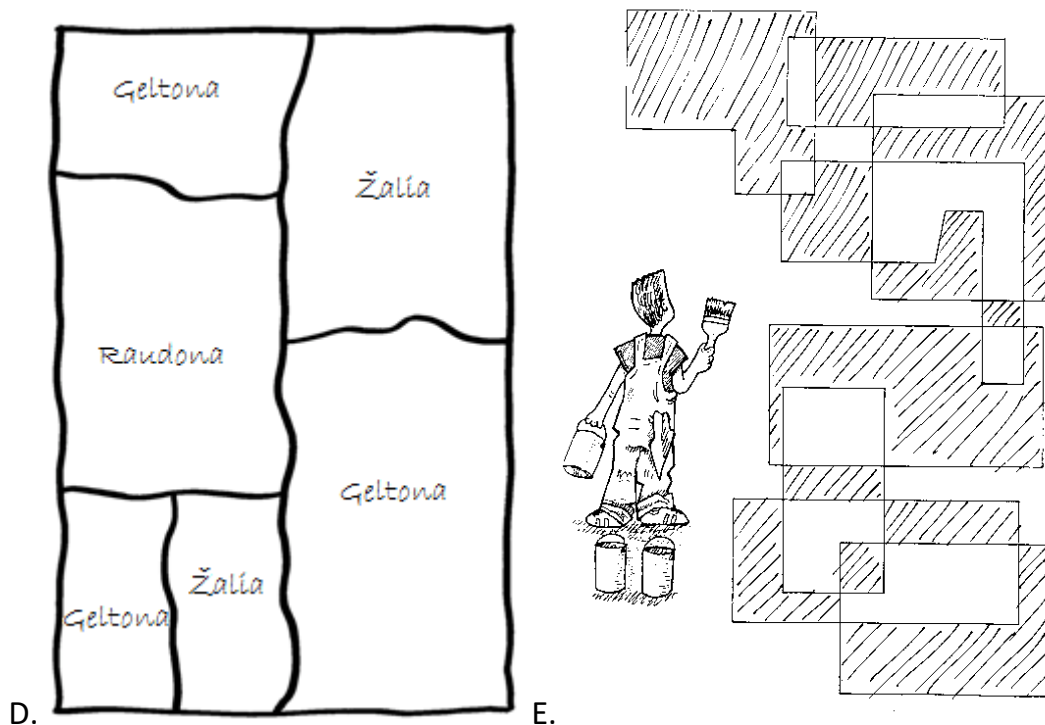


C.

Vienintelis pirmojo darbo lapo sprendimas parodytas A paveiksle (spalvos gali būti pasirenkamos).

Antrojo darbo lapo viršutiniam žemėlapiui reikia trijų spalvų. Galimas sprendimas parodytas B paveiksle. Apatiniam žemėlapiui reikia keturių spalvų. Galimas sprendimas parodytas C paveiksle.





Trečiojo darbo lapo žemėlapiui reikia trijų spalvų. Galimas sprendimas parodytas D paveiksle.

Ketvirtojo darbo lapo sprendimas parodytas E paveiksle (vienos figūros baltos, o kitos užbrūkšniuotos).

## 16 veikla

### Turistų miestas. Dominuojančios sekos

---

#### Santrauka

Daugelis realaus gyvenimo situacijų gali būti vaizduojamos abstrakčiai – grafais ar tinklais. Tinklai ir grafai suteikia daug galimybių parašyti naujų naudingų algoritmų. Atliekant šią veiklą siekiama pažymėti susikirtimus arba grafo viršūnes taip, kad kiekviena viršūnė būtų nutolusi ne daugiau kaip per vieną žingsnį nuo kurios nors iš kitų pažymėtų viršūnių. Kiek mažiausiai tokių viršūnių reikia pažymėti?

#### Ryšiai su ugdymo programomis

- ✓ Matematika: vieta ir padėtis
- ✓ Matematika: loginiai uždaviniai

#### Gebėjimai

- ✓ Žemėlapių skaitymo
- ✓ Ryšių nustatymo
- ✓ Dėlionės sprendimo
- ✓ Pasikartojančio tikslo siekimo

#### Amžius

- ✓ Nuo 7 metų

#### Priemonės

Kiekvienai mokinių grupei reikia:

- ✓ Darbo lapo „Ledų furgonas“
- ✓ Dviejų spalvų žymiklių ar spalvotų smeigtukų

Reikia:

- ✓ Projektoriaus ir baltos lentos, kad būtų galima demonstruoti medžiagą, arba tik baltos lentos, kurioje būtų galima paaikškinti medžiagą visai grupei.



# Dominuojančios sekos

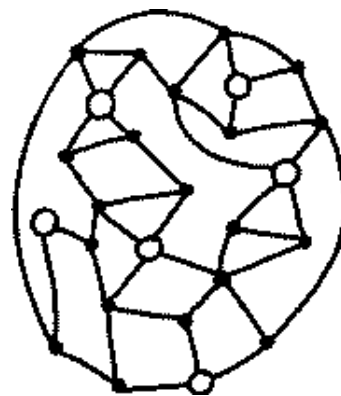
---

## Įvadas

„Ledų furgono“ darbo lape grafu vaizduojamas Turistų miesto žemėlapis. Briaunos arba lankai jame vaizduoja gatves, o viršūnės yra gatvių sankryžos. Miestas yra labai karštoje šalyje. Vasarą ledų furgonai pastatomi prie gatvių sankryžų, čia parduodami ledai turistams. Furgonai turi būti sustatyti taip, kad bet kas, gyvenantis prie gatvės, pasiektų furgoną vos tik paėjęs iki gatvės kampo, o gyvenantis name prie gatvių sankryžos pasiektų furgoną paėjęs daugiausiai vieną kvartalą. Kiek mažiausiai furgonų reikia ir kuriose vietose jie turi būti pastatyti?

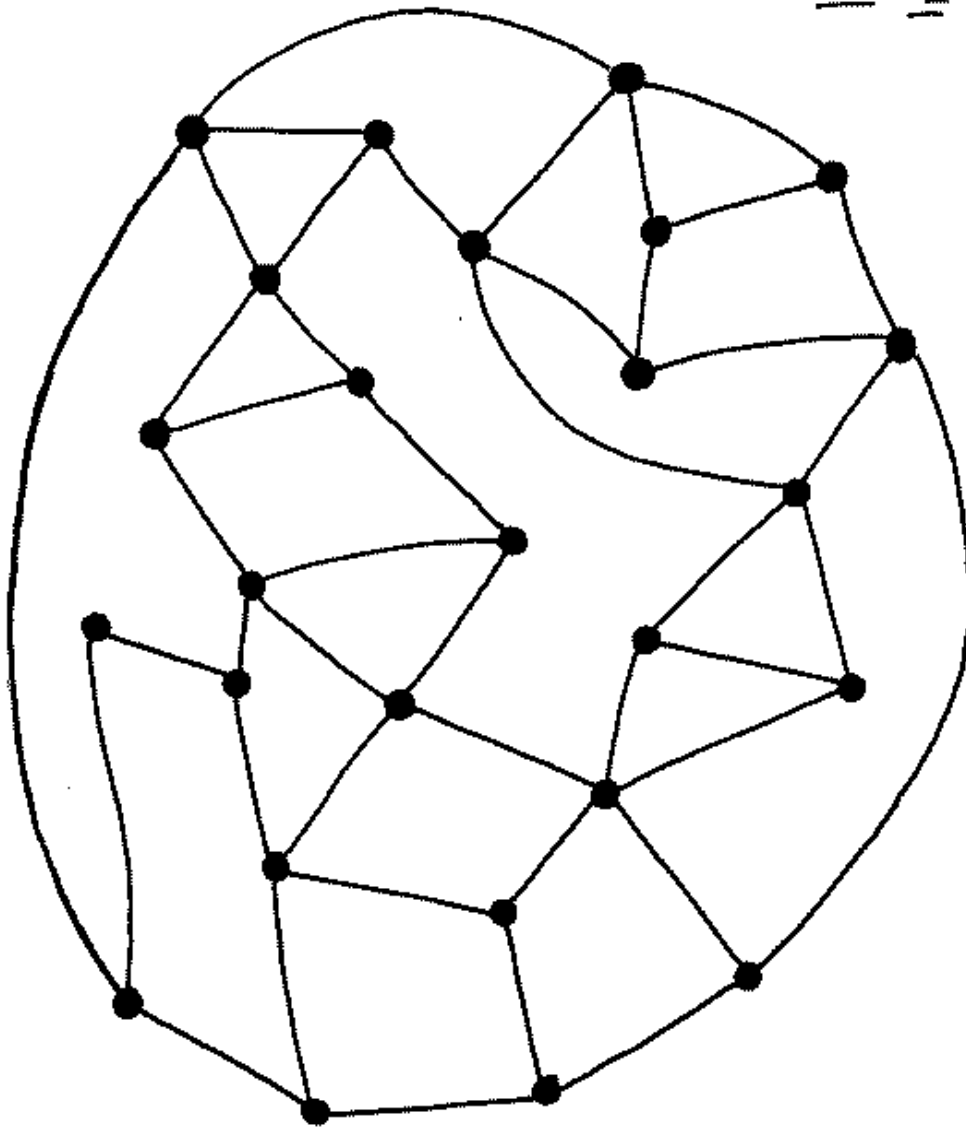
## Diskusija ir veiklos

1. Mokiniai pasiskirsto mažomis grupėmis. Kiekvienai grupei duodamas Turistų miesto žemėlapis ir keletas žymiklių. Paaškinama užduotis.
2. Mokiniam paaškinama, kaip pažymėti sankryžą, kur statomas ledų furgonas. Kitos spalvos žymikliu pažymimos sankryžos per vieną gatvę nuo furgono. Ledų furgonas skirtas žmonėms, gyvenantiems prie tų sankryžų ar gatvėse, kurios susikerta tose pažymėtose sankryžose.
3. Mokiniai eksperimentuodami žymi skirtingas ledų furgonų vietas. Kai mokiniai sudėlioja furgonus taip, kad jų vieta patogi visiems gyventojams, primenama, kad furgonai yra brangūs, todėl jų turi būti kuo mažiau. Akivaizdu, užduoties sąlygos įvykdomos, kai kiekvienoje sankryžoje pastatoma po furgoną, bet įdomesnis klausimas – kiek furgonų galima pašalinti, kad likusių vis tiek užtektų visiems gyventojams.
4. Šešių furgonų pakanka visiems Turistų miesto gyventojams. Sprendimas parodytas paveiksle dešinėje, tačiau šį sprendimą labai sunku rasti! Jei mokiniams sunku rasti mažiausią furgonų skaičių, palaukus kiek laiko galima jiems tą skaičių pasakyti ir paprašyti furgonus pažymėti grafe. Tačiau ir tai gali būti gana sunku. Mokiniam nelengva surasti sprendimą net ir su aštuoniais ar devyniais furgonais.
5. Galima paaškinti mokiniams, kaip braižomas toks žemėlapis (žr. šios veiklos sprendimus ir užuominas). Mokiniai gali pabandyti sukurti savo Turistų miestą parodytu metodu. Vieniems gali būti įdomu sukurti lengvai išsprendžiamą dëlionę, o kitiems ir tai gali būti labai sunku. Šis pavyzdys vadinamas *vienos krypties funkcija*: lengva pasiūlyti sunkiai sprendžiamą dëlionę, kai žinomas jos kūrimo nuo sprendinio metodas. Vienos krypties funkcijos yra kriptografijos pagrindas (18 ir 19 veiklos).



## Darbo lapas. Ledų furgonai

Pažymėkite, kuriose sankryžose turėtų stovėti ledų furgonai, kad būtų patogu visiems Turistų miesto gyventojams.



## Gudručiams

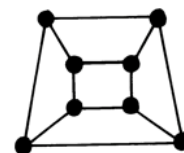
Realiaame gyvenime „Ledų furgonų“ uždavinys gana dažnas, kai reikia nustatyti pašto punktų, gaisrinių ir kitų reikalingų objektų vietas, kad būtų galima greitai aptarnauti visus gyventojus. Tačiau realiaame gyvenime negalima naudotis gudrybe, aprašyta šios veiklos skyriuje, ir lengvai išspręsti problemą. Ką daryti?

Galima pasitelkti visiškai nesudėtingą būdą: perrinkti visus įmanomus ledų furgono pastatymo variantus ir išrinkti geriausią. Kadangi Turistų mieste yra 26 gatvių sankryžos, tai yra ir 26 vietos ledų furgonui pastatyti. Nesudėtinga patikrinti visas 26 galimybes. Akivaizdu, kad nė viena iš jų netenkina uždavinio sąlygų. Dviem ledų furgonams pastatyti turime  $26 \times 25 = 650$  galimybių, nes, aišku, du furgonai nebus statomi vienoje vietoje. Patikrinti kiekvieną galimybę atskirai nėra sunku, bet patikrinti visas – varginantis ir nuobodus darbas. Be to, užtektų patikrinti pusę galimybių (325), nes nesvarbu, kuris furgonas pastatomas sankryžoje: jei patikrinamas 1 furgonas A sankryžoje, o 2 furgonas – B sankryžoje, tai nebereikia tikrinti 2 furgono A sankryžoje ir 1 furgono B sankryžoje. Pastatyti tris furgonus būtų 2600 galimybių, keturis – 14950 galimybių ir t. t. Aišku, 26 furgonų tikrai pakaktų, nes yra tik 26 sankryžos ir nėra prasmės statyti po du furgonus vienoje sankryžoje.

Kitas ledų furgonų vietų nustatymo būdas – suskaičiuoti visas įmanomas galimybes, kai sankryžos yra 26, o furgonų skaičius bet koks. Kadangi kiekvienai sankryžai yra tik dvi galimybės (yra pastatytas furgonas arba jo nėra), tai galimybių skaičius yra  $2^{26} = 67108864$ . Šis sprendimo metodas vadinamas *visiško perrinkimo algoritmu* ir užima daug laiko. Nors atrodo, kad kompiuteriai yra gana spartūs ir gali atlikti šią užduotį gana greitai, iš tikrųjų net ir spartus kompiuteris ilgai ieško sprendinio. Visiško perrinkimo algoritmo atlikimo sparta priklauso nuo to, kaip greitai patikrinama, ar galimybė yra uždavinio sprendinys, t. y. atitinka visas sąlygas. Įdomu, kiek laiko galėtų sugaišti kompiuteris tikrindamas visas  $2^{26}$  galimybių. Jei patikrinti vieną galimybę, ar ji yra sprendinys, užtruktų 1 s, tai patikrinti visas galimybes būtų sugaišta apie 67 mln. sekundžių, arba apie 777 dienų, arba dvejus metus. Net jei viena galimybė būtų tikrinama tik 0,001 s, tai per tuos dvejus metus kompiuteris galėtų patikrinti tik  $2^{36}$  galimybių. Jei kompiuteris būtų milijoną kartų spartesnis ir milijoną galimybių patikrintų per 1 s, tai per dvejus metus patikrintų miestą tik su 46 sankryžomis. O tai tikrai nedidelis miestelis. Kiek sankryžų yra jūsų mieste?

Jei visiško perrinkimo algoritmas toks lėtas, gal yra koks kitas šio uždavinio sprendimo būdas? Galima pabandyti taikyti „godumo“ principą. Pirmasis ledų furgonas statomas sankryžoje, kurioje susikerta daugiausia gatvių, antrasis – kitoje sankryžoje, kurioje vėl susikerta daugiausia gatvių ir t. t. Tačiau šio metodo rezultatas nebūtinai bus mažiausias furgonų skaičius, nes sankryža su didžiausiu gatvių skaičiumi gali būti ir ne pati geriausia vieta furgonui pastatyti pagal uždavinio sąlygas. Tai galima patikrinti kartu su mokiniais.

Aiškintis galima pradėti nuo paprastesnės užduoties. Mokiniais pasakomas furgonų skaičius ir pasiūloma išsiaiškinti, ar jis yra mažiausias. Kai kuriais atvejais tai visai nesunku. Pavyzdžiui, grafe dešinėje vaizduojamas daug paprastesnis miestas. Jei gatvės įsivaizduojamos kaip kubo briaunos, akivaizdu, kad du ledų furgonai gali būti pastatyti priešinguose kubo įstrižainės galuose. Be to, būtų galima įsitikinti, kad vieno ledų furgono tikrai nepakanka šiame mieste. Taip pat galima pabandyti įsitikinti, kad ir Turistų mieste negali būti mažiau kaip 6 furgonai.



## Apie ką visa tai?

---

Įdomu tai, kad kol kas nėra kito „Ledų furgonų“ uždavinio sprendimo metodo nei visiškai perrinkimas. Visiško perrinkimo algoritmo atlikimo laikas ilgėja eksponentiškai didėjant sankryžų skaičiui. Toks algoritmas vadinamas *eksponentinio laiko algoritmu*. Informatikoje žinomas ir *polinominio laiko* sprendimo algoritmas, kurio laikas ilgėja sankryžų skaičiaus laipsniais (kvadratu, trečiuoju ir t. t.). Toks algoritmas yra greitesnis nei eksponentinis algoritmas, kai reikia sudaryti didelius žemėlapius. Pavyzdžiui, kai viršūnių skaičius  $n$  yra didesnis už 117, tai  $n^{17}$  yra mažesnis už  $2^n$ . Ar yra polinominio laiko algoritmas „Ledų furgonų“ uždaviniui spręsti? Dar nėra, nors informatikai stengiasi jį sukurti. Lengvesnis uždavinys, kai reikia patikrinti, ar tam tikras furgonų skaičius yra mažiausias, taip pat sprendžiamas visiškai perrinkimo algoritmu. *Polinominio laiko* algoritmas šiam uždaviniui spręsti dar nėra sukurtas.

Ar šis uždavinys neprimena žemėlapių spalvinimo (15 veikla)? Turėtų! „Ledų furgonų“ uždavinys priklauso vadinamajai *minimalios dominuojančios sekos* (angl. *minimum dominating set*) uždavinių grupei, kurią sudaro tūkstančiai uždavinių, pavyzdžiui, žemėlapių spalvinimas, optimalaus maršruto paieška, tvarkaraščio sudarymas ir kt. Dar nėra žinoma, ar galima sukurti *polinominio laiko* algoritmus visiems šiems uždaviniams. Jei būtų sukurtas *polinominio laiko* algoritmas bent vienam iš šių uždavinių spręsti, jis galėtų būti pritaikytas ir visiems likusiems šio tipo uždaviniams.

Šie uždaviniai vadinami *NP pilnumo* uždaviniais. NP yra termino *nedeterministinis polinomas* santrumpa. Tai reiškia, kad uždavinys galėtų būti išspręstas per priimtina laiką, jei kompiuteris iškart galėtų apdoroti gana daug sprendinių (tai ir yra nedeterministinė dalis). Deja, neįmanoma sukurti tokio kompiuterio, nes jis turėtų būti labai didelis. Tačiau tokio kompiuterio konceptas yra iš esmės svarbus, nes NP pilnumo uždaviniai negali būti išspręsti per priimtina laiką neturint nedeterministinio kompiuterio.

Šie uždaviniai vadinami *pilnumo*, nes rastą vieno uždavinio sprendimą būtų galima pritaikyti ir kitiems tokiems uždaviniams, nors patys uždaviniai atrodo labai skirtingi: žemėlapių spalvinimas skiriasi nuo ledų furgonų statymo ir t. t. Visi kartu šie uždaviniai gali būti išspręsti arba neišspręsti.

### Daugiau informacijos

Davidas Harelas knygoje „*Algorithmics*“ pateikia keletą NP pilnumo uždavinių ir samprotauja, ar egzistuoja polinominio laiko algoritmas jiems spręsti. (The Spirit of Computing, Addison–Wesley, Reading, MA, 2nd edition, 1992. 3rd edition, 2004 (with Y. Feldman)).

Alexanderis K. Dewdney knygoje „*Turing Omnibus*“ taip pat aptaria NP pilnumą. (Press, New York, 1989).

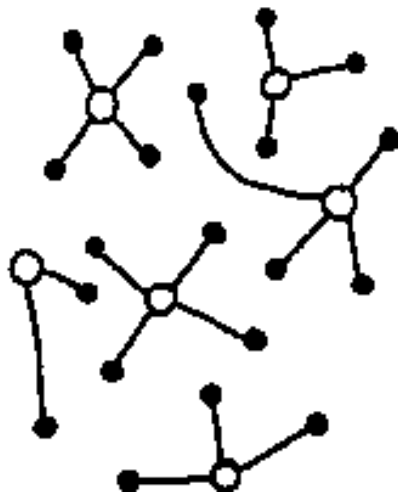
Michaelas R. Garey ir Davidas S. Johnsonas knygoje „*Computers and Intractability: A guide to the theory of NP-completeness*“ nagrinėja kelis šimtus NP pilnumo uždavinių ir NP pilnumo įrodymo metodus. (W. H. Freeman and co., New York, 1979).



## Sprendimai ir užuominos

---

Turistų miesto žemėlapis pradedamas braižyti nuo šešių viršūnių, kur turėtų stovėti po vieną ledų furgoną. Iš kiekvienos viršūnės brėžiamos gatvės, jų gale pažymimos viršūnės, kaip parodyta paveiksle.



Laisvos viršūnės sujungiamos briaunomis arba lankais, kaip parodyta paveiksle.



## 17 veikla

# Ledo kelias. Šteinerio medžiai

---

### Santrauka

Kartais tik šiek tiek pakeistas paprastas uždavinys tampa labai sunkiai sprendžiamas. Šiame skyriuje nagrinėjamas trumpiausio kelio paieškos uždavinys, panašiai kaip skyriuje „Purvinas miestas“. Tačiau šio skyriaus uždavinyje leidžiama pridėti naujų taškų, jei jie sutrumpina bendrą kelią. Uždavinys tampa daug sunkesnis ir nesusijęs su „Purvino miesto“ uždaviniu, bet algoritmavimo požiūriu atitinka „Žemėlapių spalvinimo“ ir „Ledų furgonų“ uždavinius.

### Ryšiai su ugdymo programomis

- ✓ Matematika: orientacija erdvėje
- ✓ Matematika: logika

### Gebėjimai

- ✓ Vizualizavimo
- ✓ Geometrinio pagrindimo
- ✓ Algotmavimo

### Amžius

- ✓ Nuo 7 metų

### Priemonės

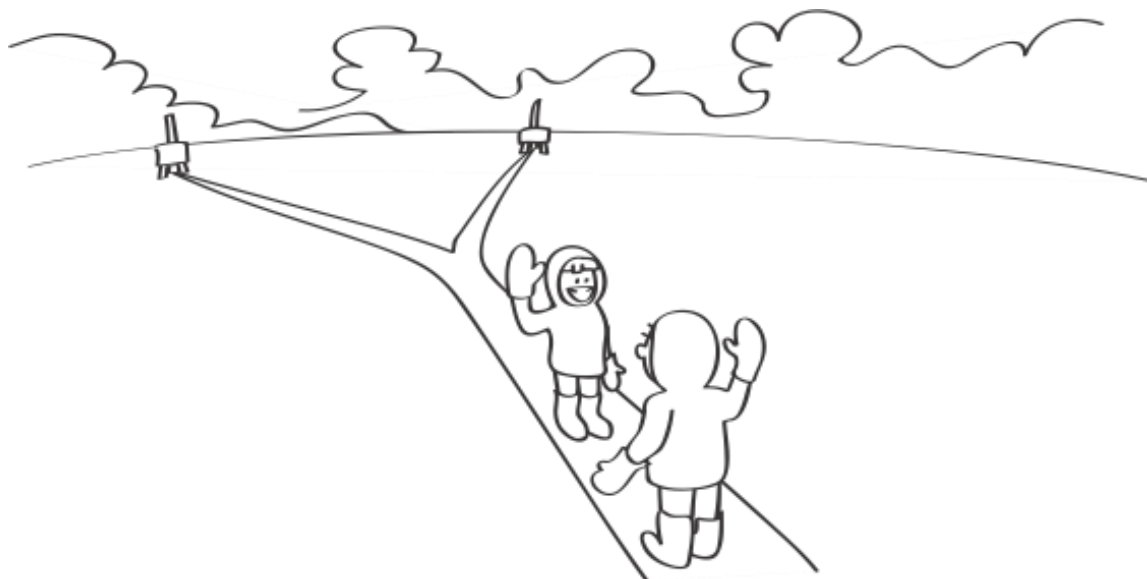
Kiekvienai mokinių grupei reikia:

- ✓ Penkių ar šešių kuolelių (tinka palapinės kuoleliai)
- ✓ Kelių metrų virvės (mažiausiai 10 m)
- ✓ Ruletės
- ✓ Rašymo priemonės ir popieriaus lapo pastaboms





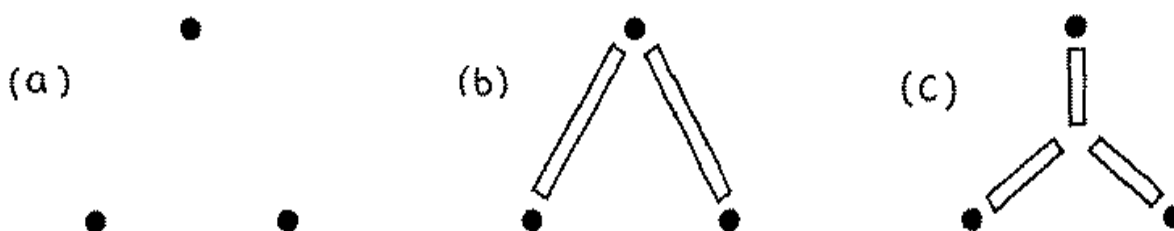
## Ledo kelias



### Ivadas

Šiaurinėje Kanados dalyje aplink didelį ežerą yra įrengti keletas gręžinių. Žiemą ežeras užšąla, jį storai užkloja sniegas. Gręžinių darbuotojai sniego valymo mašina turi pravažyti kelius per ežerą, kad galėtų susisiekti su kitomis brigadomis. Šiaurinėje Kanados dalyje žiemos labai šaltos, todėl bendras kelio ilgis turi būti kuo trumpesnis, kad būtų galima kuo greičiau kelią nuvalyti. Mokinių užduotis: nubraižyti valomus kelius per ežerą. Nėra jokių ribojimų, nes visas ežeras užšalęs ir padengtas sniegu.

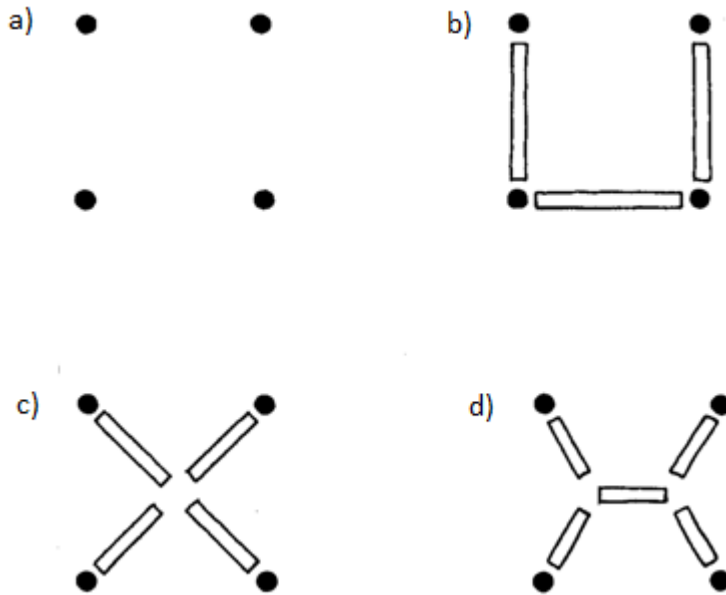
Akivaizdu, kad keliai turi būti visiškai tiesūs, nes lankai juos tik pailgina. Tačiau ne visada sujungti taškus tiesiomis linijomis yra geriausias sprendimas. Kartais, įterpus naują susikirtimo tašką, bendras kelių ilgis gali būti sutrumpintas.



Pavyzdžiui, a paveiksle pavaizduoti trys gręžiniai. Šiuos taškus galima sujungti tiesiomis linijomis, kaip parodyta b paveiksle. Kitas jungimo būdas pavaizduotas c paveiksle. Matuojant nesunku išsiaiškinti, kad c paveiksle bendras kelių ilgis yra trumpiausias. Pridėtas papildomas taškas, sutrumpinantis bendrą kelio ilgį, vadinamas Šteinerio tašku. Jakobas Šteineris (Jakob Steiner, 1796–1863) suformulavo šį uždavinį ir pirmasis pastebėjo, kad bendras kelio ilgis gali sutrumpėti pridėjus papildomą susikirtimo tašką.

## Diskusija ir veiklos

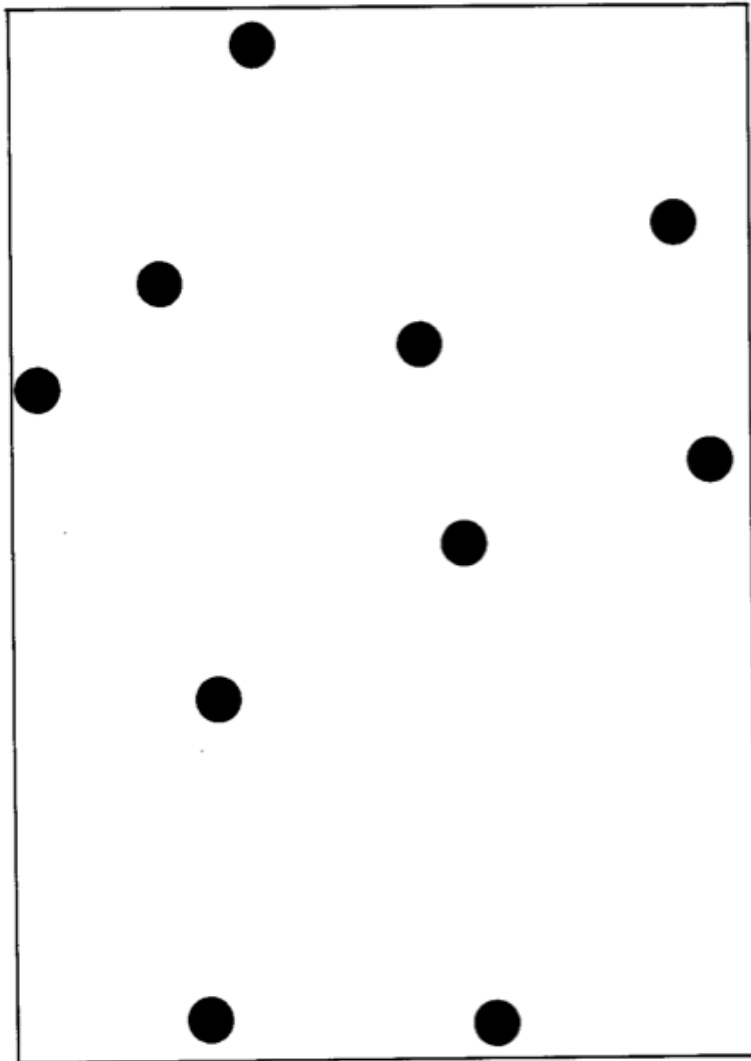
1. Užduotis aiškinama toliau paveiksle pateiktu pavyzdžiu.



- Užduotis išbandoma lauko aikštelėje. Mokiniai aikštelėje susmeigia keturis kuoliukus kvadratu, kurio kraštinės po 1 m. Iš pradžių jie nežymi Šteinerio taško, tik sujungia kuoliukus virve. Akivaizdu, kad reikia 4 m virvės. Ar būtų galima sujungti visus kuoliukus trumpesne virve?
- Toliau mokiniams siūloma surasti Šteinerio taškus. Nustačius vieną Šteinerio tašką (įsmeigus dar vieną kuoliuką kvadrato viduryje), kaip parodyta c paveiksle, reikia mažiau virvės. Bendras virvės ilgis lygus  $2\sqrt{2} = 2,83$  m. Suradus du Šteinerio taškus (įsmeigus du kuoliukus), kaip parodyta d paveiksle, panaudojama  $1 + \sqrt{3} = 2,73$  m virvės.
- Ar virvės reikėtų mažiau, jei rastumėte 3 Šteinerio taškus? (Ne. Du taškai yra geriausias variantas.)
- Diskutuojuama su mokiniais, kodėl šis uždavinys yra sudėtingas. (Nežinoma, kaip nustatyti Šteinerio taškus, todėl tenka išbandyti daug variantų.)

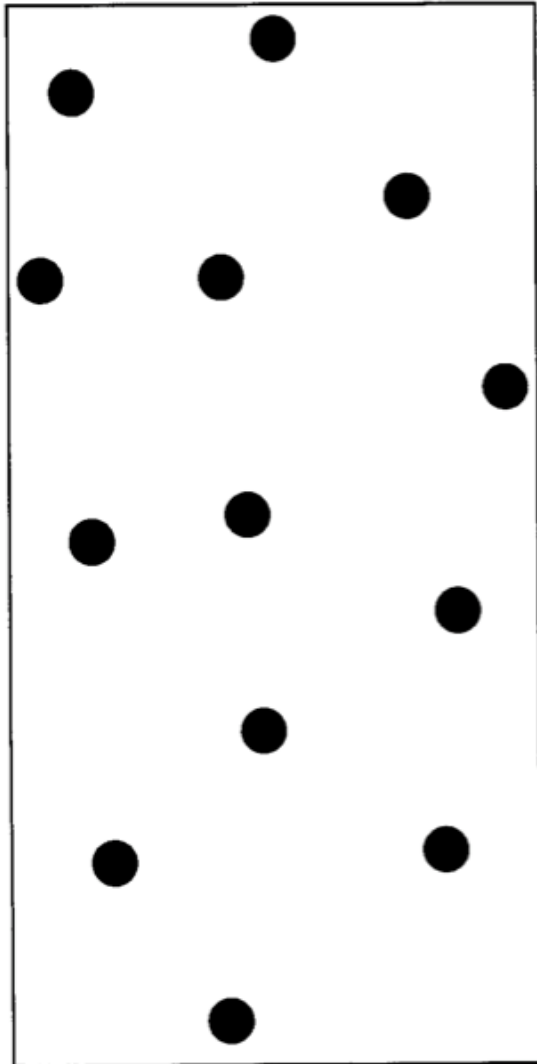
## Darbo lapas. Šteinerio medis

---



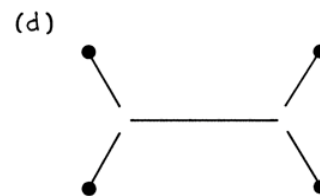
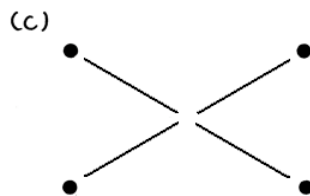
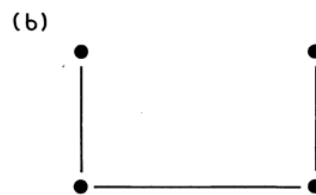
## Darbo lapas Šteinerio medis

---



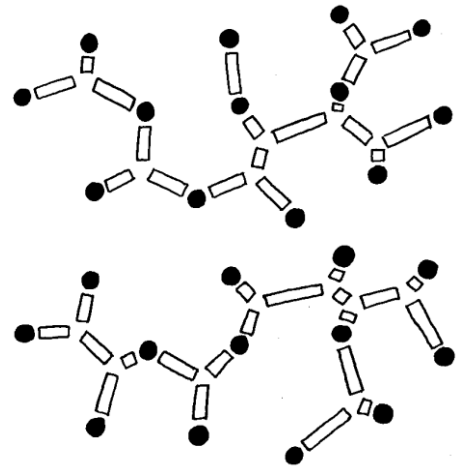
## Gudručiams

- Greitai pagrindinius uždavinius atlikę mokiniai gali bandyti rasti trumpiausią kelią stačiakampyje  $1 \times 2$  m (a paveikslas). Sujungus b variantu reikia 4 m virvės. Suradus vieną Šteinerio tašką, reikia  $2\sqrt{5} = 4,47$  m virvės (c paveikslas), kai turime du Šteinerio taškus, reikia  $2 + \sqrt{3} = 3,73$  m virvės (d paveikslas). Mokiniai galėtų pagrįsti, kodėl pridėjus vieną papildomą tašką stačiakampyje kelias sutrumpėja labiau, nei pridėjus papildomą tašką kvadrate. (Taip yra todėl, kad kai kvadratas ištempiamas į stačiakampį, tai b ir d atvejais pailgėjimų suma padidėja po vieną kartą, o c atveju padidėja abi įstrižainės).

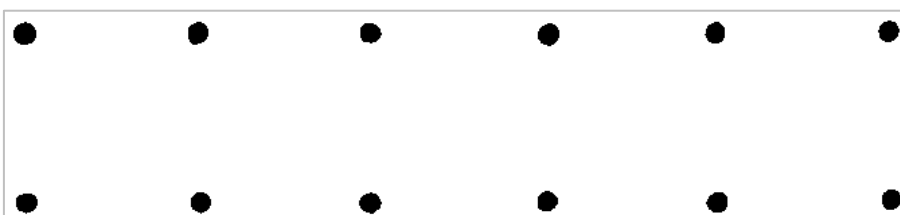


- Vyresnieji mokiniai gali nagrinėti uždavinį, kuriame yra daugiau taškų. Jie galėtų spręsti kitus darbo lapuose pateiktus uždavinius naudodami pieštukus ir trintukus arba naujas darbo lapų kopijas. Uždavinio sprendimą galima pavaizduoti ir aikštelėje, taškus sužymėti kuoliukais. Mokiniai galėtų diskutuoti tarpusavyje, kaip rasti geresnį sprendimą. (Pavyzdžių trumpiausios atstumai pavaizduoti paveiksluose dešinėje.) Pateikiami du panašūs Šteinerio medžiai rodo, kad uždavinys yra sunkiai išsprendžiamas. Čia galima pasirinkti gana daug Šteinerio taškų!

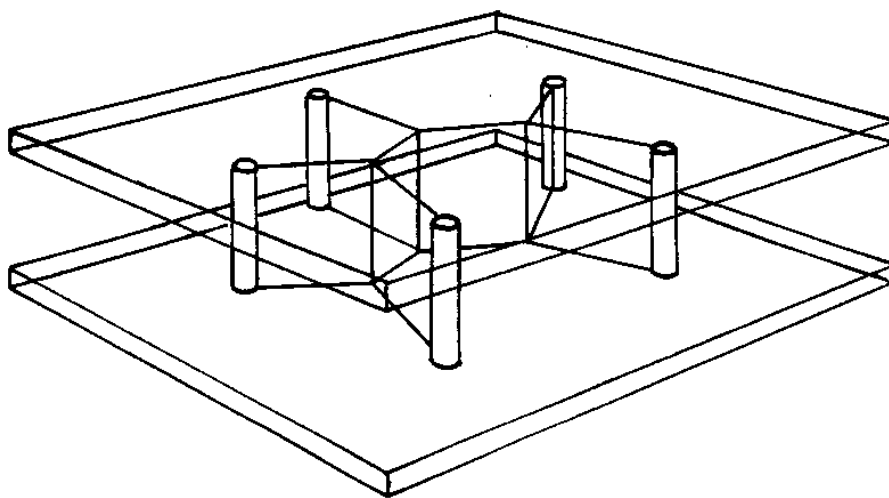
*Du galimi Šteinerio medžiai antrajam darbo lapo pavyzdžiui.*



- Toliau pateikiamas pavyzdys virvinių kopėčių uždavinio, kurį galėtų spręsti mokiniai, baigę pagrindinius uždavinius:



4. Dviejų laiptelių virvinių kopėčių uždavinys gali būti paverčiamas kvadrato uždaviniu. Trijų laiptelių virvinių kopėčių uždavinio sprendimas yra visiškai kitoks. Jį galima pabandyti nubraižyti. Keturių laiptelių virvinių kopėčių uždavinį galima paversti dviejų sujungtų kvadratų uždaviniu. Penkių laiptelių virvinių kopėčių uždavinio sprendimas yra išplėstas trijų laiptelių kopėčių uždavinys. Minimalusis Šteinerio medis virvinių kopėčių uždavinyje priklauso nuo taškų skaičiaus – ar tas skaičius yra lyginis, ar nelyginis. Jei taškų skaičius lyginis, uždavinys sprendžiamas taip, tarsi tai būtų sujungti keli kvadratai, o jei nelyginis – sprendžiamas taip, tarsi būtų kartojamas trijų laiptelių virvinių kopėčių uždavinys. Tačiau šio sprendimo įrodymas nėra lengvas.
5. Kita įdomi šių uždavinių interpretacija yra Šteinerio medžių muilo burbulai. Du permatomo plastiko lapai persmeigiami smeigėmis (ar virbalais), kaip parodyta toliau paveiksle:



Įmerkus visą konstrukciją į muilo tirpalą ir po to ištraukus, muilo burbulų plėvelė, susidariusi tarp plastiko lapų, ima judėti, ieškodama minimalios energijos būsenos, bet gana greitai viskas nurimsta – gaunamas Šteinerio medžio tinklas!

Žinoma, tai nėra įrodymas, kad gaunamas minimalusis Šteinerio medis. Muilo burbulai rado mažiausią kiekvienos dalies kelią, bet nebūtinai mažiausią bendrą kelią. Nesunkiai galima pavaizduoti visiškai kitokį Šteinerio taškų išdėstymą šiame uždavinyje.

Filmuko nuoroda: <https://youtu.be/PI6rAOWu-Og>

## Apie ką visa tai?

---

Šiame skyriuje nagrinėjami *minimalieji Šteinerio medžiai*. Jie vadinami *medžiais*, nes neturi ciklų, o tik šakas – kaip tikri medžiai; *Šteinerio medžiais*, nes į originalų medį gali būti įterpiama naujų Šteinerio taškų; *minimaliaisiais medžiais*, nes bendras tokio medžio briaunų ilgis yra mažiausias.

Įdomu tai, kad minimaliajam jungiančiajam medžiui yra sukurtas efektyvus algoritmas (14 veikla), bet minimalusis Šteinerio medis efektyvaus algoritmo neturi. Šteinerio medžių uždaviniai yra daug sunkesni, nes reikia nuspręsti, kur įterpti Šteinerio tašką, be to, tokių įterpimo galimybių yra labai daug. Tačiau tiksliai įterpti Šteinerio tašką nėra sunkiausia, kur kas sunkiau yra nuspręsti, kur apytikriai jį įterpti. Kitaip tariant, nusprendus, kur apytikriai įterpti tašką, surasti jo optimalią vietą jau ne taip sunku. Muilo burbulais tai padaroma labai efektyviai. Tą gali ir kompiuteris.

Minimalusis Šteinerio medis labai pravertė taupant lėšas telefono ryšio versle. Dar iki 1967 m. JAV vartotojų korporacija turėjo didelį privačių telefonų tinklą, kurio linijos buvo nuomojamos iš telefonų kompanijos. Mokestis buvo skaičiuojamas ne pagal faktinį reikalingą laido ilgį, bet pagal naudojamą trumpiausią tinklą. Vartotojas neprivalėjo mokėti daugiau, jei telefonų kompanija nutiesė ilgesnę liniją, nei pakaktų iki vartotojo telefono. Algoritmas, kuriuo buvo skaičiuojama, kiek reikia mokėti, nustatydamas minimalųjį jungiantįjį medį. Tačiau apie 1967 m. vartotojai pastebėjo, kad įterpus papildomą telefono linijos stotelę pakankamas atstumas iki vartotojo telefono sumažėja. Telefono kompanija buvo priversta sumažinti įkainius. Paprastai minimalusis Šteinerio medis yra tik 5–10 % trumpesnis nei minimalusis jungiantysis medis, bet mokant dideles sumas šis pokytis tampa reikšmingas. Šteinerio medžio uždavinys dar vadinamas „trumpiausiojo tinklo uždaviniu“, nes randama trumpiausią tinklą jungiančių taškų aibė.

Šteinerio medis, kaip ir anksčiau aptarti uždaviniai, yra NP pilnumo uždavinys. Didėjant taškų skaičiui, Šteinerio taškų įterpimo galimybių skaičius didėja eksponentiškai. Tai dar vienas iš anksčiau minėtų tūkstančio NP pilnumo uždavinių, kuris neturi efektyvaus sprendimo, be to, nėra žinoma, ar egzistuoja polinominio laiko algoritmas šiam uždaviniui spręsti. Žinoma tik tai, kad, jei būtų surastas polinominio laiko algoritmas šiam uždaviniui spręsti, jį būtų galima pritaikyti ir kitiems NP pilnumo uždaviniams spręsti.

Ankstesniame skyriuje buvo paaiškinta, kas yra NP pilnumas. Uždaviniai, kuriems gali būti taikomas polinominio laiko algoritmas, žymimi „P“. Pagrindinis klausimas: ar  $P = NP$ ? Atsakymas nėra žinomas ir tai didžiausia informatikos paslaptis!

Uždaviniai, sprendžiami taikant polinominio laiko algoritmus, vadinami „lengvai sprendžiamais“, nors kai kurie algoritmai yra gana lėti.

Ką galima pasakyti viršininkui, kuris liepia sugalvoti efektyvų algoritmą uždaviniui optimaliai išspręsti, o to padaryti negalima? Pavyzdžiui, kai oro linijos susiduria su faktu, kad skrydžių kaina gali būti sumažinta į skrydžių linijų tinklą įterpiančiais Šteinerio taškais. Būtų puiku įrodyti, kad geresnio sprendimo nėra, bet įrodyti neigiamus



rezultatus labai sunku, ypač informatikoje. Sumanus programuotojas gali gudrauti. Tačiau negalima tvirtai pasakyti viršininkui, kad jo paliepiamas neįvykdomas ir uždavinys sunkiai sprendžiamas. Vienaip ar kitaip, jei galima parodyti, kad tai yra NP pilnumo uždavinys, reiškia, kad jis yra ekvivalentus vienam iš tūkstančių uždavinių, kuriuos bando išspręsti daugelis informatikų įvairiose šalyse. Tai neišspręstų jums pateikto uždavinio, tačiau bent turėtumėte rimtą pasiteisinimą!



„Negaliu rasti efektyvaus algoritmo. Tikriausiai aš per kvailas.“



„Negaliu rasti efektyvaus algoritmo, nes, manau, toks algoritmas neįmanomas.“



„Negaliu rasti efektyvaus algoritmo, bet to padaryti negali ir šie protingi žmonės.“

*Trys galimybės, ką galima pasakyti viršininkui, kai nerandama efektyvaus algoritmo.*

Aišku, realiame gyvenime šie uždaviniai kyla ir turi būti sprendžiami, jiems taikomi *heuristiciniai* algoritmai, kurie neužtikrina geriausio rezultato, bet randa artimą rezultatą. Heuristiciniai algoritmai gali būti labai greiti. Jie labai praverčia realiame gyvenime, nes ir neradus geresnio sprendimo nuostolis būna minimalus. Tačiau žinojimas, kad gali būti sudarytas geresnis pamokų tvarkaraštis, geresnis koks nors tinklas arba kelių sistema, tiesiog truputį erzina.

### **Daugiau informacijos**

Animacinis filmas pagal M. Garey ir D. S. Johnsono vadovėlį „*Computers and Intractability*“.

Žurnalo „*Scientific American*“ skyrelyje „*Computer recreations*“ 1984 m. liepos mėn. išspausdintas išsamus aprašymas, kaip konstruoti Šteinerio medžius naudojant muilo burbulus.





# **V dalis**

**Informacijos šifravimas**

**Kriptografija**

# Informacijos šifravimas

Žodis „kriptografija“ sudarytas iš dviejų graikiškų žodžių: „kripto“ graikiškai reiškia „slėpti“, „graphin“ – „raštas“. Taigi kriptografija – mokslas apie slaptaraščius. Šis mokslas visada rūpėjo diplomatams, kariškiams, tačiau daugumai žmonių iki informacinių technologijų revoliucijos jis buvo visai nereikalingas. Kai atsirado kompiuterių tinklų, kai pasaulį apraizgė saitynas, kai internetu kasdien siunčiama ir gaunama svarbios informacijos, kriptografija tapo reikalinga visiems. Ji nebėra vien mokslas apie šifrų kūrimą ir jų saugumą. Per kelis pastaruosius dešimtmečius kriptografija virto matematikos ir informatikos metodų taikymo informacijos apsaugai sritimi. Apsaugoti informaciją mūsų laikais – tai ne vien tik paslėpti jos prasmę nuo tų, kuriems nederėtų jos matyti. Tai taip pat ir apsauga nuo neteisėto informacijos keitimo, klastojimo, jos naudojimo nenumatytiems tikslams.

Kartais manoma, kad kriptografija – tai slaptažodžių saugojimas kompiuteriuose ir pranešimų šifravimas, kad priešiški asmenys negalėtų jų perskaityti, tačiau iš tikrųjų taip nėra. Šiuolaikinės kompiuterių sistemos nesaugo slaptažodžių, nes, jei saugotų, bet kuris prieigą prie slaptažodžių turintis asmuo galėtų įsibrauti į visas sistemas: galėtų daryti bankų pavedimus, siųsti pranešimus apsimesdamas kitu asmeniu, skaityti slaptus failus, vadovauti kariuomenei ar net nuversti vyriausybę. Dabar slaptažodžiai yra tvarkomi „vienos krypties funkcijomis“, kurios buvo pristatytos 16 veikloje. Kriptografija taip pat nėra tik raidžių kodavimas pranešimų tekstuose: pranešimai šifruojami metodais, siejamais su itin sudėtingomis problemomis – sunkiai sprendžiamais uždaviniais, pavyzdžiui, keletas tokių sunkiai sprendžiamų uždavinių aprašyta IV dalyje.

Pasitelkiant kriptografiją galima daryti, atrodytų, neįmanomus dalykus. Šioje dalyje sužinosite, kaip galima nesunkiai apskaičiuoti grupės žmonių vidutinį amžių, kai nė vienas grupės narys nenurodo savo amžiaus; kaip du vienas kitu nepasitikintys žmonės gali mesti monetą ir susitarti, kuria puse ji nukrinta, net jei jie yra skirtinguose miestuose ir negali abu vienu metu matyti tos metamos monetos; kaip saugiai užkoduoti slaptus pranešimus, kuriuos galėtų iškoduoti tik vienas žmogus, nors ir visi kiti žinotų, kaip jie užkoduoti.

## Mokytojui

Aprašant šios dalies veiklas remiamasi šiuolaikinės kriptografijos metodais, kurie iš esmės labai skiriasi nuo įprasto žmonių supratimo apie slaptumą ir kompiuterius.

Čia norima supažindinti su dviem pagrindinėmis idėjomis. Pirmoji – tai protokolas – formalus transakcijos patvirtinimas. Protokolai reikalingi ne tik diplomatiniams santykiams ar etiketo taisyklėms nusakyti – kompiuteriams jie taip pat reikalingi. Tariamai sunkus uždavinys gali būti išsprendžiamas taikant stulbinančiai paprastą protokolą. 18 veikla parodoma, kaip grupė bendradarbiaujančių žmonių nesunkiai apskaičiuoja savo grupės amžiaus (arba pajamų) vidurkį nežinodami nė vieno grupės nario amžiaus (ar pajamų). Antroji idėja – skaičiavimų sudėtingumo priklausomybė nuo individų interaktyvios veiklos kompiuteriu. Iš 19 veiklos matyti, kaip du nebūtinai vienas kitu pasitikintys žmonės, bendraudami tik telefonu, gali susitarti, kuria puse

krinta išmesta moneta. (Ši veikla supažindina su Bulio logika ir jos taikymu.) 20 veikla supažindina, kaip žmogus skaičiavimo metodais gali saugiai užkoduoti pranešimus, net jei užkodavimo metodas yra visiems žinomas.

Atlikti kai kurias iš šių veiklų yra sunku, ypač 20 veiklą. Mokytojui reikia motyvuoti visą klasę, įtraukti mokinius į veiklas ir juos nustebinti, kad tokie dalykai, kurie daugumai atrodo neįmanomi, gali būti padaryti. Esminis dalykas – sukurti mokiniams netikėtumo atmosferą, aptariant reikiamą atlikti veiklą išlaikyti mokinių susidomėjimą, kad jie matytų ne vien smulkmenas, pavienius sunkumus, bet sugebėtų aprėpti nuostabių galimybių teikiančią visumą. Šios dalies veiklos yra techniškai sudėtingos, kartais tai tikri iššūkiai. Jei jos per sunkios, galima šią dalį praleisti ir pereiti prie VI dalies, kuri yra visiškai kitokia nei kitos knygos dalys ir neturi techninių aspektų.

### **Tiksliai mąstantiems**

Kompiuteriai įsiveržia į kasdienį gyvenimą, o kriptografijos taikymas tampa kasdiene tendencija. Dauguma žmonių nežino, ką gali šiuolaikinės kriptografijos protokolai. Didelės organizacijos (vyriausybines ir komercines) naudoja įvairias informacines sistemas, kurios apima ir privačią informaciją, o tam tikri technokratai sprendžia, kaip ta informacija turi būti tvarkoma, kas turi būti renkama, kas viešai prieinama ir t. t. Jei žmonės daugiau žinotų apie šiuolaikinių technologijų suteikiamas galimybes, galėtų aktyviau dalyvauti priimant šiuos sprendimus.

Ši medžiaga apie informaciją slepiančius protokolus, kriptografijos protokolus ir viešojo rakto kriptografiją yra gana sudėtinga. Tačiau pačios idėjos gana paprastos, nors techninius jų aspektus be gilios konceptų analizės ir sunku suvokti. Praktinėse situacijose, pavyzdžiui, užsiimant elektronine prekyba, techninės detalės paslepamos kompiuterio programose, todėl galima lengvai taikyti naujas šifravimo technologijas. Tačiau vis tiek svarbu suprasti idėjas, kuriomis šios šifravimo technologijos grindžiamos, kad įgytume daugiau patirties kriptografijoje.

Valstybės domisi kriptografijos sistemomis ne tik dėl to, kad nori išlaikyti savo informacijos ir keitimosi ja slaptumą, bet ir dėl to, kad savo informaciją dažnai užšifruoja ir nelegalia veikla užsiimantys asmenys (pavyzdžiui, narkotikų prekeiviai, teroristai). Jei, pavyzdžiui, jie užšifruoja savo telefoninius pokalbius, tų pokalbių pasiklausyti įmanoma tik žinant iššifravimo metodus. Šių metodų išaiškinimo ar panaši teisėsaugos institucijų veikla kelia daug diskusijų: vieniems žmonėms atrodo, kad reikia plėsti kriptografijos sistemų galimybes, o kiti jaučiasi suvaržyti, kai vyriausybės turi galimybių stebėti jų privačią komunikaciją. JAV Vyriausybė apribojo kai kurių kriptografijos metodų naudojimą ir prilygino juos karo ginkluotei, kuri tampa pavojinga, kai pakliūva į blogas rankas. Daug diskusijų sukėlė JAV nacionalinės saugumo agentūros sukurta lustų sistema „Clipper Chip“, kurią telekomunikacijos kompanijos naudojo balsui perduoti. Šios sistemos pagrindas buvo raktų deponavimas (angl. *keyescrow*). Kiekvienam naujam telefonui ar kitam prietaisui šia lustų sistema galėjo būti suteikiamas kriptografijos raktas, kurį būtų galėjusi turėti ir Vyriausybė. Jei kuriai nors valstybės agentūrai reikėtų pasiklausyti pokalbių tokiu telefonu, ji būtų galėjusi naudotis šiuo raktu. JAV teisingumo organai norėjo, kad šis lustas būtų naudojamas visuose komunikacijų prietaisuose, tačiau tai sulaukė piliečių pasipriešinimo dėl



grėsmės privatumui. Taigi visos kriptografijos sistemos yra techniškai įmanomos, bet nebūtinai politiškai priimtinos.

Kriptografija taikoma daug plačiau, ne tik pranešimams šifruoti. Ji pasitelkiama nustatant asmens tapatybę, pranešimo siuntėją. Kai negalima nustatyti tapatybės, neįmanoma elektroninė komercija. Taip pat neįmanomas ir elektroninis balsavimas: žmonės gali balsuoti elektroniškai nebijodami, kad kas nors (net ir paleidęs balsavimo sistemą) sužinos, už ką jie balsavo, tačiau vis dar neleidžiama balsuoti daugiau nei vieną kartą. Dar vienas pavyzdys – kortų žaidimas telefonu. Šis pavyzdys atrodo gana nereikšmingai, tačiau tik tol, kol nepagalvojama, kad verslo sandoriai yra labai panašūs į pokerio žaidimą.

Dažnai šie dalykai atrodo neįmanomi. Kaip galima sumaišyti kortų kaladę telefonu, jei žaidžiama su nepažįstamu žmogumi, kuriuo galbūt negalima pasitikėti? Kaip galima nustatyti, ar gautas laiškas yra originalus, o galbūt kas nors jį paėmė, modifikavo, užšifravo ir išsiuntė? Jei visų šių dalykų nebūtų galima nustatyti ar išsiaiškinti, tai nebūtų galima tvarkyti verslo elektroninėje erdvėje. Reikia sutrukdyti nusikaltėliams klastoti prieigas prie banko sąskaitų perimant telefono liniją tarp pardavimo vietos terminalo ir banko. Reikia sutrukdyti verslo konkurentams kenkti kuriant neteisingus pranešimus ar sutartis. Šiuolaikinės kriptografijos metodai gali išspręsti aprašytąsias problemas. Šios dalies veiklos parodo, kaip tai galima padaryti.

Keletas knygų apie šifravimą ir dešifravimą (šifrų nulaužimą):

Francis Harry Hinsley ir Alan Stripp(eds) „Codebreakers: the inside story of Bletchley Park“ (Oxford University Press, 1993) – ši knyga pasakoja, kaip pirmaisiais kompiuteriais per Antrąjį pasaulinį karą buvo iššifruojama informacija.

Įdomi matematiko Viliaus Stakėno knyga „Šifrų istorijos“ (Vilnius, TEV, 2005).



## 18 veikla

# Dalijimasis paslaptimis. Informacijos slėpimo protokoliai

---

### Santrauka

Kriptografijos metodai leidžia dalytis informacija su kitais žmonėmis ir kartu išlaikyti itin aukštą privatumo lygį. Šiame skyriuje aptariama, kaip galima dalytis neatskleista informacija: mokinių grupė skaičiuoja savo grupės amžiaus vidurkį, nors nežino tikslaus grupės narių amžiaus.

### Ryšiai su ugdymo programomis

- ✓ Matematika: sudėtis ir vidurkis

### Gebėjimai

- ✓ Vidurkio skaičiavimo
- ✓ Bendradarbiavimo

### Amžius

- ✓ Nuo 7 metų

### Priemonės

Kiekvienai mokinių grupei reikia:

- ✓ Užrašų knygelės ar sąsiuvinio
- ✓ Rašiklio



# Dalijimasis paslaptimis



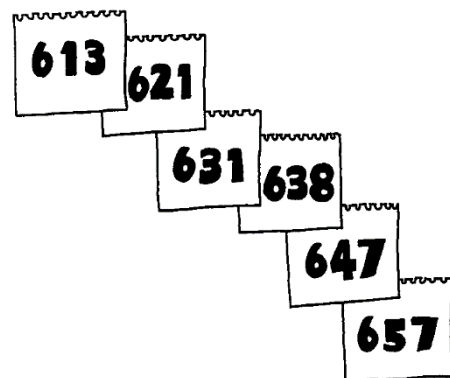
## Ivadas

Atlikdami šią veiklą mokiniai skaičiuoja savo grupės amžiaus vidurkį, nors nežino tikslaus kiekvieno grupės mokinio amžiaus. Lygiagrečiai kitos grupės gali skaičiuoti grupės gaunamų dienpinigių vidurkį. Šių statistinių duomenų skaičiavimas ypač tinkamas suaugusiesiems – juk jiems labiau rūpi informacija apie amžių ar pajamas.

Grupėse turi būti bent po 3 mokinius.

## Diskusija

1. Paaiškinama, kad grupių mokiniai vieni kitiems negali pasakyti savo tikslaus amžiaus (ar dienpinigių sumos). Jie turi suskaičiuoti amžiaus (dienpinigių) vidurkį nežinodami vienas kito amžiaus (dienpinigių sumos). Mokinių paklausiama, ar jie tiki, kad tai įmanoma padaryti, ir kaip tai būtų galima padaryti.
2. Pasirenkama 6–10 mokinių. Pirmajam mokiniui duodama užrašų knygelė ir rašiklis, tada paprašoma užrašyti bet kokį triženklį skaičių. Pavyzdyje dešinėje atsitiktinai parinktas skaičius 613.
3. Pirmasis mokinys išplėšia lapą su užrašytu atsitiktiniu skaičiumi. Jis prideda savo amžių prie pirmojo skaičiaus ir užrašo gautą rezultatą antrajame lape. Pavyzdyje pirmojo mokinio amžius yra 8, todėl antrasis triženklis skaičius yra 621. Išplėštas lapas nerodomas kitiems mokiniams.
4. Užrašų knygelė perduodama antrajam mokiniui. Jis išplėšia lapą, prideda savo amžių prie užrašyto lape skaičiaus ir užrašo gautą rezultatą trečiajame lape. Pavyzdyje antrojo mokinio amžius yra 10 metų, todėl užrašoma 631.
5. Tai tęsiama, kol visi mokiniai užrašo skaičius.



6. Užrašų knygelė grąžinama pirmajam mokiniui. Mokinys atima savo sugalvotą skaičių iš užrašyto paskutinio skaičiaus. Pavyzdyje užrašų knygelė perėjo per penkių mokinių rankas, paskutinis užrašytas skaičius – 657. Iš 657 atimamas sugalvotas skaičius 613. Gaunama 44. Tai visų mokinių amžiaus suma. Šią sumą padalijus iš 5 gaunamas grupės mokinių amžiaus vidurkis – 8,8.
7. Pabrėžiama, kad nė vieno mokinio amžius nebus žinomas, kol nebus parodyti išplėstieji lapai su skaičiais.

### **Gudručiams**

Ši sistema gali būti taikoma slaptai balsuojant, kai kiekvienas balsuojantysis prideda vienetą, jei balsuoja „taip“, arba 0, jei balsuoja „ne“. Žinoma, jei kas nors prideda daugiau kaip vieną (arba mažiau kaip 0), balsavimas yra neteisingas. Taip pat rizikuojama sukelti įtarimų, jei visi balsuoja „taip“, nes balsų „taip“ skaičius būna didesnis už balsavusių žmonių skaičių.



## Apie ką visa tai?

---

Kompiuteriuose saugoma labai daug mūsų asmeninės informacijos: banko sąskaitų likučiai, socialinių tinklų informacija, kiek mokame mokesčių, kiek galioja turimas vairuotojo pažymėjimas, kokie mūsų egzaminų rezultatai, medicininiai įrašai ir pan. Šios informacijos privatumas labai svarbus, tačiau kai kuria informacija mums reikia dalytis su kitais. Pavyzdžiui, parduotuvėje mokant už prekes banko kortele, pardavėjui reikia įsitikinti, kad pirkėjas turi lėšų savo banko sąskaitoje.

Dažnai pateikiama daugiau informacijos, negu iš tikrųjų reikia. Pavyzdžiui, kai atliekamas elektroninis mokėjimas, pardavėjas gauna pirkėjo banko pavadinimą, sąskaitos numerį, vardą ir pavardę. Be to, bankui perduodama, kur asmuo perka. Iš banko gaunamų privačių kliento duomenų būtų galima sukurti to kliento profilį: kur perkami degalai, kur bakalėjos prekės, kiek ir kur išleidžiama per dieną. Mokant grynaisiais pinigais šios informacijos nebūtų galima sužinoti. Dauguma žmonių nekreipia dėmesio į savo asmens duomenų dalijimą, tačiau visada yra tikimybė, kad privačiais duomenimis gali būti piktnaudžiaujama: jie gali būti naudojami tikslinei rinkodarai (pavyzdžiui, siunčiama kelionių reklama žmonėms, daug išleidžiantiems kelionių bilietams), jais disponuojant galima diskriminacija (pavyzdžiui, geresnių paslaugų siūlymas pasiturintiems bankų klientams) ar šantažas (pavyzdžiui, grasinimai pavišinti abejotiną sandorį). Visada galima pakeisti pirkimo būdą, jei manoma, kad perkančiojo privačiais duomenimis kas nors neteisėtai pasinaudos.

Nors nurodyti privatumo pažeidimai priimtini daugumai žmonių, jau esama kriptografijos protokolų, kurie leidžia elektronines finansines operacijas atlikti tokiu pačiu privatumo lygiu, kaip mokant grynaisiais. Sunku patikėti, kad pinigai gali būti pervedami iš jūsų banko sąskaitos į parduotuvės sąskaitą niekam nežinant, iš kurios sąskaitos ir į kurią jie pervedami. Ši veikla leidžia įsitikinti, kad tokia operacija įmanoma: abiejose situacijose ribojamas informacijos dalijimasis, o tai įmanoma pasiekti „protingu“ protokolu.

### Daugiau informacijos

Davido Chaumo straipsnyje „Security without identification: transaction systems to make Big Brother obsolete“ pateikiama paprastų informacijos slėpimo protokolų pavyzdžių, kaip gali būti atliekamos visiškai privačios elektroninės finansinės operacijos. Straipsnis išspausdintas 1985 m. žurnale „Communications of the ACM“.





## 19 veikla

# Monetos metimas. Kriptografijos protokolai

---

### Santrauka

Šia veikla sprendžiamas paprastas, bet iš pirmo žvilgsnio atrodantis neįmanomas uždavinys. Du nepažįstami ir nebūtinai vienas kitu pasitikintys žmonės, bendraujantys tik telefonu, meta monetą ir priima nešališką sprendimą, kas atsivers: herbas ar skaičius.

### Ryšiai su ugdymo programomis

- ✓ Matematika: loginis argumentavimas
- ✓ Matematika: Bulio algebra

### Gebėjimai

- ✓ Bulio algebros taikymo
- ✓ Funkcijų taikymo
- ✓ Galvosūkių sprendimo

### Amžius

- ✓ Nuo 9 metų

### Priemonės

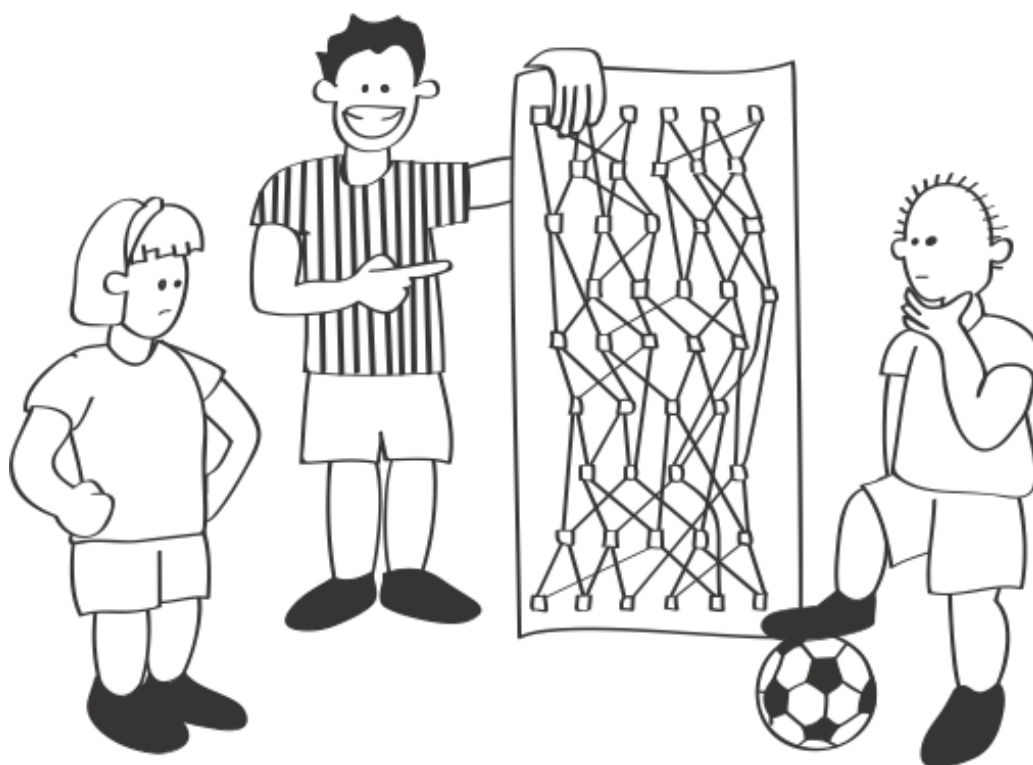
Kiekvienai grupei reikia:

- ✓ Darbo lapo „Monetos metimas“
- ✓ Po pakelį dviejų skirtingų spalvų sagų ar figūrėlių



## Peru monetos metimas

---



### Ivadas

Šią veiklą sukūrė vienas Peru mokytojas, dirbdamas su mokiniais. Veiklos istoriją galima pritaikyti savo šaliai.

Limos ir Kusko futbolo komandos turi išsiaiškinti, kuri taps šalies čempionė, tačiau niekaip negali susitarti, kur turėtų vykti rungtynės – Limoje ar Kuske. Paprasčiausias būdas tai nuspręsti – mesti monetą, bet abu miestus skiria didelis atstumas. Alisa, atstovaujanti Limai, ir Benitas, atstovaujantis Kuskui, negali skirti tiek pinigų ir laiko, kad būdami kartu vienoje vietoje galėtų mesti monetą. Ar jie gali tai padaryti telefonu? Alisa galėtų mesti monetą, o Benitas galėtų pasirinkti herbą arba skaičių, bet tai gali būti nesąžininga. Jei Benitas pasakytų „herbas“, tai Alisa galėtų pasakyti, kad iškrito skaičius, ir Benitas niekada nelaimėtų. Alisa paprastai neapgaukinėja, bet tai svarbios rungtynės, todėl pagunda labai didelė. Net jei Alisa ir pasakytų tiesą, ar Benitas ja patikėtų?

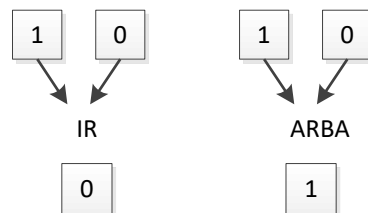
**Pastaba.** Mokiniai geriau atliktų šią veiklą, jei būtų susipažinę su dvejetainiais skaičiais (1 ir 4 veikla) ir būtų matę 16 veiklos vienos krypties funkcijos pavyzdį.

Jie nusprendė sudaryti schemą, kuri turėtų du loginius elementus – IR ir ARBA. Tai padaryti jie gali telefonu, nors būtų gana nuobodu (galima naudotis ir el. paštu). Kuriantieji schemą nori būti tikri: ji bus tokia sudėtinga, kad nė vienas negalės sukčiauti. Galutinė schema yra abiem žinoma.

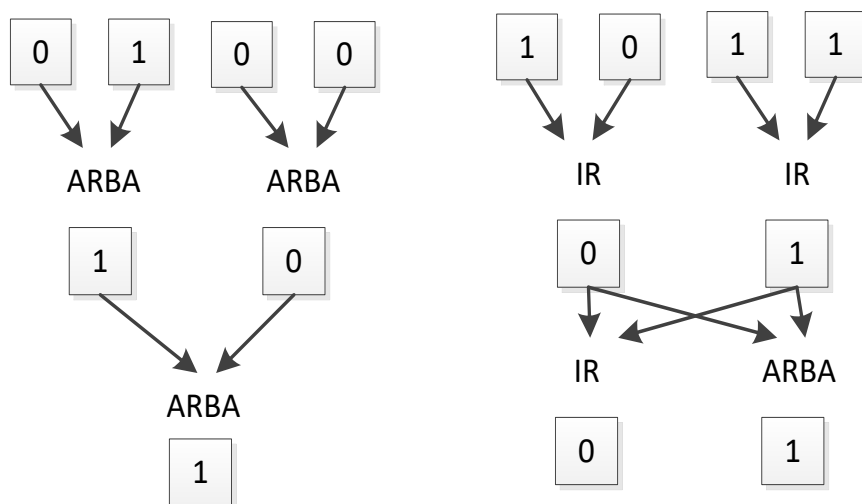


## Diskusijos

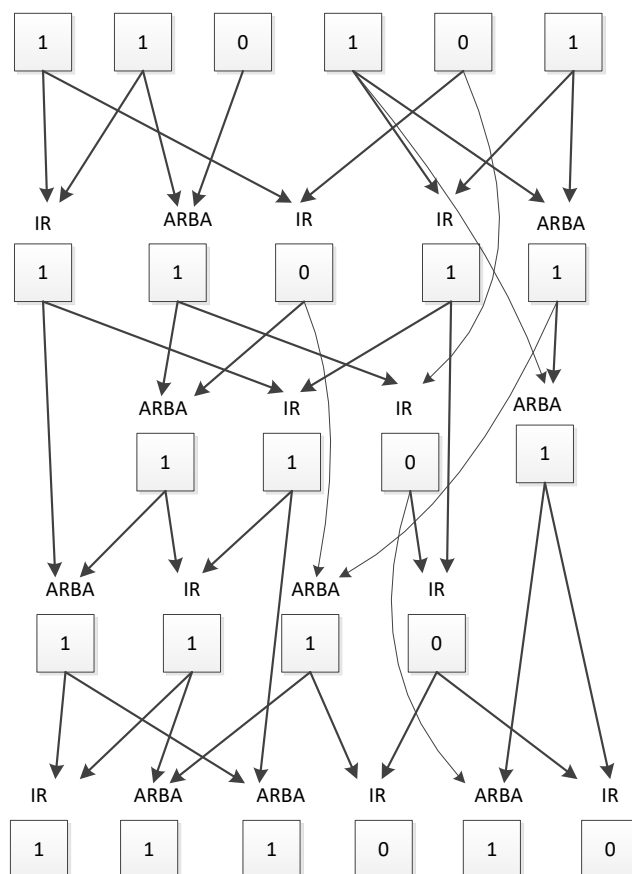
Loginių elementų IR ir ARBA taisyklės yra labai paprastos. Gali būti du įvedimai 0 arba 1, kurie atitinkamai reiškia „netiesa“ arba „tiesa“. Jei abu įvedimai yra 1 („tiesa“), loginio elemento IR išvedimas yra 1 („tiesa“), visais kitais atvejais – 0 („netiesa“). Pavyzdžiui, paveiksle dešinėje elementas IR turi du įvedimus 1 ir 0, jo išvedimas lygus 0. Loginio elemento ARBA išvedimas yra 0 („netiesa“), jei abu įvedimai yra 0, arba 1 („tiesa“) visais kitais atvejais. Pavyzdyje kairėje elemento ARBA išvedimas yra lygus 1, kai įvedimai yra 1 ir 0.



Vieno elemento išvedimas gali būti kito elemento (arba kelių elementų) įvedimas. Toliau esančiame pavyzdyje kairiosios schemos dviejų elementų ARBA išvedimas yra trečiojo elemento ARBA įvedimas. Tokios schemos rezultatas yra 1, jei bent vienas iš keturių pradinių įvedimų yra 1. Dešiniojoje schemoje aukštesniųjų elementų IR išvedimai yra žemesniųjų schemos elementų IR ir ARBA įvedimai. Ši schema turi du išvedimus.



Peru monetai mesti reikia netgi sudėtingesnės schemos. Toliau pavaizduota schema turi 6 įvedimus ir 6 išvedimus. Pateikiamas galimas schemos įvedimų ir išvedimų pavyzdys:



Pagal šią schemą gali būti metama moneta telefonu toliau aprašytu būdu. Alisa pasirenka šešis pradinius įvedimus (nulis arba vienetus), kurių nesako Benitui. Sekdama schemas rodyklėmis atlieka numatytus veiksmus ir gautus šešis išvedimus nusiunčia Benitui. Gavęs Alisos siųstus išvedimus Benitas turi atspėti, ar buvo įvestas lyginis, ar nelyginis skaičius vienetų, t. y. jis turi atspėti Alisos įvedimų lyginumą. Jei schema yra pakankamai sudėtinga, Benitas nesiaiškina atsakymo, o tiesiog spėja (rinkdamasis atsakymą jis gali net mesti monetą!). Benitas laimi, taigi papildomos rungtynės vyksta Kusko mieste, jei jo spėjimas yra teisingas. Alisa laimi, vadinasi, rungtynės vyksta Limoje, jei Benito spėjimas yra neteisingas. Kai Benitas pasako Alisai savo spėjimą, Alisa parodo savo įvedimus, kad Benitas galėtų įsitikinti, jog viskas buvo teisinga.

1. Mokiniai suskirstomi į grupes. Kiekvienai grupei duodamas darbo lapas, kuriame nubraižyta schema, keletas žaidimo figūrėlių ir paaiškinamas uždavinys. Mokiniam bus įdomiau, jei įsivaizduos, kad reikia suorganizuoti savo ir kitos mokyklos komandų rungtynes. Susitariama dėl figūrėlių spalvų, pavyzdžiui, raudona reiškia 0, o mėlyna – 1 ar panašiai. Mokiniai pasižymi spalvas darbo lapo viršuje esančioje legendoje.
2. Mokiniam parodoma, kaip išdėlioti figūrėles schemas įvedimų kvadratėliuose. Tada paaiškinami elementų IR ir ARBA išvedimai, surašyti darbo lapo apačioje. Mokiniam galima pasiūlyti nuspalvinti schemų kvadratėlius sutartinėmis spalvomis.



3. Parodoma, kaip sekant schemas rodyklėmis ir atliekant nurodytus veiksmus dėliojamos figūrėlės ant kvadratėlių ir šitaip apskaičiuojami išvedimų rezultatai. Viskas turi būti atlikta kruopščiai. Toliau lentelėje (mokiniam ji nerodoma) pateikiami visi įmanomi įvedimai ir jų galimi išvedimai, jei kam nors kiltų abejonių.

Įvedimas	000000	000001	000010	000011	000100	000101	000110	000111
Išvedimas	000000	010010	000000	010010	010010	010010	010010	010010
Įvedimas	001000	001001	001010	001011	001100	001101	001110	001111
Išvedimas	001010	011010	001010	011010	011010	011010	011010	011111
Įvedimas	010000	010001	010010	010011	010100	010101	010110	010111
Išvedimas	001000	011010	001010	011010	011010	011010	011010	011111
Įvedimas	011000	011001	011010	011011	011100	011101	011110	011111
Išvedimas	001010	011010	001010	011010	011010	011010	011010	011111
Įvedimas	100000	100001	100010	100011	100100	100101	100110	100111
Išvedimas	000000	010010	011000	011010	010010	010010	011010	011010
Įvedimas	101000	101001	101010	101011	101100	101101	101110	101111
Išvedimas	001010	011010	011010	011010	011010	011010	011010	011111
Įvedimas	110000	110001	110010	110011	110100	110101	110110	110111
Išvedimas	001000	011010	011010	011010	011010	111010	011010	111111
Įvedimas	111000	111001	111010	111011	111100	111101	111110	111111
Išvedimas	001010	011010	011010	011010	011010	111010	011010	111111

4. Kiekviena grupė turi išsirinkti savo „Alisą“ ir „Benitą“. Grupė gali pasidalyti pusiau – vieni atstovauja Alisai, o kiti – Benitui. Alisa pasirenka įvedimus ir apskaičiuoja išvedimus. Juos pasako Benitui, o šis bando atspėti įvedimo lyginumą (lyginis ar nelyginis vienetų skaičius buvo įvestas). Aišku, Benito atsakymas yra paprastas spėjimas. Alisa visiems pasako, kokie buvo įvedimai. Benitas laimi, jei atspėja lyginumą. Jis gali patikrinti pagal schemą, ar Alisa nepakeitė savo pasirinkimo.

Šiame etape monetos metimas baigiamas.

Benitas galėtų sukčiauti, jei rastų įvedimus, kurie pateikia Alisos rezultatą. Todėl Alisai svarbu, kad grandinės funkcija būtų vienos krypties, kaip aptarta 16 veiklos skyriuje. Vienos krypties funkcijos rezultatą labai lengva apskaičiuoti, kai žinomi pradiniai įvedimai, tačiau labai sunku nuspėti įvedimus, kai žinomas rezultatas.



Alisa galėtų sukčiauti, jei rastų du skirtingus išvedimus, kurie pateikia vienodą rezultatą. Kad ir ką tada Benitas spėtų, Alisa galėtų pateikti kitą atsakymą. Todėl Benitas turi įsitikinti, kad schema neatvaizduoja skirtingų įvedimų vienam rezultatui.

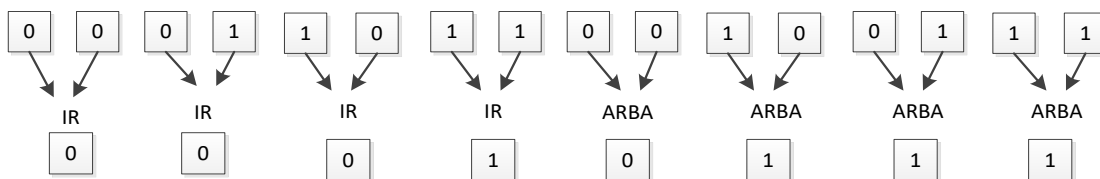
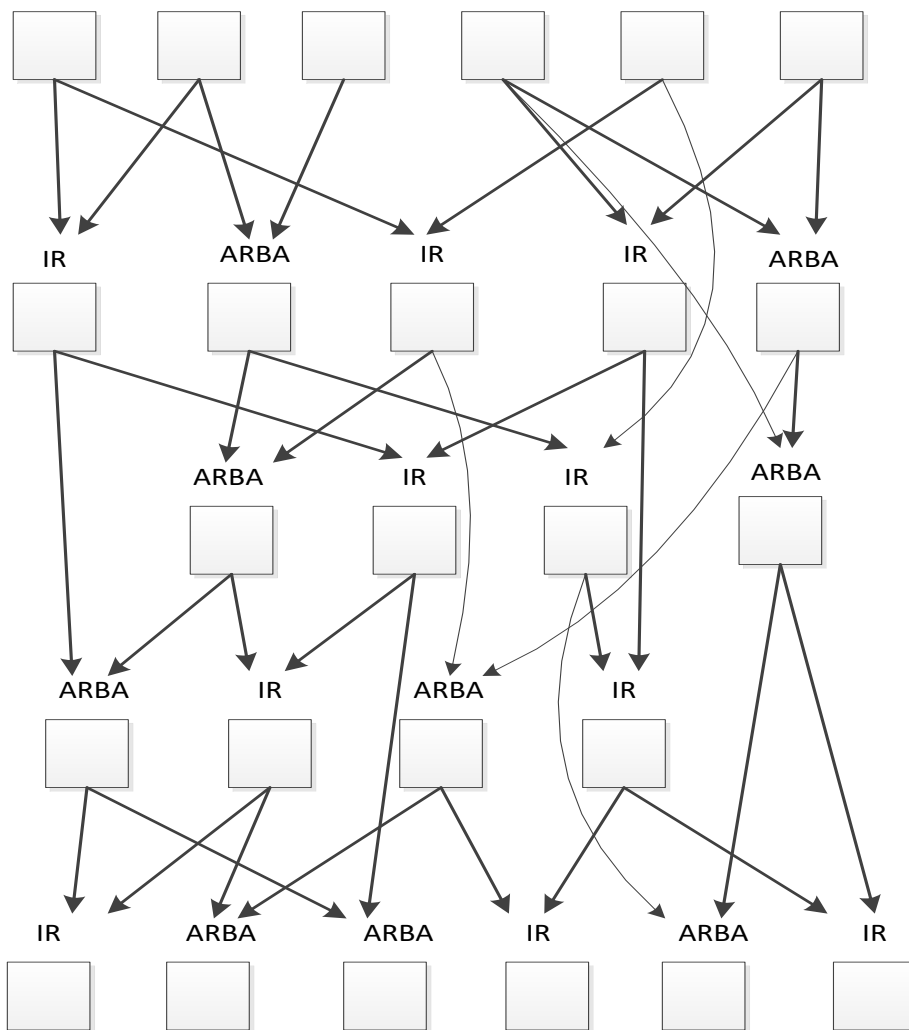
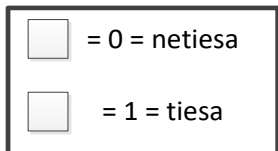
5. Reikėtų stebėti, ar mokiniams pavyks rasti būdą, kuriuo Alisa arba Benitas galėtų sukčiauti. Iš lentelės pirmosios eilutės matyti, kad keletas skirtingų įvedimų, pavyzdžiui, 000001, 000011 ir 000101, pateikia tą patį išvedimą 010010. Nurodydama išvedimą 010010 Alisa gali pasirinkti įvedimą 000001, jei Benitas spėja, kad įvedimo vienetų skaičius lyginis, arba įvedimą 000011, jei Benitas spėja, kad įvedimo vienetų skaičius nelyginis.

Pagal šią schemą Benitui sunku sukčiauti. Tačiau jei išvedimas būtų lygus 011000, tai įvedimas gali būti tik 100010, nes kitos galimybės nėra (galima įsitikinti peržiūrint lentelę). Jei Alisa pasako šį rezultatą, Benitas gali spėti lyginį lyginumą ir būti tikras, kad jo atsakymas teisingas. Kompiuterių sistemos naudoja kur kas daugiau bitų, todėl ir galimybių yra kur kas daugiau (kiekvienas papildomas bitas dvigubina galimybių skaičių).

6. Mokiniai galėtų bandyti sukurti savo schemų šiam žaidimui. Galėtų sugalvoti schemą, kuri padėtų sukčiauti Alisai, ir schemą, kuri padėtų sukčiauti Benitui. Schemose nebūtinai turi būti šešios įvedimų pozicijos. Jose įvedimų ir išvedimų skaičius netgi gali skirtis.



# Darbo lapas. Monetos metimas



Pasirinkite įvedimus ir apskaičiuokite išvedimus pagal pateiktą schemą.



Licensed under Creative Commons

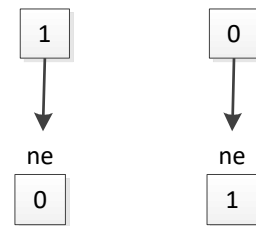
© 2015, 2023 Computer Science Unplugged (csunplugged.org)

## Gudručiams

Pagrindinis uždavinys yra sukurti schemą, priimtina ir Alisai, ir Benitui. Gana įdomu tokia veikla užsiimti telefonu, tačiau tai sudėtinga padaryti klasėje, todėl galima alternatyva. Alisa ir Benitas atskirai sudaro savo schemas ir jas visiems parodo. Alisa atlieka abiejų schemų veiksmus su savo sugalvotais įvedimais ir gautus du išvedimus sujungia lygindama atitinkamus išvedimų bitus: jei jie sutampa, galutinis išvedimas yra 1, jei nesutampa – 0. Tokiu būdu nė vienas iš dalyvių negali sukčiauti. Jei viena iš schemų yra vienos krypties funkcija, tai abiejų schemų kombinacija taip pat yra vienos krypties funkcija.

Du tolesni uždaviniai nėra susiję su kriptografijos protokolais ar monetos metimu, jie skirti loginėms schemoms sudaryti atliekant IR ir ARBA operacijas. Šie uždaviniai supažindina ne tik su kompiuterio schemų sudarymo pagrindais, bet ir su logikos algebra. Ši logika vadinama Bulio algebra, pavadinta anglų matematiko Džordžo Bulio (George Boole, 1815–1864) vardu.

1. Mokiniai gali pastebėti, kad visų nulių įvedimas 000000 pateikia visų nulių išvedimą ir, priešingai, visų vienetų įvedimas 111111 pateikia visų vienetų išvedimą. (Aišku, ir kitų įvedimų variantai gali pateikti visų nulių ar visų vienetų išvedimus. Pavyzdžiui, pirmiau nagrinėtoje schemoje įvedimas 000010 pateikia visų nulių išvedimą, o įvedimas 110111 pateikia visų vienetų išvedimą.) Toks rezultatas gaunamas todėl, kad vartojami tik IR ir ARBA logikos elementai. Pridėjus dar vieną loginį elementą NE (vadinamąjį neigimą), kurio išvedimas yra priešingas įvedimui (t. y. jei įvedamas 0, tai išvedimas yra 1, o jei įvedamas 1, tai išvedimas yra 0), galima sudaryti schemų, kurios neatitinka visų nulių ir visų vienetų taisyklės.

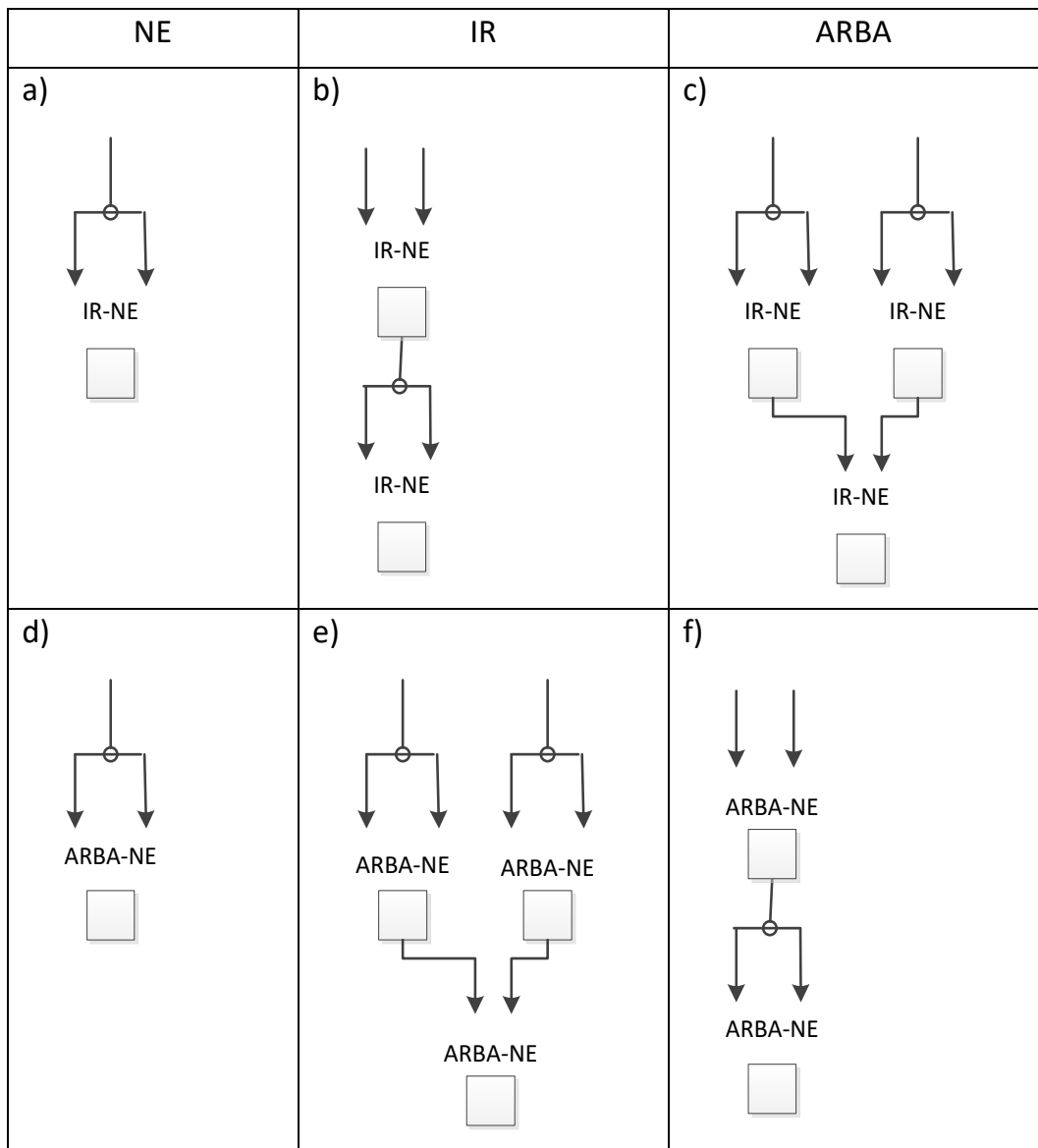


2. Kiti du svarbūs loginiai elementai yra IR – NE ir ARBA – NE, kurių įvedimai atitinkamai pateikia priešingus negu elementai IR ir ARBA išvedimus. Tad  $a$  ARBA – NE  $b$  yra tas pats kaip NE ( $a$  IR  $b$ ). Vartojant šiuos elementus negaunamas funkciškai skirtingas rezultatas, nes juos visada galima pakeisti loginiais elementais IR ir ARBA, o paskui dar pritaikyti NE. Tačiau jie turi vieną įdomią savybę: visi loginiai elementai gali būti gaunami vartojant IR – NE ir ARBA – NE.

Aptarus šiuos du elementus mokiniams galima pasiūlyti išsiaiškinti, ar bet kuris iš loginių elementų gali būti sudarytas iš kitų sujungtų elementų, be to, ar jie gali būti sudaryti iš vieno tipo sujungtų elementų. Toliau vaizduojama, kaip galima sudaryti tris pagrindinius loginius elementus IR, ARBA ir NE vartojant IR – NE elementą viršutinėje eilėje (a, b, c variantai) ir ARBA – NE apatinėje eilėje (d, e, f variantai).







## Apie ką visa tai?

---

Pastaraisiais metais labai išaugo elektroninė prekyba, todėl būtina užtikrinti piniginių operacijų ir dokumentų pasirašymo saugumą. Kriptografijos esmė yra saugi ir privati komunikacija. Prieš keletą dešimtmečių informatikos mokslininkai atrado, kad saugumas gali būti užtikrinamas metodais, kurie leidžia dalį informacijos palikti viešai prieinamą. 20 veiklos skyriuje aprašoma „viešojo rakto kriptografija“ dabar plačiai naudojama kaip pagrindinis informacijos keitimosi saugumo būdas. Pavyzdžiui, naršyklėje galima pamatyti SSL (saugiųjų jungimų lygmens) arba TLS (transporto lygmens saugumo) protokolus, kurie grindžiami viešojo rakto sistemomis, leidžiančiomis interneto naršyklei saugiai prisijungti prie saityno sistemų (pvz., banko), net jei kas nors slapta seka visus siunčiamus duomenis.

Kriptografija padeda ne tik saugoti paslaptis, bet ir kontroliuoti daugeliui žmonių prieinamą privačią informaciją, taip pat padeda užtikrinti žmonių, esančių skirtingose geografinėse vietose, pasitikėjimą vieni kitais. Kriptografijos protokolai kuriami tam, kad būtų galima naudotis, atrodo, neįmanomomis galimybėmis: skaitmeniniais parašais, sertifikatais ir pan.

Realybėje Alisa ir Benitas patys nekurtų loginės schemos, o naudotųsi kompiuterio programa, kuri atliktų šį darbą. Tikriausiai nė vienas iš jų nesidomėtų, kaip sukurta ši programa, bet abu norėtų būti tikri, kad niekas kitas negali daryti įtakos sprendimo rezultatui nepriklausomai nuo kompiuterinių įgūdžių ir bandymams sugaišto laiko.

Jei kiltų Alisos ir Benito ginčas, reikėtų kreiptis į neutralų asmenį (pavyzdžiui, teisėją). Teisėjui būtų duodama loginė schema, Alisos pradinis dvejetainis skaičius, rezultatas, kurį Alisa nusiuntė Benitui, ir Benito spėjimas. Kadangi „metimas“ jau baigtas, visa ši informacija vieša ir abu turėtų sutikti, kad šia informacija buvo remtasi priimant sprendimą. Teisėjas turėtų patikrinti, ar įvedant Alisos pradinį dvejetainį skaičių į loginę schemą galima gauti Benitui siųstą rezultatą, ir nustatyti, ar sprendimas priimtas sąžiningai. Kadangi tikrinimo procedūra aiški, ginčai mažai tikėtini, tačiau jei kalbėtume apie realią situaciją, kai Alisa meta monetą, o Benitas įvardija, kuria puse ji krinta, nė vienas teisėjas nesutiktų imtis spręsti tokio ginčo!

Šiame skyriuje pateikta loginė schema praktiškai nenaudinga, nes labai paprasta sudaryti visų galimybių lentelę ir bandyti sukčiauti. Patikimesnis 32 dvejetainių skaitmenų įvedimas, nors ir tai neapsaugo nuo sukčiavimo – viskas priklauso nuo sudarytos loginės schemos. Galimi ir kiti metodai, pavyzdžiui, vienos krypties funkcija, aprašyta 16 veikloje („Turistų miestas“). Praktiškai taikomi metodai dažniausiai susiję su labai didelių skaičių skaidymo daugikliais uždaviniais, kurie nelengvai sprendžiami (nors, kaip sužinosime tolesnės veiklos pabaigoje, jie nėra NP sudėtingumo uždaviniai). Nesunku patikrinti, kad vienas skaičius yra kito daugiklis, bet rasti visus didelio skaičiaus daugiklius trunka labai ilgai. Alisai ir Benitui (ir teisėjui) išspręsti tokį uždavinį būtų sunku, todėl praktiškai, kaip jau minėta, tai atliekama kompiuteriu tam tikromis programomis.





Skaitmeniniai parašai grindžiami panašiu principu. Viešas schemas išvedimas ir slaptas Alisos sugalvotas įvedimas įrodo, kad vienintelė Alisa žino rezultatą – ji apskaičiuoja atitinkama vienos krypties funkcija – ir niekas kitas negali pasinaudoti jos įvedimu. Niekas negali apsimesti Alisa. Tikram skaitmeniniam parašui reikia sudėtingesnio protokolo, kuris garantuotų, kad pati Alisa pasirašo atitinkamą pranešimą, be to, kad kiti galėtų įsitikinti, jog tai Alisos parašas, net jei ji pati tai neigtų.

Kriptografiją galima pritaikyti ir žaidžiant pokerį telefonu, kai nėra arbitro, dalijančio kortas ir registruojančio žaidėjų turimas kortas. Viską turi atlikti patys žaidėjai, tik kilus ginčui jie gali kreiptis į teisėją. Akivaizdu, kad žaidėjai turi slėpti savo kortas, bet kartu likti sąžiningi. Jie negali meluoti, kad turi tūzą, jei iš tikrųjų jo neturi. Tai galima patikrinti žaidimo pabaigoje, kai leidžiama tikrinti kitų žaidėjų kortas ir veiksmus. Kita problema – kaip dalyti kortas, jei žaidėjai negali žinoti vienas kito kortų. Stebėtina, bet tai įmanoma taikant kriptografijos protokolą – tokį pat kaip metant monetą. Reikia pasakyti, kad panašiai būna derinamos ir verslo ar kitokios sutartys.



Kriptografijos protokolai yra labai svarbūs, kai sudaromi elektroniniai sandoriai ir reikia nustatyti debeto kortelių savininką, skambinant mobiliuoju telefonu, ar išsiaiškinti laiško siuntėją. Šios galimybės garantuoja saugią elektroninę komerciją.

### **Daugiau informacijos**

1987 m. Davido Harello knygoje „Algorithmics“ aptariami skaitmeniniai parašai ir su jais susiję kriptografijos protokolai. Joje aprašoma, kaip žaisti pokerį telefonu.

1982 m. Dorothy Denning knygoje „Cryptography and data security“ plačiai aprašoma kriptografija.

2003 m. Alexanderio Keewatino Dewdney knygoje „The New Turing Omnibus: 66 Excursions in Computer Science“ yra skyrius apie Bulio logiką, kuriame aptariamas loginių schemų sudarymas.



## 20 veikla

# Vaikai šnipai. Viešojo rakto kriptografija

---

### Santrauka

Kriptografija – tai mokslas apie matematikos ir informatikos metodus informacijai šifruoti ir iššifruoti. Kriptografija leidžia saugoti ypač slaptą informaciją ir siųsti ją nesaugiais tinklais (pvz., internetu), kad jos negalėtų perskaityti niekas kitas, o tik teisėtas gavėjas.

Šifravimas yra informacijos saugumo esmė. Anksčiau, jei viena pusė norėdavo nusiųsti slaptus duomenis kitai, pirma turėdavo duomenis užšifruoti tam tikru raktu, paskui rasti būdą, kaip saugiai tą raktą pateikti kitai pusei. Šią saugumo problemą išsprendė viešojo rakto kriptografija. Šiuolaikinis informacijos šifravimas grindžiamas dviem raktais – viešuoju (duomenims užšifruoti) ir privačiuoju (duomenims iššifruoti). Viešasis raktas gali būti duodamas kam tik norima, o privatusis – saugomas. Viešuoju raktu užšifruoti duomenys gali būti iššifruoti tik privačiuoju raktu.

Paprastiau kalbant, kas nors nusiperka spyną, ant jos užrašo savo vardą ir padeda ant stalo, kad kiti galėtų ja naudotis. Raktą, žinoma, turi tik spynos savininkas. Tarkime, kad kas nors nori jums išsiųsti pranešimą, taigi įdeda tą pranešimą į dėžutę, užrakina ją jūsų spyna ir išsiunčia. Net jei ta dėžutė nukeliautų klaidingu adresu, niekas negalėtų jos atidaryti, nes raktą nuo spynos turite tik jūs. Dėl šios priežasties nėra būtinybės perduoti spynos rakto siuntėjui.

Šios veiklos skyriuje aiškinama, kaip tai galima padaryti skaitmeniniu būdu. Skaitmeniniame pasaulyje naudojama „spynos“ kopija. Jei realiame pasaulyje būtų daroma spynos kopija, būtų išsiaiškintas jos užraktas ir, aišku, atkurtas raktas. Tačiau skaitmeniniame pasaulyje nereikia išrasti naujo rakto, o tik nukopijuoti „spyną“ visiškai nesigilinant, kas joje.

Atrodo, kad tai neįmanoma. Pažiūrėkime ir įsitikinkime.

### Ryšiai su ugdymo programomis

- ✓ Informatika: viešojo rakto kriptografija, slaptas kodas

### Gebėjimai

- ✓ Galvosūkių sprendimas

### Amžius

- ✓ Nuo 11 metų

### Priemonės

- ✓ Projektorius „Vaikų šnipų pranešimo užšifravimas“ pateikčiai demonstruoti
- ✓ Lipniųjų lapelių schemoms komentuoti

Kiekvienai mokinių grupei reikia:

- ✓ Dviejų darbo lapų „Vaikų šnipų žemėlapiai“





# Vaikai šnipai

## Įvadas

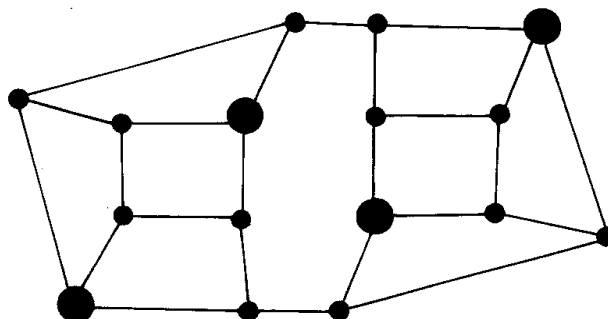
Ši veikla techniškai yra sudėtingiausia iš visų šioje knygoje aprašytų veiklų. Norint ją sėkmingai atlikti iki galo reikia kruopštaus darbo ir susikaupimo. Mokiniai turi būti susipažinę su vienos krypties funkcijomis (16 veikla „Turistų miestas“). Būtų lengviau atlikti šią veiklą, jei mokiniai atliktų aukščiau aprašytas šios dalies veiklas (18 veiklą „Dalijimasis paslaptimi“ ir 19 veiklą „Monetos metimas“). Čia mokiniams bus reikalinga tai, ko išmoko atlikdami 1 veiklą „Taškų skaičiavimas“ ir 5 veiklą „Dvidešimt spėjimų“.

Ema planuoja siųsti Bilui slaptą žinutę. Paprastai slapta žinutė suprantama kaip sakinyš ar keletas sakinių, tačiau šiame uždavinyje Ema siųs tik vieną skaičių, kuris simbolizuoja vieną ženklą. Iš tikrųjų tai atrodo labai paprasta, turint galvoje, kad ji galėtų siųsti sakinį, sudarytą iš tokių ženklų, be to, tai bus padaryta dar ir kompiuteriu. Tačiau kartais net labai trumpi pranešimai yra labai svarbūs: vienas žinomiausių pranešimų istorijoje, siųstas Polo Reviro (Paul Revere), turėjo tik dvi galimas reikšmes. Emos pranešimas bus siunčiamas Bilo viešuoju raktu, todėl, net jei patektų į kitas rankas, jo nebūtų galima iššifruoti. Tik Bilas gali iššifruoti Emos pranešimą, nes tik jis turi raktą nuo „spynos“.

Pranešimas užšifruojamas naudojantis žemėlapiu. Tai ne Lobių salų žemėlapis iš ankstesnės veiklos, o panašus į Turistų miesto žemėlapij iš 15 veiklos. Jame linijos vaizduoja gatves, o taškai atitinka gatvių sankryžas. Kiekvienas žemėlapis turi viešąją (spyną) ir privačiąją (raktą) versijas.

## Diskusija

Darbo lape „Vaikų šnipų pranešimo užšifravimas“ vaizduojamas Bilo viešasis žemėlapis. Jis nėra slaptas, Bilas jį pateikia viešai (ant stalo ar tinklalapyje), kad kiekvienas galėtų jį pamatyti, arba duoda jį tam žmogui, kuris nori jam išsiųsti pranešimą. Ema taip pat turi šio žemėlapio kopiją.



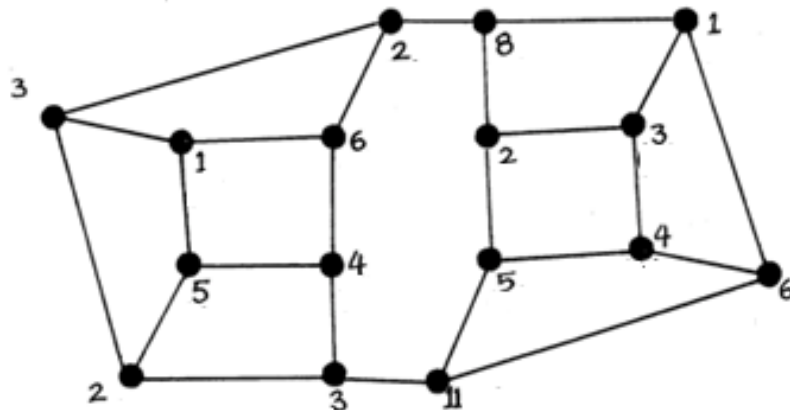
Paveiksle dešinėje yra Bilo privatusis žemėlapis. Jis panašus į viešąjį, tik kai kurie taškai paryškinti. Šis žemėlapis yra saugomas, kad niekas jo nematytų.

Rekomenduojama šią veiklą atlikti su visa klase, nes čia reikia daug kruopštaus darbo. Nors viską padaryti nėra sunku, tačiau nedidelė klaida sukelia nemažai problemų. Svarbu, kad mokiniai įsitikintų, jog šis šifravimo būdas iš viso įmanomas. Taigi jiems reikės palaikymo atliekant šią daug pastangų reikalaujančią užduotį. Mokinius motyvuoja tai, kad šiuo metodu galima perduoti slaptus pranešimus vienas kitam ir net mokytojas, nors žino, kaip pranešimai buvo užšifruoti, negali jų iššifruoti.

1. Mokiniams parodomas Bilo viešasis žemėlapis („Vaikų šnipų pranešimo užšifravimas“). Sugalvojamas skaičius, kurį Ema norėtų siųsti. Prie kiekvienos gatvių sankryžos žemėlapyje surašomi atsitiktiniai skaičiai, kurių suma lygi

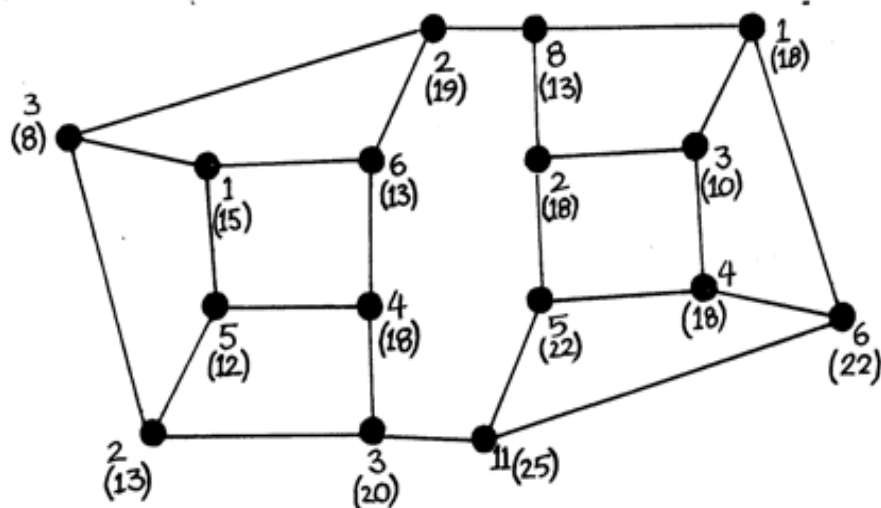


siunčiamam Emos skaičiui. Toliau pavyzdyje Ema sugalvojo siųsti 66, todėl prie gatvių sankryžų surašyti galimi skaičiai, kurių suma yra 66. Prireikus galimi ir neigiami skaičiai.



2. Toliau Ema turi nuspręsti, ką nusiųsti Bilui. Žemėlapiu ji siųsti negali, nes bet kas kitas gali nesunkiai iš jo perskaityti pranešimą.

Taigi ji pasirenka bet kurią sankryžą ir sudeda jos skaičių su trijų gretimų sankryžų skaičiais. Gautą sumą Ema užrašo skliaustuose (arba kita spalva) po pasirinktos sankryžos skaičiumi. Pavyzdžiui, toliau pateikto viešojo žemėlapiu dešinėje pusėje, apačioje, esančios sankryžos, pažymėtos skaičiumi 6, gretimų sankryžų skaičiai yra 1, 4 ir 11. Visų keturių skaičių suma yra 22 – ji užrašyta skliaustuose po 6. Šiuos skaičiavimus reikia pakartoti su kiekviena sankryža žemėlapyje. Taip gausime skaičius skliaustuose.



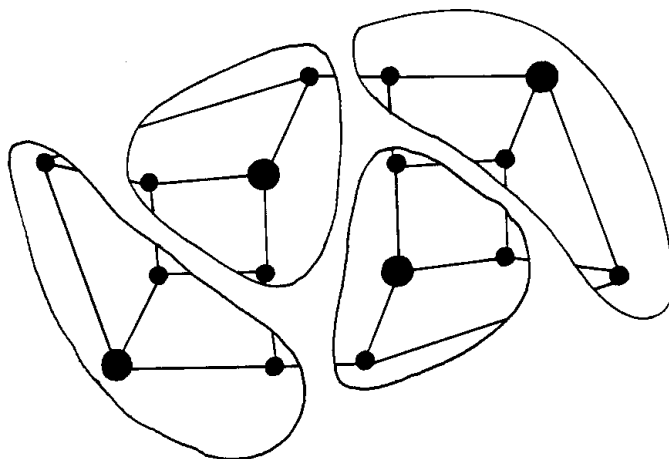
3. Ema nusiunčia Bilui žemėlapij, kuriame prie gatvių sankryžų surašyti tik skaičiai skliaustuose.

Prieš siunčiant Bilui galima nutrinti ne skliaustuose esančius skaičius arba perrašyti skaičius skliaustuose į žemėlapiu kopiją. Tada galima paprašyti mokinių spėti, kokie buvo pirmieji užrašyti skaičiai. Vargu ar jiems tai pavyks.

4. Tik su Bilo privačiuoju raktu galima iššifruoti Emos pranešimą. Bilo privačiajame žemėlapyje yra pažymėti (padidinti) taškai.

Norėdamas iššifruoti pranešimą Bilas pasižiūri į pažymėtus taškus ir sudeda jų skaičius. Pavyzdyje Bilas sudeda skaičius 13, 13, 22 ir 18. Suma yra 66 – Emos siųstas pranešimas.

5. Kaip tai veikia? Viskas priklauso nuo žemėlapio. Privačiajame Bilo žemėlapyje pasirenkama viena iš pažymėtų sankryžų ir apvedama sritis, apimanti ją ir gretimas, per vieną gatvę nuo jos esančias sankryžas. Taip padaroma ir su kitomis pažymėtomis sankryžomis, kaip parodyta toliau paveiksle. Tokiu būdu žemėlapis padalijamas į nesusikertančias sritis. Kiekvienos srities pažymėtos sankryžos skaičius gaunamas sudėjus visų tos srities sankryžų pradinius skaičius. Kadangi sritis nesusikerta, pažymėtų sankryžų suma yra visų sankryžų pradinių skaičių suma ir lygi siunčiamam skaičiui.



Atrodo, tiek daug darbo siunčiant vieną skaičių! Pažiūrėkime, kas buvo atlikta: persiųstas visiškai slaptas pranešimas viešuoju raktu, be jokio išankstinio dalyvių susitarimo. Dabar galima skelbti savo viešąjį raktą skelbimų lentoje (ar kur kitur) ir bet kas gali siųsti slaptas žinutes, bet niekas negali jų iššifruoti be privačiojo racto. Realiame gyvenime visus skaičiavimus atlieka programinės įrangos paketas, paprastai integruotas į interneto naršyklę, todėl sunkiai dirba tik kompiuteris.

Tikriausiai mokiniams įdomu sužinoti, kad dabar jie yra išskirtinės grupės nariai, kurie naudodami viešąjį raktą šifravo rankiniu būdu. Informatikai mano, kad ši užduotis yra beveik neįmanoma, ir tik keletas žmonių yra bandę tai daryti.

Viešojo žemėlapiio sudarymas yra labai panašus į ledų furgonų susstatymą Turistų mieste (16 veikla). Žemėlapij nesunku sudaryti, jei pradama nuo sričių braižymo privačiajame žemėlapyje, lygiai kaip žymint sankryžas, kur turėtų stovėti ledų furgonai, o paskui sujungiant jas gatvėmis „Turistų miesto“ uždavinyje. Spręsti „Turistų miesto“ uždavinį labai sudėtinga, jis sprendžiamas perrinkimo metodu. Tarkime, Bilas pradėtų nuo labai sudėtingo žemėlapiio su 50 ar 100 sankryžų. Regis, niekas negalėtų įveikti tokio šifro, net protingiausi matematikai, kaip ir „Turistų miesto“ uždavinyje įrodyti, kad parinktas furgonų skaičius yra mažiausias.





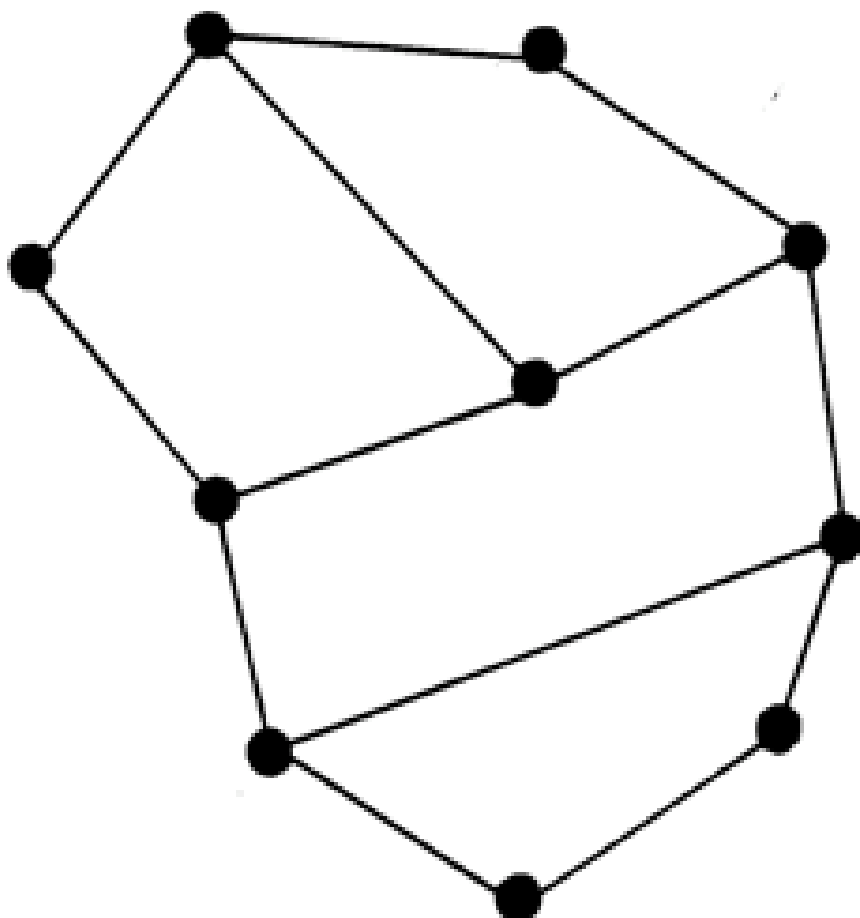
6. Su visa klase išnagrinėjus vieną pavyzdį mokiniai padalijami į grupes po 4. Kiekvienai grupės porai duodamas darbo lapas, kuriame pateiktas viešasis žemėlapis. Kiekviena pora susigalvoja siunčiamą „pranešimą“ (tai gali būti bet koks sveikasis skaičius), užšifruoja jį ir perduoda savo rezultatą kitai grupės porai. Šie bando iššifruoti, bet, aišku, jiems prireikia privačiųjų žemėlapių. Ar pavyksta mokiniams iššifruoti pranešimus su privačiuoju raktu?
7. Kiekviena pora gali pabandyti sukurti savo žemėlapij. Privatųjį žemėlapij jie saugo, o viešąjį duoda kitai grupės porai arba pakabina klasės lentoje. Žemėlapio kūrimo metodika panaši kaip ir ledų furgonų – sužymimi taškai ir tada sujungiami gatvėmis. Privačiajame žemėlapyje nubraižomos sritys, kuriose pažymimas vienas taškas ir iš jo išvedamos dvi ar trys gatvės, kurių gale pažymimas kitas taškas. Šie taškai sujungiami gatvėmis su kitų sričių tokiais pat taškais.



## Darbo lapas. Vaikų šnipų viešasis žemėlapis

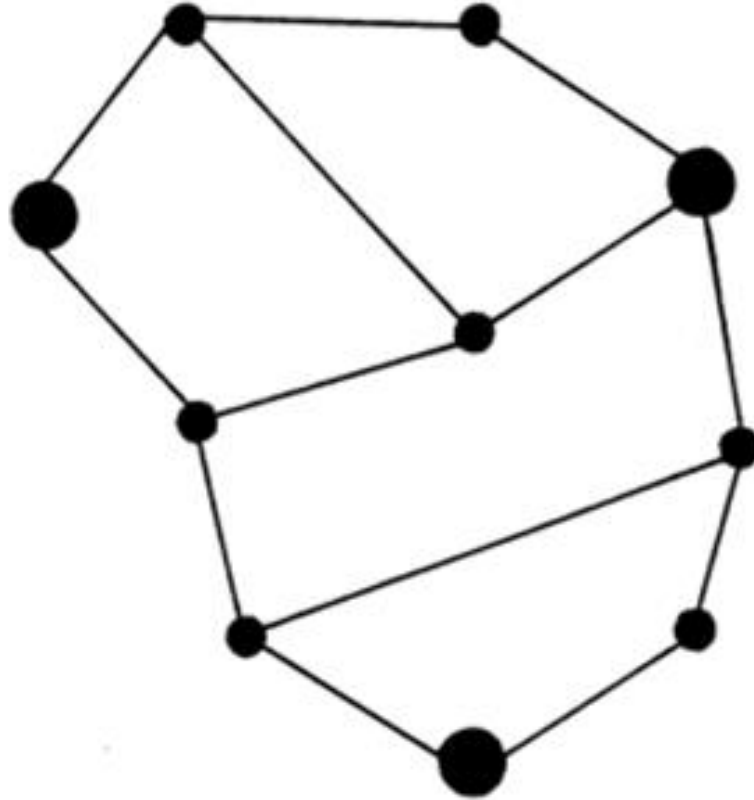
---

Naudodamiesi žemėlapiu užšifruokite pranešimus.



# Darbo lapas. Vaikų šnipų privatusis žemėlapis

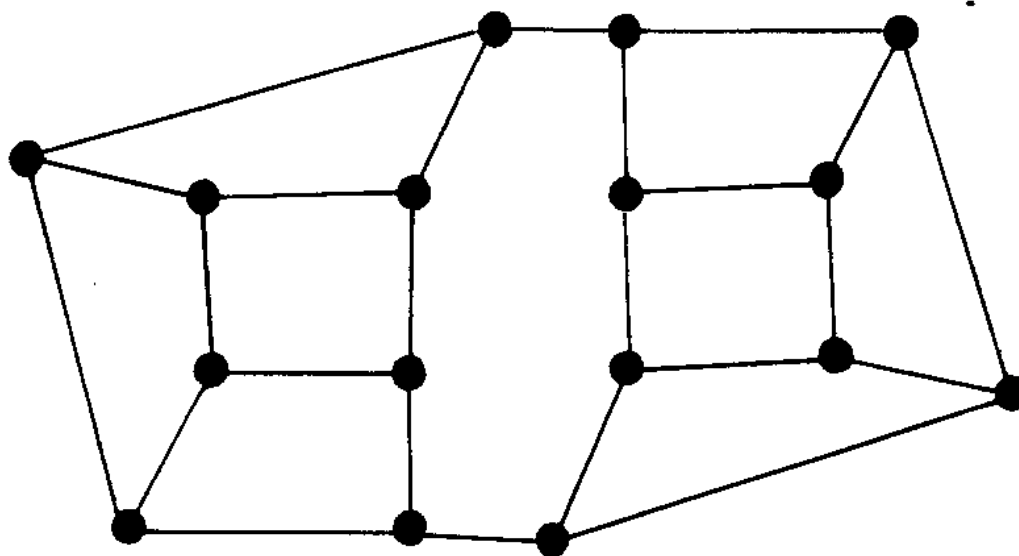
Naudodamiesi šiuo žemėlapiu iššifruokite pranešimus.



# Vaikų šnipų pranešimo užšifravimas

---

Šiuo žemėlapiu rodoma, kaip užšifruojamas pranešimas.



## Apie ką visa tai?

---

Aišku, dauguma nori siųsti slaptus pranešimus kompiuterių tinklais taip, kad tik tikrasis gavėjas galėtų juos perskaityti. Be abejo, yra daug būdų tai padaryti, jei siuntėjas ir gavėjas dalijasi šifravimo raktu, bet viešojo rakto šifravimo esmė yra ta, kad siuntėjas gali siųsti slaptą pranešimą gavėjui be išankstinio susitarimo, tiesiog pasiėmęs viešosios „spynos“ kopiją tinklalapyje.

Saugumas yra tik viena kriptografijos pusė. Kita pusė yra autentifikavimas: ar gali Ema būti tikra, kad gautas pranešimas yra tikrai nuo Bilo, o ne nuo kokio apsimetėlio siuntėjo? Įsivaizduokime, Bilas siunčia elektroninį laišką: „Brangioji, aš nebeturiu pinigų ir negaliu grįžti. Prašau pervesti į mano banko sąskaitą 100 €. Mano sąskaita 0241–45–784329. Su meile – Bilas.“ Ar Ema gali būti tikra, kad laišką siuntė Bilas? Šiuo atveju gali būti naudojama viešojo rakto kriptosistema. Kai tik Ema nusiunčia Bilui slaptą pranešimą, kurį užšifruoja jo viešuoju raktu, šis gali siųsti jai pranešimą, kurį tik jis pats gali sugeneruoti užšifruodamas savo privačiuoju raktu. Jei gautą pranešimą Ema gali iššifruoti viešuoju Bilo raktu, vadinasi, pranešimas yra tikrai nuo Bilo. Žinoma, pranešimą gali iššifruoti bet kas kitas, nes naudojamas viešasis Bilo raktas, tačiau Bilas galėtų dar kartą užšifruoti siunčiamą pranešimą Emos viešuoju raktu. Šis dvigubas šifravimas užtikrina ir saugumą, ir autentifikavimą pagal tą pačią viešojo ir privačiojo rakto schemą.

Reikia pripažinti, kad šioje veikloje aprašoma schema yra panaši į rimtą sudėtingą viešojo rakto šifravimo sistemą, tačiau praktiškai nėra saugi, nes realybėje naudojami daug didesni žemėlapiai.

Priežastis ta, kad, nors sprendimas, kaip išdėstyti mažiausiai ledų furgonų bet kuriame žemėlapyje, nežinomas ir šioje veikloje pateiktas būdas atrodo saugus, tačiau visiškai kas kita, kai norima nulaužti. Vargu ar šis klausimas iškils mokiniam, bent jau jaunesniems, tačiau reikia bent žinoti, kad tokia problema egzistuoja. Galite bent pasakyti, kad nagrinėjamas šifravimo būdas yra saugus, tačiau matematiškai nėra pagrįstas. Jei jums neįdomi matematika, galite ignoruoti tolesnius samprotavimus.

Sunumeruokime susikirtimų taškus žemėlapyje: 1, 2, 3 ir t. t. Pradiniai susikirtimų skaičiai žymimi  $b_1, b_2, b_3, \dots$ , o perskaičiuoti –  $t_1, t_2, t_3, \dots$ . Tarkime, kad 1 susikirtimas yra sujungtas su 2, 3 ir 4. Tada

$$t_1 = b_1 + b_2 + b_3 + b_4 \quad (1)$$

Panašias lygybes galima pritaikyti visiems susikirtimams. Visose lygybėse yra nežinomieji kaip 1 lygybėje  $b_1, b_2, b_3, \dots$ . Visi mato viešąjį žemėlapį ir perskaičiuotus skaičius  $t_1, t_2, t_3, \dots$ , gali išreikšti visus perskaičiuotus skaičius kintamaisiais, vaizduojančiais pradiniais skaičiais. Gautą lygybių sistemą galima išspręsti lygčių sprendimo programa. Nustatomi pradiniai skaičiai, apskaičiuojama jų suma ir gaunamas siųstas skaičius (pranešimas). Taigi nereikia atkurti privačiojo žemėlapio. Ši lygčių sistema sprendžiama Gauso eliminavimo metodu, todėl skaičiavimo laikas yra proporcingas lygčių skaičiaus kubui. Tačiau, kadangi dauguma šių lygčių koeficientų



lygūs 0, yra dar spartesnių sprendimo būdų. Palyginus šį būdą su eksponentiniu skaičiavimo laiku, iššifavimo žemėlapis sudaromas daug greičiau.

Tikimės, kad nesijaučiate apgauti! Tiesą sakant, skaičiavimai, susiję su realiomis viešojo rakto kriptosistemomis, yra labai panašūs į tuos, kurie buvo atliekami šioje veikloje. Tik realios viešojo rakto kriptosistemos šifruoja įvairiais ir daug sudėtingesniais metodais, kuriais šifruoti rankiniu būdu net neįmanoma. Vienas iš saugiausių viešojo rakto metodų, naudojamų šiuolaikinėse šifravimo sistemose, yra grindžiamas sudėtingu didelių skaičių daugiklių skaičiavimu.

Kokie yra 100 ženklų skaičiaus

9.412.343.607.359.262.946.971.172.136.294.514.357.528.981.378.983.082.541.347.532.211.942.640.121.301.590.698.634.089.611.468.911.681 daugikliai? Neužtrukite per ilgai skaičiuodami!

Šio skaičiaus daugikliai yra

86.759.222.313.428.390.812.218.077.095.850.708.048.977 ir  
108.488.104.853.637.470.612.961.399.842.972.948.409.834.611.525.790.577.216.753.

Tik šie du skaičiai yra pateiktojo 100-ženklų skaičiaus daugikliai ir jie yra pirminiai. Šių skaičių galingas superkompiuteris ieškojo keletą mėnesių.

Dabar realioje viešojo rakto kriptosistemoje Bilas gali naudoti iš 100 skaitmenų sudarytą skaičių kaip viešąjį raktą ir du jo daugiklius – kaip privatųjį raktą. Sukurti tokius raktus nėra sunku: reikia tik būdo pirminiams skaičiams rasti. Taigi randami du gana dideli pirminiai skaičiai, jie sudauginami. Sandauga yra viešasis raktas, o pirminiai skaičiai – privatusis raktas. Kompiuteris nesunkiai gali sudauginti du didelius skaičius. Kai toks didelis viešasis raktas, niekas negali įspėti privačiojo rakto, nebent galėtų prieiti prie superkompiuterio ir turėtų keletą mėnesių laiko. O jeigu vietoj 100 skaitmenų viešasis raktas būtų sudarytas iš 200 skaitmenų, daugiklių radimas užtruktų metų metus. Tokio rakto nulaužimo sąnaudos yra daug didesnės, negu informacijos, kuri juo būtų iššifruota, vertė. Praktiškai 512 bitų ar didesni raktai, kurie yra ekvivalentūs apie 155 skaitmenų po kablelio ar daugiau, dažnai sudaromi saugiems ryšiams užtikrinti.

Vis dar nėra būdo, kaip užšifruoti pranešimus pirminiais skaičiais grindžiamu viešuoju raktu, kad jo nebūtų galima iššifruoti be privačiojo rakto. Čia netinka metodas, kai du pirminiai skaičiai naudojami kaip privatusis raktas, o jų sandauga – kaip viešasis raktas, užuot skaičius išskaidytus iš sandaugos. Raktą būtų galima nulaužti išskaidant skaičių dauginamaisiais. Šiaip ar taip, galima įveikti šiuos sunkumus ir sukurti tinkamą užšifravimo ir iššifravimo algoritmą, tačiau čia to nenagrinėsime. Jau ir taip daug ką padarėme.

Ar saugi pirminiais skaičiais grindžiama sistema? Didelių skaičių skaidymas dauginamaisiais – tai problema, kurią pasaulio matematikai sprendžia jau keletą šimtmečių, bet geresnio metodo, kaip perrinkti visus daugiklius, neatrasta (kad toks metodas neegzistuoja, taip pat neįrodyta). Vienaip ar kitaip, reikia būti budriems: jei galima nulaužti Bilo raktą nesprendžiant „Ledų furgonų“ uždavinio, tai gali būti, kad pirminių skaičių raktas gali būti nulaužtas neperrinkant visų daugiklių.



Nerimą kelia tai, kad, jei yra tik keli galimi pranešimai, piktavališkas asmuo bet kurį iš jų gali užšifruoti viešuoju raktu ir palyginti tikrąjį pranešimą su visomis galimybėmis. Emos metodu galima to išvengti, nes atsiranda daug būdų, kaip užšifruoti tą patį pranešimą, priklausomai nuo prie kodų vertės pridėtų skaičių. Praktiškai kriptografijos sistemos kuriamos taip, kad būtų per daug galimų pranešimų, todėl net nevertėtų visų jų bandyti net labai sparčiu kompiuteriu.

Iki šiol nežinoma, ar galima greitai išspręsti skaidymo pirminiais dauginamaisiais uždavinius. Niekam nepavyko sukurti sprendimo metodo, bet taip pat niekas neįrodė, kad tokio metodo nėra. Jei būtų surastas efektyvus šio uždavinio sprendimo algoritmas, daugelis šiandieninių kriptografijos sistemų taptų nesaugios. IV dalyje buvo aptarti NP sudėtingumo uždaviniai: jei bent vienas iš jų būtų išspręstas, būtų galima išspręsti juos visus. Kadangi tiek daug (nesėkmingų) pastangų įdėta ieškant efektyvaus NP sudėtingumo uždavinių sprendimo algoritmo, tai skaidymo daugikliais uždaviniai puikiai tiktų kuriant saugias kriptosistemas. Šiandien kriptografija yra aktyvių informatikos tyrimų sritis.

### **Daugiau informacijos**

1987 m. Davido Harel'o knygoje „Algorithmics“ aptariami skaitmeniniai parašai ir su jais susiję kriptografijos protokolai. Joje aprašoma, kaip žaisti pokerį telefonu.

1982 m. Dorothy Denning knygoje „Cryptography and data security“ išsamiai aprašoma kriptografija.

1989 m. Alexanderio Keewatino Dewdney knygoje „Turing Omnibus“ yra skyrius apie Bulio logiką, kuriame aptariamas loginių schemų sudarymas.



## 21 veikla

### Simetrinio rakto kriptografija

---

#### Santrauka

Šiuolaikiniai simetrinio elektroninių duomenų šifravimo algoritmai, tokie kaip DES, IDEA ir kt., yra labai sudėtingi. Mokyklose ne tik neįmanoma, bet ir nebūtina išsamiai aiškinti, kaip šie algoritmai veikia. Mūsų mokiniai turėtų mokytis kriptografijos sąvokų ir idėjų įdomiai ir motyvuotai tyrinėdami detalius netrivialius istorinių šifravimo metodų pavyzdžius. Užduotyje pateikiamas simetrinio rakto šifravimo metodas, paremtas vienu iš metodų, žinomų kaip Fleissnerio grotelių perkėlimo šifrai (vok. Fleißnerschen Schablone). Šiuos šifrus kelis mėnesius Pirmojo pasaulinio karo metais naudojo Vokietijos kariuomenė.

Šią praktinę užduotį galima naudoti siekiant pradinių ir vidurinių mokyklų mokiniams suteikti platesnį supratimą apie interneto naršyklės saugaus (HTTPS) ryšio sąvokas (pvz., sesijos rakto stiprumą, apsikeitimo sesijos raktu problemą).

Ši veikla buvo paskelbta Lenkijos matematikos mokytojams skirtame profesiniame žurnale.

#### Amžius

10 m. ir daugiau

#### Priemonės

Kiekvienai mokinių grupei reikės:

- ✓ Darbo lapas „Dženės šifras“
- ✓ Žirklės
- ✓ Kvadratinis popieriaus lapas



# Skautų slaptos žinutės

---

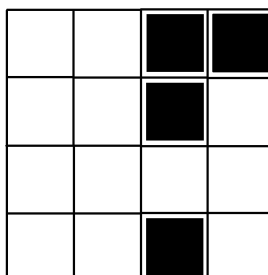


## Ką daryti?

Šioje veikloje naudojamas išgalvotas pasakojimas paremtas skautų istorija. Pasakojimas prasideda tokia istorija: „Skautė Dovilė pateko į didelę bėdą. Skautų patruliai šifruodavo savo žinutes tiesiog rašydami jas atvirkščiai. Tačiau tai jau nebe paslaptis. Dovilę, kaip geriausią matematikę komandoje, paprašė surasti geresnį šifrą“.

Mokiniai suskirstomi į grupes ir kiekvienai grupei duodamas darbo lapas „Dovilės šifras“, kuriame iliustruojama Dovilės idėja, kaip užšifruoti paprasto teksto raides. Mokytojas pasakoja, kad jis naudoja 4 x 4 groteles, kurias galima sukti pagal arba prieš laikrodžio rodyklę 90 laipsnių kampu, galima jas naudoti iš vienos arba iš kitos pusės, pradėti dėti groteles galima nuo bet kurios kraštinės.

Mokinių paprašoma iššifruoti pavyzdinį Dovilės pranešimą, kurį sudaro frazė iš 16 raidžių. Po vieną mokinį iš kiekvienos grupės turi žirkliemis iš grotelių iškirpti keturis juodus kvadratinius langelius (1 pav.). Paskui jie, bandymu būdu taikydami groteles 2 paveikslėlio lentelėi su raidėmis, atranda taisyklę, kaip galima groteles naudoti iššifravimui.



### 1 pav. Langeliai iš darbo lapo

U	O	S	Š
I	T	F	R
S	T	T	E
K	A	A	S

### 2 pav. Užšifruota žinutė iš darbo lapo

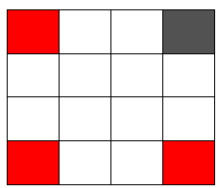
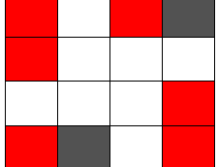
Gali paaiškėti, kad tai nėra taip paprasta. Mokiniai turėtų pastebėti, kad galima 16 padėčių, kaip galima naudoti grotelės: pasukus grotelės taip, kad prie viršutinės kraštinės būtų pridėta kiekviena grotelių kraštinė – 4 galimybės, be to, grotelės galima pasukti dviem kryptimis (pagal arba prieš laikrodžio rodyklę) ir galima grotelės apversti ir pakartoti tuos pačius veiksmus. Galiausiai turėtų būti iššifruota frazė (ŠIFRUOTAS TEKSTAS).

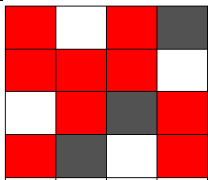

Mokiniai užrašo taisykles, kaip Dovilė naudojo šifravimo grotelės, diskutuoja, ar labai svarbu, nuo kurios kraštinės pradėti dėti grotelės, ar tuomet įmanoma (neįmanoma) iššifruoti tekstą? Ar buvo lengva atrasti būdą, kaip buvo naudojamos grotelės?

Mokytojas paaiškina svarbų šifravimo rakto vaidmenį (ir rakto saugojimo slaptumą).

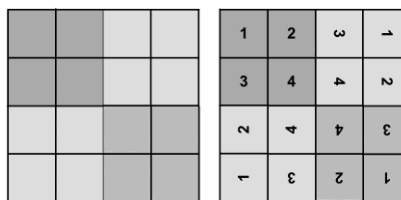
2. Kitas mokinių iššūkis – sukurti savo grotelės ir užšifruoti savo žinutę. Mokiniai suskirstomi poromis. Pirmiausia jų paprašoma pasigaminti kelis grotelių paruoštukus: padalinti kvadratinį popieriaus lapą į 16 dalių (galima perlenkti jį du kartus horizontaliai ir du kartus vertikalčiai). Tada jie iškerpa vieno iš gautų grotelių „langelius“ ir bando užšifruoti savo tekstą.

Pirmasis bandymas gali būti nesėkmingas. Mokytojas su mokiniais turėtų aptarti nesėkmės priežastis. Pasirodo, kad tai gana sudėtinga: iškirpti langeliai turi būti išdėstomi taip, kad grotelės pasukus keturis kartus iš eilės aplink jų centrą 90 laipsnių kampų, šifruojami langeliai nebūtų atidengiami, t.y., kaip užpildomi langeliai raidėmis ir grotelės pasukamos, matomi tik tušti langeliai (langeliuose nėra jau anksčiau įrašytų raidžių). Todėl simetriniai langeliai iškirpti negali būti.

	<p>Jei nusprendžiate iškirpti kampinį grotelių langelį (pilkas), tai kitų trijų kampinių langelių kirpti nebegalima (raudoni)</p>
	<p>Jei nusprendžiate iškirpti langelį prie kraštinės (pilkas prie apatinės kraštinės), tai jam simetriškų langelių kirpti nebegalima (raudoni)</p>

	Jei nusprendžiate iškirpti vidurinį langelį (viduryje pilkas), tai kitų vidurinių jam simetriškų kirpti nebegalima (raudoni)
	Galiausiai iškerpamas vienas iš likusių 4 langelių.

Mokinams galima pasiūlyti padalinti grotelės į ketvirčius ir pabandyti atrasti tinkamą šifrą (3 pav.).

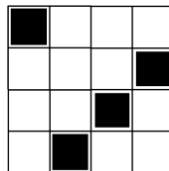


3 pav. 4 x 4 grotelės prieš iškerpant langelius

### Pažengusiems

Šis papildymas skirtas pažengusiems ar vyresniems mokiniam:

– apžvelgdami „blogas“ 4 x 4 grotelės nustatykite taisyklę, kodėl jos blogos;



4 pav. „Blogos“ grotelės

– nustatykite, kiek gali būti 4 x 4 grotelių-raktų (galite įsivaizduoti Dovelės ir jos skautų priešus, kurie žino šį šifravimo metodą);

– kaip priklauso grotelių dydis nuo šifruojamo teksto ilgio? Kaip priklauso, kiek langelių reikia iškirpti?

Tikslių atsakymų į šias problemas ieškojimas gali pareikalauti daug energijos ir laiko net ir pažengusiems mokiniam. Tačiau nesėkmingų sprendimų paieškų patirtis nėra laiko švaistymas. Tuomet mokiniai lengviau įvertina matematikos ir informatikos mokslų galią ir grožį. Galiausiai mokytojas gali paprašyti mokinių namuose išanalizuoti istorinį dokumentą, kaip Pirmojo pasaulio karo metais prancūzai naudojo kriptanalizės metodą „Elementary cipher solution“ (<https://www.nku.edu/~christensen/SRH%20212%20Elem%20Cipher%20Soln%201930.pdf>).



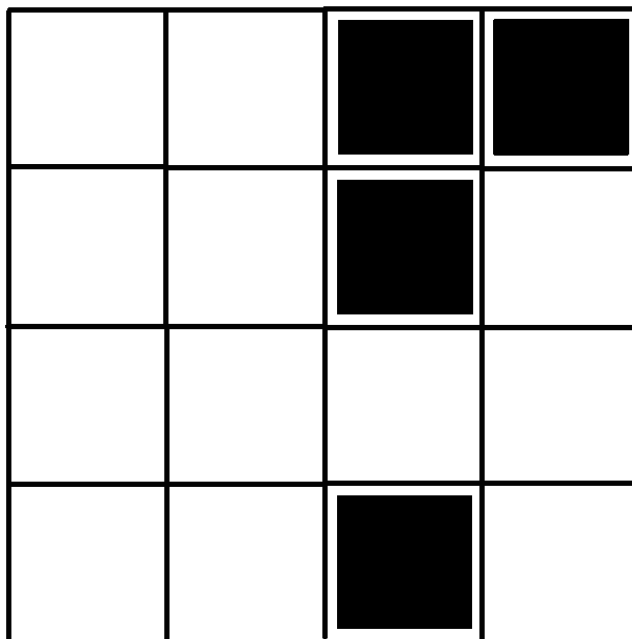
## Darbo lapas. Dovilės šifras

---

Žirklemis iškirpkite kvadratinės groteles ir juodus jos langelius.

Pabandykite iššifruoti žemiau patektą tekstą.

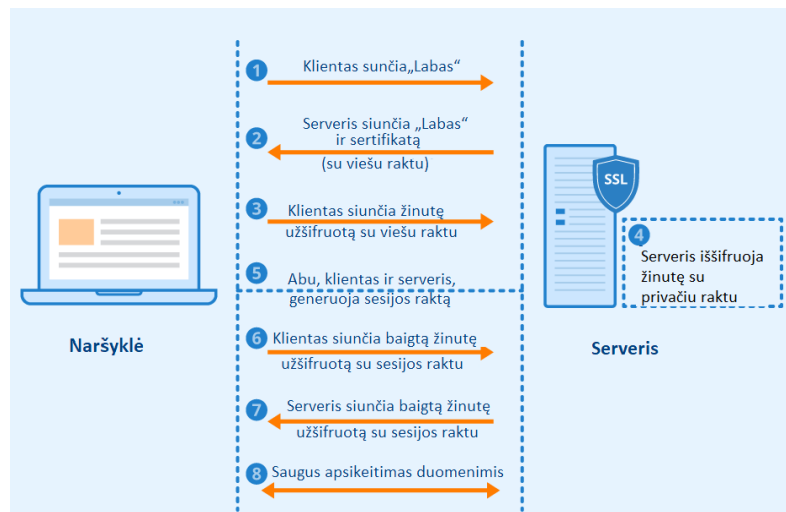
Kokias taisykles taikėte iššifruodami?



U	O	S	Š
I	T	F	R
S	T	T	E
K	A	A	S

## Apie ką visa tai?

Vienas iš pagrindinių kompiuterių tinklų saugumo užtikrinimo būdų yra šifravimas. Milijonai finansinių operacijų, kasdien atliekamų internetu, kriptografija tapo svarbesnė nei bet kada anksčiau. Toliau pateiktoje schemoje pateikta interneto kriptografijos apžvalga.



5 pav. HTTPS Autorius Seobility pagal licenciją: CC BY-SA 4.0

Tinklapiui, apsaugoto SSL/TLS, URL adresas prasideda "https://". HTTPS protokole šifruojami šie duomenų tipai: URL, HTTP antraštė, slapukai ir per formas pateikti duomenys.

Interneto naršyklių saugiam ryšiui užtikrinti naudojamas simetrinio ir asimetrinio šifravimo derinys. SSL/TLS naudoja viešąjį raktą (asimetrinį) šifravimą serverio ir kliento autentiškumui patvirtinti (pradinis rankų suvedimas). Viešojo rakto kriptografija taip pat naudojama sesijos raktui nustatyti. Kai abu partneriai susitaria dėl bendro sesijos rakto, likusioje komunikacijos dalyje naudojamas simetrinis šifravimas. Taip sujungiami asimetrinio šifravimo privalumai autentifikavimui ir greitesnis, mažiau procesoriaus sąnaudų reikalaujantis simetrinio rakto šifravimas dideliame duomenų kiekiui šifruoti.

### Pasukimo grotelės grožinėje literatūroje ir istorijoje

6 × 6 grotelėmis naudojasi Žiulio Verno romano „Mathias Sandorf“ (1885 m.) veikėjas Matijas Sandorf.

Žiulis Vernas pateikia labai gerą sistemos aprašymą. Jis savo skaitytojams sako, kad toks šifras yra ...neįveikiamas, nebent turite grotelės. Vernas su šia idėja susipažino barono Fleiβnerio (atsistatydinusio austrų kavalerijos pulkininko) knygoje „Handbuch“ (1881 m.).

Grotelės (įvairių dydžių) buvo naudojamos vokiečių kariuomenėje 1916 m. pabaigoje (kol prancūzų kriptanalitikai nesukūrė atakų, išnaudojančių grotelių silpnąsias vietas). Daugiau sužinoti apie pasukimo grotelių šifravimą (angl. rotating grille) galite:

[https://www.youtube.com/watch?v=K8AqGksf\\_Ic&ab\\_channel=TheBlackChamber](https://www.youtube.com/watch?v=K8AqGksf_Ic&ab_channel=TheBlackChamber)



# **VI dalis**

**Žmogiškasis kompiuterio veidas  
Bendravimas su kompiuteriu**

# Žmogiškasis kompiuterio veidas

---

Kodėl sunku susidraugauti su kompiuteriu? Dauguma žmonių skundžiasi, kad juo sunku naudotis, kad kompiuteris niekada nedaro to, ko nori vartotojas, arba kad daro neteisingai, kad privelia absurdiškų klaidų... Apskritai kompiuteriai yra sukurti burtininkams, o ne paprastiems mirtingiesiems. Tačiau kompiuteriai turėtų padėti paprastiems žmonėms, nes tai jau kasdieninė mokymosi, darbo ir žaidimų priemonė.

Kompiuterio programinės įrangos dalis, kurią mato vartotojas, vadinama vartotojo sąsaja. Tai svarbiausia dalis! Galima pamanyti, kad svarbiau yra tai, ką programa gali daryti, o vartotojo sąsaja tik leidžia ta programa naudotis. Taip nėra, nes, jei negali su programa „susikalbėti“, tai negali ja ir naudotis. Vartotojo sąsają labai sunku suprojektuoti ir sukurti, todėl jos kūrimas reikalauja daug daugiau pastangų nei kitų programos dalių. Yra programų, turinčių aiškiai suprantamą ir patogią vartotojo sąsają, bet ji tampa nepastebima, kai visas dėmesys skiriamas aplinkai suvokti. Labai daug išties gerų programų nenaudojamos vien dėl to, kad jų sąsaja keista ir sunkiai suprantama. Visi kompiuterių programinės įrangos gamintojai stengiasi sukurti „protingą“ vartotojo sąsają, padedančią naudotis visomis kompiuterio galimybėmis, kurios dažnai yra visiškai elementarios.

Kam reikalinga vartotojo sąsaja? Kodėl negalima tiesiog pasakyti kompiuteriui tai, kas reikalinga, kaip sakoma draugui? Geras klausimas. Gal kada nors taip ir bus, bet tikrai dar ne šiandien! Šio skyriaus veiklos padės suprasti vartotojo sąsajos kūrimo problemas, kompiuterio ribotumą ir sužinoti apie mitus, kuriais dažnai naudojasi dirbantieji kompiuterių pramonėje.

## Mokytojams

Naudojimasis kompiuteriu labiau susijęs su komunikacija nei su skaičiavimu. Kompiuteris savaime neturi vertės – jis vertas tik tada, kai jo darbo rezultatai koku nors būdu pateikiami vartotojui. Tikriausiai informatikai labiau rūpi žmonės, o ne kompiuteriai, nes pastarieji visai nenaudingi, jei koku nors būdu nepadedą žmonėms. Visi siekia, kad kompiuteris dirbtų efektyviau ir sparčiau, grindžiami tik tuo, kad žmogui reikia greitai reaguojančio ir ekonomiškai dirbančio kompiuterio.

Vartotojo sąsaja padeda žmogui bendrauti su kompiuteriu. Šioje knygoje daug rašoma apie bendravimą. Pirmoje knygos dalyje parodoma, kaip kompiuteriui gali būti perduodama įvairi informacija arba kaip ji sklinda tarp kelių kompiuterių. Trečioje dalyje supažindinama, kaip kompiuteriui perduoti informaciją, kad jis ją suprastų, kam reikalingas programavimas ir programavimo kalbos. Penktoje dalyje pasakojama, kaip koduojama slapta informacija.

Šiame skyriuje supažindinama, kaip žmogus bendrauja su kompiuteriu. Kituose skyriuose buvo stengiamasi paaiškinti techninius kompiuterio darbo aspektus, o čia apie tai nekalbama. Šis skyrius gali pasirodyti paprastesnis, nes nereikalauja jokių ypatingų mokinio žinių, tačiau iš tiesų jis gana sudėtingas, nes čia vartojama nauja terminologija, be to, šio skyriaus veiklos siejamos su platesniu kontekstu. Čia pateikiami dalykai kur kas išsamiau aiškinami nei ankstesniuose skyriuose, nes siekiama



suteikti kuo daugiau dalykinės pagalbos mokytojui, kad galėtų sėkmingai koordinuoti mokinių diskusijas ir veiklas.

Šiame skyriuje aprašomos dvi veiklos. Pirmoji – apie kompiuterio programinę sąsają. Mokiniais siūloma atlikti vartotojo sąsajos projektavimo pratimą, kuriam nereikia kompiuterio, taip pat paaiškinti pagrindinius sąsajos projektavimo principus. Kadangi kompiuterio vartotojo sąsaja priklauso nuo kiekvienos šalies kultūros, todėl čia nėra „teisingų“ atsakymų. Antroji veikla supažindina su dirbtiniu intelektu, arba DI. Mokiniai žaidžia spėjimo žaidimą, kuris skatina susimąstyti, ką kompiuteris gali, o ko negali.

### **Technologiškai mąstantiems mokiniams**

Žmogaus ir kompiuterio bendravimas tapo karščiausia informatikos tiriamąja sritimi, kai žmonės suprato, kad sukurtos programos sėkmė iš esmės priklauso nuo jos sąsajos. Ši sritis susijusi su daugeliu ne informatikos dalykų: psichologija, kognityviniu mokslu, lingvistika, sociologija ir net antropologija. Kai kurie informatikai tiria šiuos dalykus, o kompiuterio programų sąsajų projektavimo tyrimai tampa svarbia besiplėtojančia informatikos mokslo sritimi.

Dirbtinis intelektas visada sukelia labai daug diskusijų. Šioje knygoje pateikiamos vyraujančios nuomonės apie dirbtinį intelektą. Vieni mano, kad DI tikrai bus sukurtas ir juo pasižyminčios mašinos mąstys kaip žmonės, kiti – kad tai neįmanoma. Šios knygos tikslas – padrąsinti mokinius savarankiškai mąstyti apie DI ir drąsiai reikšti savo nuomonę.

Šie skyriai buvo parengti remiantis dviem knygomis: Dono Normano „The Design of Everyday Things“ (New York: Doubleday. 1988) ir Johno Haugelando „Artificial Intelligence: the Very Idea“ (Cambridge, Mass.: MIT Press. 1985).

Kompiuterių mokslas apima dar vieną labai svarbią, bet šioje knygoje neaprašytą sritį – žmonių, kuriančių kompiuterių sistemas, komunikaciją. Informatikos studijas baigę specialistai, pradėję dirbti kokiose nors įstaigose, nustemba, kiek daug visuomeninio bendravimo būdų egzistuoja jų darbe. Kompiuterinės programos yra sudėtingiausias žmogaus sukurtas dalykas, sudarytas iš milijardų painiai sujungtų dalių. Programavimo projektai rengiami uždaroje jungtinėse informatikų grupėse, kurios dirba kartu ir daug laiko skiria bendravimui. Baigus darbą bendraujama su vartotojais, organizuojami kursai, steigiamos pagalbos telefono linijos, užtikrinamas palaikymas tinkle, vyksta demonstracijos ir reklama. Apie visa tai šioje knygoje nekalbama, tačiau pakviestas į klasę informatikas galėtų papasakoti ir apie šiuos darbo aspektus.





## 22 veikla

# Šokolado fabrikas. Žmogaus sąsajos su kompiutriu projektavimas

---

### Santrauka

Šios veiklos tikslas – skatinti mokinius suvokti, kaip projektuojama žmogui lengvai suprantama vartotojo sąsaja. Kadangi visuomenėje yra paplitęs „skurdus“ dizainas, užuot įvardijus būtent netinkamo dizaino problemą, įprasta sau prisiimti „kalbę“ dėl negebėjimo tinkamai naudotis vienu ar kitu įrenginiu, aparatu ar programa („žmogiška klaida“, „nepakankamas mokymas“, „tai pernelyg sudėtinga man“). Vartotojo sąsajos dizaino problema yra aktuali ir kompiuteriuose. Be pagrindinės savo paskirties (padėti apdoroti duomenis), kompiuteriai savaime nesuteikia jokių priemonių, kurios padėtų išsiaiškinti, kam jie skirti ir kaip juos valdyti.

### Ryšiai su ugdymo programomis

- ✓ Technologijos: technologijų dizainas

### Gebėjimai

- ✓ Dizaino suvokimo
- ✓ Loginio argumentavimo
- ✓ Kasdienių objektų pažinimo

### Amžius

- ✓ Nuo 7 metų

### Medžiaga

Kiekvienai mokinių grupei reikia:

- ✓ Darbo lapų „Kaip atveriamos durys?“ ir „Viryklė“
- ✓ Darbo lapo „Piktogramos“ (jį galima rodyti projektoriumi arba padaryti ir išdalyti visai klasei didesnes demonstravimo korteles)
- ✓ Darbo lapo „Piktogramų kortelės“ (kortelės sukarpomos ir padalijamos grupėms)



# Šokolado gamykla

---

## Ivadas

Įdomų šokolado fabriką sukūrė panašių į elfus būtybių umpa lumpų<sup>2</sup> gentis. Umpa lumpai yra labai užmaršūs ir nemoka rašyti. Jiems sunku atsiminti, ką ir kaip daryti tvarkant šokolado fabriko reikalus. Todėl jie nori sukurti naują fabriką, kurį būtų labai lengva valdyti.

## Diskusijos

Mokiniam papasakojama istorija. Jie susiskirsto į grupes.

1. Pirmoji umpa lumpų problema yra praeiti pro duris nešant kibirus, pilnus skysto šokolado. Jie niekaip negali atsiminti, ar atveriant duris reikia stumti, ar traukti. Paprastai šios problemos sprendimo rezultatas – dviejų nešančiųjų susidūrimas ir šokolado ištaškymas.

Mokiniai turi užpildyti darbo lapą „Kaip atverti duris?“ Kiekviena grupė gali pažymėti daugiau kaip vieną variantą, ką daryti su kiekvienomis durimis. Nėra akivaizdu, kaip atidaryti kai kurias duris (įskaitant ir pirmąsias). Mokiniai turi parašyti, ką jie pabandytų pirmiausia. Kai jie užpildo savo lapus, visa grupė diskutuoja apie kiekvienų durų privalumus ir aiškinasi, kaip lengva yra pasakyti, ką turi daryti, ir kaip sunku tai padaryti, kai nešami pilni kibirai. Mokiniai nusprendžia, kokios durys ir rankenos patogiausios fabrike.

Toliau pateiktoje lentelėje apibūdinamos kiekvienos durys. Tikros durys gali būti atveriamos į išorę arba į vidų. Mokiniai aptaria, kokios durys yra jų mokykloje. Ar yra tokių, kurios neaišku kaip atveriamos? Kodėl? Kaip įprastai durys atveriamos: į išorę ar į vidų? (Jos atveriamos į vidų, kad žmonės, einantys koridoriais, nebūtų užgauti. Tačiau gali būti ir kitaip.)

Pagrindinis konceptas yra *objekto įgalinimas* (angl. *affordances*), kai nusakomos objekto ypatybės ar funkcijos, t. y. kokios galimybės suteikiamos šiuo objektu ar kas leidžiama juo padaryti. Pavyzdžiui, daugumai aišku, kad kėdė skirta sėdėti, stalas – daiktams padėti, mygtuką reikia paspausti ir pan. Kompiuterio sąsajos įgalinimas yra mygtukai, tekstų laukai, meniu ir t. t., kurie suteikia vartotojui informacijos, kam yra reikalingi. Jei mygtukas būtų panašus į ką nors kita, nebūtų aišku, ką su juo daryti. Tai atrodo akivaizdu, bet netinkamų objektų vaizdavimo pavyzdžių programų sąsajose yra gausybė.

---

<sup>2</sup>Idėja paimta iš Roaldo Dahlio knygos „Čarlis ir šokolado fabrikas“.



Švaistinės durys	Paprastai stumiamos.	Durys su užrašu	Trumpai užrašyta durų instrukcija. Ar reikia durų naudotojo instrukcijos? Be to, umpa lumpai nemoka skaityti.
Varstomosios durys	Stumiamos į priekį durys.	Durys su apvalia rankena	Apvali rankena rodo, už ko griebti, bet lieka neaišku, stumti ar traukti duris. Tikriausiai durys stumiamos ne į šoną?
Stumdomosios durys	Stumiamos į šoną durys.	Stiklinės durys	Vertikali stiklinių durų juosta rodo, kad duris reikia traukti, o horizontali – kad reikia stumti.
Baro durys	Visai aišku, kad baro duris reikia stumti, bet į kurią pusę? O gal jas traukti į save?	Durys su rankena	Rankenos paprastai rodo, kad duris reikia traukti arba stumti į šoną.
		Durys be rankenos	Nesimato, kaip jas atverti. Greičiausiai tokias duris reikia stumti, o ne traukti.

Durys yra paprastas objektas. Ką daryti su sudėtingais dalykais, reikia paaiškinti, bet tai nebūtina, kai kalbama apie paprastus dalykus. Kai prie paprastų dalykų pridedami aiškinamieji paveikslėliai ar instrukcijos, dizainas išdankomas.

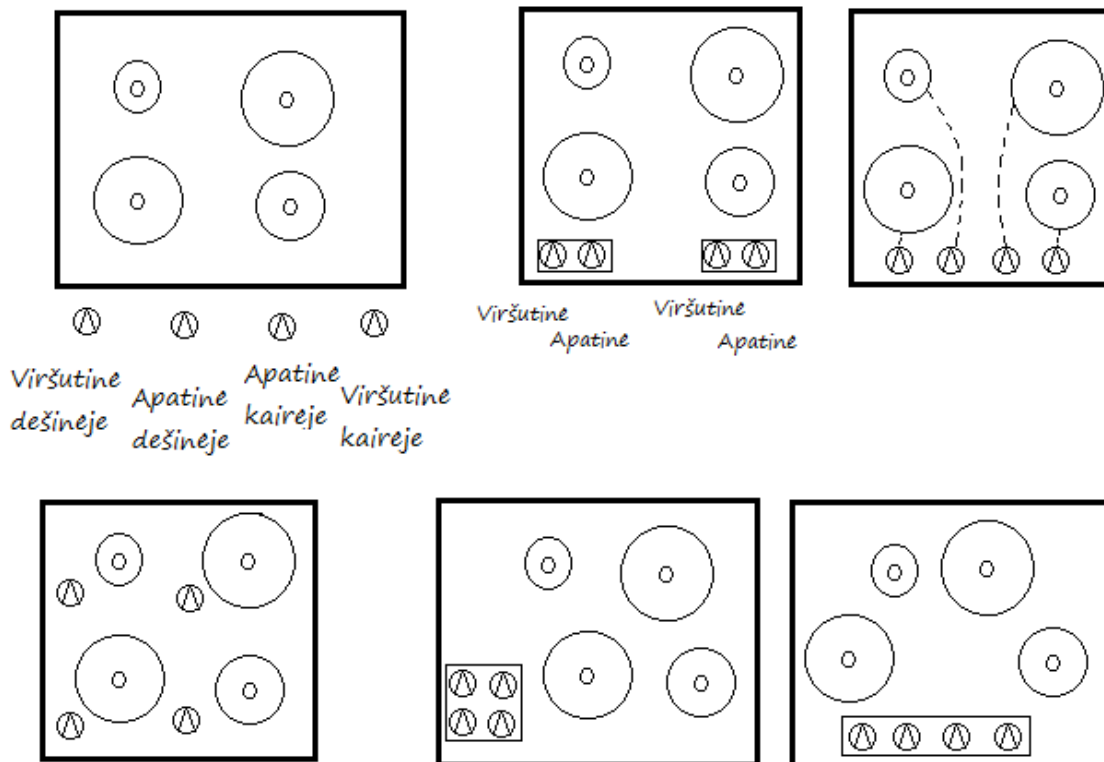
2. Skirtingoms šokolado rūšims paruošti reikia skirtingos temperatūros. Sename šokolado fabrike viryklės yra labai senos. Jos pavaizduotos darbo lape „Viryklė“. Kairioji viršutinė viryklės kaitvietė yra reguliuojama kairiausiai esančia apvalia rankenėle; priekinė kairioji kaitvietė reguliuojama antrąja iš kairės rankenėle; dešinioji viršutinė kaitvietė – trečia iš dešinės rankenėle, o apatinė dešinioji kaitvietė – paskutine, ketvirtąja, iš kairės rankenėle. Virdami šokoladą umpa lumpai visada klysta. Jie nuolat verda šokoladą nustatę netinkamą temperatūrą, apdegina savo rankoves siekdami puodo su šokoladu.

Mokiniai turėtų prisiminti, kaip išdėstytos viryklių valdymo rankenėlės ar jungikliai jų namuose, ir pasiūlyti, kaip geriausiai jas ar juos išdėstyti naujo fabriko viryklėse.

Ši užduoties dalis atliekama diskutuojant su visa klase. Toliau pateikti šeši paveikslai, kuriuose pavaizduota, kaip galima išdėstyti viryklės kaitviečių jungiklius. Visuose paveiksluose, išskyrus apatinį kairįjį, kuriame viryklės jungikliai yra prie kiekvienos kaitvietės, visi jungikliai yra priekyje. Viršutiniame kairiajame paveiksle kaitvietes įjungti viryklės jungikliais galima net 24 būdais, todėl prie jungiklių reikalingi



aiškinamieji užrašai. Viršutiniame antrajame iš kairės paveiksle jungikliai sudėti poromis, taigi šiek tiek aiškiau, kaip jais įjungti kaitvietes, nes yra tik 4 galimybės. Tačiau ir tokį jungiklių išdėstymą reikia paaiškinti. Viršutiniame dešiniajame paveiksle jungiklių ir kaitviečių ryšiai parodyti grafiškai – taip tikrai geriau umpa lumpams. Apatiniuose paveiksluose nereikia aiškinti, kaip išdėstyti viryklių jungikliai.



Pagrindinis konceptas – *atvaizdavimas*, kaip sudėlioti jungiklius realioje viryklėje, todėl mokiniai remiasi savo namų patirtimi. Ji pagreitina suvokimą. Apatinėje eilėje vaizduojama jungiklių išdėstymo tvarka yra paprasta ir lengvai įsimenama, o viršutinėje eilėje ji turi būti paaiškinta (tekstu ar grafiškai).

3. Kaip ir kiekviename automatizuotame fabrike, taip ir čia gausu transporterio juostų, kuriomis slenka šokolado pusgaminiai. Šias juostas umpa lumpai valdo rankiniu būdu pagal instrukcijas iš pagrindinio valdymo kambario. Valdytojai umpa lumpai fabriko valdymo kambaryje visada turi žinoti ir pasakyti kitiems, kada juostą sustabdyti, sulėtinti ar vėl paleisti. Anksčiau ši informacija buvo perduodama balsu: valdytojas iš valdymo kambario per garsiakalbį sakydavo, ką daryti. Tačiau fabrike visada labai triukšminga ir sunku išgirsti, kas sakoma.

Mokinių grupės turi sukurti vizualinius signalus, kuriais būtų perduodama informacija iš valdymo kambario.

Viena iš galimybių, kurią gali pasiūlyti mokiniai, – tai švieslentės su trimis signalais: „Sustoti!“, „Lėčiau!“, „Judėti!“ Mokiniai gali pasiūlyti vaizduoti signalus atitinkamomis spalvomis: raudona, geltona, žalia. Jos gali būti išdėstomos kaip šviesofore.

Tada mokiniams galima paaiškinti, kad umpa lumpai šviesoforo signalus supranta kitaip nei žmonės: geltona reiškia sustoti, raudona – judėti, o žalia įspėja, kad tuoj bus galima



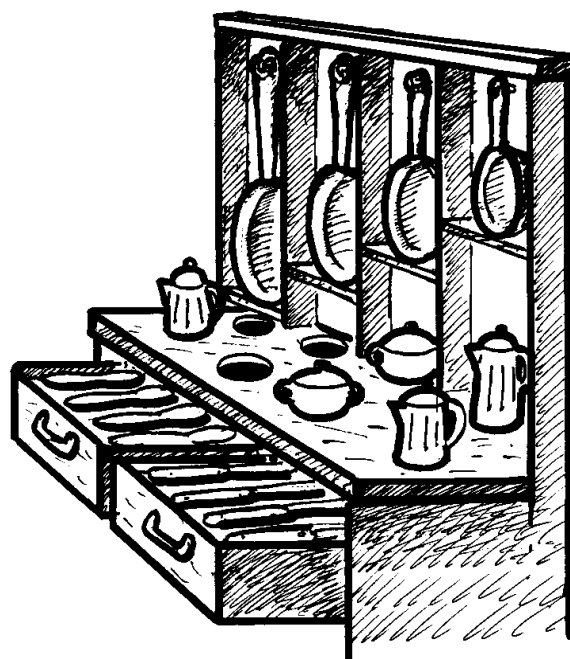
judėti. Kaip dabar turėtų viskas atrodyti? (Fabrike signalų spalvos turėtų reikšti tą patį, kaip jas supranta umpa lumpai. Nereikėtų pridėti naujų spalvų.)

Pagrindinis konceptas – *informacijos pritaikymas ir visuomeniniai stereotipai*. Tikimasi, kad taisyklės, tinkančios vienoje visuomenėje, turi tikti ir kitoje. Mokiniai pritaiko gerai žinomą informaciją (šviesoforus) naujomis sąlygomis (sukeičia spalvų reikšmes). Šios veiklos situacijos gali atrodyti dirbtinės, tačiau pasaulyje pilna pavyzdžių, kai skirtingos visuomenės turi skirtingas taisykles. Pavyzdžiui, eismas Lietuvoje vyksta dešiniaja kelio puse, o Jungtinėje Karalystėje – kairiąja; dešimtainių skaičių vaizdavimas su kableliu arba tašku; datos formatas: diena, mėnuo, metai ir metai, mėnuo, diena ir pan.

4. Kai viena pamaina baigia darbą šokolado fabrike, viską išvalo ir sudeda puodus, kaistus, ąsočius, šaukštus, maišytuvus į spintą su lentynomis. Tačiau umpa lumpams visada sunku prisiminti, į kokias lentynas kokius daiktus dėti.

Mokinių grupės turėtų sugalvoti lengvesnį sprendimą, kaip umpa lumpams priminti, kur kiekvieno daikto vieta.

Paveiksle dešinėje pavaizduota, kaip turėtų būti sudėlioti daiktai (kartais jie taip ir būna sudėti).



Pagrindinis konceptas – *vizualizavimas*. Vizualizuojant daiktų vietas akivaizdu, kur ką padėti.

5. Anksčiau minėtame valdymo kambaryje yra daug mygtukų, svirčių ir jungiklių, kuriais valdomos fabriko mašinos. Aišku, jie turi būti pavadinti, bet umpa lumpai nemoka skaityti, todėl reikia grafinio paaiškinimo – piktogramų.

Su piktogramomis mokiniai susipažįsta atlikdami darbo lapo „Piktogramos“ užduotis. Mokiniai turi nustatyti, ką reiškia pavaizduotos piktogramos. Pavyzdžiui, į voką dedamas laiškas reiškia, kad laiškas išsiunčiamas el. paštu. Nėra teisingų ar neteisingų aiškinimų. Pagrindinė šios užduoties mintis – surasti visas įmanomas piktogramų reikšmes.

6. Dabar mokiniai jau gali sukurti savo piktogramas šokolado fabriko valdymo kambariui. Paskutinio darbo lapo kortelėse surašytos funkcijų grupės. Kiekviena mokinių grupė gauna vieną arba dvi korteles. Valdymo skyde esančios piktogramos reiškia 4–5 operacijas. Nieko neaiškindamos grupės parodo savo piktogramas kitoms grupėms ir paprašo paaiškinti, ką tos piktogramos galėtų reikšti. Padrąsinkite mokinius pasitelkti vaizduotę, spalvas ir paprastas, aiškias piktogramas.

## Darbo lapas. Kaip atverti duris?

Užpildykite lapą. Pažymėkite, kas būdinga kiekvienos rūšies durims. Vienos rūšies durims gali būti tinkami ir keli požymiai.

### Durys be rankenos



- Stumti  į kairę
- Traukti  į dešinę
- Stumti į šoną

### Durys su užrašu



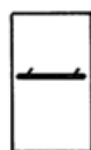
- Stumti  į kairę
- Traukti  į dešinę
- Stumti į šoną

### Švaistinės durys



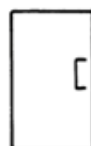
- Stumti  į kairę
- Traukti  į dešinę
- Stumti į šoną

### Baro durys



- Stumti  į kairę
- Traukti  į dešinę
- Stumti į šoną

### Durys su rankena



- Stumti  į kairę
- Traukti  į dešinę
- Stumti į šoną

### Durys su apvalia rankena



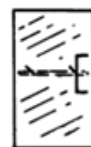
- Stumti  į kairę
- Traukti  į dešinę
- Stumti į šoną

### Varstomosios durys



- Stumti  į kairę
- Traukti  į dešinę
- Stumti į šoną

### Stiklinės durys



- Stumti  į kairę
- Traukti  į dešinę
- Stumti į šoną

### Stumdomosios durys



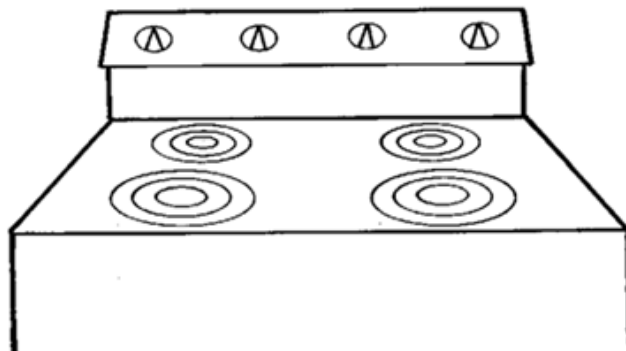
- Stumti  į kairę
- Traukti  į dešinę
- Stumti į šoną

## Darbo lapas. Viryklė

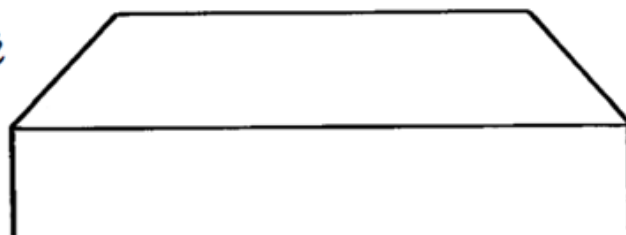
---

Išdėstykite kaitvietes ir jų jungiklius taip, kad umpa lumpams būtų patogiu.

*Senoji  
viryklė*



*Naujoji  
viryklė*

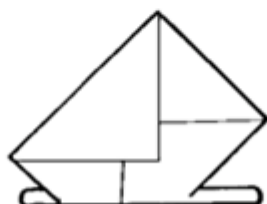
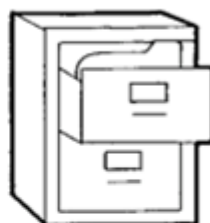
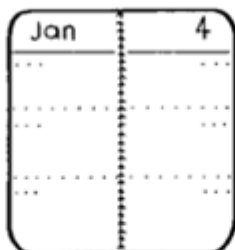
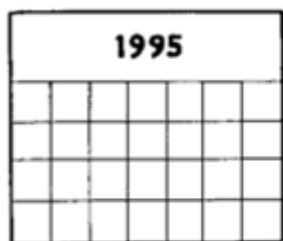


## Darbo lapas. Piktogramos

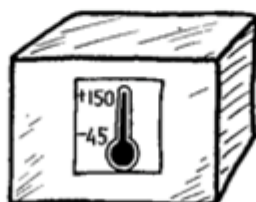
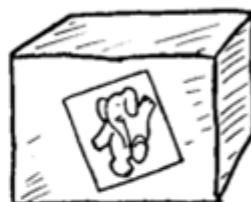
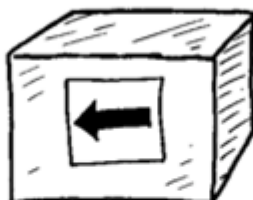
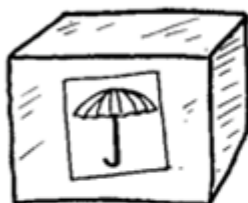
---

Kaip manote, ką vaizduoja šios piktogramos?

*Biure...*



*Ant dėžės...*





## Darbo lapas. Piktogramų kortelės

Kiekvienai grupei duodama po vieną arba dvi korteles. Grupė sugalvoja ir nupiešia piktogramą, atitinkančią kortelę.

<b>Sudedamosios dalys</b> <ul style="list-style-type: none"><li>• Kakava.</li><li>• Pienas.</li><li>• Cukrus.</li><li>• Papildomas cukrus.</li><li>• Sviestas.</li></ul>	<b>Priedai</b> <ul style="list-style-type: none"><li>• Riešutai.</li><li>• Karamelė.</li><li>• Imbieras.</li><li>• Razinos.</li><li>• Kokoso riešutai.</li></ul>
<b>Gaminimas</b> <ul style="list-style-type: none"><li>• Pradėti maišyti.</li><li>• Nustoti maišyti.</li><li>• Pradėti šildyti.</li><li>• Nustoti šildyti.</li><li>• Supilstyti į formas.</li><li>• Spausti antspaudą (daug įvairių).</li></ul>	<b>Ragavimas</b> <ul style="list-style-type: none"><li>• Paragauti jį.</li><li>• Nuostabus! – Pirmoji vieta.</li><li>• Geras. – Antroji vieta.</li><li>• Ech! – Perdaryti.</li><li>• Ech! Ech! – Išmesti.</li></ul>
<b>Pjaustymas</b> <ul style="list-style-type: none"><li>• Maža plytelė.</li><li>• Vidutinė plytelė.</li><li>• Didelė plytelė.</li><li>• Milžiniška plytelė.</li><li>• Nurodyti plytelės dydį...</li><li>• Šokolado drožlės.</li></ul>	<b>Pakavimas</b> <ul style="list-style-type: none"><li>• Įvynioti į foliją.</li><li>• Įvynioti į popierių.</li><li>• Įdėti į maišelį.</li><li>• Įdėti į dėžutę.</li><li>• Įjungti konvejerį.</li><li>• Išjungti konvejerį.</li></ul>



## Gudručiams

Ar mokiniai galėtų nustatyti laiką rankiniame laikrodyje arba mikrobangų krosnelėje? Susieti viryklės kaitvietes su jungikliais nebuvo sunku, nes yra tik keturios kaitvietės ir keturi jungikliai. Kai daugėja veiksmų, daugėja ir valdiklių. Rankinio laikrodžio rodyklės ar mikrobangų krosnelės valdikliai yra labai sudėtingi ne dėl rodyklių ar mygtukų skaičiaus (dažniausiai yra tik dvi rodyklės ir keli mygtukai), bet dėl šių prietaisų galimų atlikti funkcijų gausos. („Norint su tuo susidoroti reikia inžinieriaus mokslo laipsnio,“ – pasakė žymus vartotojo sąsajos kūrimo psichologas Donas Normanas, pažvelgęs į savo naują rankinį laikrodį. Donas neturėjo aukštojo inžinerinio išsilavinimo, todėl nustatyti laiką savo naujame laikrodyje užtruko apie valandą. Kodėl jam prireikė valandos?)

Mokiniai galėtų pagalvoti ir įvardinti, kokius prietaisus ar įrenginius naudodami žmonės jaučiasi suglumę. Pavyzdžiui, mobilieji telefonai, vaizdo įrašymo įrenginiai, kompiuteriai – visais šiais įrenginiais gali būti sunku naudotis. Mokiniai turėtų atsakyti į klausimą, kokie prietaisai ar įrenginiai glumina žmones ir kaip galėtų būti pakeista jų vartotojo sąsaja, kad būtų lengviau suprantama.

## Apie ką visa tai?

---

Žmogaus ir kompiuterio ryšys atsiranda projektuojant, vertinant ir naudojant kompiuterines sistemas, kurios šiandien padeda atlikti daugelį darbų produktyviai ir saugiai. Pirmieji kompiuteriai buvo kuriami specialistams, todėl buvo tikimasi, kad jais naudosis tik specialiai parengti vartotojai. Dabar kompiuteris yra kasdieninė priemonė, todėl jo vartotojo sąsaja turi būti suprantama ir lengvai naudojama.

Dėl kompiuterių vartotojo sąsajos netikslumų įvyksta nemažai nelaimių (lėktuvų, traukinių, branduolinių elektrinių avarių ir kt.), kai kada net prarandama žmonių gyvybių. Kai kurios dėl netinkamos vartotojo sąsajos daromos klaidos piktina žmones (pavyzdžiui, per klaidą policijos išsiunčiami pranešimai dėl skirtos baudos ir pan.).

Kai kas nors nutinka per klaidą, žmonės linkę kaltinti save – „žmogaus klaida“. Tačiau dauguma tokių „žmogaus klaidų“ yra tiesiog kompiuterio vartotojo sąsajos klaidos. Žmonių galimybės apdoroti informaciją yra ribotos, į tai turėtų atsižvelgti vartotojo sąsajos kūrėjai. Ne išeitis pateikti išsamią iš esmės blogos vartotojo sąsajos instrukciją tikintis, kad žmogus ją studijuos ir atsimins. Be to, reikėtų atsižvelgti ir į žmogaus netobulumą (žmogus klysta), taip pat nereikėtų pamiršti ir tinkamo sąsajos dizaino.

Vartotojo sąsajos vertinimas yra svarbus jos dizaino kūrimo etapas. Šiame skyriuje yra keletas užduočių, kai mokiniai turi įvertinti pateiktas ir testuoti kitų mokinių sukurtas piktogramas. Kruopštesnis vertinimas gali būti atliktas kontroliuojamu psichologiniu eksperimentu.

### Daugiau informacijos

Dono Normano knygoje „The Design of Everyday Things“, Jeffo Johnsonso knygoje „Designing with the Mind in Mind“ – apie žmonių mąstymą, apie tai, kaip vartotojo sąsaja turėtų būti kuriama atsižvelgiant į žmonių galimybes ir poreikius.



## 23 veikla

# Dialogas su kompiuteriu. Tiuringo testas

---

### Santrauka

Šios veiklos tikslas – diskutuoti, ar dabartiniai kompiuteriai turi intelektą, ar kompiuterių intelektas bus įmanomas tik ateityje. Vyresniosios kartos informatikai teigia, kad bus sunku atpažinti dirbtinį intelektą, jei jis kada nors ir bus sukurtas, juolab kad čia įmanomos apgavystės.

### Ryšiai su ugdymo programomis

- ✓ Informatika: technologinės sistemos

### Gebėjimai

- ✓ Interviu
- ✓ Loginio argumentavimo

### Amžius

- ✓ Nuo 7 metų

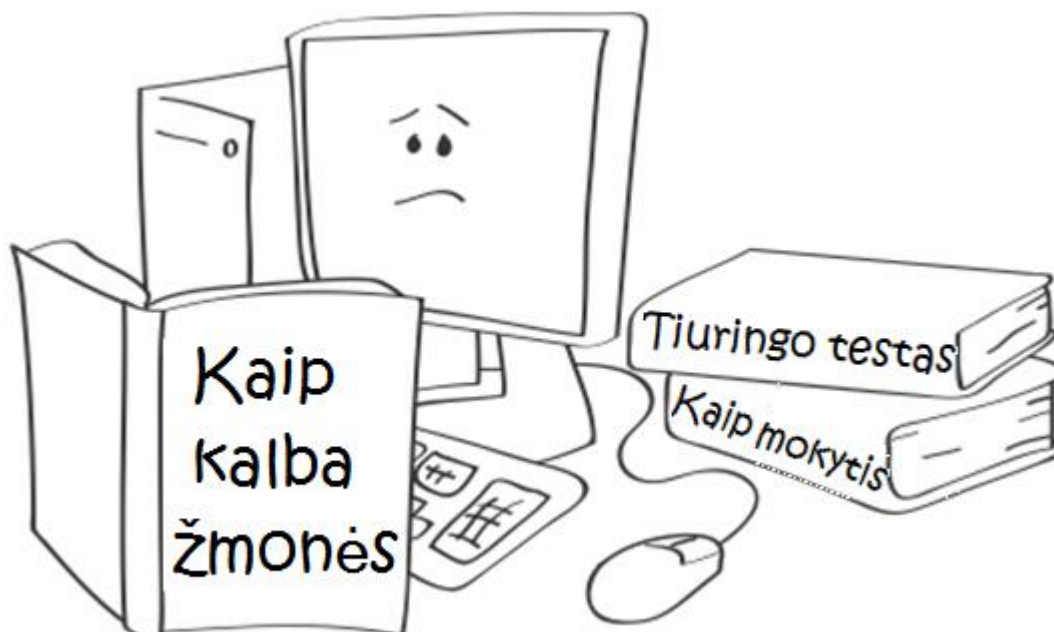
### Medžiaga

- ✓ Darbo lapas „Tiuringo testo klausimai“ (kiekvienam mokiniui)
- ✓ Darbo lapas „Tiuringo testo atsakymai“ (kiekvienam mokiniui)



## Dialogas su kompiuteriu

---



### Diskusija

Šiame skyriuje mokiniai žaidžia žaidimą, kuriame turi įžvelgti skirtumą tarp žmogaus ir kompiuterio, užduodami klausimus ir analizuodami atsakymus.

### Instrukcija

Žaidžiama keturiese. Tarkime, žaidėjų vardai Tadas, Toma, Žilvinas ir Kamilė. Pirmosios vardų raidės padės prisiminti žaidėjų atliekamus vaidmenis. Tadas ir Toma yra tarpininkai, o Žilvinas ir Kamilė atsakinėja į klausimus. Žilvinas atsakinės kaip žmogus, o Kamilė – kaip kompiuteris. Toma ir Tadas stebi, ar teisingai žaidžiama: jie perduoda klausimus Žilvinui ir Kamilei, bet nepasako, kuris klausimas kuriam skirtas. Likę klasės mokiniai yra auditorija. Auditorijos tikslas – nustatyti, kuris iš atsakinėjančiųjų vaizduoja žmogų, o kuris – kompiuterį. Žilvinas ir Kamilė yra atskirti nuo auditorijos ir vienas nuo kito (geriausia, kad jie būtų skirtingose patalpose). Žaidimą koordinuoja mokytojas.

Toma paima klausimą iš auditorijos ir perduoda Žilvinui, o Tadas tą patį klausimą perduoda Kamilei (auditorija nežino, kuris tarpininkas kuriam atsakinėtojui perduoda klausimus). Žilvinas ir Kamilė perduoda atsakymus auditorijai. Tarpininkų tikslas – saugoti, kad auditorija nesužinotų, kurį atsakymą perdavė Žilvinas, o kurį Kamilė.

Žaidimo pradžioje išrenkami mokiniai, jiems paaiškinamos taisyklės. Toma ir Tadas paima klausimus iš auditorijos, perduoda atitinkamai Žilvinui ir Kamilei, tada perduoda atsakymus auditorijai. Svarbu, kad jie neprasitartų, kieno atsakymą skaito auditorijai. Žilvinas pats sugalvoja atsakymus, o Kamilė užrašo atsakymus iš Tiuringo testo atsakymų lapo. Be to, Kamilė turi įvykdyti pasviruoju šriftu parašytas instrukcijas.

Tadas ir Toma atsakymus užrašo ant lapelių.



1. Dar nepradėjus žaisti mokinių paprašoma atsakyti, ar kompiuteris, jų nuomone, gali būti intelektualus. Jei mokiniai mano, kad gali, paprašoma paaiškinti, kaip galima tai nustatyti.
2. Mokiniai supažindinami su Tiuringo testu, kuriuo užduodant klausimus išsiaiškinami žmogaus ir kompiuterio skirtumai. Jei mokiniai nesupranta skirtumo, tai „kompiuteris“ gali įveikti testą. Paaiškinama, kad Tadas ir Toma perduos auditorijos klausimus dviem mokiniams, kurių vienas atsakinėja kaip žmogus, o kitas – kaip kompiuteris. Auditorijos tikslas – nustatyti, kuris atsakinėja kaip kompiuteris.
3. Mokiniams parodomi Tiuringo testo klausimai. Klausimų lapus galima padalyti mokiniams arba rodyti projektoriumi.

Mokiniams leidžiama pasirinkti, kokį klausimą užduoti pirmiausia. Tada prašoma paaiškinti, kodėl būtent tą klausimą jie norėtų užduoti aiškindamiesi kompiuterio ir žmogaus skirtumus. Pasirinkimo pagrindimas yra svarbiausia žaidimo dalis, nes tai skatina mokinius mąstyti, kaip į klausimą galėtų atsakyti žmogus, kaip kompiuteris negalėtų atsakyti ir pan.

Kai Tadas ir Toma grįžta su atsakymais, auditorija diskutuoja, kuris atsakymas yra žmogaus, o kuris – kompiuterio.

Žaidimas kartojamas, kol mokiniai atpažįsta, kuris iš mokinių vaizduoja kompiuterį. Jei mokiniai greitai išsiaiškina „kompiuterį“, Tadas ir Toma mesdami monetą iš naujo parenka, kuriam mokiniui – Žilvinui ar Kamilei – perduos klausimus. Auditorija ir vėl neturi žinoti, kuriam atsakinėtojų kuris tarpininkas perduoda klausimus.

Kamilės pateikiami atsakymai iš Tiuringo testo atsakymų lapo yra panašūs į kompiuterio generuojamus atsakymus. Kai kurie atsakymai iškart rodo, kad atsakinėja kompiuteris. Pavyzdžiui, tikriausiai nė vienas mokinys negalėtų iškart pasakyti, kam lygus skaičiaus, sudaryto iš 10 ar 20 skaitmenų, kvadratas. Kai kurie klausimai išduoda kompiuterį, nes atsakymai gali būti kombinuojami. Pavyzdžiui, klausimai, pradedami fraze „Ar tau patinka...“, skamba įtikinamai, bet, kai užduodama daugiau kaip vienas toks klausimas, tampa aišku, kad atsakymus į tokius klausimus generuoja paprasta programa. Kai kurie atsakymai rodo, kad klausimas buvo neteisingai suprastas, nors mokiniai gali tvirtinti, kad ir žmonės klysta.

Daug atsakymų yra mandagūs, bet „saugūs“, t. y. atsakymai į juos leidžia suprasti, kad iš tikrųjų kompiuteris nesupranta, apie ką klausinėjama. Atsakymas „Aš nežinau“ yra neutralus ir kompiuteriui suteikia žmogiškumo, nes tokio atsakymo galima tikėtis ir iš žmogaus. Tačiau, jei toks atsakymas labai dažnas arba taip atsakoma į labai paprastus klausimus, tai išduoda kompiuterį.

Kadangi kompiuterio tikslas yra įtikinti, kad jis mąsto kaip žmogus, kai kurie atsakymai yra sąmoningai klaidingi. Pavyzdžiui, pateikiamas neteisingas aritmetinių veiksmų atsakymas. Klausimai ir atsakymai gali sukelti daug diskusijų.



## Darbo lapas. Tiuringo testo klausimai

---

Pasirinkite klausimų iš sąrašo:

1. Koks yra Barto Simpsono mažosios sesers vardas?
2. Ką tu manai apie Astridą Lindgren?
3. Ar tu kompiuteris?
4. Koks yra tolesnis sekos 3, 6, 9, 12, 15 narys?
5. Ką tu manai apie masinio naikinimo ginklus?
6. Kiek yra  $2 \times 78$ ?
7. Kiek gautum ištraukęs kvadratinę šaknį iš dviejų?
8. Sudėk 34957 ir 70764.
9. Ar tau patinka mokykla?
10. Ar tau patinka šokti?
11. Kokia šiandien savaitės diena?
12. Kiek dabar valandų?
13. Kiek vasaris turi dienų keliamaisiais metais?
14. Kiek savaitė turi dienų?
15. Kokios šalies vėliavoje vaizduojamas raudonas skritulys baltame fone?
16. Ar tau patinka skaityti knygas?
17. Ką tu labiausiai mėgsti valgyti?



## Darbo lapas. Tiuringo testo atsakymai

---

Pasirinkite atsakymą į užduotą Tiuringo testo klausimą.

1. Koks yra Barto Simpsono mažosios sesers vardas?

**Nepamenu.**

2. Ką tu manai apie Astridą Lindgren?

**Jos knygos patinka vaikams.**

3. Ar tu kompiuteris?

**O tu kompiuteris?**

4. Koks yra tolesnis sekos 3, 6, 9, 12, 15 narys?

**18.**

5. Ką tu manai apie masinio naikinimo ginklus?

**Masinio naikinimo ginklai yra labai pavojingi ir turėtų būti nenaudojami.**

6. Kiek yra  $2 \times 78$ ?

**166 (Sąmoningai neteisingas atsakymas!)**

7. Kiek gautum ištraukęs kvadratinę šaknį iš dviejų?

**1,41421356237309504878**

8. Sudėk 34957 ir 70764.

**Palauk 20 s ir pateik atsakymą... 105721.**

9. Ar tau patinka mokykla?

**Taip, man patinka mokykla.**

10. Ar tau patinka šokti?

**Taip, man patinka šokti.**

11. Kokia šiandien savaitės diena?

**Parašyk teisingą savaitės dieną.**

12. Kiek dabar valandų?

**Parašyk teisingą atsakymą.**

13. Kiek vasaris turi dienų keliamaisiais metais?

**2000 ir 2004 yra lyginiai metai. (Sąmoningai neteisingas atsakymas!)**

14. Kiek savaitė turi dienų?

**Septynias.**

15. Kokios šalies vėliavoje vaizduojamas raudonas skritulys baltame fone?

**Aš nežinau.**

16. Ar tau patinka skaityti knygas?

**Taip, man patinka skaityti knygas.**

17. Ką tu labiausiai mėgsti valgyti?

**Aš nealkanas, ačiū.**





## Gudručiams

Žaidime gali dalyvauti ir mažiau nei trys mokiniai. Toma gali atlikti Tado ir Kamilės vaidmenis. Ji paima Žilvino atsakymą, pati užrašo atsakymą iš Tiuringo testo atsakymų lapo. Atsakymus pažymi A ir B, kad žinotų, kuris atsakymas yra žmogaus, o kuris – nurašytas iš testo.

Mokiniai gali aptarti, kokių žinių reikia aiškinantis, su kuo kalbama – žmogumi ar kompiuteriu. Jie gali papildyti Tiuringo testo klausimų ir atsakymų lapus.

Toliau pateikiami du galimi kompiuterio ir žmogaus pokalbiai. Pirmajame daug klausimų, į kuriuos reikia faktinių atsakymų, o antrajame svarbu plėtoti diskusiją.

### I pokalbis

Klausimas: Prašau parašyti poemą apie Trakų pilį.

Atsakymas: Manęs to neprašyk – nemoku rašyti eilių.

Klausimas: Sudėk 34957 ir 70764.

Atsakymas: *Po 30 s...* 105721.

Klausimas: Ar moki žaisti šachmatais?

Atsakymas: Taip.

Klausimas: Mano karalius yra K1 langelyje, daugiau mano figūrų lentoje nėra. Tu turi tik karalių K6 langelyje ir bokštą R1 langelyje. Tavo ėjimas.

Atsakymas: *po 15 s ...* Bokštas į R8, šachas ir matas.

### II pokalbis

Klausimas: Pirmoje soneto eilutėje parašyta „Galėčiau tave lyginti su vasaros diena“. Gal „pavasario diena“ rimuojasi geriau?

Atsakymas: Nepasakyčiau.

Klausimas: O kaip „žiemos diena“? Geriau?

Atsakymas: Taip, bet niekas nenorėtų būti lyginamas su žiemos diena.

Klausimas: Ar tu manai, kad ponui Pikvikui nepatinka Kalėdos?

Atsakymas: Tam tikra prasme.

Klausimas: Kalėdos yra žiemos diena. Ar manai, kad ponas Pikvikas prieštarautų tokiam palyginimui?

Atsakymas: Nemanau, kad tu rimtai. Paprastai „žiemos diena“ suprantama kaip paprasta žiemos diena, o ne ypatinga Kalėdų diena.

Laisvai internetu prieinama sistema „Eliza“ imituoja pokalbius su psichoterapeutu. Ji generuoja gana intelektualų pokalbį pagal labai paprastas taisykles. Skyriuje „Apie ką visa tai?“ aptariami kai kurie iš tų pokalbių. Mokiniai gali patys išbandyti „Elizą“.



## Apie ką visa tai?

---

Filosofai nuolat diskutuoja, ar mašina gali imituoti žmogaus intelektą arba atvirkščiai – ar žmogaus smegenys yra tik mašina, paleidžianti galingą kompiuterio programą. Kai kuriems ši mintis yra absurdiška, o kiti mano, kad dirbtinis intelektas tikrai bus sukurtas. Dar daugiau – bus sukurta mašina, kuri mąstys kaip žmogus. Tokia mašina galėtų sukurti dar protingesnę mašiną. Pritariantys dirbtinio intelekto (DI) idėjai mokslininkai kritikuojami, kad išsikelia labai aukštų tikslų norėdami pritraukti valstybių, kurios siekia sukurti savarankiškas karo mašinas, lėšų. Tačiau patys mokslininkai protestuoja kaskart, kai tik sukuriama bent šiek tiek daugiau intelekto turinčių karo mašinų. Egzistuoja ir šiek tiek nuosaikesnė nuomonė, kad DI nėra nei absurdiška, nei neišvengiama idėja: kol dabartinės kompiuterių programos neparodo „intelekto“, DI klausimas yra eksperimentinis ir kol kas neatsakytas.

DI diskusijos priklauso nuo intelekto apibrėžimo. Siūloma ir diskutuojama daug apibrėžimų. Vieną iš apibrėžimų 1940 m. pasiūlė Alanas Tiuringas (Alan Turing), garsus Jungtinės Karalystės matematikas, karo laikotarpio kontržvalgybininkas, ilgų nuotolių bėgikas. Jis aprašė atvejį, kai kompiuteris galėtų parodyti savo intelektą. Jo scenarijus buvo panašus į aprašytąjį šiame skyriuje. Svarbiausia parinkti žmogaus ir kompiuterio (teletaipo – ankstyva 1940 m. technologija) tarpininką. Jei tarpininkas negalėdavo patikimai atskirti kompiuterio ir žmogaus, tai kompiuteris išlaikydavo Tiuringo intelekto testą. Šis kompiuterio naudojimo eksperimentas atmetė galimybę suteikti kompiuteriui fizinių savybių ar balso teisę. Kaip žinome, galima sukurti kalbančius, liečiančius, matančius kompiuterius, bet tai nesiejama su intelektu.

Originalus Tiuringo testas šiek tiek skiriasi nuo aprašyto šiame skyriuje. Tiuringas pasiūlė parengiamąjį pratimą, kuriame klausinėjami vyras ir moteris, o klausėjas turi nuspėti jų lytį. Vyro tikslas – įtikinti klausėją, kad jis yra moteris, o moters – kad ji yra vyras. Tiuringas pasiūlė šį pratimą tik kaip mąstymo eksperimentą, kur kompiuteris turėjo pavaduoti vieną iš veikėjų ir patikrinti, ar yra tinkamas imituoti žmogų. Tiuringo testas buvo pritaikytas šiai veiklai.

Intelekto imitavimas yra sudėtingas procesas. Jei vaidmenys būtų apkeisti ir žmogus turėtų imituoti kompiuterį, į kai kuriuos klausimus jis sunkiai atsakytų, pavyzdžiui, tikrai per ilgai skaičiuotų  $123456 \times 789012$  sandaugą ar ilgai užtruktų atlikti kitus aritmetinius veiksmus su dideliais skaičiais.

Tačiau kompiuteriui gana paprasta vaizduoti natūralų pokalbį. 1960 m. sukurta gerai žinoma programa „Eliza“ imituoja psichoterapeuto pokalbį su pacientu. Pateikiame to pokalbio ištrauką.

Žmogus:	Visi žmonės panašūs.
Kompiuteris:	Kodėl?
Žmogus:	Jie visada dėl ko nors jaudinasi.
Kompiuteris:	Gal galite papasakoti kokį pavyzdį?
Žmogus:	Gera, mano draugas liepė čia ateiti.
Kompiuteris:	Tavo draugas liepė čia ateiti?
Žmogus:	Jis pasakė, kad aš dažnai depresuoju.



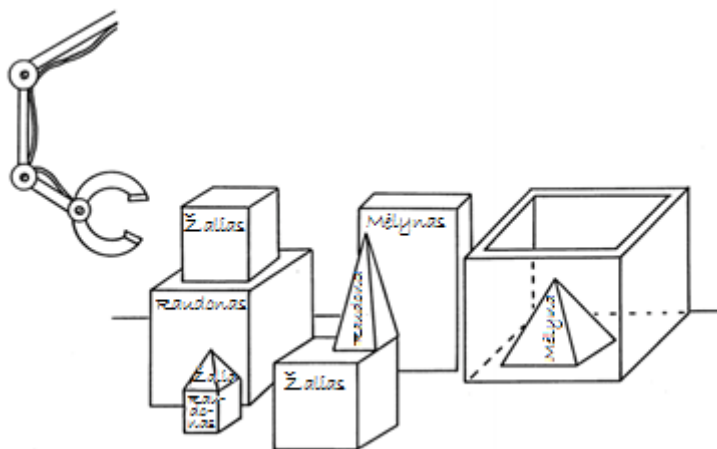
Kompiuteris: Gaila, kad jūs depresuojate.  
 Žmogus: Tai tiesa. Aš nelaiminga.  
 Kompiuteris: Ar manote, kad lankymasis čia jums padės būti laimingesnei?  
 Žmogus: Man reikia pagalbos.  
 Kompiuteris: Kas jums padėtų?  
 Žmogus: Gal galėčiau išmokti sutarti su savo mama.  
 Kompiuteris: Papasakokite daugiau apie savo šeimą.  
 ...  
 Kompiuteris: Ką dar galėtumėte pridurti, kai galvojate apie savo tėvą?  
 Žmogus: Peštukas.  
 Kompiuteris: Ar tai nesusiję su tuo, kad jūsų draugas liepė jums čia ateiti?  
 ...

Kai kurias natūralaus pokalbio detales sugeneruoja kompiuteris:

1. Generuoja įrašytus atsakymus pagal pašnekovo pasakytą teiginį (pvz., „Gal galite papasakoti kokį atvejį?“, kai pašnekovas pradeda sakyti „Jie visada...“; „Gaila tai girdėti...“, kai pašnekovas pradeda sakyti „Jis sako...“);
2. Pakartoja pašnekovo teiginį (pvz., „Tavo draugas liepė čia ateiti“, kai pašnekovas sako „Mano draugas liepė čia ateiti“);
3. Atpažįsta reikšminius žodžius (pvz., „Papasakok daugiau apie savo šeimą“, kai pašnekovo kalboje atpažįsta „mama“ ar pan.);
4. Sako bendras frazes (pvz., „Ką jums reiškia...“);
5. Persako svarstymus iš ankstesnio pokalbio (pvz., „Ar ką nors darėte, kad...“).

Aišku, tai nereiškia, kad ši programa išlaikė Tiuringo testą, nes žmogus gyvame pokalbyje neklausinėja turėdamas tikslą išsiaiškinti, ar pašnekovas yra mašina ar ne.

1960 m. buvo sukurta kita programa SHRDLU, kuri imitavo intelektualų pokalbį su žmogumi, kaip dėlioti geometrines figūras ekrane. Šią programą galėtų vykdyti ir tikras robotas. Toliau paveiksle pavaizduotas roboto mikropasaulis.



SHRDLU galėjo tęsti sklandų pokalbį. Toliau pateikiamas kompiuterio ir žmogaus pokalbio pavyzdys. Jis parodo, kaip programa išlaiko eiliškumą, vykdo nedviprasmiškas instrukcijas, supranta, ką pakeičia įvardžiai, taip pat naujus terminus.



Žmogus: Pakelk didelį raudoną kubą.  
 Robotas: Gerai.  
*Programa atsako „Gerai“, kai supranta komandą. Kad pakeltų raudoną kubą, programa turi suprasti, kad pirma reikia patraukti žalią kubą į šoną, o tik tada galima pakelti raudoną.*

Žmogus: Paimk piramidę.  
 Robotas: Nesuprantu, kurią piramidę paimti.  
*Kadangi yra trys piramidės, programa nieko nedaro.*

Žmogus: Surask figūrą, kuri yra aukštesnė už tą, kurią laikai, ir įdėk ją į dėžę.  
*Programa turi išsiaiškinti, ką reiškia „ją“.*

Robotas: Sakydamas „ją“ tu turi galvoje figūrą, kuri yra aukštesnė už tą, kurią laikau dabar.  
*Informuoja, ar gerai suprato.*

Robotas: Gerai.  
*Robotas ranka padeda raudoną kubą, paima aukštesnę mėlyną figūrą ir įdeda ją į dėžę.*

Žmogus: Kokios figūros yra dėžėje?  
 Robotas: Mėlyna piramidė ir mėlyna figūra.  
 Žmogus: Kur laikoma piramidė?  
*Anksčiau programa klausė, kurią piramidę paimti. Dabar ji supranta, kad kalbama apie ką tik minėtą piramidę.*

Robotas: Dėžėje.  
 Žmogus: Padaryk bokštą...  
 Robotas: Atsiprašau, bet nežinau, ką reiškia „bokštą“.  
*Programa iškart reaguoja, kai išgirsta nežinomą žodį.*

Žmogus: „Bokštas“ – sudėti vienas ant kito du žali kubai ir piramidė.  
*Kabutės reiškia, kad apibrėžiamas naujas žodis.*

Robotas: Supratau.  
 Žmogus: Ar yra bokštų ekrane?  
 Robotas: Ne.  
*Patikrinama, ar suprasta naujo žodžio „bokštas“ apibrėžtis.*

Žmogus: Pastatyk.  
 Robotas: Gerai.  
*Apibrėžtyje nurodytų instrukcijų pakanka, kad robotas pastatytų bokštą.*

Tačiau intelekto iliuzija gali būti lengvai sugriaunama.

Toliau pateikiamas pokalbis, kuris nebuvo, bet galėjo būti sugeneruotas, nes roboto intelektas labai ribotas.

Žmogus: Išmainyk didelį raudoną kubą į vandens pistoletą.  
 Robotas: Atsiprašau, nesuprantu, ką reiškia „išmainyk“.  
 Žmogus: „Išmainyk“ – nemokamai apsikeisk daiktais.  
 Robotas: Atsiprašau, nežinau, ką reiškia „nemokamai“.  
 Žmogus: „Nemokamai“ – poelgis, padarytas noriai, be prievartos.  
 Robotas: Atsiprašau, nežinau, ką reiškia „poelgis“.  
 Žmogus: „Poelgis“ – žmogaus tikslingai, o ne atsitiktinai atliekamas veiksmas.  
 Robotas: Atsiprašau, nežinau, ką reiškia „žmogaus“.



Žmogus: Atsiprašau, maniau, kad tu protingesnis.  
Robotas: Atsiprašau, nežinau, ką reiškia „atsiprašau“.

Pagaliau programa pripažįsta, kad nesupranta žodžio, kurį pati vartoja.

Galime tik įsivaizduoti, kaip robotas galėtų tęsti pokalbį (tai galėtų sugeneruoti mokiniai). Šis trumpas pokalbis parodo žinių platumą:

Žmogus: Išmainyk raudoną didelį kubą į vandens pistoletą.  
Robotas: Aš turiu vandens pistoletą, bet tau duosiu du kubus ir piramidę už tavo gleivėtą varlę.

1. Robotas įvertina, kad vandens pistoletas praranda vertę, jei tokį pistoletą jis jau turi.
2. Be to, robotas tikisi, kad žmogus taip pat tai žino, ir nesiruošia aiškinti, kodėl nuvertino vandens pistoletą.
3. Regis, žmogus nelabai nori išmainyti ką nors svarbaus į figūrą.
4. Be to, aiškėja, kad, kitaip nei vandens pistoletų, kitų figūrų skaičius yra svarbus.
5. Robotas bando dar labiau nuvertinti žmogaus pasiūlymą, jį lygindamas su varle.
6. Tai reiškia, kad robotas yra pasiruošęs derėtis.

Aišku, kad tokio gudrumo šiuolaikiniai kompiuteriui dar neturi.

Toliau pateiktą istoriją 1980 m. sugeneravo kita programa. Aišku, ši istorija iliustruoja kompiuterio kalbos ir gramatikos skurdumą.

Seniai seniai gyveno arktinė žuvėdra, vardu Trumanas. Trumanas buvo naminis paukštis. Trumanui reikėjo lizdo. Jis nuskrido į krantą. Trumanas ieškojo šakelių. Trumanas šakelių nerado. Jis nuskrido į tundrą. Jis sutiko poliarinį lokį, vardu Horacijus. Trumanas paklausė Horacijaus, kur rasti šakelių. Horacijus slėpė šakeles. Horacijus pasakė Trumanui, kad šakelių yra ant ledkalnio. Trumanas nuskrido ant ledkalnio. Jis ieškojo šakelių. Jis nerado šakelių. Horacijus ieškojo mėsos. Jis rado mėsos. Jis suėdė Trumaną. Trumanas mirė.

Galima įsivaizduoti, kaip ją pagyvintų papildomos detalės. Tačiau ši istorija svarbi ne savo paviršutiniškumu, bet istorijos platumu. Nors tai dar toli nuo žmogaus sukurtos istorijos, bet jaučiami žmogiškų konfliktų aspektai. Šiandien yra daugybė sistemų, kurios automatiškai generuoja istorijas, nors jas ir sunku įvertinti. Reikia nustatyti, kokia dalis istorijos yra tik standartinė žodžių dėlionė ir kokia dalis yra kūrybiškai sukonstruota.

Organizuojamos kasmetinės varžybos Loebnerio premijai gauti. Jose varžomasi, kuri programa išlaikys Tiuringo testą. Kaip žinoma (šis tekstas rašomas 2015 m.), nė viena programa nelaimėjo aukso ar sidabro medalio ir premijos, kuriuos vertintojai įsteigia kiekvienais metais, bet bronzos medalis ir premija įteikiami kiekvienais metais programai, kurios atsakymai panašiausi į žmogaus. Pirmaisiais varžybų metais (1991 m.) programa, laimėjusi bronzos medalį, be kitų gudrybių, darė klaidas, būdingas žmogui.



Dar nesukurtas dirbtinis intelektas, kuris visiškai įveiktų Tiuringo testą. Net jei jis būtų sukurtas, daugelis filosofų tai neigtų, sakydami, kad Tiuringo testas iš tikrųjų neišmatuoja to, ką dauguma žmonių supranta kaip intelektą. Šis testas testuoja tik elgseną – jis sukurtas nustatyti, ar tam tikra kompiuterio programa rodo intelekto požymius, o tai nėra tas pats, kas neapsimėtinis įgytas intelektas. Ar galima būti intelektualiam be žinių, savęs pažinimo, suvokimo, gebėjimo jausti, sąmoningumo, meilės patirties,... gyvybės?

### **Daugiau informacijos**

Knygoje „Artificial intelligence: the very idea“ (The MIT Press, Cambridge, MA, 1985) filosofas Johnas Haugelandas aprašo diskusijas apie dirbtinį intelektą, tai daugiausiai SHRDLU pokalbiai ir jų aptarimas. Šiame skyriuje pateikti pavyzdžiai iš šios knygos.

Originalus Tiuringo testas aprašytas Alano Turingo straipsnyje „Computing machinery and intelligence“, 1950 m. išspausdintame filosofijos žurnale „Mind“, ir dar kartą aprašytas knygoje „Computers and thought“, kurią sudarė Edwardas A. Feigenbaumas ir Julianas Feldmanas (AAAI Press; New edition edition August 28, 1995).

Psichoterapijos programa aprašyta J. Weizenbaumo straipsnyje „ELIZA — a computer program for the study of natural language communication between man and machine“, 1966 m. išspausdintame kompiuterijos žurnale „Communications of the Association for Computing Machinery“.

Figūras dėliojantis robotas aprašytas Terry Winogrado disertacijoje, kuri buvo išspausdinta knyga „Understanding natural language“ (Academic Press, New York, 1972).

Istoriją generuojančią programą aprašė Tony Smithas ir Ianas Wittenas knygoje „A planning mechanism for generating story text“ („Proceedings of the 10th International Conference on Computing and the Humanities“, 1990).



## 24 veikla

### Protingas popieriaus lapas

---

#### Santrauka

Rengiamos dirbtinio intelekto varžybos: „labai protingo popieriaus lapo“ ir žmogaus. Šiame nuolatiniam iššūkyje tarp geriausių žmonijos ir geriausios popieriaus rūšies varžybose popierius yra nepralenkiamas. Jis dar dar nėra pralaimėjęs nė vieno žaidimo. Ši veikla buvo paskelbta Lenkijos matematikos mokytojams skirtame profesiniame žurnale.

Šios veiklos tikslas – supažindinti, kas yra kompiuterio programa ir kaip viskas, ką daro kompiuteris, yra paprasčiausiai susiję su instrukcijų, parašytų kūrybingų kompiuterių programuotojų, vykdymu. Taip pat siekiama pradėti diskusiją apie tai, kas yra intelektas ir ar kažką, kas tiesiog akiai laikosi taisyklių, galima laikyti protingu.

#### Amžius

nuo 8 metų

#### Priemonės

Balta lenta arba popierius, ant kurio galima rašyti, kad visi matytų.

lentos rašikliai

„Protingo popieriaus lapo“ kopija (galima laminuota)

Muzikinė atvirutė su amžiaus grupės atpažįstama melodija (neprivaloma)





# Ką daryti?

---

Ką daryti?

Skelbimas: Paskelbkite, kad popieriaus lapas, kurį laikote rankose, yra protingesnis už bet kurį žmogų kambaryje (net ir už labai protingą mokytoją). Tvirtinkite, kad jis „protingiausias“, bet neaiškinkite, kodėl. Mojuokite juo, nerodydami prirašytos jo pusės auditorijai.

Pasiruošimas: Iš pradžių paklauskite auditorijos, kad tie, kurie tiki jūsų žodžiai, pakelti rankas. Po to tegul pakelia rankas tie, kurie mano, kad kalbate visiškus niekus ir negali būti, kad tik popieriaus lapas būtų „protingas“.

Paprastai dauguma renkasi, kad tai visiškai šlamštas. Padėkokite už jų išmintį. Tiek už tai, kad tiki tokiu išmintingu žmogumi kaip jūs, ir ypač tuos, kurie netiki – juk geras mokslininkas netiki atsitiktinių žmonių teiginiais, kurie daro didelius pareiškimus kad ir kokie puikūs jie būtų, be tam tikrų įrodymų

Paprašykite, kad jie kurį laiką su jumis padiskutuotų – galbūt tai bus protinga, o galbūt ne, bet paprašykite, pagalvoti, kas galėtų būti popierius lape, kad būtų galima tvirtinti, kas jis „protingiausias“.

Galite sulaukti pasiūlymų, pvz., kad rašalas yra kažkuo ypatingas arba kad dėl to, kad jis laminuotas. Jei tai pirmieji dalykai, pagirkite juos už įdomią idėją, bet paklauskite, kaip būtent dėl to jis gali būti protingas. Jei tai antrasis variantas, paaiškinkite, kad plastikinė dangą nėra ypatingas dalykas – ji tiesiog apsaugo popierių, nes jums nepatinka, kai visi jį liečia pirštais. Kitas dažnas pasiūlymas yra toks, kad lapas yra kompiuteris. Tai proga ištraukti muzikinę sveikinimo atvirutę, kuri groja muziką (ir yra pakankamai protingas, kad žinotų, jog tai reikia daryti per jūsų gimtadienį) ir paaiškinti, kad jis veikia per įmontuotą lustą. Galite paminėti, kad tokia mikroschema yra tokia pat sudėtinga, kaip ir integruotas kompiuteris, naudotas Neilui Armstrongui nuskraidinti į Mėnulį. Atkreipkite dėmesį, sakydami, kad jūsų dokumentas galėtų tai padaryti tokiu būdu, bet jūs to nepadarėte.

Gali būti pasiūlymas, kad lapas yra protingiausias dėl to, kas užrašyta jam. Paklauskite, kas gali būti parašyta, kad popierius būtų protingas. Sudėtingos lygtys? Nuostabi poezija? Įspūdingi faktai? Pasiūlykite pavyzdžių ir paklauskite, ar klausytojai mano, kad tai būtų protingiausia. Jei ne, turime ieškoti ko nors daugiau. Pakalbėkite apie tai, kad žinios nėra tas pats, kas intelektas – ir kad tai tikrai nėra tik žinių įsiminimas egzaminams, bet ir bandymas suprasti, o tai nėra tas pats. Sutikite, kad tokių dalykų užrašymo neužtektų, kad tai būtų protinga.

Atkreipkite dėmesį, kad norėdamas mus įtikinti, jog jis yra protingas, jis turi sugebėti ką nors padaryti, kad parodytų, jog yra protingas. Ką gali padaryti popierius? Na, jis niekada nepralaimėjo žaidimo (ir jis reguliariai žaidžia su žmonėmis). Priminkite jiems, kad žaidimas turėtų baigtis lygiosiomis, jei abu žaidėjai žaidžia puikiai. Jūs negalite priversti laimėti. Nepaisant to, popierius laimėjo maždaug pusę partijų, kurias žaidė prieš žmones, o likusias sužaidė lygiosiomis. Tai tobulas intelektas. Žmonės tokie nėra.





Paklauskite jų, ar jie jums tiki, ar nori pamatyti kokių nors įrodymų? Įrodymui jums reikės dviejų savanorių.

Veikla: Lentoje nupieškite lentelę su nuliukais ir kryžiuokais. Kiekvienam savanoriui duokite po rašiklį. Paaiškinkite, kad norint pamatyti, kiek protingas yra popierius, reikės žaisti žaidimą "Nuliukai ir kryžiuokai". Tai bus ne dviejų žmonių kova, o tarp popieriaus lapo ir žmonijos. Popierius yra „periferiškai išprusęs“ – jūs jam nedavėte roboto rankos ar kitos įrangos, todėl jam reikia įrankio, kuris vykdytų jo nurodymus. Galbūt norėtumėte atkreipti dėmesį, kad vien dėl to, jog kas nors yra paralyžiuotas, nereiškia, kad jis nėra protingesnis už jus.

Todėl vienas asmuo žais už popieriaus lapą. Jo darbas - tiesiog daryti tai, ką liepia popierius. Jie turi išjungti savo labai protingas smegenis ir daryti tiksliai taip, kaip jiems įsakyta: mes nenorime žinoti, kaip gerai jis žaidžia žaidimą, o norime žinoti, kaip gerai žaidžia popieriaus lapas. Jis turės tiesiog garsiai perskaityti popieriaus lapo nurodymus (kad visi galėtų pasakyti, jog žaidžia popierius, o ne žmogus) ir daryti taip, kaip liepia popierius.

Kitas žaidėjas yra tam, kad atstovautų geriausiems žmonijos atstovams. Galbūt geriausia būtų nesirinkti ko nors, kas labai norėtų ir, atrodo, manytų, kad niekada nepralaimės. Kad sumažėtų tikimybė, jog žaidimas baigsis lygiosiomis (nors dažnai tokie savanoriai vis tiek pralaimi). Jų užduotis – pasitelkti visą savo intelektą, kad sužaistų kuo geriau. Kadangi popierius yra toks protingas, tai kad būtų teisingiau, pasakykite, kad jie gali sulaukti pagalbos iš žiūrovų, jei žmogui jos reikia. Pasakykite, kad žiūrovai šauktų, jei mano, kad daroma klaida, arba žino ėjimą, kurį reikia atlikti.

Dabar liepkite asmeniui, žaidžiančiam už popierių, perskaityti lapo instrukciją (pakomentuokite, kad tai gana protinga, jog jis nori eiti pirmas). Jei kas nors skundžiasi, kad tai nesąžininga, tai pabrėžkite, kad žaidimas turėtų baigtis lygiosiomis. Ėjimas nėra priežastis pralaimėti.

Tada instrukcijų vykdytojas turėtų perskaityti pirmąjį ėjimą ir atlikti nurodytą ėjimą. Toliau perduokite ėjimą žmogui. Gali būti daug šūksnių apie skirtingus ėjimus. Jei žmogus yra užtikrintas, paskatinkite jį eiti ten, kur, jo manymu, yra geriausia iš visų siūlomų variantų. Tęskite taip toliau, įsitikindami, kad vykdytojas perskaito ir tiksliai seka nurodymus ir padėdami jam suprasti, kur jam liepiama eiti, jei reikia. Pavyzdžiui, priešingas kampas reiškia įstrižai priešingą kampą – šioje vietoje galima aptarti, kodėl reikalingos specialios programavimo kalbos. Tam kad būtų tiksliai vienareikšmiškai nurodoma, ką reikia atlikti.

Kartais po antro ar trečio ėjimo žmonės iš auditorijos pareiškia žaidimą pralaimėję. Atkreipkite dėmesį, kad žmonija dažnai atsitraukia pripažindama pralaimėjimą. Priminkite jiems, kad tai tik popieriaus lapas. Gali būti, kad iki šiol jam tiesiog pasisekė, todėl jis vis dar gali suklysti ir nematyti to, ką mato jie.

Jei popieriaus instrukcija išsišakoja, dažnai žaidėjas tada juokaudamas sukčiauja, pvz. rašydamas du nuliukus. Paminėkite, kad žmonija tokiu atveju dažnai griebiasi sukčiavimo, paskatinkite žaisti tinkamai, primindami, kad tai tik popierius ir gali suklysti.



Popieriaus lapas laimės arba bus lygiosios (jei žmogus supranta, kad jam reikia eiti į šoną, o ne į kampus). Jei taip nutinka, priminkite, kad tai buvo numatoma, bet net ir tokiu atveju vis tiek buvo protinga neleisti žmogui laimėti. Praneškite, kad popieriaus lapas dar kartą įrodė, kad jis nepralaimi. Pasakykite, kad sutinkate, jog galbūt jis nėra protingesnis už žmogų, bet jis įrodė, kad yra jiems lygus. Jei laimės popieriaus lapas, paskelbkite, kad dar popieriaus lapas dar kartą pasirodė esąs protingesnis už žmones ir kad jūs tai įrodėte. Bet kuriuo atveju paprašykite plovimų tiek savanoriams, tiek popieriaus lapui.

Paaiškinimas: Atkreipkite dėmesį į tai, kad auditorija paprašė įrodymų ir jūs juos pateikėte. Paprašykite dar kartą pakelti ranką, kas dabar mano, kad popieriaus lapas yra protingas, ir kas mano, kad kalbate niekus ir popierius negali būti protingas. Paprastai visi dabar yra įsitikinę, kad tai nėra protingas, nepaisant jo gebėjimų įrodymų.

Atkreipkite dėmesį, kad jis parodė protingą elgesį, taigi kažkur yra protingas. Kur jis yra protingas? Kažkas beveik neabejotinai pasakys, kad jis yra žmoguje, kuris parašė instrukcijas. Paklauskite, ar visi sutinka, kad intelektas yra būtent ten, ir paprašykite pakelti rankas.

Dabar paaiškinkite, kad popieriuje iš esmės yra kompiuterio programa: instrukcijos, kurių reikia akiai laikytis. Viskas, ką jie kada nors matė darant kompiuterį, buvo tiesiog taip pat akiai vykdydamas instrukcijas. Pabrėžkite, kad jei sako, kad popierius tiesiog yra tik taisyklės, nėra protingas, tada jie sako, kad joks kompiuteris niekada negalėjo būti protingas.

Šios instrukcijos buvo parašytos tokia kalba, kad žmogus galėtų jomis vadovautis. Jei jos būtų parašytos kompiuteriui, jos būtų parašytos programavimo kalba, kurią kompiuteris gali suprasti, todėl ja gali vadovautis. Atkreipkite dėmesį, kad jei jie galvoja, kad būtent instrukcijų rašytojas yra kūrybingas protingas žmogus, tada jie sako, kad kompiuterių programuotojai yra protingi ir kūrybingi (o tai tiesa). Būtent kompiuterių programuotojai parašė visas instrukcijas, kurias vykdo kompiuteriai.

#### Galimybės ir išplėtimai

Jei yra laiko, pabaigoje galite ištirti, kas nutiks, jei žais du popieriaus lapai. Pakvieskite dar du savanorius, kad jie tai išbandytų. Popierius iš karto pralaimi ir jo žaidimas atrodo labai kvailas. Tačiau galite pasakyti, kad „mano popieriaus lapas yra antras geriausias žaidėjas“. Tai gali paskatinti diskusiją apie tai, ką yra dirbtinio intelekto tyrėjai vadina „kadro problema“.

Kompiuteris gali atrodyti gana protingas, kai atlieka užduotį, kuriai buvo suprogramuotas, bet gali atrodyti labai kvilai, jei tik šiek tiek pakeisite užduotį, kurią jis bando atlikti. Kai programuotojas rašo programą, jis turi užtikrinti, kad ji veiktų ir iš anksto apgalvoti visas galimybes.

Tai gali paskatinti diskusiją apie šachmatais žaidžiantį kompiuterį „Deep Blue“, kuris įveikė geriausią planetos šachmatininką Kasparovą. Jis tai padarė tik vadovaudamasis programuotojų parašytomis taisyklėmis. Tačiau „Deep Blue“ gali žaisti šachmatais geriau nei jį sukūrę žmonės, kuriuos Kasparovas gali lengvai įveikti šachmatų žaidime



asmeniškai. Programuotojai vis tiek sugebėjo sukurti kompiuterį, kuris buvo protingesnis (žaidžiant šachmatais) už juos pačius.

Po to klasė grupelėmis gali pabandyti sukurti savo pačių instrukcijas, pagal kurias būtų galima puikiai žaisti „nuliukus ir kryžiuokus“ nepriklausomai nuo to, ar jie pradeda pirmi, ar ne. Tai galima daryti rašant instrukcijas ant kortelių, naudojant įvairius fiksuotus teiginius, pavyzdžiui, „eik viduryje“ ir pan. Klasėje suorganizuokite instrukcijų turnyrą.

Daugiau apie „nuliukus ir kryžiuokus“:

<http://www.cs4fn.org/programming/noughtscrosses/>.

Daugiau informacijos

<http://www.cs4fn.org/fundamentals/programming.php>



## Protingas lapas

Esu labai protingas popieriaus lapas. Pažaiskime „nuliukus ir kryžiukus“.

Aš esu X... ir einu pirmas...

1 Ėjimas:

Eikite į kampą.

2 Ėjimas:

JEIGU kitas žaidėjas ten neina.

TAI eikite į priešingą kampą nei 1 ėjimas.

KITAIP eikite į laisvą kampą.

3 Ėjimas:

JEIGU eilutėje yra 2 X ir tarpas

TAI eikite į tą vietą.

KITAIP, JEIGU eilutėje yra 2 O ir tarpas.

TAI eikite į tą vietą.

KITAIP eikite į laisvą kampą.

4 Ėjimas:

JEIGU eilutėje yra 2 X ir tarpas

TAI eikite į tą vietą.

KITAIP, JEIGU eilutėje yra 2 O ir tarpas.

TAI eikite į tą vietą.

KITAIP eikite į laisvą kampą.

5 Ėjimas:

eikite į laisvą vietą

