Kuidas arvuti juhuslikkust tekitab ja miks seda üldse vaja on?

50 min tagasi - 14.09.2026 Autor: AM

(Sisuturundus)

Mängus avaneb aardekirst. Kaardipakk segatakse uuesti. Ilmaäpp joonistab järgmise nädala vihmasaju kohta mitu võimalikku rada. Kõigis neis kohtades vajab arvuti arve, mis ei jookseks etteaimatava mustrina silma.

Arvuti ise on aga masin, mis täidab käske. Kui talle anda sama algus ja sama reegel, tuleb tavaliselt sama tulemus. Sellepärast on juhuslikkus arvutis palju huvitavam teema, kui esmapilgul tundub.

Kui mäng vajab uut tulemust

Digitaalses mängus ei saa iga kaarti, vaenlast või auhinda käsitsi ette kirjutada. Programm vajab mehhanismi, mis valib järgmise tulemuse piisavalt ootamatult. Mängija näeb ainult lõppu: kaart tuli kätte, ratas jäi seisma, ese kukkus pärast võitlust maha.

Kasiinomängude puhul räägitakse samast asjast eriti otse, sest tulemus peab sündima iga vooru jaoks eraldi. Veebileht LatvijasKazino käsitleb Läti kasiinode ja mängukeskkondade infot, kus juhuslikkus on üks praktiline taustateema. Mängija jaoks on nähtav osa lihtne, aga programmi poolel käib töö numbrite, reeglite ja kontrollitava süsteemi kaudu.

Sama loogika on ka tavalises arvutimängus. Kui rollimängus leitakse koopast haruldane mõõk, ei “mõtle” mäng nagu inimene. Ta võtab juhuarvu, vaatab tõenäosuste tabelit ja valib sobiva tulemuse.

Päris juhus ja arvuti tehtud juhus

Päris juhuslikkus tuleb füüsilisest maailmast. Selle all võib mõelda näiteks elektrilist müra, radioaktiivset lagunemist või muud mõõdetavat nähtust, mida ei ole lihtne täpselt ette korrata. Sellist juhust kasutatakse kohtades, kus ennustatavus oleks halb uudis.

Igapäevases tarkvaras kohtab aga väga sageli pseudojuhuslikkust. See tähendab, et arvud arvutatakse algoritmiga, kuid nad näevad kasutajale välja piisavalt juhuslikud. AKITi terminibaas selgitab mõistet pseudojuhuarvude generaator kui mehhanismi, mis tekitab algoritmiliselt arve, mille statistilised omadused meenutavad juhuslikke arve.

See kõlab kuiva definitsioonina, aga mõte on lihtne. Arvuti ei viska nähtamatut täringut. Ta jookseb läbi retsepti, mille tulemus peab välja nägema nii segane, et inimene ei oska järgmist arvu ära arvata.

Seed on väike algus suurele jadale

Pseudojuhuslik generaator vajab alguspunkti. Seda nimetatakse sageli seed’iks ehk seemneks. Kui seeme on sama ja algoritm sama, võib arvude jada uuesti samamoodi tekkida.

Mänguarenduses on see väga kasulik. Testija leiab veidra vea: kaart tekib seina sisse, vaenlane jääb ukse taha kinni, maailm genereerib võimatu tee. Kui arendajal on sama seed, saab ta sama olukorra uuesti avada ja vea rahulikult läbi vaadata. Seed aitab eriti sellistes kohtades:

- Maailma loomine. Sama seed võib anda sama kaardi või tasemepaigutuse.
- Testimine. Viga saab korrata, kui algandmed on alles.
- Simulatsioon. Sama mudelit saab võrrelda eri algustega.
- Mänguloot. Eseme või auhinna valik liigub tõenäosuste järgi.
- Kaardid. Pakki saab segada arvujada abil.

Selline korduvus ei tee süsteemi kehvaks. Vastupidi, see annab arendajale võimaluse kontrollida, mis juhtus. Kasutaja jaoks jääb tulemus siiski piisavalt muutlikuks, kui generaator on hästi valitud ja õigesti kasutatud.

Simulatsioon ei saa läbi ühe variandiga

Ilmateade, liiklusmudel või majanduslik riskistsenaarium ei ela ühest arvutusest. Mudel pannakse käima mitu korda, muudetakse algtingimusi ja vaadatakse, millised tulemused korduvad. Juhuarvud aitavad sellist hajumist läbi mängida.

Tartu Ülikooli ajakirjas käsitletud tõenäosusteooria praktiline kasutus näitab hästi, miks tõenäosus ei ole ainult koolimatemaatika harjutus. Seda kasutatakse otsustes, kus kindlat vastust pole veel käes, aga võimalikke tulemusi tuleb hinnata.

Arvutisimulatsioonis tähendab see tihti kümneid, sadu või tuhandeid katseid. Üks jooks võib anda ühe pildi. Paljud jooksud näitavad, kas mingi tulemus on haruldane, tavaline või sõltub väga väikesest algmuutusest.

Krüptograafias ei tohi jada lekkida

Mängudes võib pseudojuhuslikkus olla piisav, kui mängija ei näe mustrit. Turvalisuses on latt kõrgem. Paroolid, krüptovõtmed ja ühekordsed koodid vajavad arve, mida ründaja ei suuda ette aimata.

Kui generaator on nõrk või seed ära arvatav, võib kogu süsteem ohtu sattuda. Sellepärast kasutatakse turvatarkvaras eraldi krüptograafilisi juhuarvude generaatoreid. Need koguvad lisaandmeid seadmest ja väldivad lihtsat kordumist.

Siin pole juhuslikkus kaunistuseks. See on lukumehhanismi osa. Kui võti sünnib ennustatavast jadast, pole tähtis, kui ilus kasutajaliides välja näeb.

Protseduuriline maailm vajab piire

Mängudes kasutatakse juhuslikkust kaartide, tasemete ja maailmade loomisel. Programm võib paigutada ruume, teid, metsi, vastaseid või ressursse, kuid mäng peab jääma mängitavaks.

Juhuarvust üksi ei piisa. Kui väljapääs satub suletud seina taha või algusala ümber tekib liiga tugev vastaste ring, peab süsteem selle valiku tagasi lükkama. Juhus pakub variante, reeglid hoiavad maailma koos.

Juhuslikkus töötab paremini, kui seda ei märgata

Arvuti loodud juhuslikkus mõjub kõige paremini siis, kui kasutaja ei hakka seda eraldi uurima. Kaart tundub segatud, mängumaailm uus ja simulatsioon annab usutava vahemiku.

Pseudojuhuslikkus on praktiline viis anda arvutile muutlikkust seal, kus iga tulemust ei saa käsitsi kirjutada. Kui järgmine kaart ilmub ekraanile või mäng loob uue saare, taustal töötavad algväärtus, algoritm, reeglid ja kontrollid.

- Uudised

- Sisuturundus

Pilt