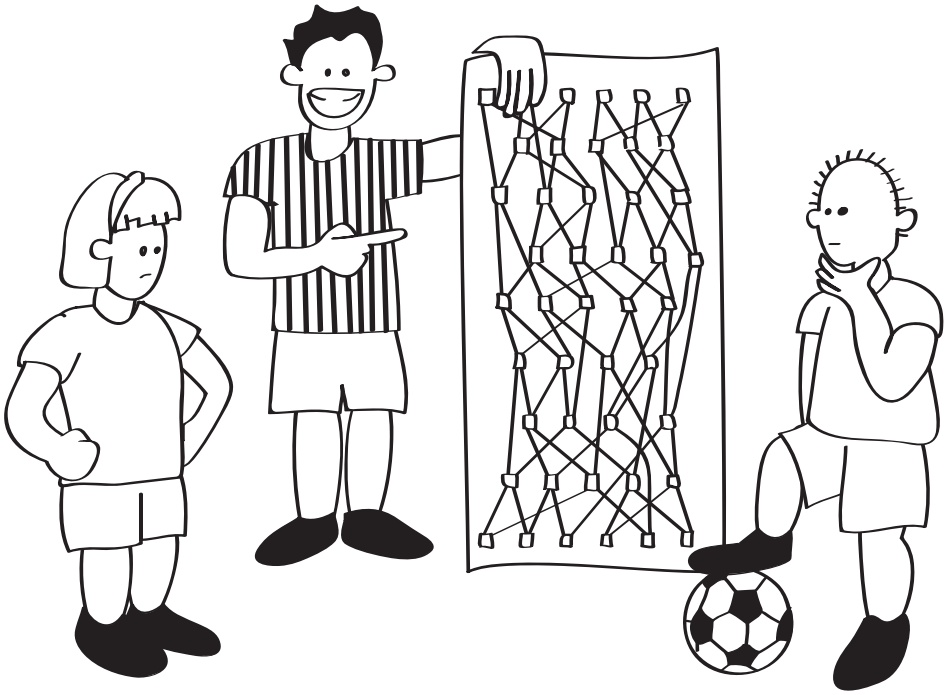
Aktivnost 17

Nogometni žreb

Po prejšnji misiji nemogoče – izračunu vsote podatkov, ki jih ne poznamo, nas že čaka nova: kako pošteno žrebati po telefonu.



Namen

Otroci spoznajo enosmerne funkcije in primere problemov, ki jih rešujemo z njimi.

Spoznajo logična vrata IN in ALI ter osnovno idejo vezij.

Potrebščine

Vsak otrok potrebuje

- polo z mrežo za kodiranje,
- 25 figuric, gumbov, perlic, kamenčkov... dveh različnih barv, po možnosti bele in črne oz. svetle in temne.

Vir: vidra.fri.uni-lj.si; izvirnik: csunplugged.org

Nogometni žreb

Potek

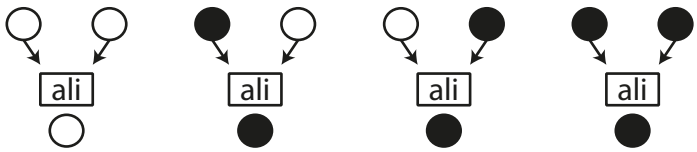
1. Otrokom razdeli pole in žetone.
2. Razloži jim spodnjo zgodbo. Računanje izhodov pri razlagi mrež (dva izhoda) opravi skupaj z otroki, pri čemer otroci sledijo na svojih polah.
3. Za računanje izhoda za pravo mrežo, ki se uporablja pri žrebanju, si izmisli razpored za prvo vrstico. Spodnjo vrstico naj otroci najprej izračunajo sami. Nato ponovite izračun skupaj, da ga bodo otroci gotovo razumeli.
4. Nato otroci igrajo igro v parih. Pari naj ne sedijo skupaj, da ne bodo mogli škiliti na pole.

Žrebanje po telefonu

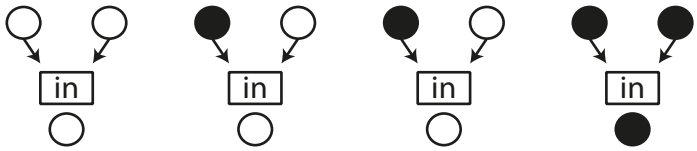
Nogometni ekipi Kranja in Kočevja bi se radi pomerili na tekmi. Vse je dogovorjeno, le, kje bo tekma, še ne. Najraje bi žrebali, recimo, metali kovanec. Ker pa se pogovarjajo samo po telefonu in elektronski pošti, imajo problem: če Janez iz Kranja reče "grb", lahko Tone iz Kočevja vrže kovanec in se zlaže, da je padla cifra. Če bo metal Tone, lahko laže Janez.

Znašla sta se na nenavaden način:izmislila sta si nekakšno mrežo z dvema vrstama "škatlic". Eni vrsti pravita škatlice "ali", drugi škatlice "in". V vsako škatlico prideta dva žetona (figurici, perlici, fižola). Žetoni so dveh barv, črni in beli.

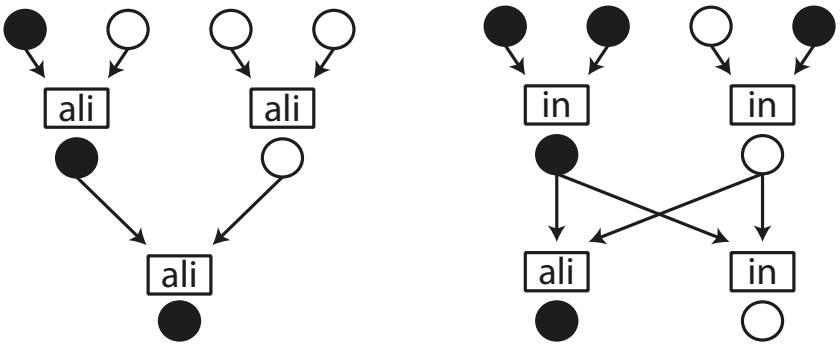
- Iz škatlice vrste "ali" pride črn žeton, kadar je črn *vsaj eden od žetonov*, ki gresta vanjo ("ali" jim pravita zato, ker je lahko črn eden *ali* drugi *ali* oba).



- Iz škatlice tipa A pride črn žeton samo takrat, kadar sta črna *oba žetona*, ki gresta vanjo (torej eden *in* drugi).

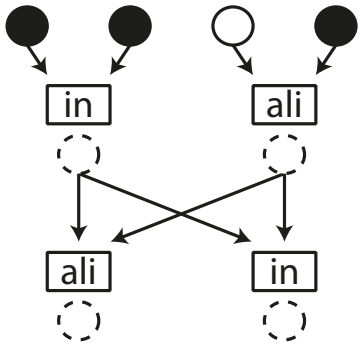


Škatlice lahko vežemo eno za drugo, kot kaže leva slika. Žeton lahko gre tudi v več škatlic hkrati; to nam pokaže desna slika.



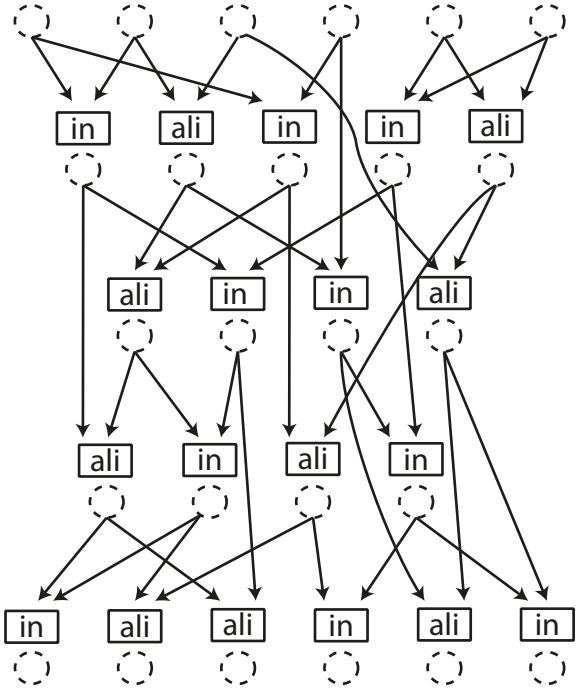
Razumemo desno sliko? Škatlici v zgornji vrsti sta "in". Leva dobi dva črna, zato da črnega. Desna nima dveh črnih, izhod je bel. Tadva žetona, črni in beli, gresta v dve škatlici. Leva spodnja je "ali": ker je eden od teh dveh žetonov črn, da škatlica na črn žeton. Desna škatlica pa je "in" in da bel žeton,.

Malo povadimo: kaj dobimo s spodnjo mrežo?



Dva črna kroga.

Zdaj pa zares: Janez in Tone sta si izmislila spodnjo zapleteno mrežo. (Večja slika je na poli, ki jo dobijo učenci.)



Dogovorila sta se, da bosta žrebala takole:

- Janez določi barve krogov v prvi vrsti tako, da šestkrat meče kovanec; za vsak grb postavi na krog črn žeton in za vsako cifro belega.
- Nato "izračuna", kaj dobi iz škatlic v zadnji vrsti. Rezultat (samo škatlice v zadnji vrsti, ne pa tudi v prvi!) pove Tonetu.
- Tone poskuša uganiti, ali je število črnih žetonov v prvi vrsti sodo ali liho. Če ugane, bo tekma v Kočevju, sicer v Kranju.
- Janez pove Tonetu ali je uganil ali ne.

Nato preverimo, da se Janez ni zlagal, takole:

- Janez pove Tonetu, barve žetonov v prvi vrsti, od leve proti desni.
- Tone izračuna rezultat škatlic v zadnji vrsti, da preveri ali je res takšen, kot je rekel Janez.

Pogovor

Kako nas postopek zavaruje pred goljufanjem?

Kako ju to zavaruje pred goljufanjem? Goljufije na eni ali drugi strani preprečuje dejstvo, da iz zadnje vrste ne moremo izračunati prve, ker škatle delujejo samo v eno smer: iz tega, kaj je prišlo v škatlo "in", ne moremo uganiti, kaj je šlo vanjo.

Bi lahko Janez goljufal in rekel, da je število črnih žetonov v prvi vrsti, recimo, sodo, čeprav je v resnici liho? Ne. Tone ve, kako so razporejeni žetoni v zadnji vrsti; če si bo Janez izmislil, da je število črnih v prvi vrsti sodo, si bo moral *izmisliti* tak razpored žetonov v prvi vrsti, da bo število črnih žetonov res sodo, zadnja vrsta pa bo takšna, kot je rekel, da bo. Tega pa ne more narediti.

Bi lahko Tone goljufal in iz podatkov, ki jih je dobil od Janeza izračunal, koliko črnih žetonov je v prvi vrsti, oziroma, kar v resnici potrebuje, ali jih je sodo ali liho število? Ne more, iz istega razloga – iz zadnje vrstice ne moremo računati prvi.

Je mogoče s postopkom vseeno goljufati?

Se zna kateri otrok domisliti načina za goljufanje? (Verjetno ne.)

Koliko je različnih možnih prvih vrstic? Na to vprašanje bi morali znati odgovoriti že po prvi aktivnosti: do koliko lahko štejemo s šestimi prsti? Do 127. Toliko je torej možnih prvih vrstic. Če si Janez ali Tone vzame čas, lahko za vsako možno prvo vrstico izračuna zadnjo. Kako si bo izmislil vse možne prve vrstice? Seveda: prav tako, kot štejemo od 0 do 127. Tule je tabela: ker smo že (skoraj) pravi računalnikarji, smo jo namesto s praznimi in polnimi krožci zapisali z ničlami in enicami.

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

Kdor si naredi takšno tabelo, lahko iz zadnje vrstice izve, kakšna je bila prva in je zmagal, ne? Ne nujno. Lahko se namreč zgodi, da več različnih prvih vrstic vodi v isto zadnjo vrstico. Janez in Tone morata goljufati na različne način.

Janezova goljufija: poišče dve prvi vrstici, eno s sodim, drugo z lihim številom črnih žetonov, ki obe vodita v isto zadnjo vrstico. To vrstico pove Tonetu. Če Tone ugiba, da je število črnih žetonov sodo, Janez reče, da je liho in mu pove ustrezno prvo vrstico... in obratno. Kako naj izpelje to goljufijo? Kako bo najpreprosteje poiskal zadnjo vrstico, ki izvira iz dveh ali več prvih? Če se otroci ne spomnijo sami, jih spomni, kaj so počeli ob ladjicah in urejanju. Se spomnijo telefonskih številk? Če hočemo iskati po spodnjih vrsticah, je potrebno tudi seznam urediti po spodnjih vrsticah.

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

Vidimo, da mreža pravzaprav ni kaj prida: zelo veliko izhodov je 011010. Če si Janez izmisli, da je bila prva vrstica takšna, da je dala zadnjo vrstico 011010, in Tone ugiba, da je število črnih krožcev liho, lahko Janez zatrdi, da na, saj je bila prva vrstica, recimo 100010. Če bi Tone stavil na sodo število črnih krožcev, si Janez gladko izmisli, da je bilo število liho, namreč 001101.

Kako pa lahko goljufa Tone? Tone lahko goljufa samo pri tistih zadnjih vrsticah, ki jih lahko dobimo samo iz ene, točno določene prve vrstice. Pri teh lahko Tone ugane prvo vrstico in prešteje pobarvane krožce. Žal tu sploh in takšnih vrstic! Vsaka spodnja vrstica izhaja iz vsaj dveh gornjih, pri čemer ima ena sodo, druga liho število črnih krožcev. Tole mrežo si je najbrž izmislil Janez!

Je mogoče postopek zavarovati pred goljufijo?

Znajo otroci najti pot mimo tega problema?

Spomniti se moramo, kako postopek preprečuje goljufanje in zakaj z njim vseeno lahko goljufamo. Deluje zato, ker se iz zadnje vrstice ne da izračunati prve. Pokvarili smo jo zato, ker smo našli način, da jo vseeno izračunamo – ne tako, da bi šli po mreži nazaj, temveč tako, da sestavimo tabelo, v kateri za vsak vhod piše, kakšen izhod da.

Preprečiti moramo torej sestavljanje take tabele. To naredimo kar preprosto: izmislimo si mrežo, ki nima samo šest temveč, recimo 128 vhodov. Takšna mreža ima 2^{128}, to je 340282366920938463463374607431768211456 različnih prvih vrstic. Tako velika tabela pa je prevelika za katerikoli računalnik. Če bi bilo to premalo, vzamemo 256 vhodov in dobimo 115792089237316195423570985008687907853269984665640564039457584007913129639936 različnih prvih vrstic.

Smo tako varni pred goljufijami? Morda, odvisno od tega, kako dobro mrežo smo sestavili. Če je mreža sestavljena tako nerodno, da je mogoče iz zadnje vrstice uganiti, kako, približno, izgleda prva. Čim jo približno poznamo, nam to pomaga, da jo bomo z dovolj truda izračunali.

Mreže, ki jih uporabljamo v resnici, vsebujejo poleg škatel "in" in "ali" še eno škatlo, ki pove, ali sta žetona na vhodih različnih barv. Poleg tega takšne mreže sestavljajo matematiki, ki že znajo poskrbeti, da je iz zadnje vrstice čim težje uganiti prvo.

Pa se to v resnici kje uporablja? Kolikokrat pa žrebamo po internetu?

Takšne mreže, ki jih lahko uporabimo v eno smer, v drugo pa ne, so osnova varnosti na internetu. Ko se računalniki predstavljajo en drugemu, si izmenjajo "podpise", ki temeljijo na enosmernih mrežah. Ko starši prek interneta plačujejo račune v banki, morajo za dostop do spletne strani uporabiti nekaj, čemur se v resnici reče "certifikat", v resnici pa gre samo za nekakšno "elektronsko osebno izkaznico", ki je spet zaščitena z enosmerno mrežo, ki jo je znal sestaviti samo ta, ki je "izkaznico" izdal. Ko kupujemo prek spleta, je povezava zaščitena pred tem, da bi, recimo, kak nepridiprav spremenil naslov, kamor naj trgovina pošlje nakupljeno robo, s pomočjo enosmernih mrež.