1.

Paslučajni brojevi

Simulirati slučajnu veličinu znači načiniti njen uzorak proizvoljne dužine. Temeljna ideja sastoji se u reprezentaciji slučajne veličine pomoću funkcije jednog ili više slučajnih brojeva, te generiranje uzorka tražene dužine treba nadomjestiti generiranjem uzorka slučajnih brojeva. Time slučajni broj dobiva iznimnu važnost, te je čitavo prvo poglavlje posvećeno metodama za simuliranje uzoraka slučajnog broja. Kvaliteta simuliranog uzorka slučajnog broja je centralno pitanje u primjenama. Stoga se u drugom dijelu ovog poglavlja raspravlja detaljnije o mogućnostima upotrebe uzorka slučajnog broja za procjenu vjerojatnosti višedimenzionalnih događaja.

1.1. Slučajni broj i Monte Carlo simulacija

Pri simuliranju slučajnih veličina metodama Monte Carlo istaknuto mjesto ima slučajna veličina koja je jednoliko distribuirana na intervalu $[0, 1]$. Zbog toga istaknutog mjesta zovemo ju *slučajni broj* i označavamo s γ. Vjerojatnostna razdioba slučajnog broja zadana je funkcijom

$$F_\gamma(x) = \begin{cases} 0 & \text{za} \quad x \in (-\infty, 0), \\ x & \text{za} \quad x \in [0, 1), \\ 1 & \text{za} \quad x \in [1, \infty), \end{cases}$$

čiji je graf prikazan na slici 1.1.

Pokušajmo objasniti suštinu Monte Carlo metode. Neka je slučajna veličina ξ zadana izrazom $\xi = g(\gamma)$, gdje je g funkcija koja preslikava interval $[0, 1]$ u realne brojeve uključujući $\pm\infty$. Na primjer, funkcija:

$$g(x) = \begin{cases} -\ln x & \text{za} \quad x \in (0, 1], \\ \infty & \text{za} \quad x = 0, \end{cases}$$

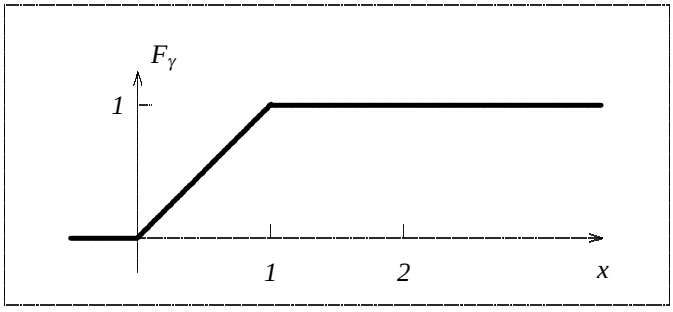
ima takvo svojstvo. Metoda Monte Carlo za simulaciju slučajne veličine ξ može se ukratko opisati na sljedeći način. Pretpostavlja se da je na raspolaganju niz realizacija slučajnog broja γ, tj. niz brojeva $\{\beta_k : k = 1, 2, \ldots\}$ koji su nastali nezavisnim mjerenjima slučajnog broja γ. Tada se nizom brojeva $\{y_k : k = 1, 2, \ldots\}$, gdje su $y_k = g(\beta_k)$, realizira slučajna veličina ξ. Ovaj jednostavni program može se raščlaniti na dvije cjeline, kojima treba dodati i treću cjelinu u kojoj je obuhvaćeno testiranje kvalitete obavljenog simuliranja.

S1) Zadana je slučajna veličina ξ pomoću svoje vjerojatnostne razdiobe $x \to F_\xi(x)$. Prva zadaća simulacije sastoji se u pronalaženju funkcije g zadane na $[0, 1]$ tako da bude

$$\xi = g(\gamma). \tag{1.1}$$

S2) Druga zadaća simulacije je generiranje niza $\{\beta_k : k = 1, 2, \ldots\}$ koji realizira slučajni broj γ i računanje niza brojeva $y_k = g(\beta_k)$ koji realizira slučajnu veličinu ξ.

S3) Treća zadaća simulacije je provjera kvalitete simuliranog niza pomoću statističkih testova.



Razdioba vjerojatnosti slučajnog broja

Slika 1.1.

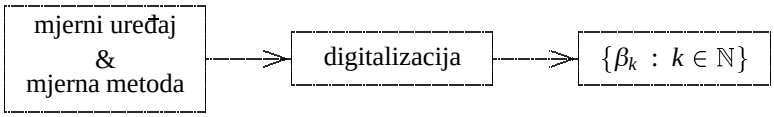
Ovako definirani postupak zove se Monte Carlo simulacija slučajne veličine ξ.

Opisani postupak može se uopćiti i u slučaju da se ξ prikaže pomoću niza nezavisnih slučajnih brojeva:

$$m = g_0(\gamma_0), \quad \xi = g_m(\gamma_1, \gamma_2, \ldots, \gamma_m), \tag{1.2}$$

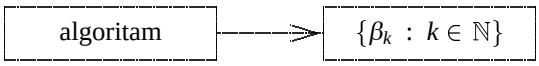
ali je ideja simulacije nepromijenjena. U izrazu (1.1) je g_0 funkcija s intervala $[0, 1]$ u skup prirodnih brojeva $\mathbb{N}$, a funkcije g_m s $[0, 1]^m$ u $\mathbb{R}$.

Prva navedena zadaća, tj. pronalaženje izraza (1.1) ili (1.2), zadaća je matematičke prirode. Druga zadaća se po svojstvu slučajne veličine svodi na mjerenje ili eksperiment, pa je shematski možemo prikazati ovim dijagramom toka:



Ovaj postupak nije isključivo matematičke prirode, jer mjerenje i mjerna metoda nisu matematički objekti.

Znamo da niz $\{\beta_k : k = 1, 2, \ldots\}$ mora imati izvjesna statistička svojstva koja proizlaze iz svojstava slučajnog broja. Provjeravanjem tih statističkih svojstava zaključujemo da taj niz jest ili nije niz realizacija slučajnog broja. Obično se kaže da testiramo niz statističkim testovima. Ta činjenica nam omogućuje da načinimo iskorak prema sljedećem uopćavanju. Možemo reći da nas ne zanima porijeklo niza $\{\beta_k : k = 1, 2, \ldots\}$, već samo njegova statistička svojstva koja možemo provjeriti statističkim testovima. Dakle, za nas će biti prihvatljivi i algoritamski generirani brojevi, ako udovoljavaju kriterijima koji slijede iz statističkih svojstava slučajnog broja. Velika prednost tako dobivenih "realizacija" $\{\beta_k : k = 1, 2, \ldots\}$ slučajnog broja je očita, jer se ne izlazi izvan objekata matematičke prirode:



Algoritmom dobiveni niz $\{\beta_k : k = 1, 2, \ldots\}$ zove se niz *paslučajnih brojeva* (lažno slučajnih), ako ima određena statistička svojstva koja posjeduje beskonačni uzorak slučajnog broja. Ne zahtijevaju se sva svojstva već minimalna. Traži se da relativne frekvencije brojeva β_r u bilo kojem podintervalu intervala $[0, 1]$ budu jednake duljini toga podintervala. Ostala svojstva beskonačnog uzorka slučajnog broja mogu biti neispunjena. Na primjer, relativna frekvencija uzastopnih trojki $\beta_{r-1}, \beta_r, \beta_{r+1}$, takvih da bude $\beta_{r-1} < \beta_r < \beta_{r+1}$, ne treba biti jednaka $1/6$. Stoga se uvode klase paslučajnih brojeva koje imaju dodatna svojstva. Naposljetku se pitamo o postojanju paslučajnih brojeva koji imaju svako svojstvo koje posjeduje beskonačni uzorak slučajnog broja. Važnost dodatnih svojstava je jasna kada ustanovimo da matematički modeli, koji opisuju prirodne, tehničke ili društvene pojave sa slučajnim parametrima, imaju oblik (1.2).

Većina danas korištenih algoritama za numeričko generiranje paslučajnih brojeva temelji se na sljedećem algoritmu paslučajnih brojeva:

$$\beta_k \;=\; M\,\beta_{k-1} \;+\; \delta \;[\bmod 1], \quad k = 1, 2, \ldots, \tag{1.3}$$

gdje su $\beta_0 = t,\ \delta$ i M parametri algoritma. Oni su brojevi s ovim ograničenjima, $\beta_0 = t \in (0, 1),\ \delta \in \mathbb{R}$, a M je prirodni broj veći od 1. Algoritam (1.3) se zove *multiplikativni*. Često se koristi ime kongruentni ili modularni.

Generator slučajnih brojeva zove se naprava kojom se generiraju nizovi $\{\beta_k : k \in \mathbb{N}\}$. U naprave se ubrajaju i datoteke (tablice) slučajnih brojeva koji su jednom generirani i zapisani. Algoritam kojim se generiraju nizovi paslučajnih brojeva zove se generator paslučajnih brojeva.

Paslučajni brojevi izučavaju se teorijskim postupcima. Tako treba dokazati da multiplikativni algoritam (1.3) generira niz paslučajnih brojeva za skoro svaki iracionalni broj $t \in (0, 1)$. Kada se od teorijskih razmatranja pređe na numeričku realizaciju susreće se niz problema druge prirode, a jedan od neugodnih je činjenica da se numerički ne može realizirati iracionalni broj t u multiplikativnom algoritmu (1.3). Ako umjesto iracionalnog t izaberemo racionalni t onda postoji prirodni broj L takav da je $\beta_L = \beta_0$, tj. tako generirani niz $\{\beta_r : r \in \mathbb{N}\}$ ima period L. Uvijek se može potražiti optimalni t u smislu, da uz zadanu

strojnu (binarnu) reprezentaciju brojeva imamo najveći mogući period. Međutim još uvijek smo daleko od zadovoljavajućeg rezultata. Zato autori generatora paslučajnih brojeva koriste dodatne "slučajne" poremećaje tokom generiranja niza brojeva β_r da bi postigli čim bolja svojstva. To nam nalaže da svaki generator paslučajnih brojeva podvrgnemo statističkim testovima iz kojih se upoznajemo s kvalitetom generiranog niza. Najčešće se koriste Pearsonov hi-kvadrat test, Kolmogorov-Smirnovljev test i testovi korelacije.

Simulacija u primjeni služi da se procijene statistički momenti slučajnih veličina $\xi = g(\gamma)$ ili vjerojatnost nekog događaja, D, pomoću indikatora događaja, $\xi = \mathbb{1}_D$. Razumije se da se ova metoda koristi za računanje statističkih momenata ili vjerojatnosti događaja kada su deterministčke metode računanja složenije od simuliranja. Promatrajmo sljedeći jednostavni primjer. Zadan je normalni slučajni vektor s 5 komponenata. Očekivanje svake komponente je nula, a njihova kovarijacijska matrica zadana je na sljedeći način:

$$c_{ij} \;=\; \frac{2}{\pi}\,\exp\,\left(-\frac{1}{5}|i-j|\right)\;\frac{\sin\left(\frac{\pi}{2}(i-j)\right)}{i\;-\;j}, \quad i,j=1,2,\ldots,5. \tag{1.4}$$

Da bismo procijenili sljedeću vjerojatnost:

$$\mathbf{P}\left(\;\xi_1<\xi_2+\xi_3+\xi_4<\xi_5\;\right), \tag{1.5}$$

možemo se poslužiti definicijom promatranog događaja pomoću 5-dimenzionalne gustoće. Dobiveni izraz je složen s numeričkog stanovišta, pa je jednostavnije poslužiti se simulacijama.

Neka je $\mathcal{F}(d)$ algebra događaja koja je generirana s d nezavisnih slučajnih brojeva $\gamma_1,\ldots,\gamma_d$. Na primjer, događaj $\{\gamma_1<\gamma_2<\;\cdots\;<\gamma_d\}$ sadržan je u toj algebri. Pomoću beskonačnog uzorka slučajnog broja mogu se simulirati događaji iz $\mathcal{F}(d)$ i procijeniti njihove vjerojatnosti. Niz paslučajnih brojeva općenito ne posjeduje to svojstvo za $d>1$. Stoga se nizom paslučajnih brojeva ne može procijeniti broj (1.5) ukoliko niz nema dodatna svojstva. Dodatna svojstva će osigurati simuliranje događaja u algebri $\mathcal{F}(d)$ za neki čvrsti d. Zato nizove paslučajnih brojeva klasificiramo dodatno prema najvećem broju d takvom da se mogu simulirati događaji u algebri $\mathcal{F}(d)$. Ispitivanje ovih dodatnih svojstava važno je za teoriju i primjene paslučajnih brojeva.

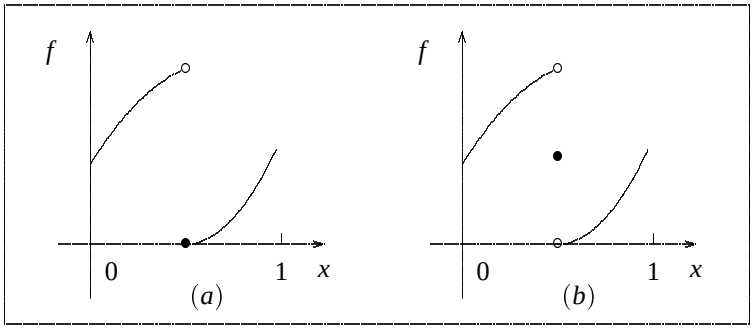
1.2. Jednoliko razdijeljeni brojevi u Weylovom smislu

Pitamo se kako ćemo prepoznati da je neki niz brojeva iz intervala $[0,1]$ upravo nastao realizacijom ili mjerenjem slučajnog broja. Odgovor nam daju statistike. Kazat ćemo da je niz

$$U_N \;=\; \{\,\gamma_1,\gamma_2,\ldots,\gamma_N\,\} \tag{1.6}$$

uzorak slučajnog broja γ dužine N, ako su svi γ_k slučajni brojevi koji su međusobno nezavisni. Ako uzorak nije konačne duljine, zove se beskonačni uzorak. Kazat ćemo da

je $\{\beta_1, \beta_2, \ldots, \beta_N\} \in [0, 1]$ niz mjerenja slučajnog broja, ako su β_k realizacije slučajnih brojeva γ_k. Da bismo opisali svojstva uzorka (1.6) slučajnih brojeva, treba nam pojam po dijelovima neprekidne funkcije. Realnu funkciju f sa intervala $[a, b]$ u skup realnih brojeva označavamo s $f : [a, b] \to \mathbb{R}$, a ponekad s $x \to f(x)$.



Po dijelovima neprekidne funkcije na $[0, 1]$.
(a) : $f(0.5) = 0$, (b) : $f(0.5) = 0.5$.

Slika 1.2.

Definicija 1.1. *Funkcija $f : [a, b] \to \mathbb{R}$ je po dijelovima neprekidna (p.d.n.) na zatvorenom intervalu $[a, b]$, ako u tom intervalu postoji konačno mnogo točaka, $a = x_0 < x_1 < x_2 < \cdots < x_m = b$, takvih da je f neprekidna na podintervalima $(x_j, x_{j+1}), j = 0, 1, \ldots, m-1$, te ima limese u graničnim točkama x_j tih intervala.*

Dva primjera po dijelovima neprekidne funkcije ilustrirana su na slici 1.2. Primijetimo da su u drugom primjeru lijevi i desni limesi u točki $x = 1/2$ međusobno različiti i razlikuju se od vrijednosti funkcije u $x = 1/2$.

Indikator intervala $[a, b] \subset [0, 1]$ često je korištena po dijelovima neprekidna funkcija. Definirana je ovim izrazom:

$$\mathbb{1}_{[a,b]}(x) \;=\; \begin{cases} 1 & \text{za} \quad x \in [a, b], \\ 0 & \text{za} \quad x \notin [a, b]. \end{cases}$$

Iz uzorka (1.6) definiraju se razne statistike. Neka je zadana po dijelovima neprekidna funkcija $f : [0, 1] \to \mathbb{R}$, neka je njom definirana slučajna veličina $\eta = f(\gamma)$, i neka je zadana pripadna statistika

$$S_{Nf} \;=\; \frac{1}{N} \sum_{k=1}^{N} f(\gamma_k)$$

pomoću uzorka (1.6). Tada očekivanje i varijanca statistike S_{Nf} imaju ove vrijednosti:

$$\begin{aligned} \mathbf{E}[S_{Nf}] \;&=\; \mathbf{E}[\eta] \;=\; \textstyle\int_0^1 f(x)dx, \\ \mathbf{Var}[S_{Nf}] \;&=\; \tfrac{1}{N}\mathbf{Var}[\eta] \;=\; \tfrac{1}{N}\left[\textstyle\int_0^1 f(x)^2 dx \;-\; \mathbf{E}[\eta]^2\right]. \end{aligned}$$

Ponekad je važno znati koji je dovoljan broj statistika da bi se utvrdilo da je neki niz nedvojbeno nastao mjerenjem uzorka slučajnog broja. Lako je ustanoviti da potpuni niz statistika čine statistike za sve moguće indikatore $f(x) = \mathbb{1}_{[a,b]}(x)$, kojima intervali $[a, b]$ imaju sljedeće racionalne krajeve: $a_k = (k-1)2^{-n}$, $b_k = k2^{-n}$, $k = 1, 2, \ldots, 2^n$, $n = 1, 2, \ldots$. Tih intervala ima prebrojivo mnogo. Iz prethodnih izraza slijedi

$$S_N\mathbb{1}_{[a,b]} = \frac{1}{N}\sum_{k=1}^{N} \mathbb{1}_{[a,b]}(\gamma_k), \quad \mathbf{E}\left[S_N\mathbb{1}_{[a,b]}\right] = b - a. \tag{1.7}$$

Jedan drugi niz dovoljnih statistika čine svi momenti, tj. $S_{Nm} = N^{-1}\sum_k (\gamma_k)^m$, $\mathbf{E}[S_{Nm}] = (m+1)^{-1}$. Postoje i drugi nizovi potpunih statistika s kojima ćemo se upoznati kasnije. Oni su vezani uz neke druge baze linearnog prostora svih po dijelovima neprekidnih funkcija $f : [0, 1] \to \mathbb{R}$. Uobičajeno je definirati paslučajne brojeve pomoću statistika (1.7):

Definicija 1.2. (NIZA PASLUČAJNIH BROJEVA (H. WEYL)) *Kaže se da je* $\{\beta_k : k \in \mathbb{N}\} \subset [0, 1]$ *niz paslučajnih brojeva, ako za svaki interval* $[a, b] \subset [0, 1]$ *vrijedi jednakost:*

$$\lim_{N\to\infty} \frac{1}{N}\sum_{k=1}^{N} \mathbb{1}_{[a,b]}(\beta_k) = b - a. \tag{1.8}$$

Brojevi sa svojstvom (1.8) zovu se također jednoliko razdijeljeni brojevi u Weylovom smislu. Kasnije će biti definirani višestruko jednoliko razdijeljeni brojevi. Stoga su ovom definicijom zadani jednostruko jednoliko razdijeljeni brojevi.

Treba odgovoriti na nekoliko važnih pitanja o paslučajnim brojevima, kao o postojanju takvih nizova, o testiranju njihovih svojstava, o numerički prihvatljivim algoritmima, itd. Uz definiciju niza paslučajnih brojeva vežu se na prirodan način statistike slučajnog broja koje su definirane pomoću indikatora $\mathbb{1}_{[a,b]}$. Sada treba pokazati da je ta definicija ekvivalentna bilo kojoj drugoj.

Neka je $\{\beta_k : k \in \mathbb{N}\}$ niz paslučajnih brojeva. Za po dijelovima neprekidnu funkciju f definira se

$$\langle f \rangle = \lim_N \frac{1}{N}\sum_{k=1}^{N} f(\beta_k), \tag{1.9}$$

kada god postoji limes na desnoj strani ovog izraza. Skup svih takvih po dijelovima neprekidnih funkcija označimo s $\mathcal{L}$. Očito je $\mathcal{L}$ linearni prostor, tj. $\langle \alpha_1 f_1 + \alpha_2 f_2 \rangle = \alpha_1\langle f_1\rangle + \alpha_2\langle f_2\rangle$ za bilo koji par funkcija $f_1, f_2 \in \mathcal{L}$ i par realnih brojeva α_1, α_2. Linearni prostor $\mathcal{L}$ sadrži indikatore svih intervala $I \subset [0, 1]$.

Stavak 1.3. *Neka je* f *po dijelovima neprekidna funkcija i neka za svaki* $\varepsilon > 0$ *postoje dvije funkcije* f_-, f_+ *iz prostora* $\mathcal{L}$ *takve da je*

$$\begin{gathered} f_-(x) \le f(x) \le f_+(x), \\ \sup_{x\in[0,1]} |\, f(x) - f_\pm(x)\,| < \varepsilon. \end{gathered} \tag{1.10}$$

Tada je f *također u prostoru* $\mathcal{L}$.

DOKAZ. Iz nejednakosti (1.10) o funkcijama f, f_- i f_+ slijedi

$$\frac{1}{N}\sum_{k=1}^{N} f_-(\beta_k) \;\le\; \frac{1}{N}\sum_{k=1}^{N} f(\beta_k) \;\le\; \frac{1}{N}\sum_{k=1}^{N} f_+(\beta_k).$$

Definiraju se brojevi

$$\overline{\alpha} \;=\; \limsup_N \frac{1}{N}\sum_{k=1}^{N} f(\beta_k), \quad \underline{\alpha} \;=\; \liminf_N \frac{1}{N}\sum_{k=1}^{N} f(\beta_k),$$

te se prethodne dvije nejednakosti napišu u sljedećem jednostavnom obliku:

$$\langle f_- \rangle \;\le\; \underline{\alpha} \;\le\; \overline{\alpha} \;\le\; \langle f_+ \rangle,$$

što implicira $0 \le \overline{\alpha} - \underline{\alpha} \le 2\varepsilon$. Ova je nejednakost valjana za svaki ε. Iz toga slijedi $\overline{\alpha} = \underline{\alpha}$. □

Neka je $\{\beta_k : k \in \mathbb{N}\}$ bilo kakav niz brojeva u intervalu $[0,1]$. Promatraju se po dijelovima neprekidne funkcije na $[0,1]$ za koje vrijedi

$$\langle f \rangle \;=\; \lim_N \frac{1}{N}\sum_{k=1}^{N} f(\beta_k) \;=\; \int_0^1 f(x)\,dx. \tag{1.11}$$

Sve takve funkcije čine linearni prostor $\mathcal{K}$.

Prostor $\mathcal{L}$ definiran je nekim određenim nizom paslučajnih brojeva, a prostor $\mathcal{K}$ nekim određenim beskonačnim nizom brojeva u $[0,1]$ koji nije nužno paslučajan. Poistovjetiti linearne prostore $\mathcal{L}$ i $\mathcal{K}$ znači kazati da su $\mathcal{L}$ i $\mathcal{K}$ jedan te isti linearni prostor za svaki niz paslučajnih brojeva. U idućem se stavku iznose uvjeti kojima spomenuta jednakost biva ostvarena.

Stavak 1.4. *Neka je $\{\beta_k : k \in \mathbb{N}\}$ niz brojeva u intervalu $[0,1]$ i neka je $\mathcal{K}$ linearni prostor svih po dijelovima neprekidnih funkcija f na $[0,1]$ za koje je ispunjena jednakost (1.11). Ako za svaki indikator $\mathbb{1}_I$, gdje je I interval u $[0,1]$, i svaki $\varepsilon > 0$ postoji par f_-, f_+ iz skupa $\mathcal{K}$ takav da to bude*

$$f_-(x) \le \mathbb{1}_I(x) \le f_+(x),$$
$$\langle f_+ \rangle \;-\; \langle f_- \rangle \;<\; \varepsilon,$$

onda je $\{\beta_k : k \in \mathbb{N}\}$ niz paslučajnih brojeva.

DOKAZ. Iz pretpostavljenih nejednakosti slijedi ocjena:

$$\left| \int_0^1 f_\pm(x)\,dx \;-\; (b-a) \right| \;<\; \varepsilon$$

za $I = [a,b]$. Nadalje, iz prve pretpostavljene nejednakosti dobije se niz novih nejednakosti:

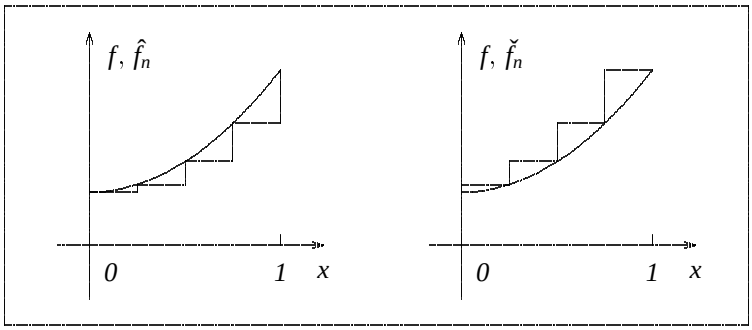
$$\tfrac{1}{N}\textstyle\sum_{k=1}^{N} f_-(\beta_k) \;\le\; \tfrac{1}{N}\sum_{k=1}^{N} \mathbb{1}_I(\beta_k) \;\le\; \tfrac{1}{N}\sum_{k=1}^{N} f_+(\beta_k),$$
$$b - a - \varepsilon \;\le\; \liminf_N \tfrac{1}{N}\textstyle\sum_{k=1}^{N} \mathbb{1}_I(\beta_k)$$
$$\le \limsup_N \tfrac{1}{N}\textstyle\sum_{k=1}^{N} \mathbb{1}_I(\beta_k) \;\le\; b - a + \varepsilon.$$

Zbog proizvoljnosti broja ε mora vrijediti uvjet paslučajnosti (1.8). □

Teorem 1.5. (O NUŽNOM I DOVOLJNOM UVJETU PASLUČAJNOSTI) *Neka je zadan niz* $\{\beta_k : k \in \mathbb{N}\} \subset [0,1]$. *Nužan i dovoljan uvjet da on bude niz paslučajnih brojeva je jednakost*

$$\lim_N \frac{1}{N} \sum_{k=1}^{N} f(\beta_k) = \int_0^1 f(x)\,dx \tag{1.12}$$

za svaku neprekidnu funkciju f *na* $[0,1]$.



Neprekidna funkcija f je aproksimirana
funkcijama skokova odozdo i odozgo.

Slika 1.3.

DOKAZ. *Nužnost.* Neka je $\{\beta_k : k \in \mathbb{N}\}$ niz paslučajnih brojeva i f neprekidna funkcija na $[0,1]$. Podijeli se interval $[0,1]$ u 2^n podintervala jednake duljine:

$$J(k) = \left[\frac{k-1}{2^n}, \frac{k}{2^n}\right), \quad k = 1, 2, \ldots, 2^n - 1, \quad J(2^n) = \left[1 - \frac{1}{2^n}, 1\right].$$

Na svakom podintervalu postoji supremum i infimum funkcije f, i označeni su simbolima $\underline{f_k}$ i $\overline{f_k}$. Zato se mogu definirati dvije aproksimacije funkcije f pomoću funkcija skokova,

$$\hat{f}_n(x) = \sum_{k=1}^{2^n} \underline{f_k}\, \mathbb{1}_{J(k)}(x), \quad \check{f}_n(x) = \sum_{k=1}^{2^n} \overline{f_k}\, \mathbb{1}_{J(k)}(x),$$

kao što je ilustrirano na slici 1.3. Po pretpostavci u dokazu, one su u linearnom prostoru $\mathcal{L}$. Za konstruirane funkcije valjane su sljedeće nejednakosti:

$$\hat{f}_n(x) \le f(x) \le \check{f}_n(x),$$
$$\sup_{x\in[0,1]} \left\{ |f(x) - \check{f}_n(x)|, \quad |f(x) - \hat{f}_n(x)| \right\} < \varepsilon(n),$$

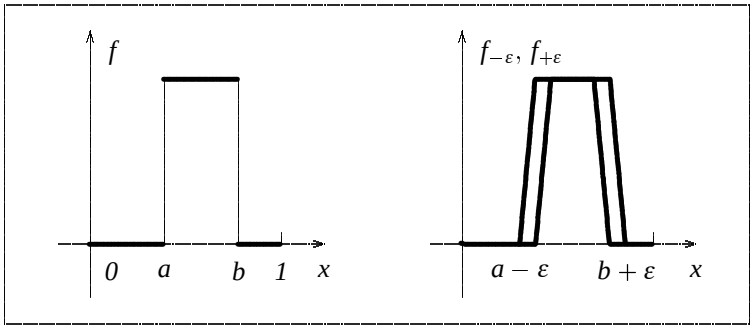
i

$$\lim_n \varepsilon(n) = 0.$$

Iz stavka 1.3, o prostoru $\mathcal{L}$, slijedi $f \in \mathcal{L}$. Pored toga je po svojstvu Riemannova integrala za neprekidnu funkciju ustanovljena jednakost (1.12).

Dovoljnost. Neka je $\{\beta_k : k \in \mathbb{N}\}$ niz brojeva, takav da vrijedi (1.12) za svaku neprekidnu funkciju f. Treba dokazati da vrijedi (1.8). Dovoljno je načiniti dokaz za $I = [a, b] \subset (0, 1)$. Prostor $\mathcal{K}$ iz stavka 1.4 sastoji se od neprekidnih funkcija na $[0, 1]$. Za izabrani $\mathbb{1}_{[a,b]}$ i svaki $\varepsilon > 0$ postoje dvije "trapezaste" funkcije $f_{-\varepsilon}$, $f_{+\varepsilon}$ kao na slici 1.4., takve da bude $\langle f_{-\varepsilon} \rangle < (b-a) < \langle f_{+\varepsilon} \rangle$, a isto tako $\langle f_{+\varepsilon} \rangle - \langle f_{-\varepsilon} \rangle < \varepsilon$. One su neprekidne i za njih vrijedi (1.12) po pretpostavci u dokazu. Tada iz stavka 1.4 slijedi tvrdnja teorema. □

Neprekidne funkcije na $[0, 1]$ možemo razviti u Fourierov red koji konvergira funkciji skoro svuda na (0,1). Zato je sljedeći rezultat prirodna posljedica prethodnog rezultata.



Aproksimacija indikatora pomoću neprekidnih trapezastih funkcija

Slika 1.4.

Teorem 1.6. (WEYLOV KRITERIJ) *Neka je zadan niz* $\{\beta_k : k \in \mathbb{N}\} \subset [0, 1]$. *Nužno i dovoljno da on bude niz paslučajnih brojeva su jednakosti*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} \exp\left(2\pi i m \beta_k\right) = 0, \tag{1.13}$$

za svaki $m \in \mathbb{N}$.

DOKAZ. *Nužnost.* Neka je $\{\beta_k : k \in \mathbb{N}\}$ niz paslučajnih brojeva. Eksponencijalne su funkcije neprekidne pa nužnost slijedi iz prethodnog teorema.

Dovoljnost. Pretpostavlja se da za niz $\{\beta_k : k \in \mathbb{N}\}$ vrijede uvjeti (1.13). Funkcija šator sa slike 1.5., s centrom u r i otvorom $2h$, definirana je izrazom

$$\check{s}_h(r, x) = \begin{cases} 1 - \dfrac{|x-r|}{h} & \text{za} \quad |x-r| \le h, \\ 0 & \text{inače.} \end{cases}$$

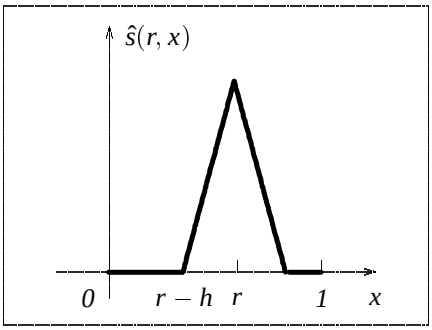
Promatraju se šatori za koje je otvor $2h \le 1$. Označimo s $p(h, r, \cdot)$ periodičku funkciju s periodom 1 koja nastaje produženjem po periodičnosti šatora $\check{s}_h(r, \cdot)$. Funkcija $p(h, 0, \cdot)$

ima sljedeći razvoj u Fourierov red:

$$p(h,0,x) \;=\; h \;+\; \sum_{k=1}^{\infty} a_k \cos(2\pi k x), \quad a_k \;=\; \frac{2}{h(\pi k)^2}\sin^2(\pi k h).$$

Red je očito apsolutno konvergentan i predstavlja $x \to p(h,0,x)$ u svakoj točki intervala $[0,1]$. Zbog jednakosti $p(h,r,x) = p(h,0,x-r)$ funkcija $x \to p(h,r,x)$ može se razviti u red po kosinusima i sinusima:

$$p(h,r,x) \;=\; h \;+\; \sum_{k=1}^{\infty} a_k \Big\{ \cos(2\pi k r)\cos(2\pi k x) \;+\; \sin(2\pi k r)\sin(2\pi k x) \Big\}.$$



Funkcija šator

Slika 1.5.

Za svaki član ovog reda, izuzev nultog, $(k = 0)$, vrijedi pretpostavka u teoremu, pa tako i za njegovu parcijalnu sumu $x \to p_n(h,r,x)$. To znači da je ispunjena jednakost:

$$\lim_N \frac{1}{N} \sum_{k=1}^{N} p_n(h,r,\beta_k) \;=\; h,$$

za sve n. Prethodna jednakost je valjana i u limesu, $n \to \infty$, zbog apsolutne konvergencije $p_n(h,r) \to p(h,r)$ na intervalu $[0,1]$,

$$\lim_N \frac{1}{N} \sum_{k=1}^{N} p(h,r,\beta_k) \;=\; h.$$

Iz ove diskusije slijedi da linearna kombinacija šatora pripada linearnom prostoru $\mathcal{K}$. Kako se svaka neprekidna funkcija na $[0,1]$ može po volji dobro aproksimirati linearno po dijelovima slijedi da $\mathcal{K}$ sadrži sve neprekidne funkcije. Iz prethodnog teorema slijedi tvrdnja. □

Definiramo brojeve

$$B_{N\,\exp}(m) \;=\; \frac{1}{N} \sum_{k=1}^{N} \exp\Big(2\pi i m \beta_k\Big) \tag{1.14}$$

u skladu s tvrdnjom prethodnog teorema. Tada se beskonačni niz jednakosti

$$\lim_{N\to\infty} B_{N\,\exp}(m) = 0, \quad \text{za} \quad m = 1,2,\ldots,$$

zove Weylov kriterij za testiranje niza paslučajnih brojeva.

Ponekad se neposredno mogu dokazati jednakosti $\lim_N B_{N\,\exp}(m) = 0$, samo za neki podniz brojeva iz $\mathbb{N}$. Pitamo se koliko nam to može pomoći da zaključimo da je $\{\beta_k : k \in \mathbb{N}\}$ niz paslučajnih brojeva. U tu svrhu se definira podniz $\mathcal{I}(\alpha) \subset \mathbb{N}$ na sljedeći način:

$$\mathcal{I}(\alpha) \;=\; \{N(1), N(2), \ldots, N(k), \ldots\}, \quad N(k) \;\in\; [k^\alpha, k^\alpha + 1). \tag{1.15}$$

Iz definicije je jasno da je nužno $\alpha > 1$.

Posljedica 1.7. *Neka je* $\alpha > 1$, $\{\beta_k : k \in \mathbb{N}\} \subset [0,1)$ *i neka je ispunjen beskonačni niz uvjeta*

$$\lim_{N \in \mathcal{I}(\alpha)} B_{N\ \exp}(m) \ = \ 0, \quad m \in \mathbb{N}.$$

Tada je $\{\beta_k : k \in \mathbb{N}\}$ *niz paslučajnih brojeva i za njega je ispunjen Weylov kriterij.*

DOKAZ. Promatraju se brojevi $N \in [N(k), N(k+1)]$. Za njih vrijedi sljedeća nejednakost:

$$\begin{aligned} \left| B_{N\ \exp}(m) \ - \ \frac{N(k)}{N} B_{N(k)\ \exp}(m) \right| \ &\leq \ \frac{1}{N}\Big(N(k+1) \ - \ N(k)\Big) \\ \leq \left(1 \ + \ \frac{1}{k} \right)^{\alpha} \ + \ \frac{1}{k} \ - \ 1 \ &\leq \ \frac{1 \ + \ \alpha \exp(\ \alpha/k\ )}{k}, \end{aligned}$$

za sve $k > 1$. Zbog $N(k)/N \to 1$ slijedi

$$\limsup_{N \to \infty} \left| B_{N\ \exp}(m) \right| \ = \ 0.$$

tj. Weylov kriterij. □

Posljedica 1.8. *Neka je* t *iracionalni broj i neka je zadan niz*

$$\beta_k \ = \ tk \ [mod\ 1], \quad k = 1, 2, \ldots. \tag{1.16}$$

Tada brojevi β_k *tvore niz paslučajnih brojeva.*

DOKAZ. Definiraju se brojevi $x_k = tk$. Očito je $\exp(2\pi i m x_k) = \exp(2\pi i m \beta_k)$ za svaki prirodni broj m. Prema prethodnom teoremu treba promatrati red:

$$\sum_{k=1}^{N} \exp(2\pi i m t k) \ = \ \frac{\exp(2\pi i m t)}{1 - \exp(2\pi i m t)} \left[1 - \exp\left(2\pi i N m t \right) \right],$$

kojemu suma po apsolutnoj vrijednosti nije veća od $|\sin(\pi m t)|^{-1}$, jednoliko obzirom na N. Stoga je

$$\lim_{N \to \infty} \frac{1}{N} \sum_{k=1}^{N} \exp(2\pi i m \beta_k) \ = \ 0. \quad \square$$

Stavak 1.9. *Neka su zadani nizovi brojeva* x_k *i* $y_k = x_k + \alpha$, *gdje je* $\alpha \in \mathbb{R}$. *Ako brojevi* $\beta_k = x_k \ [mod\ 1]$ *tvore niz paslučajnih brojeva, onda i brojevi* $\sigma_k = y_k \ [mod\ 1]$ *također tvore niz paslučajnih brojeva.*

Dokaz slijedi neposredno iz Weylova kriterija kada u njega uvrstimo nizove brojeva x_k i y_k.

Neposrednom konstrukcijom niza (1.16) ustanovljeno je da paslučajni brojevi postoje. Taj niz brojeva ima izvjesna neželjena svojstva pa se simulacije procesa u primjenama temelje na nizu paslučajnih brojeva (1.3). Njih ćemo promatrati u preostalom dijelu ovog odjeljka.

Za svaki $t \in (0,1)$ i $M \in \mathbb{N},\ M > 1$, promatra se beskonačni niz brojeva $x_k = M^k t,\ k = 1, 2, \ldots$. Tada su $\beta_k = x_k \ [\mathrm{mod}\ 1]$ iz intervala $[0,1)$, te se može koristiti Weylov kriterij da se provjeri pripada li niz $\{\beta_k : k \in \mathbb{N}\}$ familiji paslučajnih brojeva. Koristimo sljedeći rezultat

Teorem 1.10. (O MULTIPLIKATIVNOM GENERATORU) *Za $M \in \mathbb{N},\ M > 1, \delta \in \mathbb{R}$ i skoro svaki $t \in (0,1)$, brojevi*

$$\beta_k \ = \ M\beta_{k-1} \ + \ \delta \ [mod\ 1], \quad \beta_0 \ = \ t, \quad k \in \mathbb{N}, \tag{1.17}$$

generiraju niz paslučajnih brojeva.

DOKAZ. Za dokaz se treba poslužiti Weylovim kriterijem. Neka je m nepromjenjiv prirodni broj tokom dokaza. Promatraju se funkcije

$$t \to f_N(t) \ = \ B_{N\ \exp}(m) \ = \ \frac{1}{N} \sum_{k=1}^{N} \exp(2\pi i m M^k t). \tag{1.18}$$

Dovoljno je promatrati slučaj $\delta = 0$ kao što će biti pokazano na kraju dokaza. Zbog jednostavnosti pisanja eksponencijalne funkcije se označavaju s $t \to \phi_k(t)$. Treba dokazati da postoji limes funkcija f_N kada N teži u beskonačnost i da je granična funkcija skoro svuda nula na $[0,1]$.

Funkcije ϕ_k su međusobno ortonormirane u $L_2(0,1)$, pa je:

$$\| f_N \|_2 \ = \ \frac{1}{\sqrt{N}},$$

gdje $\| \cdot \|$ označava $L_2(0,1)$ normu. Slijedi da niz f_N konvergira nuli u $L_2(0,1)$. To ne znači da limes funkcija $t \to f_N(t)$ teži nuli skoro svuda u intervalu $[0,1]$ (vidi primjer s neželjenim ishodom u referenci [Sa]). Međutim, postoji podniz funkcija f_N za koji je to ispunjeno. Dovoljno je odabrati podniz (1.15) s bilo kojim izborom broja $\alpha > 1$. Pomoću Čebiševljeve nejednakosti dobivamo ocjenu

$$\mu_k(\varepsilon) \ = \ \text{mjera} \ \{ \ |f_{N(k)}| \ > \ \varepsilon \ \} \ \leq \ \frac{1}{\varepsilon^2} \ \| f_{N(k)} \|_2^2 \ \leq \ \frac{1}{k^\alpha \varepsilon^2},$$

tako da je

$$\sum_{k=1}^{\infty} \mu_k(\varepsilon) \ < \ \infty$$

za svaki $\varepsilon > 0$. Iz Borel-Cantellijeve leme slijedi da niz $f_{N(k)}$ konvergira nuli skoro svuda na $[0,1]$. Dakle, za skoro svaki $t \in (0,1)$ ispunjeno je $\lim_{N(k)} B_{N(k)}(m) = 0$. Za $m = 1, 2, \ldots$, dobiju se skupovi $S(m) \subset [0,1]$, jedinične Lebesgueove mjere, za koje vrijede ove jednakosti:

$$\lim_{N \to \infty, N \in \mathcal{I}(\alpha)} B_{N\ \exp}(m) \ = \ 0, \quad t \in S(m).$$

Skup $S = \cap_m S(m)$ također ima jediničnu Lebesgueovu mjeru. Povrh toga je

$$\lim_{N\to\infty, N\in\mathcal{I}(\alpha)} B_{N\ \exp}(m) \ = \ 0, \quad m \in \mathbb{N},$$

za svaki $t \in S$. Primjenom posljedice Weylova teorema 1.7 slijedi da je $\{\beta_k : k \in \mathbb{N}\}$ niz paslučajnih brojeva za skoro svaki t iz $(0, 1)$. Zapravo je do sada dokazan nešto općenitiji rezultat. Definiraju se dva niza brojeva $x_k = M^k t$ i $z_k = x_k + \alpha$, gdje je $\alpha \in \mathbb{R}$. Prema stavku o translaciji, 1.9, slijedi da $z_k \ [\mathrm{mod}\ 1]$ tvore niz paslučajnih brojeva za skoro svaki t.

Broj δ u definiciji (1.17) je realan. Može se prikazati kao $\delta = M\rho - \rho$ i promatrati dva niza brojeva $x_k = Mx_{k-1} + \delta$ i $y_k = x_k + \rho$. Za drugi niz slijede jednakosti:

$$y_k = Mx_{k-1} + \delta + \rho = M(x_{k-1} + \rho) = My_{k-1} = \ \cdots \ = M^k y_0 = M^k(t + \rho).$$

Dakle, brojevi $y_k \ [\mathrm{mod}\ 1]$ čine niz paslučajnih brojeva prema dosadašnjem dijelu dokaza. Zbog toga i translatirani brojevi $(x_k = y_k - \rho) \ [\mathrm{mod}\ 1]$ čine niz paslučajnih brojeva. □

Algoritam (1.17) definira preslikavanje intervala $[0, 1)$ u sebe. To svojstvo omogućuje upotrebu preslikavanja za generiranje paslučajnih brojeva (vidi primjedbe).

Uz dokaz prethodnog teorema treba istaknuti da funkcija $t \to f(t)$, $f = \lim_N f_N$, nije nula za svaki $t \in (0, 1)$. Neka je $\mathcal{R}$ skup racionalnih točaka oblika

$$\frac{r}{N}, \quad r \ = \ 1, 2, \ldots, M^p - 1, \quad p \in \mathbb{N}.$$

One čine gusti skup u $[0, 1]$. Pokažimo da je $f(t) \neq 0$ za $t \in \mathcal{R}$. Promatra se samo slučaj $m = 1$. Neka je $t = r/M^p$. Tada je $\phi_k(t) = 1$ za $k = M^p, M^p + 1, \ldots$, tako da $f_N(t) \to 1$ kada $N \to \infty$. Postoje iracionalni brojevi za koje je $f(t) \neq 0$ (vidi Franklin [Fr2]).

Skupovi $T_M \subset [0, 1]$ za koje su brojevi (1.17) paslučajni imaju maksimalnu mjeru, tj. jednaku 1. Zato i njihov presjek $T = \cap_M T_M$, po svim $M = 2, 3, \ldots$, ima mjeru 1. Broj $t \in T_M$ zovemo sjeme. Dokazali smo sljedeći rezultat:

Teorem 1.11. (O SJEMENU MULTIPLIKATIVNOG ALGORITMA) *Neka je T_M skup sjemena algoritma (1.17) za čvrsti M. Tada $T = \cap_M T_M$ ima Lebesgueovu mjeru jednaku* 1.