Osječki matematički list 23 (2023), 147–159

Malo kombinatorike

Petar Žugec*, Eric Andreas Vivoda†

Sažetak

U članku nalazimo broj riječi koje možemo sastaviti pod uvjetom da se dva specifična znaka ne pojavljuju zajedno. Problem rješavamo korištenjem rekurzivnih relacija, nakon kratkog pregleda povijesti njihova korištenja.

Ključne riječi: *prebrojavanje, rekurzivne relacije, početne vrijednosti, očekivana vrijednost, varijanca, statistička nepouzdanost*

A bit of combinatorics

Abstract

We find the number of words that can be composed by avoiding a consecutive appearance of two selected characters. We make use of the recurrence relations in solving the problem, after a short review on the history of their use.

Keywords: *enumeration, recurrence relations, initial values, expected value, variance, statistical uncertainty*

*Fizički odsjek, Prirodoslovno-matematički fakultet, Sveučilište u Zagrebu, email: pzugec@phy.hr

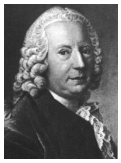
†Fizički odsjek, Prirodoslovno-matematički fakultet, Sveučilište u Zagrebu, email: evivoda@phy.hr

1 O rekurzivnim nizovima

Leonardo iz Pise (oko 1170. – oko 1250.), poznat kao Fibonacci; talijanski matematičar

Albert Girard (1595.–1632.) francuski matematičar; među ostalim, zaslužan za uvođenje oznaka sin, cos, tan *za osnovne trigonometrijske funkcije. [Na internetu se može pronaći navodni portret Girarda. No radi se o portretu kartografa Jodocusa Hondiusa]*

Abraham de Moivre (1667.–1754.) francuski matematičar



Daniel Bernoulli (1700.–1782.) švicarski matematičar i fizičar

Leonhard Euler (1707.–1783.) švicarski erudit, jedan od najvećih matematičara u povijesti

Kad kažemo da je neki niz zadan rekurzivno, tada podrazumijevamo da je n-ti član ($n > m$) toga niza zadan kao funkcija (moguće svih) prethodnih članova s m početnih uvjeta. Rekurzija može ovisiti i o samome rednom broju člana n. Simbolički zapisano,

$$a_1 = \alpha_1,\ \ldots,\ a_m = \alpha_m \quad \text{uz} \quad a_n = f_n(a_1, \ldots, a_{n-1}); \quad n > m \tag{1}$$

predstavlja rekurzivni niz zadan pravilom f_n te skupom od m početnih uvjeta $\alpha_1, \ldots, \alpha_m$. Riješiti rekurziju znači odrediti eksplicitan izraz F_n za sve članove niza ($n \geq 1$), određen samo indeksom n i početnim uvjetima

$$a_n = F_n(\alpha_1, \ldots, \alpha_m); \quad n \geq 1, \tag{2}$$

bez ovisnosti o ostalim prethodnim članovima $(a_{m+1}, \ldots, a_{n-1})$.

Općenitost ovoga iskaza odražava širinu pojma rekurzivnih nizova. U općenitom slučaju pojedini član niza može biti zadan svima prethodnima. U tom slučaju odredbenu rekurzivnu relaciju teško bismo mogli okarakterizirati jedinstvenim redom („dubinom“ koja karakterizira raspon prethodnih članova kojima je definiran svaki sljedeći u nizu). Naposljetku, i samo pravilo f_n može varirati od člana do člana. Stoga postoji vrlo malo tvrdnji općenite valjanosti koje bismo mogli dati o toliko širokome pojmu.

Osobito važnu i korisnu klasu rekurzija čine linearne rekurzije. Posebno, *linearna rekurzija s konstantnim koeficijentima, reda m,* relacija je oblika

$$a_n = \mu_n + \sum_{k=1}^{m} \lambda_k a_{n-k}, \quad n > m, \tag{3}$$

popraćena skupom od m početnih vrijednosti $a_1 = \alpha_1, \ldots, a_m = \alpha_m$. Pri tome su koeficijenti λ_k ($k = 1, \ldots, m$) neovisni o n. Ako je $\mu_n = 0$ za svaki $n > m$, rekurzivna relacija naziva se *homogenom*, a u suprotnome *nehomogenom*.

Jedan od prvih dokumentiranih rekurzivnih nizova zadan je u Fibonaccijevoj knjizi *Liber Abaci* (1202) [1] u sklopu tzv. problema zečeva. Štoviše, najraniji poznati zapisi o Fibonaccijevim brojevima i rekurzivnoj metodi njihove konstrukcije dolaze iz Indije, 700 godina pr. n. e. [2] No trebalo je čekati sve do 17. st. na objavu Girardove spoznaje (1634) [3] da se njihova odredbena relacija može rekurzivno zapisati kao

$$F_n = F_{n-1} + F_{n-2}; \quad F_1 = 1,\ F_2 = 1. \tag{4}$$

Ova relacija generira slavne Fibonaccijeve brojeve 1, 1, 2, 3, 5, 8, 13, 21, ...

Nešto manje od sto godina nakon njezine uspostave de Moivre (1722) [4], D. Bernoulli (1728) [5] i Euler (1765) [6] odredili su njezino rješenje u zatvorenom obliku

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right], \tag{5}$$

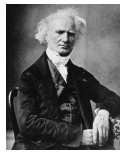
što je danas poznato kao Binetova formula[1], iako je Binet (1843) [7] došao do rješenja nakon de Moivrea i Bernoullija. Pri tome je upravo de Moivre dao prvi formalniji pristup rekurzivnim relacijama u djelu *Miscellanea analytica de seriebus et quadraturis* (1730) [8], gdje je Fibonaccijevu rekurziju riješio metodom diferencijskih jednadžbi.

Sljedeća značajnija primjena rekurzivnih relacija pojavila se u formiranju aksioma prirodnih brojeva, danas poznatih kao Peanovi aksiomi [9]. Dedekind (1888) [10] i Peano (1889) [11] zbrajanje prirodnih brojeva rekurzivno su formalizirali pomoću funkcije sljedbenika $s(\cdot)$ na način

$$m + s(n) = s(m + n). \tag{6}$$

U novijoj povijesti rekurzivne relacije imale su veliku primjenu u matematičkoj logici, gdje se posebno ističu Gödelovi teoremi nepotpunosti (1931) [12]. Među predvodnicima teorije rekurzivnih funkcija [13] posebno mjesto zauzima Rózsa Péter, koju se smatra majkom teorije izračunljivosti [14].

Referenca [15] nudi pregled temeljnih činjenica o rekurzijama, njihovim primjenama i metodama njihova rješavanja, s posebnim naglaskom na linearne rekurzije kakve se često pojavljuju u praksi. Neke od najzanimljivijih rekurzivinih problema čitatelj može pronaći i u [16]. Osim u čistoj matematici rekurzije nalaze široku primjenu i u ostalim spoznajnim i praktičnim disciplinama, a posebice u prirodnim znanostima. Među takvim primjerima nalaze se i brojni problemi iz fizike [17].[2] Jedan od najraširenijih primjera s kojim se susrećemo studenti fizike problem je nalaženja ukupnog električnog otpora specifičnog niza otpornika (vidi *Primjer 16* iz [15]). Međutim manje je poznato da u granici s beskonačno mnogo strujnih elemenata rješenje tog problema nije nužno konvergentno za opću kombinaciju impedancija (vidi zadatak 4.4 iz [17]).



Jacques Philippe Marie Binet (1786.–1856.) francuski matematičar i fizičar

Julius Wilhelm Richard Dedekind (1831.–1916.) njemački matematičar

Giuseppe Peano (1858.–1932.) talijanski matematičar i lingvist

Kurt Friedrich Gödel (1906.-1978.) filozof, matematičar i jedan od najvećih logičara u povijesti

Rózsa Péter (1905.–1977.) mađarska matematičarka i logičarka, poznata kao majka teorije izračunljivosti

[1] Jedna od zanimljivih činjenica o Fibonaccijevim brojevima jest da omjer dvaju uzastopnih članova teži u povijesno poznat omjer *zlatnoga reza*

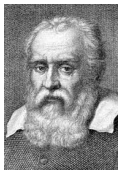
$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \frac{1+\sqrt{5}}{2} \approx 1.618,$$

što se lako može vidjeti iz Binetove formule na temelju $|(1-\sqrt{5})/2| < 1$.

[2] Vidi zadatke 3.3 (*Relativistički motociklisti*), 4.4 (*Impedancijski krug*), 5.4 (*Titranje sa suhim trenjem*) i 5.6 (*Nabijeno njihalo*).

Neka od najpoznatijih imena vezanih uz rani razvoj kombinatorike i teorije vjerojatnosti:

Gerolamo Cardano (1501.–1576.)



Galileo Galilei (1564.–1642.)

Pierre de Fermat (1607.–1665.)

Blaise Pascal (1623.–1662.)

Jacob Bernoulli (1655.–1705.)

Johann Carl Friedrich Gauss (1777.–1855.)

Mnoštvo primjera iz [15] jasno pokazuje da rekurzivne relacije imaju neprocjenjivu ulogu u rješavanju najrazličitijih kombinatoričkih problema. Vjerojatno najljepša ilustracija toga jest činjenica da se osnovna kombinatorička funkcija *faktorijel* – koja u oznaci $n!$ odgovara umnošku prvih n prirodnih brojeva te predstavlja broj svih permutacija n raspoznatljivih objekata – može rekurzivno definirati kao

$$n! = n \cdot (n-1)!, \quad 0! = 1. \tag{7}$$

Kao nadopunu riznici primjera iz [15], upravo ćemo u ovome članku primjenom rekurzija riješiti jedan zanimljiv kombinatorički problem.

2 Kombinatorički problem

Na raspolaganju imamo abecedu od n različitih znakova ($n \geq 2$); npr. A, B, C, ... Koliko je riječi od k znakova ($k \geq 1$) – tj. duljine k, ne nužno različitih znakova – u kojima se određena dva znaka (npr. A i B) ne pojavljuju zajedno?

Umjesto pokušajem *izravnog* prebrojavanja mogućnosti problem ćemo riješiti uspostavom rekurzivne relacije kojom je određeno traženo rješenje. U daljnjem računu općom oznakom p podrazumijevamo broj riječi u kojima se pod danim okolnostima A i B *ne pojavljuju* zajedno. Označimo s p_k broj *svih* takvih riječi duljine k. Neka su dalje $p_k^{(\mathrm{A})}$ i $p_k^{(\mathrm{B})}$ brojevi takvih riječi koje *završavaju* ili s A ili s B, a $p_k^{(\overline{\mathrm{AB}})}$ brojevi takvih riječi koje *ne završavaju* niti s A niti s B. Očito vrijedi

$$p_k = p_k^{(\mathrm{A})} + p_k^{(\mathrm{B})} + p_k^{(\overline{\mathrm{AB}})}. \tag{8}$$

Ukupan broj kombinacija p_k možemo rastaviti i ovako: (1) početni dio riječi duljine $k-1$ završava ili s A ili s B pa se onda na mjestu zadnjeg znaka smije naći neki od preostalih $n-1$ znakova (uz predzadnji A ne smije doći zadnji B, i suprotno); (2) početak riječi duljine $k-1$ ne završava niti s A niti s B pa na mjesto zadnjeg znaka može doći bilo koji od n dostupnih. Prema tome, ukupan broj p_k traženih mogućnosti zadovoljava i

$$p_k = (n-1)\left(p_{k-1}^{(\mathrm{A})} + p_{k-1}^{(\mathrm{B})}\right) + np_{k-1}^{(\overline{\mathrm{AB}})}; \quad n \geq 2,\, k \geq 2. \tag{9}$$

Među riječima u kojima se A i B ne pojavljuju zajedno, s A mogu završiti samo riječi čija kraća baza ne završava s B, i suprotno

$$p_k^{(\mathrm{A})} = p_{k-1} - p_{k-1}^{(\mathrm{B})} \quad \text{i} \quad p_k^{(\mathrm{B})} = p_{k-1} - p_{k-1}^{(\mathrm{A})}; \quad k \geq 2. \tag{10}$$

Zbog simetrije između A i B vrijedi $p_k^{(\mathrm{A})} = p_k^{(\mathrm{B})}$ pa radi kratkoće i jasnoće zapisa uvodimo pokratu

$$q_k \equiv p_k^{(\mathrm{A})} = p_k^{(\mathrm{B})}. \tag{11}$$

Sada od (8) i (11) preostaje

$$p_k^{(\overline{\mathrm{AB}})} = p_k - 2q_k, \tag{12}$$

dok uvrštavanjem (11) i (12) u (9), uz pomake indeksa $k \to k-1$, slijedi

$$p_k = np_{k-1} - 2q_{k-1}; \quad k \geq 2. \tag{13}$$

Konačno, (10) vodi na

$$q_k = p_{k-1} - q_{k-1}; \quad k \geq 2. \tag{14}$$

Izrazi (13) i (14) dvije su vezane rekurzivne relacije koje trebamo riješiti. Eliminacijom q_{k-1} iz (13): $q_{k-1} = (np_{k-1} - p_k)/2$ te njegovim uvrštavanjem u (14) – uz pomak indeksa $k-1 \to k$ za potrebe člana q_k – preostaje razvezana rekurzivna relacija: $p_{k+1} = (n-1)p_k + (n-2)p_{k-1}$. U svrhu olakšane čitljivosti indekse pomičemo jedno mjesto unatrag ($k \to k-1$) te njezin konačan oblik zapisujemo kao

$$p_k = (n-1)p_{k-1} + (n-2)p_{k-2}; \quad n \geq 2,\, k \geq 3 \tag{15}$$

jer je „najviši“ član koji se u takvom zapisu pojavljuje upravo traženi p_k. Da bismo eksplicitno izračunali rješenje rekurzije (15), trebamo poznavati njezine početne vrijednosti. Dana rekurzija drugoga je reda, odnosno k-ti član niza p_k izražen je pomoću dvaju prethodnih članova pa je potrebno zadati dvije početne vrijednosti. Prvi član ($k = 1$) jednak je n jer uvjet problema ne postavlja nikakva ograničenja na *samostalnu* pojavu bilo kojeg od n dostupnih znakova abecede; jedan znak sam za sebe ne može se pojaviti u kombinaciji niti s jednim drugim. Drugi član ($k = 2$) jednak je $n^2 - 2$ jer od svih mogućih kombinacija dvaju znakova (njih n^2 jer i na prvo i na drugo mjesto možemo postaviti bilo koji od n znakova) nisu dozvoljene dvije specifične kombinacije: AB i BA. Radi preglednosti izdvojeno navodimo ove vrijednosti

$$p_1 = n \quad \text{i} \quad p_2 = n^2 - 2. \tag{16}$$

Rekurzija (15) linearna je homogena rekurzivna relacija s konstantnim koeficijentima (članovi $n-1$ i $n-2$ ne ovise o k) i rješava se uobičajenom tehnikom [15]: rješenje treba potražiti u obliku $p_k = r^k$, za neko $r \neq 0$ (jer nas trivijalna rješenja ne zanimaju). Uvrštavanjem ovog pretpostavljenog oblika u (15) te dijeljenjem čitave jednadžbe s r^{k-2} preostaje tzv. karakteristična jednadžba za sam r

$$r^2 - (n-1)r - (n-2) = 0. \tag{17}$$

Rješenja kvadratne jednadžbe (17) su

$$r_{1,2} = \frac{n-1 \pm \sqrt{n^2+2n-7}}{2} \tag{18}$$

te oba, kao linearno nezavisne komponente, doprinose ukupnome rješenju (za dokaz vidi *Propoziciju 3* iz [15])

$$p_k = ar_1^k + br_2^k, \tag{19}$$

gdje se konstante a i b određuju iz početnih vrijednosti (16). Njihovim uvrštavanjem u (19) dobivamo dvije jednadžbe s dvije nepoznanice

$$ar_1 + br_2 = n \quad \text{i} \quad ar_1^2 + br_2^2 = n^2 - 2, \tag{20}$$

čija se rješenja lako nalaze

$$a = \frac{1}{2}\left(1 + \frac{n+1}{\sqrt{n^2+2n-7}}\right) \quad \text{i} \quad b = \frac{1}{2}\left(1 - \frac{n+1}{\sqrt{n^2+2n-7}}\right). \tag{21}$$

Konačno, povratkom (18) i (21) u (19) te uvođenjem sljedećih pokrata radi preglednosti zapisa

$$n_\pm \equiv n \pm 1, \tag{22}$$

$$\eta \equiv n^2 + 2n - 7, \tag{23}$$

možemo zapisati konačno rješenje problema[3]

$$p_k = \frac{\left(n_+ + \sqrt{\eta}\right)\left(n_- + \sqrt{\eta}\right)^k - \left(n_+ - \sqrt{\eta}\right)\left(n_- - \sqrt{\eta}\right)^k}{2^{k+1}\sqrt{\eta}} \tag{24}$$

[3]Naš problem savršeno se uklapa u klasu tzv. Lucasovih nizova [18], određenih rekurzijom

$$x_k = Px_{k-1} - Qx_{k-2}; \quad k \geq 3. \tag{$*$}$$

Za zadane konstante P i Q tipično se definiraju dva istaknuta rješenja ove relacije: nizovi $U_k(P,Q)$ i $V_k(P,Q)$ koji se razlikuju prema početnim vrijednostima, takvima da je

$$U_1(P,Q) = 1; \quad U_2(P,Q) = P; \quad V_1(P,Q) = P; \quad V_2(P,Q) = P^2 - 2Q.$$

Bilo koje rješenje rekurzije $(*)$, tj. rješenje za bilo koji skup početnih vrijednosti može se izraziti kao linearna kombinacija dvaju rješenja $U_k(P,Q)$ i $V_k(P,Q)$. Usporedbom (15) i $(*)$ nalazimo da u kontekstu našeg problema vrijedi $P = n-1$ te $Q = 2-n$. Koeficijente α i β iz tražene linearne kombinacije $p_k = \alpha U_k(n-1, 2-n) + \beta V_k(n-1, 2-n)$ nalazimo primjenom te kombinacije na početne uvjete (16): $p_1 = \alpha + \beta(n-1)$ te $p_2 = \alpha(n-1) + \beta(n^2-3)$. Odavde slijedi $\alpha = (n+1)/2$ i $\beta = 1/2$ pa rješenje (24) možemo iskazati kao

$$p_k = \frac{n+1}{2}U_k(n-1, 2-n) + \frac{1}{2}V_k(n-1, 2-n).$$

Kroz ovu relaciju sva poznata svojstva Lucasovih nizova primjenjiva su i na naše rješenje.

koje, podsjećamo, određuje koliko riječi duljine od k znakova možemo sastaviti iz abecede od n različitih dostupnih znakova, s time da se dva specifična znaka ne pojavljuju zajedno.

Nekome tko se po prvi put susreće s ovakvim zapisom cjelobrojnog rješenja može biti neobično kako takav izraz uopće može rezultirati cijelim brojevima. Sve što trebamo da bismo to dokazali jest izravnim uvrštavanjem $k = 1$ i $k = 2$ provjeriti da izraz rekonstruira cjelobrojne početne vrijednosti pa zatim pokazati, uvrštavanjem (24) u (15), da rješenje zadovoljava početnu rekurzivnu relaciju s cjelobrojnim koeficijentima. To jamči da cjelobrojne početne vrijednosti uzastopno generiraju cjelobrojne vrijednosti kasnijih članova niza. Čitav postupak provjere rješenja u osnovi je ekvivalentan matematičkoj indukciji.

Želimo li doista dobiti osjećaj za to na koji se način iracionalnost korijenskih članova $\sqrt{\eta}$ gubi u konačnome rješenju, samo trebamo raspisati potencijske članove prema binomnom teoremu

$$p_k = \frac{1}{2^{k+1}\sqrt{\eta}} \left[\left(n_+ + \sqrt{\eta}\right) \sum_{m=0}^{k} \binom{k}{m} \sqrt{\eta}^m n_-^{k-m} - \left(n_+ - \sqrt{\eta}\right) \sum_{m=0}^{k} \binom{k}{m} (-1)^m \sqrt{\eta}^m n_-^{k-m} \right]. \quad (25)$$

Sada sjedinjujemo sume množene s n_+ i one množene s $\sqrt{\eta}$

$$p_k = \frac{1}{2^{k+1}\sqrt{\eta}} \left[n_+ \sum_{m=0}^{k} \binom{k}{m} \sqrt{\eta}^m n_-^{k-m} [1-(-1)^m] + \sqrt{\eta} \sum_{m=0}^{k} \binom{k}{m} \sqrt{\eta}^m n_-^{k-m} [1+(-1)^m] \right]. \quad (26)$$

Zbog člana $1 - (-1)^m$ u prvoj sumi ostaju samo članovi s neparnim m, dok u drugoj sumi zbog $1 + (-1)^m$ ostaju samo članovi s parnim m. Stoga ćemo u prvom slučaju neparne indekse reparametrizirati kao $m = 2\ell + 1$, a u drugom slučaju parne indekse kao $m = 2\ell$. Uz pažljivo određivanje gornjih granica sumacije po novouvedenome indeksu ℓ, korištenjem *pod* funkcije $\lfloor \cdot \rfloor$ koja vraća najveći cijeli broj ne veći od argumenta pišemo

$$p_k = \frac{1}{2^{k+1}\sqrt{\eta}} \left[2n_+ \sum_{\ell=0}^{\lfloor (k-1)/2 \rfloor} \binom{k}{2\ell+1} \sqrt{\eta}^{2\ell+1} n_-^{k-(2\ell+1)} + 2\sqrt{\eta} \sum_{\ell=0}^{\lfloor k/2 \rfloor} \binom{k}{2\ell} \sqrt{\eta}^{2\ell} n_-^{k-2\ell} \right]. \quad (27)$$

Konačno, završnim manipulacijama svih korijenskih članova dolazimo do

$$p_k = \frac{1}{2^k} \left[n_+ \sum_{\ell=0}^{\lfloor (k-1)/2 \rfloor} \binom{k}{2\ell+1} \eta^\ell n_-^{k-2\ell-1} + \sum_{\ell=0}^{\lfloor k/2 \rfloor} \binom{k}{2\ell} \eta^\ell n_-^{k-2\ell} \right]. \quad (28)$$

Vidimo da su nestali svi korijeni, tj. ostaju samo cjelobrojne potencije od η. To je način na koji nestaje prividna iracionalnost iz (24).

Opće rješenje za abecedu od dva znaka ($n = 2$) jest trivijalno jer se tada sve dozvoljene riječi (bilo koje duljine k) smiju sastojati samo od istih znakova (npr. AAA ili BBB za $k = 3$), s obzirom na to da prva pojava jedinog dostupnog različitog znaka narušava uvjet problema. Stoga za $n = 2$ i svaki $k \geq 1$ od preostaje jednostavno rješenje

$$p_k^{(n=2)} = 2. \tag{29}$$

Prema tome, abeceda od tri znaka ($n = 3$) predstavlja minimalni netrivijalni slučaj, u kojem se rješenje našeg problema svodi na

$$p_k^{(n=3)} = \frac{(1+\sqrt{2})^{k+1} + (1-\sqrt{2})^{k+1}}{2^k}. \tag{30}$$

Počevši s p_1, navodimo prvih nekoliko vrijednosti predviđenih ovim izrazom: 3, 7, 17, 41, 99, ...U svrhu provjere ispravnosti rješenja izravnim prebrojavanjem, tablica 1 navodi sve riječi koje za $n = 3$ te $k = 1, 2, 3$ zadovoljavaju uvjet zadatka te one koje su tim uvjetom izbačene. Ukupan broj *svih* riječi duljine k koje možemo sastaviti abecedom od n znakova je, naravno, n^k jer na svako od k mjesta možemo postaviti bilo koji od n dostupnih znakova.

Zadatak 2.1. *U programskom jeziku po vlastitom izboru napišite program koji za zadane n i k nalazi sve riječi koje zadovoljavaju uvjet problema, kako biste izravnim prebrojavanjem provjerili ispravnost rješenja* (24) *za veće n i k.*

Tablica 1. Skup svih riječi koje možemo sastaviti abecedom od 3 dostupna znaka (A, B, C), s time da se dva specifična znaka (A i B) ne pojavljuju zajedno. Navedene su i riječi izbačene tim uvjetom. Ukupan broj svih riječi duljine k jednak je 3^k.

k	p_k	**Prihvatljive kombinacije**	**Izbačeno**
1	3	A, B, C	/
2	7	AA, AC, BB, BC, CA, CB, CC	AB, BA
3	17	AAA, AAC, ACA, ACB, ACC, BBB, BBC, BCA, BCB, BCC, CAA, CAC, CBB, CBC, CCA, CCB, CCC	AAB, ABA, ABB, ABC, BAA, BAB, BAC, BBA, CAB, CBA

3 Korak dalje

Zadatak 3.1. *U programskom jeziku po vlastitom izboru napišite računalnu simulaciju koja za ulazne parametre n, k te željeni broj N slučajno generiranih riječi procjenjuje ukupan broj riječi u kojima se dva specifična znaka ne pojavljuju zajedno, tj. simulaciju koja (unutar granica statističke nepouzdanosti) procjenjuje poznato rješenje (24) na temelju omjera povoljnih i svih generiranih riječi.*

Zanima nas: koliko bismo puta trebali generirati slučajne riječi da bi *statistička nepouzdanost*[4] procijenjenog rješenja za broj povoljnih riječi bila manja od neke željene vrijednosti? Na primjer, manja od 0.5 tako da s velikom vjerojatnošću možemo tvrditi da smo traženo rješenje p_k simulacijom točno odredili do na posljednju znamenku.

Krenimo korak po korak. Neka je N broj svih slučajno generiranih riječi duljine k, sastavljenih iz abecede od n znakova (naravno, uniformno generiranih tako da se svaka od n^k mogućih riječi pojavljuje s jednakom vjerojatnošću). Neka smo među njima računalnom provjerom željenog uvjeta (nepojavljivanja dvaju specifičnih znakova zajedno) našli M riječi koje zadovoljavaju uvjet te kao takve predstavljaju povoljne događaje. Pri tome

[4] Ovaj dio teksta pisan je s pretpostavkom da je čitatelj upoznat s osnovnim statističkim pojmovima, prvenstveno s pojmovima očekivane vrijednosti i varijance slučajne varijable [19]. Radi potpunosti ukratko ćemo ćemo definirati te pojmove, i to samo za slučaj *diskretne* varijable, što odgovara prirodi našeg problema. Neka je x diskretna slučajna varijabla, a $\{x_i\}$ neka je skup svih njezinih mogućih vrijednosti (ishoda). Nadalje, neka je (u skladu s uskoro korištenim oznakama iz glavnog teksta) μ_i vjerojatnost pojave i-te vrijednosti x_i. Tada je, uz primjereno normiranje ukupne vjerojatnosti na jedinicu ($\sum_i \mu_i = 1$ gdje suma prebrisuje sve moguće ishode), *očekivana vrijednost* $\langle f(x)\rangle$ bilo koje funkcije $f(x)$ slučajne varijable x definirana kao

$$\langle f(x)\rangle \equiv \sum_i \mu_i f(x_i).$$

Prema tome, očekivana vrijednost same slučajne varijable jednostavno je $\langle x\rangle \equiv \sum_i \mu_i x_i$. *Varijanca* slučajne varijable definira se kao *očekivana vrijednost kvadrata odstupanja* slučajne varijable od njezine očekivane vrijednosti

$$\mathrm{Var}(x) \equiv \langle (x - \langle x\rangle)^2\rangle = \sum_i \mu_i (x_i - \langle x\rangle)^2.$$

Preko pojma varijance posredno se definira i *statistička nepouzdanost* slučajne varijable kao *korijen varijance*. U pojednostavnjenoj kasnijoj oznaci iz glavnog dijela teksta: $\sigma \equiv \sqrt{\mathrm{Var}(x)}$. Također uvodimo i pojam *statističkog procjenitelja* $\hat{f}$ funkcije f slučajne varijable x. Statistički procjenitelj $\hat{f}$ funkcija je skupa $\{x_i\}$ slučajnih ishoda kojom se procjenjuje neko svojstvo statističke raspodjele slučajne varijable x; svojstvo određeno upravo funkcijom f. Posebnu klasu procjenitelja čine *nepristrani procjenitelji*, definirani zahtjevom da se njihova očekivana vrijednost podudara s očekivanom vrijednošću procjenjivane funkcije

$$\langle \hat{f}(\{x_i\})\rangle = \langle f(x)\rangle,$$

tj. upravo s ispravnom vrijednošću traženog statističkog svojstva raspodjele.

svakoj generiranoj riječi pridružujemo varijablu x_i kojom ćemo pratiti uspješnost ishoda: $x_i = 0$ ako je i-ta generirana riječ nepovoljna, a $x_i = 1$ ako je povoljna. Budući da nam je već poznato egzaktno rješenje za ukupan broj p_k povoljnih riječi, unaprijed znamo da je vjerojatnost μ_k generiranja povoljnih riječi jednaka $\mu_k = p_k/n^k$. Međutim, najbolje što možemo napraviti simulacijom jest *procijeniti* tu vjerojatnost omjerom povoljnih i svih mogućih ishoda

$$\hat{\mu}_k = \frac{M}{N} = \frac{1}{N}\sum_{i=1}^{N} x_i. \tag{31}$$

Ovdje je $\hat{\mu}_k$ nepristrani procjenitelj tražene vjerojatnosti μ_k, u smislu da je njegova očekivana vrijednost – u oznaci $\langle\cdot\rangle$ za statističko očekivanje – jednaka točnoj vrijednosti: $\langle\hat{\mu}_k\rangle = \mu_k$. Najbolji procjenitelj $\hat{p}_k$ ukupnog broja povoljnih riječi izravno je određen procijenjenim udjelom tih riječi među svima mogućima

$$\hat{p}_k = \hat{\mu}_k n^k, \tag{32}$$

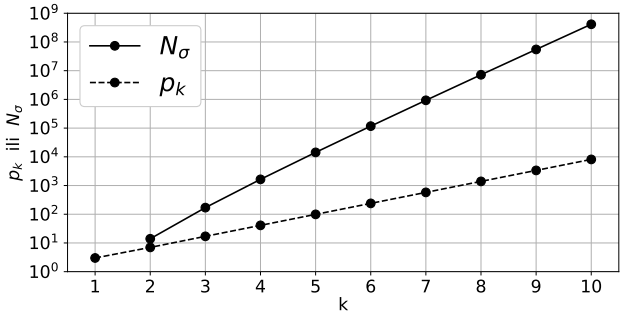
i to upravo zato jer je njegova očekivana vrijednost jednaka točnome rješenju problema: $\langle\hat{p}_k\rangle = p_k$. Naravno, ovakva metoda procjene postaje korisna onda kad je problem toliko složen da nam nije unaprijed dostupno točno rješenje p_k.

Svaki rezultat dobiven računalnim simulacijama, na temelju slučajno generiranih ishoda, podložan je statističkim nepouzdanostima. Upravo radi procjene tih nepouzdanosti bilo je u (31) bitno prepoznati omjer M/N kao sumu pojedinih ishoda x_i jer njihovo statističko ponašanje izravno određuje sva statistička svojstva konačnoga rezultata. Za mjeru statističke nepouzdanosti tipično se uzima korijen *varijance* statističkoga uzorka (u našem slučaju skupa ishoda x_i). Ako nam je unaprijed poznato statističko ponašanje tih ishoda – prvenstveno statistički očekivana varijanca *svakog pojedinog ishoda* $\mathrm{Var}(x)$ – tada za varijancu $\mathrm{Var}(\hat{\mu}_k)$ *srednje vrijednosti* iz (31) vrijedi: $\mathrm{Var}(\hat{\mu}_k) = \mathrm{Var}(x)/N$. A varijanca $\mathrm{Var}(x)$ nam jest poznata! Kako ishodi x_i predstavljaju diskretne događaje koji mogu poprimiti vrijednosti 0 ili 1, njihovo ponašanje opisano je Bernoullijevom raspodjelom. Varijanca bilo kojeg od dvaju Bernoullijevih ishoda jednaka je $\mathrm{Var}(x) = \mu_k(1-\mu_k)$, pri čemu je μ_k vjerojatnost jednoga od njih (pojave povoljne riječi: $x_i = 1$), a $1-\mu_k$ vjerojatnost drugoga ($x_i = 0$). Iz ranije tvrdnje slijedi

$$\mathrm{Var}(\hat{\mu}_k) = \mu_k(1-\mu_k)/N, \tag{33}$$

što je *očekivana* varijanca procjenitelja vjerojatnosti $\hat{\mu}_k$. Za nepouzdanost procjenitelja ukupnog broja povoljnih riječi iz (32), u oznaci σ, prema pravilima za varijancu vrijedi

$$\sigma^2 = \mathrm{Var}(\hat{p}_k) = n^{2k}\mathrm{Var}(\hat{\mu}_k) = n^{2k}\frac{\mu_k(1-\mu_k)}{N}. \tag{34}$$



Slika 1. Broj povoljnih riječi p_k iz (30) za abecedu od tri znaka ($n = 3$), zajedno s potrebnim brojem generiranih riječi N_σ iz (35) za $\sigma = 1$.

Znajući unaprijed točnu vrijednost μ_k, predvidjeli smo očekivano ponašanje nepouzdanosti procijenjenog rješenja $\hat{p}_k$. Bitan dio tog ponašanja jest ovisnost $\sigma \propto 1/\sqrt{N}$ o ukupnome broju slučajno generiranih riječi. Završnom inverzijom prethodnog izraza konačno nalazimo koliko bismo riječi trebali generirati da bi očekivana nepouzdanost procjenitelja $\hat{p}_k$ bila jednaka željenoj vrijednosti σ

$$N_\sigma = n^{2k} \frac{\mu_k(1-\mu_k)}{\sigma^2} = \frac{p_k(n^k - p_k)}{\sigma^2}. \tag{35}$$

U situaciji kad nam točna vrijednost p_k nije unaprijed poznata – upravo slučaj kad simulacije postaju korisne – u izrazu (35) koristili bismo vrijednost samog procjenitelja[5] $\hat{p}_k$. Sa svakom novom generiranom riječi ovako procijenjena vrijednost za N_σ postaje sve pouzdanija.

[5]Formalno govoreći, u *procjenitelju* $\widehat{\mathrm{Var}}(\hat{\mu}_k)$ varijance srednje vrijednosti $\hat{\mu}_k$ – koji bismo računali na temelju samog procjenitelja $\hat{\mu}_k$ umjesto unaprijed poznate točne vrijednosti μ_k – trebali bismo koristiti dijeljenje faktorom $N-1$ umjesto N (vidi [19]) jer je očekivana vrijednost upravo takvog procjenitelja jednaka očekivanoj varijanci iz (33), u smislu: $\langle \widehat{\mathrm{Var}}(\hat{\mu}_k) \rangle = \mathrm{Var}(\hat{\mu}_k)$, to jest: $\langle \hat{\mu}_k(1-\hat{\mu}_k)/(N-1) \rangle = \mu_k(1-\mu_k)/N$. Ova statistička činjenica poznata je kao Besselova korekcija, a svojstvo da je očekivana vrijednost procjenitelja upravo jednaka točnoj vrijednosti procjenjivane veličine zove se *nepristranost procjenitelja*. Prema tome, formalno ispravan oblik nepristranog procjenitelja varijance (tj. kvadrata nepouzdanosti) srednje vrijednosti iz (31) jest

$$\hat{\sigma}_\mu^2 = \widehat{\mathrm{Var}}(\hat{\mu}_k) = \frac{\hat{\mu}_k(1-\hat{\mu}_k)}{N-1} = \frac{M(N-M)}{N^2(N-1)}.$$

Tipičan način zapisa statističkog rezultata zajedno s njegovom statističkom nepouzdanošću jest: $\hat{\mu}_k \pm \hat{\sigma}_\mu$. Procjenitelj nepouzdanosti procjenitelja $\hat{p}_k$ iz (32) tada je jednostavno $\hat{\sigma}_p = n^k \hat{\sigma}_\mu$ te bismo taj rezultat zapisali kao: $\hat{p}_k \pm \hat{\sigma}_p$. Izravna posljedica ovog tehničkog detalja je sljedeća: korištenjem procjenitelja $\hat{p}_k$ za procjenu N_σ iz (35), formalno ispravan procjenitelj poprima oblik: $\hat{N}_\sigma = [\hat{p}_k(n^k - \hat{p}_k)/\sigma^2] + 1$. No tipične vrijednosti N_σ toliko su velike da je doprinos dodatne jedinice sasvim zanemariv, a na grešku procjenitelja $\hat{N}_\sigma$ (s obzirom na „točnu" vrijednost N_σ) više utječe nepouzdanost samog procjenitelja $\hat{p}_k$.

Za $n = 3$ slika 1 prikazuje broj p_k povoljnih riječi iz (30) te broj N_σ potrebnih slučajno generiranih riječi za $\sigma = 1$. Primijetimo da za riječ od jednog znaka ($k = 1$) izraz (35) predviđa $N_\sigma = 0$, tj. ne daje koristan rezultat za potrebe procjene ukupnog broja povoljnih riječi p_1. To je zato jer je $p_1 = n$, tj. svaka od n mogućih riječi od jednoga znaka je prema uvjetu problema povoljna. Naime, izraz za N_σ izgradili smo na temelju nepouzdanosti *omjera* $\hat{\mu}_k$ iz (31). Kako je za $k = 1$ sa svakom generiranom riječi procijenjeni omjer odmah točan ($\hat{\mu}_k = 1$) i ni u najmanjoj mjeri ne odstupa od te vrijednosti, njegova nepouzdanost sve vrijeme je $\sigma = 0$ i ne evoluira s povećanjem broja generiranih riječi. Stoga nepouzdanost omjera više nije koristan kriterij za procjenu *ukupnog* broja povoljnih riječi p_k. U tom slučaju morali bismo reformulirati pitanje na način: koliki je potreban broj generiranih riječi da bismo sa željenom *vjerojatnošću* (umjesto nepouzdanosti) generirali sve povoljne riječi? No to je problem za neki drugi put.

Literatura

[1] L. E. Sigler, *Fibonacci's Liber Abaci: A Translation Into Modern English of Leonardo Pisano's Book of Calculation*, Springer, New York, 2002.

[2] P. ingh, *The So-called Fibonacci Numbers in Ancient and Medieval India*, Historia Mathematica, **12** (1985), 229–244. [DOI:10.1016/0315-0860(85)90021-7]

[3] R. Simson, *An Explication of an Obscure Passage in Albert Girard's Commentary upon Simon Stevin's Works* (*Vide Les Oeuvres Mathem. de Simon Stevin, a Leyde, 1634, p. 169, 170*), Philosophical Transactions of the Royal Society of London, **48** (1753), 368–377. [DOI:10.1098/rstl.1753.0056]

[4] A. de Moivre, *De Fractionibus Algebraicis Radicalitate Immunibus ad Fractiones Simpliciores Reducendis, Deque Summandis Terminis Quarumdam Serierum Aequali Intervallo a Se Distantibus. Auctore Abrahamo de Moivre, S. R. Socio*, Philosophical Transactions, **32** (1722), 162–178. [DOI:10.1098/rstl.1722.0029]

[5] D. Bernoulli, Commentarii Academiae scientiarum imperialis Petropolitanae, **3** (1728), 85–100.

[6] L. Euler, *Observationes analyticae*, Novi commentarii ascaemiae scientiarum imperialis Petropolotanae, **11** (1765), 124–143.

[7] J. P. Binet, *Mémoire sur l'intégration des équations linéaires aux différences finies, d'un ordre quelconque, à coefficients variables*, Comptes Rendus hebdomadaires des séances de l'Académie des Sciences (Paris), **17** (1843), 559–567.

[8] A. de Moivre, *Miscellanea analytica de seriebus et quadraturis*, J. Tonson & J. Watts, London, 1730.

[9] M. Segre, *Peano's axioms in their historical context*, Archive for History of Exact Sciences, **48** (1994) 201–342. [DOI:10.1007/BF00375085]

[10] R. Dedekind, *Was sind und was sollen die Zahlen?*, Vieweg, Braunschweig, 1888.

[11] G. Peano, *Arithmetices Principia, Nova Methodo Exposita*, Fratres Bocca, Turin, 1889.

[12] K. Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*, Monatshefte für Mathematik und Physik **38** (1931), 173–198. [DOI:10.1007/BF01700692]

[13] R. Adams, *An Early History of Recursive Functions and Computability from Gödel to Turing*, Docent Press, Boston, 2011.

[14] E. Morris. L. Harkleroad, *Rózsa Péter: recursive function theory's founding mother*, The Mathematical Intelligencer, **12** (1990), 59–64. [DOI:10.1007/BF03023988]

[15] D. Veljan, *Kombinatorna i diskretna matematika*, Algoritam, Zagreb 2001.

[16] D. Jankov Maširević, J. Jankov, *Zanimljive rekurzije*, Matematičko fizički list, **65**(259) (2015), 147–155. [https://hrcak.srce.hr/242520]

[17] P. Žugec, *Izabrani problemi iz Opće fizike – Zbirka 3^3 riješenih zadataka*, Školska knjiga, Zagreb, 2017.

[18] L. E. Dickson, *History of the Theory of Numbers, Vol. 1: Divisibility and Primality*, Dover, New York, 2005.

[19] S. Pfaff, *Osnove statistike*, Element, Zagreb, 2012.