UNIVERSITATEA BUCUREŞTI
FACULTATEA DE MATEMATICĂ

CEZAR CÂMPEANU

Metode Topologice în Complexitatea Calculului

TEZĂ DE DOCTORAT

CONDUCĂTOR ŞTIINŢIFIC
PROFESOR CRISTIAN CALUDE

BUCUREŞTI, 1995

Cuprins

Introducere

Este posibil să comprimăm o informaţie — dată sub forma unui text — astfel încât ea să ocupe cât mai puţin spaţiu? Una din metode este aceea de a observa regularităţi sau secvenţe care se repetă, înlocuind scrierea acestora cu o referinţă. Folosind instrumente din statistică putem găsi eventual un algoritm care să reproducă informaţia iniţială din texte de lungime mai mică. Altă metodă este aceea de a reţine doar partea cea mai semnificativă a informaţiei (o parte, mai puţin semnificativă, pierzîndu-se). În practică, aceste idei sunt valorificate prin construirea programelor de codificare, comprimare şi arhivare. O întrebare naturală pe care ne-o putem pune este aceea dacă putem să comprimăm orice informaţie. În practică, se ştie că un text “comprimat” printr-un anumit program nu mai poate fi micşorat printr-o nouă “comprimare”; mai mult, există texte care prin acest tip de operaţie, ocupă mai mult spaţiu după “comprimare”. Acest fapt ne duce la ideea că nu orice informaţie poate fi algoritmic comprimată. Lucrarea de faţă îşi propune să studieze, din punct de vedere teoretic, acest fenomen. Instrumentele principale de studiu vor fi cele de topologie; vom compara din punctul de vedere al mărimii topologice diferite mulţimi de numere şi cuvinte aleatoare; de asemenea, vom studia “mărimea” unor mulţimi în raport cu diverse topologii.

În primul capitol vom prezenta notaţiile folosite în lucrare, vom introduce noţiunile de complexitate Chaitin şi Chaitin-Kolmogorov, calculator şi calculator universal (Chaitin şi Kolmogorov), Definiţiile 1.1, 1.4 şi 1.9. Se introduce de asemenea pentru numere naturale reprezentate într-o anumită bază, noţiunea de complexitate Kolmogorov, Definiţia 1.12 şi pentru aceasta se demonstrează existenţa algoritmilor universali, Teorema 1.13; se studiază, de asemenea, relevanţa alfabetului subiacent pentru algoritmii universali Lemele 1.14 şi 1.16, precum şi Observaţiile 1.15 şi 1.17.

În Capitolul doi introducem noţiunile de cuvânt aleator Chaitin-Kolmogorov şi aleator Chaitin. Un cuvânt este aleator dacă nu poate fi algoritmic comprimat. Începem prin a introduce câteva definiţii indispensabile studiului fenomenului de hazard. Un cuvânt este ε-limiting dacă toate literele apar în cuvântul respectiv de aproape acelaşi număr de ori. Se introduce noţiunea de cuvânt Borel normal. Un cuvânt se numeşte Borel normal dacă toate grupurile de cifre, de lungime suficient de mică faţă de lungimea cuvântului, apar în cuvântul dat, de aproape acelaşi număr de ori. Cuvintele aleatoare (Chaitin şi Chaitin-Kolmogorov) suficient de mari (în sensul ordinei cvasi-lexicografice) sunt Borel normale. Să mai notăm că cele două mulţimi de cuvinte aleatoare (Chaitin şi Chaitin-Kolmogorov) sunt imune (Teorema 2.7). Amintim că o mulţime este imună, dacă nici o parte infinită a sa nu poate fi enumerată printr-un algoritm. Se dă o condiţie necesară şi suficientă pentru reprezentabilitatea testelor Martin-Löf prin calculatoare Chaitin (Teorema 2.15). În secţiunea a doua se introduc noţiunile de hazard algoritmic pentru numerele naturale în reprezentare poziţională. Astfel, definim noţiunea de număr aleator într-o anumită bază şi număr p-normal. La fel ca pentru cuvinte, un număr natural este aleator într-o anumită bază dacă nu poate fi obţinut algoritmic dintr-un număr de lungime (în aceeaşi bază) mai mică. Un număr natural este p-normal dacă pentru orice bază mai mică sau egală cu p, în reprezentarea poziţională, toate cifrele bazei apar de aproape acelaşi număr de ori.

Demonstrăm că mulţimea numerelor aleatoare într-o bază oarecare este o mulţime imună (Teorema 2.25). Aceste rezultate justifică Definiţia 2.21, prin care se introduce noţiunea de număr natural aleator.

Sunt două categorii de numere naturale aleatoare: una definită cu ajutorul complexităţii uniforme, cealaltă cu ajutorul complexităţii condiţionate.

În lucrare vom studia ambele mulţimi de numere naturale aleatoare, ele avînd proprietăţi asemănătoare.

În secţiunea a treia, arătăm că orice număr aleator în baza p este p-normal (Corolarul 2.34 şi Corolarul 2.35); acest rezultat reprezintă încă un argument pentru Definiţia 2.21.

În Capitolul trei, vom prezenta unele topologii induse de relaţii recursive de ordine parţială. Pentru prima oară aceste noţiuni au fost introduse şi studiate în 1986 de Zimand în [38], unde a fost definită mulţimea *recursiv rară* pentru cazul binar şi ordinea prefix. Definiţia mulţimii recursiv rare apărea restrictiv, condiţia 2) din Definiţia 1 [38] fiind îndeplinită aproape peste tot. Pentru relaţii de ordine nemărginite, definiţia lui Zimand este echivalentă cu definiţia naturală dată în Capitolul 3, unde am cerut ca 2) să fie îndeplinită peste tot (Definiţia 3.6). Acest rezultat este evidenţiat prin Propoziţia 3.7. Vechea definiţie a devenit bază pentru definiţia mulţimii aproape recursiv rare. Cele două definiţii sunt total diferite în cazul relaţiilor de ordine mărginite.

O relaţie de ordine este nemărginită dacă pentru orice cuvînt putem găsi un altul mai mare, (în raport cu relaţia de ordine considerată,) de lungime oricât de mare. Teorema 3.8 este o generalizare a Propoziţiei 3 din Zimand [38] ce dă o condiţie suficientă ca să existe mulţimi rare care nu sunt recursiv rare; ordinile prefix şi sufix satisfac această condiţie. De asemenea, în Propoziţia 3.11, studiem o condiţie suficientă pentru ca o mulţime rară să fie recursiv rară şi orice mulţime care nu este rară să fie densă; ordinile infix, hipercod, masking şi prefix-masking satisfac această din urmă condiţie (v Exemplul 3.1, pentru definiţiile acestor relaţii de ordine). Sunt introduse noţiuni noi, ca mulţime *aproape rară, aproape recursiv rară, şi aproape densă* (Definiţia 3.13). Acestea sunt utile în special în studiul relaţiilor de ordine mărginite (v. Capitolul 3 şi Exemplul 3.3). Mulţimile aproape (recursiv) rare (dense) sunt diferite de mulţimile (recursiv) rare (dense) dacă relaţia de ordine considerată este mărginită, Teorema 3.17 şi Teorema 3.16.

În secţiunea a doua a Capitolui 3, sunt date definiţiile mulţimilor (aproape) rare, dense, recursiv rare, dar de această dată pentru topologii induse de relaţii de ordine pe mulţimea numerelor naturale (Definiţiile 3.25 şi 3.31). Ca şi în cazul cuvintelor, mulţimile aproape (recursiv) rare (dense) coincid cu cele (recursiv) rare (dense), dacă topologiile considerate sunt generate de o relaţie de ordine nemărginită, teoremele 3.33 şi 3.34. Existenţa mulţimilor rare care nu sunt recursiv rare este asigurată de Teorema 3.27.

În Capitolul 4 vom obţine principalele rezultate de natură topologică privind cuvintele şi numerele naturale aleatoare. Studiind fenomenul de hazard din punctul de vedere al complexităţilor descriptive Chaitin-Kolmogorov şi Chaitin, am obţinut o caracterizare topologică a mulţimilor RAND şi non-RAND. Rezultatele au fost obţinute atât pentru cuvinte peste un alfabet finit, cât şi pentru numere naturale în reprezentare poziţională. Ele extind rezultatele lui Zimand în [38] care demonstra pentru cazul binar că mulţimea cuvintelor aleatoare Chaitin-Kolmogorov este recursiv rară în raport cu topologia generată de relaţia de ordine prefix pe cuvinte.

Arătăm că mulţimile de cuvinte şi numere ne-aleatoare sunt dense în raport cu relaţiile de ordine nemărginite (Corolarul 4.2, Corolarul 4.18, Corolarul 4.22). Studiem mărimea topologică a mulţimii cuvintelor aleatoare Chaitin-Kolmogorov şi a numerelor aleatoare în raport cu diverse relaţii de ordine (mărginite şi nemărginite) (Corolarul 4.5, Propoziţia 4.6, Propoziţia 4.7, Teorema 4.12). Aceste rezultate arată că dacă avem un cuvânt şi îl prelungim doar într-o singură parte (la stânga sau la dreapta), găsim un cuvânt pentru care nici o altă prelungire în acelaşi sens nu este cuvânt aleator, dar dacă prelungim cuvântul în ambele direcţii, în mod sigur vom obţine un cuvânt aleator (Teorema 4.12). Această problemă, pentru numere naturale, nu este rezolvată decât în sensul următor : orice număr natural poate fi prelungit cu alt număr natural, astfel încât nici o prelungire în aceeaşi direcţie nu este un număr aleator (Teorema 4.25). În final vom arăta că în raport cu anumite relaţii de ordine, complexităţile Chaitin şi Chaitin-Kolmogorov se comportă identic (Teorema 4.19 şi Teorema 4.20).

În Capitolul 5 arătăm că nu există calculatoare Chaitin şi Chaitin - Kolmogorov, care să fie universale pentru calculatoarele definite pe un alfabet cu mai multe elemente decât alfabetul peste care este considerat domeniul lor de definiţie. (Teorema 5.1 şi Teorema 5.2). În secţiunea a doua, studiem comportarea mulţimii cuvintelor aleatoare la modificarea complexităţii descriptive, prin înmulţirea sa cu o constantă egală cu logaritmul în baza doi a numărului de litere al alfabetului (Corolarul 5.5, Corolarul 5.6 şi Corolarul 5.10). Secţiunea a treia intitulată "Sunt codificările binare universale?", este o concluzie a ultimului capitol. Această întrebare a fost formulată de C. Rackhoff [33] şi are un răspuns negativ. Aparent,impresia generală este că este suficient să considerăm că întreaga arie de generalitate a codificării, cel puţin din punctul de vedere algoritmic este acoperită de cazul binar. Această idee apare în cea mai puternică formă în Li şi Vitányi [30].

Noi credem că, dimpotrivă, *există diferenţe esenţiale pentru complexitatea descriptivă în cazul binar şi cel ne-binar;* unele dintre acestea au fost studiate în Calude [2], Calude şi Chiţescu [7], şi în special, Calude, Jürgensen şi Salomaa [11] (v. de asemenea [3]). Aceste rezultate sunt compatibile cu fapte din teoria clasică a informaţiei; vezi, spre exemplu, Rissanen ([34], p 27) sau analiza din Fenwick [17].

Aceste rezultate întăresc argumentele ce arată că există diferenţe esenţiale între complexităţile descriptive în cazul binar şi cazul nebinar.

* *

În încheiere aduc

- Mulţumiri speciale
  - Dr. Marius Zimand, pentru problemele studiate în [38], ce au constituit o bază de pornire pentru o mare parte din rezultate.
  - Colegilor din cadrul seminarului ştiinţific condus de Profesorul Cristian Calude, în special, pentru comentariile şi discuţiile interesante, purtate pe teme de topologie constructivă.
  - Profesorilor Cristian Calude şi Ion Chiţescu, pentru lucrările interesante privind cuvintele şi şirurile aleatoare, ce mi-au trezit interesul pentru acest domeniu, încă din anii studenţiei.
- Mulţumiri membrilor comisiei de doctorat, Profesorilor Monica Dumitrescu, Ioan Tomescu, Doru Ştefňescu, pentru discuţiile critice purtate pe baza tezei; ele vor ameliora unele lucrări aflate în curs de publicare.
- Mulţumiri
  - Conducerii facultăţii, Catedrelor de informatică şi şefilor acestor catedre, Profesorii Virgil Căzănescu şi Ioan Tomescu, pentru sprijinul acordat.
  - Tuturor celor ce m-au ajutat — într-un fel sau altul — sau nu m-au împiedicat —în nici un fel — la elaborarea şi definitivarea tezei. Tuturor celor care m-au sprijinit moral, pe toată această perioadă.
  - Profesorului Doru Ştefănescu, pentru încurajări şi multiplele consultări privind limbajul LaTeX .
  - Profesorului Cristian Calude; spaţiul este prea mic pentru a enumera totul.

1

Complexităţi descriptive

O metodă de a măsura conţinutul de informaţie a unui text, pentru un calculator dat, este să determinăm necesarul de resurse pentru a obţine textul dat, folosind acel calculator. Încercînd să comprime informaţia, adică să folosească cât mai puţin spaţiu pentru o cantitate de informaţie cât mai mare, au fost descoperite mai multe modalităţi; o metoda importantă este aceea de a detecta şabloane cu ajutorul cărora putem reface informaţia. Încercînd această modalitate la o tabelă de calcul, spre exemplu pentru calculul logaritmilor, constatăm că o metodă mult mai avantajoasă de a pune informaţia într-o astfel de tabelă este de a scrie instrucţiuni de calcul a tabelei (de exemplu folosind formula lui Moivre). Această metodă nu numai că este mai compactă, dar permite să calculăm tabele oricât de mari dorim. Metoda de mai sus nu mai este performantă pentru date empirice (rezultatele la olimpiade v. Rozenberg şi Salomaa [35]). În acest caz gradul de compresie este practic nul; mai mult, deoarece tendinţa este aceea de a îmbunătăţi, cele mai semnificative cifre au regularităţi care fac posibilă chiar predicţia. Datele empirice produc şiruri care trebuie explicate şi altele noi produse. Aceasta idee a fost formalizată în mod independent în diferite moduri de Solomonoff, Kolmogorov şi Chaitin.

În acest capitol vom prezenta notaţiile folosite în lucrare, vom introduce noţiunile de complexitate Chaitin şi Chaitin-Kolmogorov, calculator şi calculator universal (Chaitin şi Kolmogorov), Definiţiile 1.1, 1.4 şi 1.9. Se introduce de asemenea pentru numere naturale reprezentate într-o anumită bază, noţiunea de complexitate Kolmogorov, Definiţia 1.12, şi pentru aceasta se demonstrează existenţa algoritmilor universali, Teorema 1.13, şi cum depind aceştia de alfabetul pe care lucrăm, Lemele 1.14 şi 1.16, precum şi Observaţiile 1.15 şi 1.17.

1.1 Complexităţi pe cuvinte

Lucrăm cu un alfabet finit $X = \{a_1, a_2, \cdots, a_p\}$, $p \geq 2$. Monoidul liber generat de X este X^*. Funcţia care enumeră acest monoid în ordine cvasi-lexicografică este *string* : $\mathbf{N} \longrightarrow X^*$, definită prin relaţiile:

$$string(0) = \lambda \text{ (cuvântul vid)}, string(1) = a_1, \ldots, string(p) = a_p,$$

$$string(p+1) = a_1a_1,\ string(p+2) = a_1a_2, \ldots$$

În cazul în care vrem să punem în evidenţă numărul de elemente din X, utilizăm funcţia *string* cu două argumente, *string* : $\mathbf{N} \times \mathbf{N} \longrightarrow X^*$,

$$string(p, 0) = \lambda,\ string(p, 1) = a_1, \ldots, string(p, p) = a_p,$$

$$string(p, p+1) = a_1a_1,\ string(p, p+2) = a_1a_2, \ldots$$

O relaţie de ordine pe X^* se va nota cu $\preceq$, urmată, eventual, de indici; de exemplu, în cazul ordinei prefix folosim notaţia $\preceq_p$ (pentru $x, y \in X^*$, $x \preceq_p y$ dacă există $z \in X^*$ astfel încât $y = xz$; pentru detalii v. cap 3 (Topologii constructive)). Spunem că un cuvânt w este prefixul cuvântului v dacă $w \preceq_p v$. O mulţime A se numeşte *liberă de prefixe* dacă pentru orice două cuvinte v şi w din A niciunul nu este prefixul celuilat ($w \not\preceq_p v$ şi $v \not\preceq_p w$). Utilizăm convenţia că minimul mulţimii vide este infinit. Prin calculator vom înţelege o funcţie parţial recursivă ce are ca intrare cuvinte peste monoidul liber X^* şi produce elemente din X^*. Dacă gândim calculatorul ca fiind un "program +date", atunci el va fi o funcţie unară; altfel, el este o funcţie de două argumente. Complexitatea unui cuvânt peste un alfabet în raport cu un calculator este lungimea celui mai mic cuvânt, care, folosit ca intrare pentru acel calculator, produce la ieşire cuvântul cerut. La început, Kolmogorov şi Chaitin nu au impus restricţii privind calculatoarele, prin calculator înţelegîndu-se orice funcţie parţial recursivă. În Chaitin [18] sunt considerate calculatoare, cele avînd domeniul de definiţie liber de prefixe . O motivaţie a acestui fapt este dată de Chaitin în [21]:

"Un lucru esenţial care trebuie cerut.. este ca programul primit la intrare să fie auto-limitat: lungimea sa totală (în biţi) trebuie să fie dată înăuntrul programului însuşi. (Aceasta pare să fie un lucru minor, care a oprit progresul în acest domeniu, deoarece implica redefinirea hazardului algoritmic.) Limbajele de programare reale sunt auto-limitate, deoarece ele necesită construcţii de început şi sfârşit de program. Asemenea construcţii permit programului să conţină subprograme bine definite conţinute în el. Deoarece un program auto-limitat este construit prin concatenări şi înglobări de subprograme auto-limitate, un program este sintactic complet numai când ultimul subprogram început este terminat. În esenţă, construcţiile de început şi sfârşit pentru programe şi subprograme funcţionează ca parantezele stângi şi drepte dintr-o expresie matematică.”

Definiţie 1.1 *Un calculator este o funcţie parţial recursivă* $\phi : X^* \times X^* \stackrel{\circ}{\longrightarrow} X^*$*. Un calculator Chaitin este un calculator* C *astfel încât pentru orice* $v \in X^*$*, domeniul lui* C_v *este liber de prefixe, unde* $C_v : X^* \stackrel{\circ}{\longrightarrow} X^*$*,* $C_v(x) = C(x, v)$*, pentru orice* $x \in X^*$*.*

Comentariu 1.2 *Pentru un calculator Chaitin, dacă* $C(x, v) \neq \infty$ *şi* $y \preceq_p x$*, atunci* $C(y, v) \neq \infty$ *implică* $y = x$*; cu alte cuvinte, programele trebuie să fie auto-limitate.*

Definiţie 1.3 *Un calculator (Chaitin)* ψ *este universal dacă pentru orice alt calculator (Chaitin)* ϕ *există o constantă naturală* c *(care depinde doar de* ϕ *şi* ψ*) cu următoarea proprietate: dacă* $\phi(x) \neq \infty$*, atunci există* x' *astfel încât*

$$\psi(x') = \phi(x) \text{ şi } l(x') \leq l(x) + c.$$

Dacă ϕ *este un calculator cu două argumente, atunci pentru* $\phi(x, y) \neq \infty$ *există* x' *astfel încât*

$$\psi(x', y) = \phi(x, y) \text{ şi } l(x') \leq l(x) + c.$$

Definiţie 1.4 *a) Complexitatea absolută Kolmogorov-Chaitin (pe scurt complexitatea absolută) asociată calculatorului* ϕ *este funcţia parţială* $K_\phi : X^* \stackrel{\circ}{\to} \mathbf{N}$*,*

$$K_\phi(x) = min\{l(u) |\, u \in X^*,\ \phi(u, \lambda) = x\}.$$

În cazul în care $\phi = \psi$*, notăm* $K(x) = K_\psi(x)$*.*

b) Complexitatea absolută auto-limitată Chaitin (pe scurt complexitatea absolută Chaitin) asociată calculatorului Chaitin C este funcţia parţială $H_C : X^* \overset{\circ}{\to} \mathbf{N}$,

$$H_C(x) = min\{l(u) |\, u \in X^*,\, C(u, \lambda) = x\}.$$

În cazul în care $C = U$, notăm $H(x) = H_U(x)$.

c) Programul canonic definit în raport cu un calculator universal Chaitin C este:

$$x^* = min\{u \in X^* | U(u, \lambda) = x\},$$

unde minimul este dat de ordinea cvasi-lexicografică pe X^* indusă de $a_1 < a_2 < \cdots < a_p$.

Teorema 1.5 *(Calude [3]) Se pot construi efectiv calculatoare universale (Chaitin).*

Consecinţe imediate ale acestor definiţii sunt:

Corolar 1.6 *Pentru orice calculator ϕ şi orice calculator Chaitin C avem:*

$$K(x) \leq K_\phi(x) + O(1), H(x) \leq H_C(x) + O(1). \tag{1.1}$$

Să fixăm un calculator universal ψ şi un calculator universal Chaitin U.

Corolar 1.7 *Orice secţiune ψ_y, U_y este surjectivă.*

Lema 1.8 *Pentru orice $x \in X^*$:*

$$x^* \text{ există, } x^* \neq \lambda \tag{1.2}$$

$$x = U(x^*, \lambda), \tag{1.3}$$

$$H(x) = l(x^*) \tag{1.4}$$

Pentru calculatoarele ce au două argumente (program + date), definiţiile corespunzatoare celor de mai sus devin:

Definiţie 1.9 *a) Complexitatea condiţionată Kolmogorov-Chaitin (pe scurt complexitatea condiţionată) asociată calculatorului ϕ este funcţia parţială $K_\phi : X^* \times \mathbf{N} \overset{\circ}{\to} \mathbf{N}$,*

$$K_\phi(x|v) = min\{l(y)|\, y \in X^*,\, \phi(y,v) = x\}.$$

Notăm $K(x|v) = K_\psi(x|v)$.

b) Complexitatea condiţionată auto-limitată Chaitin (pe scurt complexitatea condiţionată Chaitin) asociată calculatorului Chaitin C este funcţia parţială $H_C : X^* \times X^* \overset{\circ}{\to} \mathbf{N}$,

$$H_C(x|v) = min\{l(y)|\, y \in X^*,\, C(y,v^*) = x\}.$$

Notăm $H(x|v) = H_U(x|v)$.

Corolar 1.10 *Pentru orice calculator ϕ şi orice calculator Chaitin C avem:*

$$K(x|v) \le K_\phi(x|v) + O(1), H(x|v) \le H_C(x|v) + O(1). \qquad (1.5)$$

Corolar 1.11 *Pentru orice $x, v \in X^*$,*

$$0 < K(x|v) < \infty, 0 < H(x,v) < \infty.$$

În ceea ce urmează, Corolarul 1.6 şi Corolarul 1.10 vor fi referite ca Teorema de Invarianţă. Să mai notăm că pentru două calculatoare universale ψ şi ω există o constantă c, astfel încât pentru orice $x, y \in X^*$ avem:

$$|K_\psi(x) - K_\omega(x)| \le c,$$

$$|K_\psi(x|v) - K_\omega(x|v)| \le c.$$

Aceleaşi rezultate sunt valabile şi pentru complexitatea Chaitin. De aici, rezultă că toate rezultatele care nu se prevalează de forma particulară a unui calculator universal fixat sunt valabile şi pentru alt calculator universal, deci acestea nu depind de calculatoarele universale alese. Pentru detalii, recomandăm Calude [3] şi Chaitin [18]

Importanţa proprietăţii de libertate de prefixe a fost descoperită independent de Schnorr [36], Levin [29] şi Chaitin [19]; teoria complexităţii auto-limitate a fost dezvoltată în special de către Chaitin.

1.2 Complexităţi pentru numere naturale

Pentru numere naturale, dacă vom considera reprezentările poziţionale în diferite baze de numeraţie, putem să considerăm mulţimea numerelor naturale ca fiind o parte a lui X^*, mai precis $\mathbf{N}$ va fi constituită din toate cuvintele de lungime unu şi cele de lungime mai mare sau egală cu doi care nu încep cu a_1. Funcţia care va face corespondenţa bijectivă între $\mathbf{N}$ şi aceste cuvinte va fi $number_p : \mathbf{N} \longrightarrow \mathbf{N}$ definită prin

$$number_p(0) = a_1,\ number_p(1) = a_2, \ldots, number_p(p-1) = a_p,$$

$$number_p(p) = a_2a_1, number_p(p+1) = a_2a_2, \ldots, number_p(i), \ldots$$

$number_p(i)$ este reprezentarea numărului natural i în baza p folosind cifrele din X^*.

Notăm $l_p(n) = l(number_p(n))$.

Analog situaţiei de la cuvinte, avem următoarele definiţii pentru complexităţi:

Definiţie 1.12 *a) Fie* $f : \mathbf{N} \stackrel{\circ}{\longrightarrow} \mathbf{N}$. *Numim complexitatea Kolmogorov indusă de* f *peste alfabetul* X, *funcţia parţială* $K_f^p : \mathbf{N} \longrightarrow \mathbf{N}$, *definită prin*

$$K_f^p(n) = min\{l_p(v) | v \in \mathbf{N},\ f(v) = n\}.$$

b) Fie $f : \mathbf{N} \times \mathbf{N} \stackrel{\circ}{\longrightarrow} \mathbf{N}$. *Numim complexitatea Kolmogorov condiţionată indusă de* f *peste alfabetul* X, *funcţia parţială* $K_f^p : \mathbf{N} \times \mathbf{N} \stackrel{\circ}{\longrightarrow} \mathbf{N}$, *definită prin*

$$K_f^p(n|m) = min\{l_p(v) | v \in \mathbf{N},\ f(v, m) = n\}.$$

Fixînd alfabetul X avem:

Teorema 1.13 *(Câmpeanu [14]) a) Există o funcţie p.r.* $U_n : \mathbf{N} \longrightarrow \mathbf{N}$, *numită algoritm uniform universal Kolmogorov, care are următoarea proprietate: pentru orice funcţie p.r.* $\phi : \mathbf{N} \stackrel{\circ}{\longrightarrow} \mathbf{N}$, *există o constantă naturală* c *astfel încât*

$$K_{U_n}^p(n) \leq K_\phi^p(n) + c,$$

oricare ar fi $n \in \mathbf{N}$.

b) Există o funcţie p.r. $U_c : \mathbf{N} \times \mathbf{N} \overset{\circ}{\longrightarrow} \mathbf{N}$ *numită algoritm universal Kolmogorov care are următoarea proprietate: pentru orice funcţie p.r.* $\phi : \mathbf{N} \times \mathbf{N} \overset{\circ}{\longrightarrow} \mathbf{N}$*, există o constantă naturală c astfel încât*

$$K^p_{U_c}(n|m) \leq K^p_\phi(n|m) + c,$$

oricare ar fi $n \in \mathbf{N}$*.*

Demonstraţie. Considerăm următoarele funcţii:

$T : number_p(\mathbf{N}) \longrightarrow number_p(\mathbf{N})$, $T(a_1) = a_2a_1$, $T(x_1x_2\cdots x_n) = x_1x_1x_2x_2\cdots x_nx_na_2a_1$.

$f : number_p(\mathbf{N}) \longrightarrow number_p(\mathbf{N})$, $f(x) = z$, dacă există y astfel ca $x = T(z)y$, a_1 altfel,

$g : number_p(\mathbf{N}) \longrightarrow number_p(\mathbf{N})$, $g(x) = y$, dacă există z astfel ca $x = T(z)y$, a_1 altfel.

a) Utilizînd funcţia universală: $\phi_{univ_1} : \mathbf{N} \times \mathbf{N} \overset{\circ}{\longrightarrow} \mathbf{N}$, obţinem funcţia $U_n : \mathbf{N} \overset{\circ}{\longrightarrow} \mathbf{N}$ definită prin:
$U_n(x) = \phi_{univ_1}(number_p^{-1}(f(number_p(x))), number_p^{-1}(g(number_p(x))))$.

Fie $\phi : \mathbf{N} \longrightarrow \mathbf{N}$, $\phi = \phi_i$.

$$K^p_\phi(n) = min\{l_p(v)|v \in \mathbf{N}, \phi(v) = n\} =$$

$$min\{l_p(v)|v \in \mathbf{N}, \phi_i(v) = n\} = min\{l_p(v)|v \in \mathbf{N}, \phi_{univ_1}(i, v) = n\} =$$

$$min\{l_p(v)|v \in \mathbf{N}, \phi_{univ_1}(i, v) = n, f(number_p(i))\} =$$

$$min\{l_p(v)|v \in \mathbf{N}, U_n(number_p^{-1}T(number_p(i), number_p(v))) = n\},$$

$$K^p_{U_n}(n) = min\{l_p(s)|s \in \mathbf{N}, U_n(s) = n\} = min\{l_p(v)|v \in \mathbf{N},$$

$$\phi_{univ_1}(number_p^{-1}f(number_p(s)), number_p^{-1}g(number_p(s))) = n\};$$

$$c = 2 \cdot l_p(i) + 2$$

b) Utilizînd funcţia universală $\phi_{univ_2} : \mathbf{N} \times \mathbf{N} \times \mathbf{N} \overset{\circ}{\longrightarrow} \mathbf{N}$, obţinem funcţia $U_c : \mathbf{N} \times \mathbf{N} \overset{\circ}{\longrightarrow} \mathbf{N}$ definită prin:
$U_c(x|m) = \phi_{univ_2}(number_p^{-1}(f(number_p(x))), number_p^{-1}(g(number_p(x))), m)$

Fie $\phi : \mathbf{N} \times \mathbf{N} \longrightarrow \mathbf{N}$, $\phi = \phi_i$.

$$K^p_\phi(n|m) = min\{l_p(v)|v \in \mathbf{N}, \phi(v|m) = n\} =$$

$$min\{l_p(v)|v \in \mathbf{N}, \phi_i(v|m) = n\} = min\{l_p(v)|v \in \mathbf{N}, \phi_{univ_2}(i, v, m) = n\} =$$

$$min\{l_p(v)|v \in \mathbf{N}, U_c(number_p^{-1}(T(number_p(i), number_p(v))), m) = n\}$$

$$K^p_{U_n}(n|m) = min\{l_p(s)|s \in \mathbf{N}, U_c(s, m) = n\} =$$

$$min\{l_p(v)|v \in \mathbf{N}, \phi_{univ_2}(f(number_p(s)), g(number_p(s)), m) = n\};$$

$$c = 2 \cdot l_p(i) + 2$$

□

Lema 1.14 *(Câmpeanu [14]) Funcţia U_c din Teorema 1.13 b) nu depinde de alfabetul X.*

Demonstraţie. Fie $\phi : \mathbf{N} \times \mathbf{N} \stackrel{\circ}{\longrightarrow} \mathbf{N}$ şi $n, m \in \mathbf{N}$. Este suficient să demonstrăm că există $c_1 \in \mathbf{N}$, astfel încât $K^s_U(n|m) \leq K^s_\phi(n|m) + c_1$, dacă există $c \in \mathbf{N}$ cu $K^p_U(n|m) \leq K^p_\phi(n|m) + c$. Din definiţia complexităţii Kolmogorov deducem că:

$$K^s_U(n|m) = min\{l_s(v)|U(v, m) = n\}.$$

Distingem două cazuri:

1) $K^p_\phi(n|m) < \infty$ şi
2) $K^p_\phi(n|m) = \infty$.

În primul caz, rezultă că există numerele naturale v_0 şi w_0, astfel încât $l_p(v_0) = K^p_U(n|m)$ şi $l_p(w_0) = K^p_\phi(n|m)$ şi v_0, w_0 sunt cele mai mici cu aceste proprietăţi. Deci

$$K^s_U(n|m) = l_s(v_0) \text{ şi } K^s_\phi(n|m) = l_s(w_0).$$

Deoarece există $c \in \mathbf{N}$ cu $l_p(v_0) \leq l_p(w_0) + c$, există $c_1 \in \mathbf{N}$ astfel ca:

$$K^s_U(n|m) \leq K^s_\phi(n|m) + c_1.$$

În cazul al doilea, deoarece $K^s_\phi(n|m) = min\{l_s(w)|\phi(w, m) = n\}$, inegalitatea cerută este evidentă. □

Observaţia 1.15 *Constanta c_1 din lema anterioară depinde doar de p, s, U şi ϕ.*

Lema 1.16 *(Câmpeanu [14]) Funcţia U_n din Teorema 1.13 a) nu depinde de alfabetul X.*

Demonstraţie. Similar cu demonstraţia Lemei 1.14. □

Observaţia 1.17 *Constantele din Teorema 1.13 există indiferent de numărul literelor din alfabetul X, dar depind de el.*

2

Cuvinte şi numere aleatoare

În acest capitol introducem noţiunile de cuvânt aleator Chaitin-Kolmogorov şi aleator Chaitin. Se introduce noţiunea de cuvânt Borel normal, cuvintele aleatoare (Chaitin şi Chaitin-Kolmogorov) suficient de mari (în sensul ordinei cvasi-lexicografice) fiind Borel normale. Să mai notăm că cele două mulţimi de cuvinte aleatoare (Chaitin şi Chaitin-Kolmogorov) sunt imune (Teorema 2.7). Se dă o condiţie necesară şi suficientă pentru reprezentabilitatea testelor Martin-Löf prin calculatoare Chaitin (Teorema 2.15). În secţiunea a doua se introduc noţiunile de hazard algoritmic pentru numerele naturale în reprezentare poziţională. Astfel, vom defini ce înţelegem prin număr aleator într-o anumită bază şi număr p-normal. Vom arăta că numerele aleatoare în baza p sunt p-normale. De asemenea, arătăm că mulţimea numerelor naturale aleatoare într-o bază oarecare este o mulţime imună (Teorema 2.25). În secţiunea a treia arătăm că orice număr aleator în baza p este p-normal (Corolarul 2.34 şi Corolarul 2.35). Aceste rezultate sunt argumente în favoarea adecvării Definiţiei 2.21.

2.1 Cuvinte aleatoare

Vom începe acest capitol prin a introduce câteva definiţii indispensabile studiului fenomenului de hazard, fiind corespondentul legii numerelor mari din statistică pentru monoizi liberi liber generaţi de mulţimi finite.

Definiţie 2.1 *(Calude [3]) Un cuvânt nevid $x \in X^*$ se numeşte ε-limiting*

(ε este un număr real pozitiv fixat), dacă pentru orice $1 \le i \le p$, x satisface inegalitatea:

$$\left|\frac{N_i(x)}{l(x)} - \frac{1}{p}\right| \le \varepsilon,$$

unde $N_i(x)$ este numărul de apariţii ale literei a_i în cuvântul x. $\square$

Altfel spus, un cuvânt este ε-limiting dacă toate literele apar în cuvântul respectiv de aproape acelaşi număr de ori. Notăm $x[n] = x_1 \dots x_n$, $x \in X^*$. Dacă pe $x \in X^*$ îl considerăm ca fiind un cuvânt peste alfabetul X^m, atunci notăm noua sa lungime cu $l^m(x)$. Evident, dacă $m \not| l(x)$ atunci $x \notin (X^m)^*$. În acest caz, prin $l^m(x)$ vom înţelege lungimea în X^m a cuvântului w, $w \preceq_p x$ şi $l(x) - l(w) < m$, adică lungimea celui mai mare prefix a lui x care are lungimea multiplu de m. Pentru $1 \le i \le p^m$ $N_i^m(x)$ este numărul de apariţii a celui de-al i-lea cuvânt din X^m (în ordine cvasi-lexicografică) în x.

Definiţie 2.2 *Fie $\varepsilon > 0$ şi $m \ge 1$.*
a) Spunem că $x \in X^+$ este (ε, m)-limiting dacă

$$\left|\frac{N_i^m(x)}{l^m(x)} - p^{-m}\right| \le \varepsilon,$$

pentru orice $1 \le i \le p^m$.

b) Spunem că $x \in X^+$ este Borel (ε, m)-normal dacă x este (ε, j)-limiting, pentru orice $1 \le j \le m$.

Definiţie 2.3 *Fie $m \ge 1$.*
a) Spunem că $x \in X^+$ este m-limiting dacă x este $(\sqrt{\frac{\log_p l(x)}{l(x)}}, m)$-limiting, adică

$$\left|\frac{N_i^m(x)}{l^m(x)} - p^{-m}\right| \le \sqrt{\frac{\log_p l(x)}{l(x)}},$$

pentru orice $1 \le i \le p^m$.

b) Dacă pentru orice $m \in \mathbf{N}$, $1 \le m \le \log_p \log_p l(x)$, x este m-limiting, atunci spunem că x este Borel normal.

Dacă notăm:

$$\sum(n) = \max_{x \in X^n} H(x),$$
$$\sigma(n) = \max_{x \in X^n} K(x),$$

în virtutea rezultatelor din Chaitin [18] şi Calude [3] avem:

$$\sum(n) = n + H(string(n)) + O(1)$$
$$\sigma(n) = n + O(1).$$

Un şir se numeşte t-aleator dacă complexitatea sa este mai mare sau egală cu cea mai mare complexitate a cuvintelor de aceeaşi lungime minus t. Astfel, pentru complexităţile Chaitin şi Kolmogorov obţinem următoarele definiţii:

Definiţie 2.4 *Un cuvânt x se numeşte t-aleator Kolmogorov dacă*

$$K(x) \geq l(x) - t.$$

Definiţie 2.5 *Un cuvânt x se numeşte t-aleator Chaitin dacă*

$$H(x) \geq \sum(l(x)) - t.$$

Mulţimile de şiruri t-aleatoare le notăm cu:

$$RAND_t^C = \{x \in X^* |\, H(x) \geq l(x) + H(string(l(x))) - t\},$$
$$RAND_t^K = \{x \in X^* |\, K(x) \geq l(x) - t\}.$$

În cazul în care $t = 0$, mulţimile de mai sus se scriu fără indicele t; şirurile 0-aleatoare se numesc şi aleatoare. Mai notăm:

$$R_t^C = \{x \in X^* |\, H(x) \geq l(x) - t\}.$$

Avem:

$$\text{card}\{x \in X^* |\, l(x) = m,\, x \in non\ - RAND_t^K\} \leq \sum_{i=0}^{m-t-1} p^i =$$
$$\frac{p^{m-t} - 1}{p - 1} < \frac{p^{m-t}}{p - 1};$$

deci

$$\text{card}\{n \in \mathbf{N} |\, l_p(n) = m,\, n \in RAND_t^K\} \geq p^m - \frac{p^{m-t} - 1}{p - 1} =$$

$$p^m \cdot \left(1 - \frac{1}{p^t \cdot (p-1)}\right).$$

Teorema 2.6 *(Calude [3]) a) Există m astfel încât pentru orice $x \in RAND_t^K$ cu $l(x) > m$, x este Borel normal.*

b) Există m astfel încât pentru orice $x \in RAND_t^C$ cu $l(x) > m$, x este Borel normal.

Teorema 2.7 *(Calude [3]) a) Mulţimea $RAND_t^K$ este imună.*

b) Mulţimea $RAND_t^C$ este imună.

2.1.1 Teste Martin-Löf

Definiţie 2.8 *O mulţime recursiv enumerabilă $V \subseteq X^* \times \mathbf{N}$ se numeşte test Martin-Löf (M-L) dacă satisface următoarele condiţii:*
i) $V_m \subseteq V_{m+1}$, unde $V_m = \{x \in X^* | (x, m) \in V\}$;
ii) card$\{x \in V_m \cap X^n\} \leq \frac{p^{n-m}-1}{p-1}$.
Un test Martin-Löf se numeşte secvenţial dacă în plus este satisfăcută proprietatea:
iii) $x \in V_m$, x este prefix al lui y implică $y \in V_m$.

Iată câteva exemple:

Exemplul 2.9 *a) Pentru $l(x) > m$, mulţimea*

$$H(x, m) = \{(x, 1), (x, 2), \ldots, (x, m)\}$$

este un test M-L.
b) Dacă $H(x, m)$ este un test M-L, atunci mulţimea

$$\overline{H(x, m)} = \{(y, n) | x \preceq_p y (x, n) \in H(x, m)\}$$

este de asemenea un test M-L.

Definiţie 2.10 *Un test M-L U se numeşte universal dacă, pentru orice alt test M-L V, există o constantă $c \in \mathbf{N}$ (care depinde de U şi V), astfel încât:*

$$V_{c+m} \subseteq U_m, \text{ oricare ar fi } m \in \mathbf{N} \setminus \{0\}.$$

Teorema 2.11 *(Calude [2]) Mulţimea*

$$V(\phi) = \{(x, m) | K_\phi(x|l(x)) < l(x) - m\}$$

este un test M-L. Dacă $\phi = \psi$, atunci $V(\psi)$ este universal.

Teorema 2.12 *(Calude, Chiţescu [7]) Mulţimea*

$$V(C) = \{(x, m) | H_C(x|l(x)) < l(x) - m\}$$

este un test M-L.

Definiţie 2.13 *Spunem că un test M-L V este test M-L reprezentabil Chaitin dacă există un calculator Chaitin C, astfel încât $V = V(C)$.*

Lema 2.14 *(Câmpeanu [13]) Fie $W = V(C)$ un test M-L reprezentabil Chaitin. Atunci*

$$\sum_{m \geq 1} \sum_{m_V(x)=m} p^{-l(x)+m+1} \leq 1.$$

Demonstraţie. Dacă $m_V(x) = m \geq 1$, atunci $H_C(x) = l(x) - m - 1$, deci

$$\sum_{m \geq 1} \sum_{m_V(x)=m} p^{-l(x)+m+1} = \sum_{m \geq 1} \sum_{H_C(x)=l(x)-m-1} p^{-l(x)+m+1} \leq$$

$$\sum_{m \geq 1} \sum_{\substack{l(y)=l(x)-m-1 \\ C(y,\lambda)=x}} p^{-l(x)+m+1} \leq \sum_{m \geq 1} \sum_{\substack{C(y,\lambda)=x \\ l(y)=l(x)-m-1}} p^{-l(y)} \leq \sum_{y \in dom(C_\lambda)} p^{-l(y)} \leq 1,$$

în virtutea faptului că domeniul lui C_λ este liber de prefixe. □

Teorema 2.15 *(Câmpeanu [13]) Fie V un test M-L. Atunci V este un test M-L reprezentabil Chaitin dacă şi numai dacă*

$$\sum_{(x,m) \in V} p^{-l(x)+m+1} \leq 1.$$

Demonstraţie. În virtutea inegalităţii

$$\sum_{(x,m)\in V} p^{-l(x)+m+1} \leq 1,$$

putem utiliza Teorema Kraft-Chaitin (v. Calude [3]) pentru a construi (efectiv), pentru orice $(x,m) \in V$, cuvântul $u_{x,m} \in X^*$, astfel încât $(u_{x,m})_{(x,m)\in V}$ este liberă de prefixe şi $l(u_{x,m}) = l(x) - m - 1$. Construim calculatorul $C : X^* \times X^* \xrightarrow{\circ} X^*$, $C(u_{x,m}, \lambda) = x$. Fie $(x,m) \in V$, deci $dom(C_\lambda) = \{u_{x,m} | \ (x,m) \in V\}$. Cum $C(u_{x,m}, \lambda) = x$, avem

$$H_C(x) \leq l(u_{x,m}) = l(x) - m - 1 < l(x) - m,$$

deci $(x,m) \in V(C)$.

Reciproc, din $(x,m) \in V(C)$ rezultă că $H_C(x) < l(x) - m$, adică $\min\{l(y) | \ C(y,\lambda) = x\} < l(x) - m$. Deoarece $dom(C_\lambda) = \{u_{x,m} | \ (x,m) \in V\}$, va rezulta că există n astfel încât $C(u_{x,n}, \lambda) = x$ şi $l(u_{x,n}) < l(x) - m$, şi $(x,n) \in V$. Dar $l(u_{x,n}) = l(x) - n - 1$, deci $l(x) - n - 1 < l(x) - m$; de aici $m < n + 1$. Dar $(x,n) \in V$, deci $(x,m) \in V (m \leq n)$. □

Pentru orice test M-L V asociem funcţia $q_V : \mathbf{N}_+ \to \mathbf{N}_+$, dată de

$$q_V(m) = \sum_{m_V(x)=m} p^{-l(x)}.$$

(Să notăm că q_V poate să nu fie recursivă, deoarece V nu este întotdeauna recursiv!).

Corolar 2.16 *(Câmpeanu [13]) Dacă $q_V(m) < p^{-2m-2}$ pentru orice m, atunci V este reprezentabil Chaitin.*

Demonstraţie. Datorită relaţiilor

$$\begin{aligned}\sum_{(x,m)\in V} p^{-l(x)+m+1} &= \sum_{m\geq 1} \sum_{m_V(x)=m} p^{-l(x)+m+1} \\ &= \sum_{m\geq 1} p^{m+1} \cdot q_V(m) \\ &\leq \sum_{m\geq 1} p^{-m} \leq 1,\end{aligned}$$

putem utiliza Teorema 2.15 pentru a arăta că V este reprezentabil Chaitin. □

Definiţie 2.17 *Spunem că testul M-L V este un test M-L scufundabil Chaitin dacă există un calculator Chaitin C astfel încât $V \subseteq V(C)$.*

În contrast cu situaţia de la complexitatea Kolmogorov, unde nu se cunoaşte decât o condiţie necesară dar nu şi suficientă, pentru complexitatea Chaitin putem să demonstrăm următorul rezultat:

Corolar 2.18 *(Câmpeanu [13]) Un test M-L este scufundabil Chaitin dacă şi numai dacă este reprezentabil Chaitin.*

Demonstraţie. Dacă V este reprezentabil Chaitin, atunci evident el este scufundabil Chaitin. Reciproc, utilizăm Definiţia 2.17 şi Teorema 2.15: există un calculator Chaitin C astfel încât $V \subseteq V(C)$ şi $V(C)$ este reprezentabil, deci

$$\sum_{(x,m)\in V} p^{-l(x)+m+1} \leq \sum_{(x,m)\in V(C)} p^{-l(x)+m+1} \leq 1. \ \square$$

Exemplul 2.19 *a) Testul M-L $H(x,m)$ este reprezentabil Chaitin dacă şi numai dacă $l(x) > m+1$.*

b) Orice test secvenţial M-L nu este reprezentabil Chaitin.

Teorema 2.20 *Testele universale M-L nu pot fi reprezentabile Chaitin.*

Demonstraţie. Fie $W = V(C)$. Dacă W ar fi universal, atunci pentru orice test M-L V, există $c \in \mathbf{N}$ astfel încât:

$$V_{m+c} \subseteq W_m, \text{ oricare ar fi } m \in \mathbf{N}.$$

De aici rezultă că

$$1 \geq \sum_{x\in W_m} p^{-l(x)+m+1} \geq \sum_{x\in V_{m+c}} p^{-l(x)+m+1}. \tag{2.1}$$

Luăm V test secvenţial M-L, $m \in \mathbf{N}$, $V_{m+c} \neq \emptyset$ şi $x_m \in V_{m+c}$. Pentru orice $x \in V_{m+c}$, $x \preceq_p y$ implică $y \in V_{m+c}$, deci:

$$\sum_{x\in V_{m+c}} p^{-l(x)+m+1} = p^{m+1} \cdot \sum_{x\in V_{m+c}} p^{-l(x)} \geq$$

$$p^{m+1} \cdot \sum_{x_m \preceq_p x} p^{-l(x)} = p^{-l(x_m)+m+1} \cdot \sum_{x\in X^*} p^{-l(x)} = \infty,$$

adică:

$$\sum_{x\in V_{m+c}} p^{-l(x)+m+1} = \infty. \tag{2.2}$$

Din 2.1 şi 2.2 rezultă o contradicţie, deci W nu poate fi universal. $\square$

2.2 Numere aleatoare

Folosind argumentele de la cuvinte, definim numerele aleatoare în baza p astfel:

Definiţie 2.21 *Un număr natural se numeşte t-aleator în baza p dacă complexitatea sa Kolmogorov în baza p este mai mare sau egală cu lungimea reprezentării sale în baza p minus t.*

Notăm cu:

$$RAND_t^p = \{n \in \mathbf{N} | K^p(n|l_p(n)) \geq l_p(n) - t\},$$

$$uRAND_t^p = \{n \in \mathbf{N} | K^p(n) \geq l_p(n) - t\}.$$

Observaţia 2.22 *Sunt două categorii de numere naturale aleatoare: una definită cu ajutorul complexităţii uniforme, iar cealaltă cu ajutorul complexităţii condiţionate.*

În continuare vom studia ambele mulţimi de numere naturale aleatoare, ele avînd proprietăţi asemănătoare.

Teorema 2.23 *(Câmpeanu [14]) Dacă $n \in uRAND_t^p$ atunci*

$$n \in uRAND^s_{l_s(p^{t+1})}.$$

Demonstraţie. Dacă $n \in uRAND_t^p$, atunci $n \neq U_u(r)$ pentru nici un r natural cu $l_p(r) \leq l_p(n) - t$. Dacă $n \notin uRAND^s_{l_s(p^{t+1})}$, atunci există z astfel încât $l_s(z) < l_s(n) - l_s(p^{t+1})$ şi $n = U_n(z)$. Avem:

$$\lceil \log_s z \rceil + 1 < \lceil \log_s n \rceil + 1 - \lceil \log_s p^{t+1} \rceil - 1,$$

deci

$$\log_s z + 1 < \log_s n - \lceil \log_s p^{t+1} \rceil - 1,$$

adică

$$\log_s z \leq \log_s n - \log_s p^{t+1}.$$

De aici

$$z \leq n/p^{t+1}, \text{ deci } l_p(z) < l_p(n) - t,$$

ceea ce înseamnă că $n \notin uRAND_t^p$. $\square$

Corolar 2.24 *(Câmpeanu [14]) Dacă $n \in uRAND_t^p$, atunci $n \in uRAND_{t+c}^s$, unde c este o constantă care depinde de p, s şi t.*

Demonstraţie. Luăm c astfel încât $l_s(p^{t+1}) - t \leq c$. □

Ne putem pune în mod natural întrebarea următoare: “ Cât de multe numere aleatoare în baza p de lungime m există ? ” Răspunsul la această întrebare este dat de evaluările:

$$\mathrm{card}\{n \in \mathbf{N} |\, l_p(n) = m,\, n \in non - RAND_t^p\} \leq$$
$$\sum_{i=1}^{m-t-1} (p-1) \cdot p^{t-1} + 1 = (p-1) \cdot \frac{p^{m-t-1} - 1}{p-1} + 1 = p^{m-t-1};$$

deci

$$\mathrm{card}\{n \in \mathbf{N} |\, l_p(n) = m,\, n \in RAND_t^p\} \geq$$
$$(p-1) \cdot p^{m-1} - p^{m-t-1} = p^{m-t-1} \cdot ((p-1) \cdot p^t - 1).$$

De asemenea, avem

$$\mathrm{card}\{n \in \mathbf{N} |\, l_p(n) = m,\, n \in non - uRAND_t^p\} \leq$$
$$\sum_{i=1}^{m-t-1} (p-1) \cdot p^{t-1} + 1 = (p-1) \cdot \frac{p^{m-t-1} - 1}{p-1} + 1 = p^{m-t-1};$$

deci

$$\mathrm{card}\{n \in \mathbf{N} |\, l_p(n) = m,\, n \in uRAND_t^p\} \geq$$
$$(p-1) \cdot p^{m-1} - p^{m-t-1} = p^{m-t-1} \cdot ((p-1) \cdot p^t - 1).$$

2.2.1 Imunitate pentru numerele aleatoare în baza p

Fixăm doi algoritmi universali U_n şi U_c.

Teorema 2.25 *(Câmpeanu [14]) Mulţimile $RAND_t^p$ şi $uRAND_t^p$ sunt imune.*

Demonstraţie. Mai întâi, vom demonstra teorema pentru $RAND_t^p$. Presupunem că există o funcţie recursivă F astfel încât $F(\mathbf{N}) \subseteq RAND_t^p$, $F = \phi_i$. Construim funcţia auxiliară g definită prin recurenţă primitivă de ecuaţiile

$$g(0, x) = F(0),$$

$$g(n+1, x) = F(\min\{m|\, F(m) > p^{p^{n+1}}, F(m) \geq g(n, x)\}).$$

Deoarece F este recursivă, g este parţial recursivă. Dacă $n, v \in \mathbf{N}$, $n \in \mathrm{dom} g$, atunci $K_g^p(g(n)|v) = l_p(n)$, deci

$$K(g(n)|v) \leq l_p(n) + c.$$

De aici, deoarece

$$g(\mathbf{N}) \subseteq F(\mathbf{N}) \subseteq RAND_t^p,$$

$$l_p(g(n)) - t \leq K^p(g(n)|l_p(g(n))),$$

deci

$$l_p(g(n)) - l_p(n) \leq c + t, \text{ oricare ar fi } n \in \mathbf{N}.$$

Dar $l_p(g(n)) \geq l_p(p^{p^n}) \geq p^t$, deci

$$l_p(g(n)) - l_p(n) \geq p^n - l_p(n);$$

prin urmare,

$$p^n - l_p(n) \leq c + t,$$

deci $n < c + t$. Rezultă $\mathrm{card}(\mathrm{dom} g) < c + t$. Din definiţia lui g deducem

$$\mathrm{card}(\mathrm{dom} g) < p^{p^{c+t}} + 1.$$

De aici, rezultă că $RAND_t^p$ este imună.

Pentru $uRAND_t^p$ putem utiliza o construcţie similară, folosind de această dată funcţia:

$$f : \mathbf{N} \xrightarrow{\circ} \mathbf{N},$$

$$f(0) = F(0),$$

$$f(n+1) = F(\min m | F(m) > p^{p^n+1}, F(m) \leq f(n)$$

în loc de g. □

Deci, am demonstrat că mulţimea numerelor aleatoare în baza p este o mulţime imună.

2.2.2 Uniformitatea numerelor aleatoare

Pentru numere, corespondentul pentru noţiunea de ε-limiting este noţiunea de număr ε-p-limiting.

Definiţie 2.26 *Fie $p \in \mathbf{N}$, $p \geq 2$, $x \in \mathbf{N}$ şi $\varepsilon > 0$. Spunem că x este ε-p-limiting, dacă*

$$\left| \frac{N_i^p(x)}{l_p(x)} - \frac{1}{p} \right| < \varepsilon, \text{ pentru orice } 1 \leq i \leq p,$$

unde $N_i^p(x)$ este numărul de apariţii ale celei de a i-a cifre din baza p în x, acesta fiind reprezentat de asemenea în baza p.

Definiţie 2.27 *Fie $p \geq 2$. Numărul natural x se numeşte p-limiting, dacă*

$$\left| \frac{N_i^p(x)}{l_p(x)} - \frac{1}{p} \right| < \sqrt{\frac{\log_p l_p(x)}{l_p(x)}}, \text{ pentru orice } 1 \leq i \leq p.$$

Definiţie 2.28 *Fie x un număr natural. x este p-normal dacă x este q-limiting pentru orice $2 \leq q \leq p$.*

Observaţia 2.29 *Dacă x este p-normal şi $2 \leq q \leq p$, atunci x este q-normal.*

Fapt 2.30 *(Natanson [32]) Pentru orice numere naturale $n \geq k \geq 0$ şi $x > 0$ număr real, avem:*

$$\sum_{k=0}^{n} \binom{n}{k} (k - n \cdot x)^2 x^k (1-x)^{n-k} = n \cdot x(1-x).$$

Utilizînd Faptul 2.30 vom da în continuare câteva rezultate privind numerele p-normale:

Lema 2.31 *Următoarele inegalităţi sunt adevărate:*

$$card\{x \in \mathbf{N} |\, l_p(x) = n,\ x \text{ nu este } \varepsilon\text{-p-limiting}\} < \frac{p^{n-2} \cdot (p-1)^2}{n \cdot \varepsilon^2},$$

$$card\{x \in \mathbf{N} |\, l_p(x) = n,\ x \text{ nu este p-limiting}\} < \frac{p^{n-2} \cdot (p-1)^2}{\log_p n}.$$

Demonstraţie.

$$\mathrm{card}\{x \in \mathbf{N} \mid l_p(x) = n,\ x \text{ nu este } \varepsilon\text{-}p\text{-limiting}\} =$$

$$\sum_{\substack{k=0 \\ |\frac{k}{n}-\frac{1}{p}|>\varepsilon}}^{n} \mathrm{card}\{x \in \mathbf{N} \mid l_p(x) = n,\ \text{există } 1 \le i \le p,\ N_i^p(x) = k\} =$$

$$\sum_{\substack{k=0 \\ |\frac{k}{n}-\frac{1}{p}|>\varepsilon}}^{n} \mathrm{card}\{x \in \mathbf{N} \mid l_p(x) = n,\ N_1^p(x) = k\} +$$

$$\sum_{\substack{k=0 \\ |\frac{k}{n}-\frac{1}{p}|>\varepsilon}}^{n} \mathrm{card}\{x \in \mathbf{N} \mid l_p(x) = n,\ \text{există } 2 \le i \le p,\ N_i^p(x) = k\} \le$$

$$\sum_{\substack{k=0 \\ |\frac{k}{n}-\frac{1}{p}|>\varepsilon}}^{n-1} \mathrm{card}\{x \in \mathbf{N} \mid l_p(x) = n,\ N_1^p(x) = k\} +$$

$$\sum_{i=2}^{p} \sum_{\substack{k=0 \\ |\frac{k}{n}-\frac{1}{p}|>\varepsilon}}^{n} \mathrm{card}\{x \in \mathbf{N} \mid l_p(x) = n,\ N_i^p(x) = k\} \le$$

$$\sum_{\substack{k=0 \\ |\frac{k}{n}-\frac{1}{p}|>\varepsilon}}^{n-1} \begin{pmatrix} n-1 \\ k \end{pmatrix} (p-1)^{n-k} +$$

$$\sum_{i=2}^{p} \sum_{\substack{k=0 \\ |\frac{k}{n}-\frac{1}{p}|>\varepsilon}}^{n} \left[\begin{pmatrix} n-1 \\ k \end{pmatrix} (p-2)(p-1)^{n-k-1} + \begin{pmatrix} n-1 \\ k-1 \end{pmatrix} (p-1)^{n-k} \right] \le$$

$$\sum_{\substack{k=0 \\ |\frac{k}{n}-\frac{1}{p}|>\varepsilon}}^{n-1} \begin{pmatrix} n-1 \\ k \end{pmatrix} (p-1)^{n-k} + \sum_{\substack{k=0 \\ |\frac{k}{n}-\frac{1}{p}|>\varepsilon}}^{n-1} \begin{pmatrix} n-1 \\ k \end{pmatrix} (p-2)(p-1)^{n-k} +$$

$$\sum_{\substack{k=1\\ |\frac{k}{n}-\frac{1}{p}|>\varepsilon}}^{n} \binom{n-1}{k-1}(p-1)^{n-k+1} \leq$$

$$\sum_{\substack{k=0\\ |\frac{k}{n}-\frac{1}{p}|>\varepsilon}}^{n-1} \binom{n-1}{k}(p-1)^{n-k+1} + \sum_{\substack{k=1\\ |\frac{k}{n}-\frac{1}{p}|>\varepsilon}}^{n} \binom{n-1}{k-1}(p-1)^{n-k+1} \leq$$

$$\sum_{\substack{k=0\\ |\frac{k}{n}-\frac{1}{p}|>\varepsilon}}^{n} \binom{n}{k}(p-1)^{n-k+1} \leq \sum_{k=0}^{n} \binom{n}{k}(p-1)^{n-k+1}\frac{(\frac{k}{n}-\frac{1}{p})^2}{\varepsilon^2} =$$

$$\sum_{k=0}^{n} \binom{n}{k}(k-\frac{n}{p})^2(1-\frac{1}{p})^{n-k}\left(\frac{1}{p}\right)^k \frac{(p-1)p^n}{n^2\varepsilon^2} = \frac{(p-1)^2p^n}{n\varepsilon^2}.$$

Luînd

$$\varepsilon = \sqrt{\frac{\log_p l_p(x)}{l_p(x)}}$$

obţinem:

$$\mathrm{card}\{x \in \mathbf{N} |\, l_p(x) = n,\ x \text{ nu este } p\text{-limiting}\} < \frac{p^{n-2}\cdot(p-1)^2}{\log_p n}. \square$$

Fie $(\phi_i)_{i\in\mathbf{N}}$ o gödelizare acceptabilă Rogers. Fixăm doi algoritmi universali U_n şi U_c, $U_n = \phi_j$, $U_c = \phi_k$, şi două funcţii recursive $q_c, q_n : \mathbf{N}\times\mathbf{N} \longrightarrow \mathbf{N}$, astfel încât

$$K^p(x) \leq K^p_{\phi_i}(x) + q_n(j,i) \text{ şi } K^p(x|m) \leq K^p_{\phi_i}(x|m) + q_c(k,i).$$

Teorema 2.32 *Pentru orice $p \in \mathbf{N}$, $p \geq 2$ există un număr natural $M(p,t)$(care depinde p şi t), astfel încât pentru orice $n \in \mathbf{N}$ cu $n > M(p,t)$ şi $n \in uRAND^p_t$, rezultă că n este p-limiting.*

Demonstraţie. Fie $f : \mathbf{N} \longrightarrow \mathbf{N}$ funcţia recursivă definită prin:

$$f(x) = \text{al } x\text{-lea număr ce nu este } p\text{-limiting şi } l_p(x) > p.$$

Dacă $z \in \mathbf{N}$ nu este p-limiting, atunci

$$K_f^p(z) \leq l_p\left(\sum_{l=p+1}^{l_p(z)} \frac{p^{l-2}(p-1)^2}{\log_p l}\right) =$$

$$l_p\left(\left(\frac{p-1}{p}\right)^2 \sum_{l=p+1}^{l_p(z)} \frac{p^l}{\log_p l}\right) \leq$$

$$l_p\left(\left(\frac{p-1}{p}\right)^2 \sum_{l=p+1}^{l_p(z)} \frac{p^l}{\sqrt{\log_p l}}\right) \leq \log_p\left(\frac{p-1}{p}\right)^2 + \log_p\left(\sum_{l=p+1}^{l_p(z)} \frac{p^l}{\sqrt{\log_p l}}\right) + 1 \leq$$

$$\log_p\left(\frac{p-1}{p}\right)^2 + \log_p \frac{p^{l_p(z)+3}}{\sqrt{\log_p l_p(z)}} + 1 \leq l_p(z) + 4 - \frac{1}{2}\log_p \log_p l_p(z).$$

Dacă $f = \phi_{i_f}$, atunci

$$K^p(z) \leq l_p(z) + 4 - \frac{1}{2}\log_p \log_p l_p(z) + 4 + q_n(i_f, p).$$

Luînd

$$M(p,t) = \min\{n \in \mathbf{N} | -\frac{1}{2}\log_p \log_p l_p(z) + 4 + q_n(i_f, p) < -t\},$$

rezultă că $K^p(z) < l_p(z) - t$, deci $z \in non - uRAND_t^p$. Acum, rezultatul este evident. □

Corolar 2.33 *Pentru orice $p \in \mathbf{N}$, $p \geq 2$, există un număr natural $CM(p,t)$ astfel încât, pentru orice $n \in RAND_t^p$ cu $n > CM(p,t)$, rezultă că n este p-limiting.*

Demonstraţie. Luăm $CM(p,t) = M(p, t + q_n(u,p))$. □

Corolar 2.34 *Pentru orice $p \in \mathbf{N}$, $p \geq 2$, există un număr natural $L(p,t)$ astfel încât pentru orice $n \in uRAND_t^p$, $n > L(p,t)$, rezultă că n este p-normal.*

Demonstraţie. Luăm $L(p,t) = \max_{2 \leq s \leq p}\{M(s, l_s(p^{t+1})\}$. □

Corolar 2.35 *Pentru orice $p \in \mathbf{N}$, $p \geq 2$, există un număr natural $CL(p,t)$ astfel încât pentru orice $n \in RAND_t^p$, $n > CL(p,t)$, rezultă că n este p-normal.*

Demonstraţie. Luăm $CL(p,t) = \max_{2 \leq s \leq p} \{M(s, l_s(p^{t+1})\} + q_n(u,s)$. $\square$

3

Topologii constructive

În acest capitol vom prezenta unele topologii induse de relaţii recursive de ordine parţială. Pentru prima oară aceste noţiuni au fost introduse şi studiate în Zimand [38], unde a fost definită mulţimea *recursiv rară* pentru cazul binar şi ordinea prefix. Definiţia mulţimii recursiv rare apărea restrictiv, condiţia 2) din Definiţia 1 [38] fiind îndeplinită aproape peste tot. Pentru relaţii de ordine nemărginite, definiţia lui Zimand este echivalentă cu definiţia naturală dată în acest capitol, unde am cerut ca 2) să fie îndeplinită peste tot (Definiţia 3.6). Acest rezultat este evidenţiat prin Propoziţia 3.7. Teorema 3.8 este o generalizare a Propoziţiei 3 din Zimand [38] ce dă o condiţie suficientă ca să existe mulţimi rare care nu sunt recursiv rare; ordinile prefix şi sufix satisfac această condiţie. De asemenea, în Propoziţia 3.11 studiem o condiţie suficientă pentru ca o mulţime rară să fie recursiv rară şi orice mulţime care nu este rară să fie densă, ordinile infix, hipercod, masking şi prefix-masking satisfăcînd această din urmă condiţie. Sunt introduse noţiuni noi, ca mulţime *aproape rară, aproape recursiv rară, şi aproape densă* (Definiţia 3.13). Acestea sunt utile în special în studiul relaţiilor de ordine mărginite (v. capitolul următor şi Exemplul 3.3). Mulţimile aproape (recursiv) rare (dense) sunt diferite de mulţimile (recursiv) rare (dense) dacă relaţia de ordine considerată este mărginită, Teorema 3.17 şi Teorema 3.16.

În secţiunea a doua sunt date definiţiile mulţimilor (aproape) rare, dense, recursiv rare, dar de această dată pentru topologii induse de relaţii de ordine pe mulţimea numerelor naturale (Definiţiile 3.25 şi 3.31). Ca şi în cazul cuvintelor, mulţimile aproape (recursiv) rare (dense) coincid cu cele (recursiv) rare (dense), dacă topologiile considerate sunt generate de o relaţie de ordine nemărginită, teoremele 3.33 şi 3.34.

3.1 Topologii pe cuvinte

Pentru o relaţie de ordine recursivă pe X^*, topologia ordinei este topologia generată de mulţimile $U_x = \{y \in X^* | \, x \preceq y\}$, $x \in X^*$. O relaţie de ordine este nemărginită dacă pentru orice cuvânt x şi orice număr natural n, putem găsi un cuvânt y, $x \preceq y$ şi $l(y) \geq n$, adică pentru orice cuvânt putem să găsim un alt cuvânt mai mare decât primul (relativ la ordinea considerată), de lungime oricât de mare dorim. O relaţie de ordine este total mărginită dacă pentru orice cuvânt x există un număr natural n, astfel încât $x \preceq y$ implică $l(y) < n$. O relaţie de ordine este mărginită dacă nu este nemărginită. Orice relaţie de ordine total mărginită este mărginită.

Exemplul 3.1 *(Calude, Câmpeanu [5]) Următoarele relaţii sunt relaţii de ordine recursive şi nemărginite (utilizăm* $w = w_1 w_2 \cdots w_n$*,* $l(w) = n$*, şi* $v = v_1 v_2 \cdots v_m$*,* $l(v) = m$*;* $a_1 < a_2 < a_3 < \cdots < a_p$ *este ordinea pe X):*

(1) $w \preceq_p v$ *ddacă există* $u \in X^*$*,* $v = wu$ *(ordinea prefix),*

(2) $w \preceq_s v$ *ddacă există* $u \in X^*$*,* $v = uw$*(ordinea suffix),*

(3) $w \preceq_i v$ *ddacă există* $u, x \in X^*$*,* $v = uwx$ *(ordinea infix),*

(4) $w \preceq_h v$ *ddacă există* $u_1, \cdots u_{n+1} \in X^*$*,* $v = u_1 w_1 u_2 \cdots u_n w_n u_{n+1}$ *(ordinea hipercod),*

(5) $w \preceq_m v$ *ddacă* $w_{n-i} \leq v_{m-i}$*, pentru orice* $0 \leq i \leq min(m, n) - 1$ *şi dacă* $n > m$*, atunci* $w_j = a_1$*, pentru toţi* $1 \leq j \leq n - m$ *(ordinea masking),*

(6) $w \preceq_{pm} v$ *ddacă* $l(w) \leq l(v)$ *şi* $w_i \leq v_i$*, pentru toţi* $1 \leq i \leq l(w)$ *(ordinea prefix-masking),*

(7) $w \preceq_d v$ *ddacă* $w \preceq_p v$ *şi* $w \preceq_s v$ *(ordinea 2-ps-coduri),*

(8) $w \preceq_l v$ *ddacă există* $x, y, z \in X^*$*,* $w \preceq_p v$ *sau* $w = x a_i y$*,* $v = x a_j z$ *cu* $i < j$*, (ordinea lexicografică).*

Exemplul 3.2 *(Calude, Câmpeanu [5]) Dacă* $\preceq$ *este o relaţie de ordine recursivă (nemărginită) pe* X^* *şi* $f : X^* \to X^*$ *este o funcţie recursivă bijectivă, atunci relaţia de ordine parţială definită prin* $x \preceq_f y$ *ddacă* $f(x) \preceq f(y)$*, este recursivă (nemărginită).*

Exemplul 3.3 *(Câmpeanu [12]) Pentru* $x, y \in X^*$ *spunem că* $x \preceq_t y$ *dacă* $x = y$ *sau există* $x' \preceq_p x$*,* $y' \preceq_p y$*,* $x \neq x'$*,* $y \neq y'$*,* $l(x') = l(y')$ *şi* $x' \preceq_l y'$*,* $x' \neq y'$*.*

Observaţia 3.4 *De exemplu* $a_2a_1a_1a_1 \preceq_t a_2a_2$*, dar* a_1 *şi* $a_1a_2a_1$ *sunt incomparabile; mai mult,* $\preceq_t$ *este o relaţie de ordine recursivă mărginită şi pentru orice* $n \in \mathbf{N}$*, ea este totală pe* X^n*.*

Topologia generată de aceste relaţii de ordine este un spaţiu T_0, care nu este T_1 (în cazurile netriviale). Închiderea unei mulţimi A în acest spaţiu este:

$$\overline{A} = \{x \in X^* | \text{ există } z \in A,\, x \preceq z\}.$$

Lema 3.5 *Pentru* $A \subseteq X^*$ *şi* $w \in X^*$*, următoarele trei afirmaţii sunt echivalente:*
(i) $A \cap U_w = \emptyset$,
(ii) $\overline{A} \cap U_w = \emptyset$,
(iii) $w \notin \overline{A}$.

Demonstraţie. Vom demonstra că (i)⇒(ii)⇒(iii).

Considerînd (i) adevărată avem: oricare ar fi $w \preceq x$ $x \notin A$, deci dacă $w \preceq x$ şi $x \in \overline{A}$, atunci există $y \in A$ astfel încât: $w \preceq x$, $x \preceq y$ şi $y \in A$, adică $w \preceq y$ şi $y \in A$, ceea ce este imposibil, deci (i) implică (ii).

Dacă (ii) este adevărată, atunci oricare ar fi $y \in A$ dacă $x \preceq y$ $y \notin U_w$, rezultă cum $w \in U_w$ $w \not\preceq y$, oricare ar fi $y \in A$, deci $w \notin \overline{A}$; deci (ii) implică (iii).

Dacă (iii) este adevărată, atunci oricare ar fi $w \preceq x$, $x \notin A$, deci $A \cap U_w = \emptyset$ şi demonstraţia este încheiată. □

O mulţime este densă dacă $\overline{A} = X^*$. Pentru mai multe detalii privind topologia, recomandăm Jürgensen [23] şi Kelley [24].

Într-un spaţiu topologic o mulţime este rară dacă interiorul aderenţei este vid, adică dacă închiderea sa nu conţine deschişi; în cazul în care avem o bază pentru topologia studiată, o mulţime este rară dacă închiderea sa nu conţine nici o mulţime deschisă din bază. Definim conceptul de mulţime recursiv rară. Aici trebuie nu numai să demonstrăm că nici o mulţime deschisă nu este cuprinsă în închiderea sa, ci chiar să găsim o dovadă efectivă pentru acest lucru. Reformulînd, A este recursiv rară dacă $U_w \not\subseteq \overline{A}$ pentru nici un $w \in X^*$ în mod recursiv, adică putem găsi în mod recursiv pentru orice $w \in X^*$ un cuvânt $v \in X^*$, astfel încât $v \notin \overline{A}$. Obţinem astfel următoarea definiţie:

Definiţie 3.6 *O mulţime A se numeşte recursiv rară dacă există o funcţie recursivă $r : \mathbf{N} \longrightarrow \mathbf{N}$ astfel încât:*

1) $string(n) \preceq string(r(n))$,

2) $U_{string(r(n))} \cap A = \emptyset$,

pentru toţi $n \in \mathbf{N}$.

Această definiţie este o generalizare a celei date de Zimand în [38], acolo fiind cerut ca (2) să fie indeplinită doar de la un anumit rang încolo (aproape peste tot). Totuşi, dacă relaţia de ordine este nemărginită, cele două definiţii sunt echivalente:

Propoziţia 3.7 *(Calude, Câmpeanu [5]) Presupunem că $\preceq$ este recursivă şi nemărginită. O mulţime $A \subseteq X^*$ este recursiv rară dacă şi numai dacă există o funcţie recursivă $f : \mathbf{N} \longrightarrow \mathbf{N}$ şi un număr natural i, astfel încât $string(n) \preceq string(f(n))$, pentru toţi $n \in \mathbf{N}$ şi $U_{string(r(n))} \cap A = \emptyset$, pentru toţi n cu $l(string(n) > i$.*

Demonstraţie. Definim funcţia recursivă $q : \mathbf{N} \longrightarrow \mathbf{N}$, prin

$$q(n) = min\{m \geq 0 | string(n) \preceq string(m) \text{ şi } l(string(m)) > i\}.$$

Luăm $r = f \circ q$. Avem

$$string(n) \preceq string(q(n)) \preceq string(f(q(n))) = string(r(n)).$$

Dar $l(string(q(n))) > i$ implică

$$U_{string(r(n))} \cap A = U_{string(f(q(n)))} \cap A = \emptyset. \square$$

Teorema 3.8 *(Calude, Câmpeanu [5]) Presupunem că $\preceq$ este recursivă şi nemărginită şi în plus, că există o funcţie recursivă $s : \mathbf{N} \longrightarrow X^*$ astfel încât:*

(*) dacă pentru orice $i, j \in \mathbf{N}$ există x astfel ca $s(i) \preceq x$ şi $s(j) \preceq x$, atunci $i = j$;

atunci există o mulţime rară care nu este recursiv rară.

Demonstraţie. Fie $(\phi_n)_{n\geq 0}$, $\phi_n : \mathbf{N} \stackrel{\circ}{\longrightarrow} \mathbf{N}$ o gödelizare acceptabilă Rogers a funcţiilor parţial recursive. Definim mulţimea $A = \{string(t_n) | n \geq 0\}$, unde t_n este definit doar pentru $\phi_n(n) \neq \infty$ şi

$$t_n = min\{j \in \mathbf{N} | s(n) \preceq string(j), l(string(j)) \geq l(s(n)) + \phi_n(n)\}.$$

Afirmăm că A este rară, dar nu este recursiv rară. Într-adevăr, dacă presupunem că A nu este rară, atunci există $x \in X^*$ astfel încât $U_x \subseteq \overline{A}$. Deci există $n \geq 0$ astfel încât

$$x \preceq string(t_n),\ s(n) \preceq string(t_n),\ l(string(t_n)) \geq l(s(n)) + \phi_n(n).$$

Luăm un cuvânt z, $string(t_n) \preceq z$ şi $l(z) > l(string(t_n))$. Evident, $z \in U_x$. Vom demonstra că $z \notin \overline{A}$, o contradicţie. Pentru $z \in \overline{A}$, există $m \geq 0$ şi w astfel încât

$$s(m) \preceq w,\ z \preceq w,\ l(w) \geq l(s(m)) + \phi_m(m)$$

şi w este cel mai mic cuvânt (în raport cu ordinea cvasi-lexicografică) având proprietăţile de mai sus. Deci

$$s(n) \preceq string(t_n) \preceq z \preceq w,\ s(m) \preceq w;$$

din (*), $n = m$ adică $l(string(t_n)) = l(z)$.

Demonstrăm acum prin reducere la absurd că A nu este recursiv rară. Presupunem că există o funcţie recursivă $r : \mathbf{N} \longrightarrow \mathbf{N}$ astfel încât

$$string(n) \preceq string(r(n)) \text{ şi } A \cap U_{string(r(n))} = \emptyset,$$

pentru toţi $n \in \mathbf{N}$.

Fie $f, g : \mathbf{N} \longrightarrow \mathbf{N}$ funcţiile recursive date de relaţiile:

$$string(f(n)) = s(n) \text{ şi } g(n) = l(string(r(f(n)))) \dot{-} l(string(f(n))).$$

Mai întâi, să remarcăm că $string(r(f(n))) \notin A$, pentru nici un $n \geq 0$, deoarece

$$string(r(f(n))) \in U_{string(f(n))} \text{ şi } A \cap U_{string(r(f(n)))} = \emptyset.$$

Apoi, $g(n) \neq \phi_n(n)$ pentru toţi $n \geq 0$. Dacă există $n \geq 0$ cu $g(n) = \phi_n(n)$ atunci alegem cel mai mic $j \geq 0$ cu

$$s(n) \preceq string(j) \text{ şi } l(string(j)) \geq l(s(n)) + \phi_n(n) = l(string(r(f(n))));$$

avem

$$string(j) = string(r(f(n))); \text{ deci } string(r(f(n))) \in A.$$

În final, fie $i \geq 0$ cu $g = \phi_i$. Deoarece g este totală, avem $g(i) = \phi_i(i) \neq \infty$, o contradicţie. $\Box$

Exemplul 3.9 *(a) Ordinile sufix şi prefix satisfac ipoteza Teoremei 3.8. Spre exemplu, pentru ordinea sufix putem să luăm* $s(i) = a_1 a_2^i$.

(b) Dacă $\preceq$ *este parţial recursivă şi nemărginită avînd proprietatea (*) în raport cu* s, *atunci relaţia de ordine* $\preceq_f$ *are aceeaşi proprietate pentru* $f^{-1} \circ s$.

Observaţia 3.10 *Teorema 3.8 a fost demonstrată în Zimand [38] în cazul binar pentru ordinea prefix.*

Propoziţia 3.11 *(Calude, Câmpeanu [5]) Presupunem că* $\preceq$ *este recursivă, nemărginită şi filtrantă la dreapta. Atunci*

(i) orice mulţime rară este recursiv rară,

(ii) orice mulţime care nu este rară este densă.

Demonstraţie. (i) Fie $z \in X^*$ astfel ca $U_z \cap A = \emptyset$ şi definim funcţia recursivă $f : \mathbf{N} \longrightarrow \mathbf{N}$ prin

$$f(n) = min\{i \in \mathbf{N} | z \preceq string(i) \text{ şi } string(n) \preceq string(i)\}.$$

Evident

$$string(n) \preceq string(f(n)) \text{ şi } U_{string(f(n))} \cap A \subseteq U_z \cap A = \emptyset.$$

(ii) Fie $A \subseteq X^*$ o mulţime care nu este rară, adică există w astfel ca $U_w \subseteq \overline{A}$. Fie $x \in X^*$. Luăm $y \in X^*$ astfel ca $w \preceq y$ şi $x \preceq y$. Avem

$$x \in U_y \subseteq \overline{U_w} \subseteq \overline{\overline{A}} = \overline{A}. \Box$$

Exemplul 3.12 *Ordinile infix, hipercod, masking şi prefix-masking, satisfac ipoteza Propoziţiei 3.11.*

Prin expresia "pentru aproape toţi $n \in \mathbf{N}$", vom înţelege "există o mulţime finită $A \subseteq \mathbf{N}$, astfel încât $n \in \mathbf{N} \setminus A$".

Definiţie 3.13 *a) O mulţime $A \subseteq X^*$ se numeşte aproape densă, dacă $\overline{A} = X^*$ aproape peste tot (adică $X^* \setminus \overline{A}$ este finită).*

b) O mulţime $A \subseteq X^*$ se numeşte aproape rară, dacă pentru aproape toţi $x \in X^*$ există y (care depinde de x) astfel încât $U_y \cap A = \emptyset$.

c) O mulţime $A \subseteq X^*$ se numeşte aproape recursiv rară, dacă există o funcţie recursivă $r : \mathbf{N} \longrightarrow \mathbf{N}$ astfel încât:

c1) $string(n) \preceq string(r(n))$,

c2) $U_{string(r(n)))} \cap A = \emptyset$,

pentru aproape toţi $n \in \mathbf{N}$.

Observaţia 3.14 *a) Orice mulţime aproape recursiv rară este aproape rară;*

b) orice mulţime (recursiv) rară este aproape (recursiv) rară;

c) orice mulţime densă este aproape densă;

d) există mulţimi aproape dense care nu sunt dense;

e) există mulţimi aproape recursiv rare care nu sunt recursiv rare.

Observaţia 3.15 *Mulţimea recursiv rară din Definiţia 1 din Zimand [38] este în cazul de faţă între mulţimea aproape recursiv rară şi mulţimea recursiv rară.*

Teorema 3.16 *(Câmpeanu [12]) Dacă $\preceq$ este nemărginită, atunci orice mulţime aproape densă este densă, şi orice mulţime aproape (recursiv) rară este (recursiv) rară.*

Demonstraţie. Fie $\overline{A} = X^*$ aproape peste tot şi $\overline{A} \neq X^*$. Atunci

$$X^* \setminus \overline{A} = \{x_1, x_2, \cdots, x_n\},\ n > 0.$$

Fie $m = max\{l(x_i) | 1 \leq i \leq n\} + 1$, deci pentru fiecare x_i putem găsi un $z_i \in X^*$, $x_i \preceq z_i$ şi $l(z_i) > m$. Deoarece $l(z_i) > m$, atunci $z_i \in \overline{A}$, deci $x_i \in \overline{A}$, o contradicţie, deci dacă $\overline{A} = X^*$ a.p.t. atunci $\overline{A} = X^*$.

Fie A astfel încât dacă $x \notin \{x_1, x_2, \cdots, x_n\}$ atunci, există z astfel încât $x \preceq z$ şi $A \cap U_z = \emptyset$. Fie $x_0 = x_i$, $1 \leq i \leq n$. Relaţia $\preceq$ este nemărginită, deci luînd $m = max\{l(x_i) | 1 \leq i \leq n\} + 1$, atunci există un w, cu $l(w) > m$ şi $x_0 \preceq w$. De aici $w \notin \{x_1, x_2, \cdots, x_n\}$, deci $A \cap U_w = \emptyset$ şi $x_0 \preceq w$.

Fie A astfel încât există o funcţie recursivă $r : \mathbf{N} \longrightarrow \mathbf{N}$, cu proprietatea că, dacă $x = string(u) \notin \{x_1, x_2, \cdots, x_n\}$, atunci

$$string(u) \preceq string(r(u)) \text{ şi } A \cap U_{string(r(u))} = \emptyset.$$

Luăm din nou $m = max\{l(x_i)|1 \le i \le n\} + 1$. Deoarece $\preceq$ este nemărginită, funcţia $s : \mathbf{N} \longrightarrow \mathbf{N}$ definită prin

$$s(u) = min\{q \in \mathbf{N}|string(u) \preceq string(q),\, m < l(string(q))\}$$

este recursivă şi pentru toţi $u \in \mathbf{N}$

$$string(u) \preceq string(r \circ s(u)),\, A \cap U_{string(r \circ s(u))} = \emptyset. \square$$

Teorema 3.17 *(Câmpeanu [12]) a) Dacă $\preceq$ este o relaţie de ordine (recursivă) mărginită pe X^*, astfel încât pentru orice $w \in X^*$,*

$$card\{x \in X^*|x \preceq w\} < \infty, \tag{3.1}$$

atunci există mulţimi aproape (recursiv) rare care nu sunt (recursiv) rare.

b) Dacă $\preceq$ este mărginită pe X^*, atunci există mulţimi aproape dense, care nu sunt dense.

Demonstraţie. Deoarece $\preceq$ este mărginită, există măcar un cuvânt w $w \in X^*$, astfel încât w este maximal în raport cu $\preceq$. Luăm $A = w$ şi $B = X^* \setminus A$. Se arată uşor că A este aproape rară, dar nu este rară şi B este aproape densă, dar nu este densă (pentru punctul b) condiţia 3.1 nu este necesară). $\square$

Observaţia 3.18 *În teorema anterioară este suficient să cerem ca $\preceq$ să aibă cel puţin un element maximal ce satisface 3.1, în loc de $\preceq$ mărginită.*

Exemplul 3.19 *a) Dacă $\preceq$ este definită prin $x \preceq x$, $x \preceq \lambda$, oricare ar fi $x \in X^*$, atunci mulţimea $A = \{\lambda\}$ este densă şi aproape rară în $\tau(\preceq)$ şi $B = X^* \setminus A$ este recursiv rară şi aproape densă.*

b) Fie $N \in \mathbf{N}$. Dacă $\preceq$ este definită prin $x \preceq x$, $x \preceq \lambda$, oricare ar fi $x \in X^*$, $l(x) < N$, atunci mulţimea $A = \{\lambda\}$ este aproape rară dar nu este rară în $\tau(\preceq)$ şi $B = X^* \setminus A$ este aproape densă şi nu este densă.

c) Ordinea anti-lexicografică $\preceq_{al}$

$$x \preceq_{al} y \;\Leftrightarrow\; y \preceq_l x,$$

nu satisface condiţia 3.1, dar este mărginită (λ este cel mai mare element). Aici, orice mulţime aproape recursiv rară este recursiv rară.

d) Ordinea prefix satisface condiţia 3.1, dar nu este mărginită.

3.2 Topologii pe mulţimea numerelor naturale

Fie $\preceq$ o relaţie de ordine pe $\mathbf{N}$ şi considerăm relaţia de ordine corespunzătoare din $number_p(\mathbf{N})$. $number_p(x) \preceq^p number_p(y)$ dacă şi numai dacă $x \preceq y$. În $\mathbf{N}$ considerăm mulţimile $U_x = \{y \in \mathbf{N} | x \preceq y\}$. Acestea, ca şi în cazul cuvintelor, constituie o bază de topologie pentru topologia generată de relaţia de ordine "$\preceq$". O relaţie de ordine $\preceq$ este nemărginită, dacă oricare ar fi baza de numeraţie q, oricare ar fi $x \in \mathbf{N}$ şi oricare ar fi $n \in \mathbf{N}$, există $y \in \mathbf{N}$ astfel încât $x \preceq y$ şi $l_q(y) > n$.

Exemplul 3.20 *Fixăm alfabetul X. Următoarele relaţii sunt relaţii de ordine recursive şi nemărginite: (utilizăm $number_p(w) = w_1 w_2 \cdots w_n$, $l_p(w) = n$, şi $number_p(v) = v_1 v_2 \cdots v_m$, $l_p(v) = m$):*

(1) $w \preceq_p v$ ddacă $w = v$ sau există $u \in \mathbf{N}$, $number_p(v) = number_p(w) number_p(u)$ (ordinea prefix),

(2) $w \preceq_s v$ ddacă $w = v$ sau există $u \in \mathbf{N}$, $number_p(v) = number_p(u) number_p(w)$ (ordinea suffix),

(3) $w \preceq_i v$ ddacă $w = v$ sau există $u, x \in \mathbf{N}$, $number_p(v) = number_p(u) number_p(w) number_p(x)$ (ordinea infix),

(4) $w \preceq_h v$ ddacă $w = v$ sau există $u_1, \cdots u_{n+1} \in \mathbf{N}$, $number_p(v) = number_p(u_1)\ w_1\ number_p(u_2) \cdots number_p(u_n)\ w_n\ number_p(u_{n+1})$ (ordinea hipercod),

(5) $w \preceq_m v$ ddacă $m \geq n$ şi $w_{n-i} \leq v_{m-i}$, pentru orice $0 \leq i \leq n-1$ (ordinea masking),

(6) $w \preceq_{pm} v$ ddacă $l(w) \leq l(v)$ şi $w_i \leq v_i$, pentru toţi $1 \leq i \leq l(w)$ (ordinea prefix-masking),

(7) $w \preceq_d v$ ddacă $w \preceq_p v$ şi $w \preceq_s v$ (ordinea 2-ps-coduri),

(8) $w \preceq_l v$ ddacă $w \preceq_p v$ sau există $x \in \mathbf{N}, y, z \in X^*$, $number_p(w) = x a_i y$, $number_p(v) = x a_j z$ cu $i < j$, (ordinea lexicografică),

(9) $w \preceq_l v$ ddacă există $x \in \mathbf{N}$ cu $v = x \cdot w$ (ordinea dată de divizibilitate).

Observaţia 3.21 *Relaţiile (1)-(8) din exemplul anterior sunt introduse asemănător ca cele pe X^* din Exemplul 3.1, dar nu sunt neapărat imaginea prin $number_p^{-1}$ a relaţiilor induse pe $number_p(\mathbf{N})$.*

Exemplul 3.22 *(Câmpeanu [14]) Dacă $\preceq$ este o relaţie de ordine recursivă (nemărginită) pe* $\mathbf{N}$ *şi* $f : \mathbf{N} \longrightarrow \mathbf{N}$ *este o funcţie recursivă bijectivă, atunci relaţia de ordine parţială definită prin:* $x \preceq_f y$ *ddacă* $f(x) \preceq f(y)$*, este recursivă (nemărginită).*

Exemplul 3.23 *Pentru* $x, y \in \mathbf{N}$ *spunem că* $x \preceq_t y$ *dacă* $x = y$*, sau există* $x' \preceq_p x$*,* $y' \preceq_p y$*,* $x \neq x'$*,* $y \neq y'$*,* $l_p(x') = l_p(y')$ *şi* $x' \preceq_l y'$*,* $x' \neq y'$*.*

Observaţia 3.24 *De exemplu,* $number_p^{-1}(a_2a_1a_1a_1) \preceq_t number_p^{-1}(a_2a_2)$*, dar* $number_p^{-1}(a_2)$ *şi* $number_p^{-1}(a_2a_1a_2)$ *sunt incomparabile; mai mult,* $\preceq_t$ *este o relaţie de ordine recursivă mărginită şi pentru orice* $n \in \mathbf{N}$ *este totală pe* $number_p^{-1}(X^n)$*.*

La fel ca pentru cuvinte, topologia generată de aceste relaţii de ordine este un spaţiu T_0 care nu este T_1 (în cazurile netriviale). Calculînd închiderea unei mulţimi A în acest spaţiu obţinem: $\overline{A} = \{x \in \mathbf{N} |\text{ există } z \in A,\ x \preceq z\}$. La fel ca în cazul cuvintelor avem că, pentru $A \subseteq \mathbf{N}$ şi $w \in \mathbf{N}$, următoarele trei afirmaţii sunt echivalente:

(i) $A \cap U_w = \emptyset$,
(ii) $\overline{A} \cap U_w = \emptyset$,
(iii) $w \notin \overline{A}$.

Demonstraţia este imediată (urmăm aceiaşi paşi ca în cazul cuvintelor).

O mulţime este densă dacă $\overline{A} = \mathbf{N}$.

Definiţie 3.25 *O mulţime* $A \subseteq \mathbf{N}$ *se numeşte recursiv rară, dacă există o funcţie recursivă* $r : \mathbf{N} \longrightarrow \mathbf{N}$*, astfel încât următoarele două condiţii sunt adevărate pentru toţi* $n \in \mathbf{N}$*:*

1) $n \preceq r(n)$*,*
2) $A \cap U_{r(n)} = \emptyset$*.*

Propoziţia 3.26 *Presupunem că* $\preceq$ *este recursivă şi nemărginită. O mulţime* $A \subseteq \mathbf{N}$ *este recursiv rară dacă şi numai dacă există o funcţie recursivă* $f : \mathbf{N} \longrightarrow \mathbf{N}$ *şi un număr natural* i*, astfel încât* $n \preceq f(n)$*, pentru toţi* $n \in \mathbf{N}$ *şi* $U_{f(n)} \cap A = \emptyset$*, pentru toţi* n *cu* $n > i$*.*

Demonstraţie. Similar cu demonstraţia Propoziţiei 3.7, luînd $q : \mathbf{N} \longrightarrow \mathbf{N}$, definită prin

$$q(n) = min\{m \geq 0 | n \preceq m \text{ şi } m > i\}$$

şi $r = f \circ q$. □

Teorema 3.27 *(Câmpeanu [14]) Presupunem că $\preceq$ este recursivă şi nemărginită şi în plus că există o funcţie recursivă $s : \mathbf{N} \longrightarrow \mathbf{N}$ astfel încât:*

(**) dacă pentru orice $i, j \in \mathbf{N}$ există x astfel ca $s(i) \preceq x$ şi $s(j) \preceq x$, atunci $i = j$;

atunci există o mulţime rară care nu este recursiv rară.

Demonstraţie. Paşii demonstraţiei sunt aceiaşi cu cei din Teorema 3.8, mulţimea

$$A = \{string(t_n) | n \geq 0\},$$

unde t_n este definit doar pentru $\phi_n(n) \neq \infty$ şi

$$t_n = min\{j \in \mathbf{N} | s(n) \preceq j, j \geq s(n) + \phi_n(n)\},$$

fiind rară, dar nu şi recursiv rară. □

Exemplul 3.28 *(a) Ordinile sufix şi prefix satisfac ipoteza Teoremei 3.27. Spre exemplu, pentru ordinea sufix putem să luăm $s(i) = a_1 a_2^i$.*

(b) Dacă $\preceq$ este parţial recursivă şi nemărginită avînd proprietatea (**) în raport cu s, atunci relaţia de ordine $\preceq_f$ are aceeaşi proprietate pentru $f^{-1} \circ s$.

Propoziţia 3.29 *Presupunem că $\preceq$ este recursivă, nemărginită şi filtrantă la dreapta. Atunci*

(i) orice mulţime rară este recursiv rară,

(ii) orice mulţime care nu este rară este densă.

Demonstraţie. (i) Similar cu (i) din Propoziţia 3.11, luînd funcţia recursivă $f : \mathbf{N} \longrightarrow \mathbf{N}$,

$$f(n) = min\{i \in \mathbf{N} | z \preceq i \text{ şi } n \preceq i\}.$$

(ii) Similar cu (ii) din Propoziţia 3.11. □

Exemplul 3.30 *Ordinile infix, hipercod, masking şi prefix-masking, satisfac ipoteza Propoziţiei 3.29.*

Definiţie 3.31 *a) O mulţime $A \subseteq \mathbf{N}$ se numeşte aproape densă, dacă închiderea sa $\overline{A} = \mathbf{N}$ aproape peste tot (adică $\mathbf{N} \setminus \overline{A}$ este finită).*

b) O mulţime $A \subseteq \mathbf{N}$ se numeşte aproape rară dacă pentru aproape toţi $x \in \mathbf{N}$ există y (care depinde de x) astfel încât $U_y \cap A = \emptyset$.

c) O mulţime $A \subseteq \mathbf{N}$ se numeşte aproape recursiv rară dacă există o funcţie recursivă $r : \mathbf{N} \longrightarrow \mathbf{N}$ astfel încât:

c1) $n \preceq r(n)$,

c2) $U_{r(n)} \cap A = \emptyset$,

pentru aproape toţi $n \in \mathbf{N}$.

Observaţia 3.32 *a) Orice mulţime aproape recursiv rară este aproape rară;*

b) orice mulţime (recursiv) rară este aproape (recursiv) rară;

c) orice mulţime densă este aproape densă;

d) există mulţimi aproape dense care nu sunt dense;

e) există mulţimi aproape recursiv rare care nu sunt recursiv rare.

Teorema 3.33 *(Câmpeanu [14]) Dacă $\preceq$ este nemărginită atunci orice mulţime aproape densă este densă şi orice mulţime aproape (recursiv) rară este (recursiv) rară.*

Demonstraţie. Similar cu demonstraţia Teoremei 3.16. □

Teorema 3.34 *(Câmpeanu [14]) a) Dacă $\preceq$ este mărginită pe $\mathbf{N}$, astfel încât pentru orice $w \in \mathbf{N}$,*

$$card\{x \in \mathbf{N} | x \preceq w\} < \infty, \tag{3.2}$$

atunci există mulţimi aproape (recursiv) rare, care nu sunt (recursiv) rare;

b) Dacă $\preceq$ este mărginită pe $\mathbf{N}$, atunci există mulţimi aproape dense care nu sunt dense.

Demonstraţie. Similar cu demonstraţia Teoremei 3.17. □

Exemplul 3.35 *Dacă $\preceq$ este definită prin $x \preceq 0$, oricare ar fi $x \in \mathbf{N}$, atunci mulţimea $A = \{0\}$ este densă şi aproape rară în $\tau(\preceq)$ şi $B = \mathbf{N} - A$ este recursiv rară şi aproape densă.*

4

Extensii (aleatoare) ale cuvintelor (numerelor) (aleatoare)

În acest capitol vom obţine principalele rezultate de natură topologică privind cuvintele şi numerele naturale aleatoare. Arătăm că mulţimile de cuvinte şi numere ne-aleatoare sunt dense în raport cu relaţiile de ordine nemărginite (Corolarul 4.2, Corolarul 4.18, Corolarul 4.22). Studiem mărimea topologică a mulţimii cuvintelor aleatoare Chaitin-Kolmogorov şi a numerelor aleatoare în raport cu diverse relaţii de ordine (mărginite şi nemărginite) (Corolarul 4.5, Propoziţia 4.6, Propoziţia 4.7, Teorema 4.12). Aceste rezultate arată că, dacă avem un cuvânt şi îl prelungim doar într-o singură parte (la stânga sau la dreapta), găsim un cuvânt pentru care nici o altă prelungire în acelaşi sens nu este cuvânt aleator, dar dacă prelungim cuvântul în ambele direcţii, în mod sigur vom obţine un cuvânt aleator (Teorema 4.12). Această problemă, pentru numere naturale, nu este rezolvată decât în sensul următor: orice număr natural poate fi prelungit cu alt număr natural, astfel încât nici o prelungire în aceeaşi direcţie nu este un număr aleator (Teorema 4.25). În final vom arăta că, în raport cu anumite relaţii de ordine, complexităţile Chaitin şi Chaitin-Kolmogorov se comportă identic (Teorema 4.19 şi Teorema 4.20).

4.1 Extensii pentru cuvinte

Teorema 4.1 *(Calude, Câmpeanu [5]) Fie $\preceq$ o relaţie de ordine recursivă şi nemărginită. Atunci există o constantă naturală $c > 0$, astfel încât pentru orice numere naturale m şi d, cu $d \geq c$, mulţimea*

$$A(m,d) = \{x \in X^* |\, l(x) \geq m,\ K(x|l(x)) \leq d\}$$

este densă.

Demonstraţie. Definim funcţia recursivă $f : \mathbf{N} \to \mathbf{N}$ prin

$$f(n) = min\{i \geq 0 | l(string(i)) \geq n, string(n) \preceq string(i)\}.$$

Notăm

$$B(m) = \{string(f(n)|n \geq m\}$$

şi construim funcţia parţial recursivă $\phi : X^* \times \mathbf{N} \stackrel{\circ}{\to} X^*$,

$$\phi(x, l(string(f(n)))) = string(f(n)), \text{ pentru toţi } x \in X^* \text{ şi } n \geq m.$$

Este clar că

$$K_\phi(string(f(n))|l(string(f(n)))) = 0,$$

pentru toţi $n \geq m$; deci conform Teoremei de Invarianţă, există o constantă $c > 0$ astfel încât

$$K(string(f(n)|l(string(f(n)))) \geq c,$$

pentru toţi $n \geq m$.

În continuare, vom arăta că pentru orice $d \geq c$, $B(m) \subseteq A(m,d)$.

Într-adevăr, dacă $n \geq m$, atunci

$$l(string(f(n)) \geq n \geq m \text{ şi } K(string(f(n))|l(string(f(n)))) \leq c \leq d.$$

În final, pentru a arăta că $\overline{B(m)} = X^*$, demonstrăm că pentru orice $x \in X^*$, există $n \geq m$ astfel încât

$$x \preceq string(f(n)).$$

Distingem două cazuri:

1. Dacă $x = string(k)$, $k \geq m$, luăm $n = k$ (deoarece $x \preceq string(f(k))$, $k \geq m$).

2. Dacă $x = string(k)$ cu $k < m$, atunci luăm $string(i)$ cu $x \preceq string(i)$ şi $l(string(i)) \geq m$:

$$x \preceq string(i) \preceq string(f(i)) \text{ şi } i \geq m. \square$$

Corolar 4.2 *(Calude, Câmpeanu [5]) Mulţimea* $non - RAND_t^K$ *este densă în orice topologie generată de relaţii de ordine recursive nemărginite pe* X^*.

Demonstraţie. Pentru orice $d \geq 0$,

$$A(1 + d + t, d) \subseteq non - RAND_t^K$$

(aici $A(1 + d + t, d)$ este mulţimea din Teorema 4.1). Luăm $d \geq c$, unde c este cel din Teorema 4.1. $\square$

Observaţia 4.3 *a) Un rezultat mai puternic decât cel de mai sus poate fi uşor obţinut: pentru orice funcţie* $f : \mathbf{N} \longrightarrow \mathbf{N}$, *crescătoare şi nemărginită nu neapărat recursivă, mulţimea* $T(f) = \{x \in X^* | K(x|l(x)) \leq f(l(x))\}$ *este densă. Într-adevăr, luînd* D *astfel încât* $f(m) > d$ *de îndată ce* $m \geq D$ *(aici* d *este din Teorema 4.1), dacă* $x \in X^*$, $l(x) \geq D$, *atunci* $f(l(x)) > d$; *deci,* $A(D, d) \subseteq T(f)$ *ş.a.m.d.*

b) Putem să interpretăm Corolarul 4.2 după cum urmează: orice secţiune a unui test universal Martin-Löf $V(\psi)$ *este densă; pentru detalii, trimitem la Calude, Chiţescu, Staiger [9] şi Calude [2].*

Deci, orice mulţime $non - RAND_t^K$ este "mare" în raport cu toate topologiile considerate în Exemplele 3.1 şi 3.2 (pentru $\preceq$ nemărginite). Vom trece la studiul lui $RAND_t^K$. O verificare imediată ne conduce la :

Lema 4.4 *(Calude, Câmpeanu [5]) O mulţime* $A \subseteq X^*$ *este rară (recursiv rară, densă) în* $\tau(\preceq)$ *dacă şi numai dacă* $f(A) = \{f(x) | x \in A\}$ *este rară (recursiv rară, densă) în* $\tau(\preceq_f)$, *unde* $f : X^* \longrightarrow X^*$ *este recursivă şi bijectivă.*

Corolar 4.5 *(Calude, Câmpeanu [5]) Pentru orice* $t \geq 0$, $RAND_t^K$ *este recursiv rară în* $\tau(\preceq_p)$, $\tau(\preceq_s)$, $\tau(\preceq_d)$.

Demonstraţie. Prima parte se găseşte în Zimand [38], Teorema 4; următoarea rezultă din Lema 4.4 şi Exemplul 3.2. Pentru cea de a treia parte, fie rs şi rp funcţiile recursive ce satisfac Definiţia 3.6(1) şi 3.6(2) pentru $RAND_t^K$ în $\tau(\preceq_p)$ şi respectiv $\tau(\preceq_s)$; funcţia recursivă

$$r(n) = min\{k \geq 0 | string(rp(n)) \preceq_p string(k) \text{ şi } string(rs(n)) \preceq_s string(k)\}$$

va funcţiona pentru $RAND_t^K$ în $\tau(\preceq_d)$. □

Propoziţia 4.6 *Pentru orice $t \geq 0$, $RAND_t^K$ este recursiv rară în $\tau(\preceq_m)$.*

Demonstraţie. Definim funcţia recursivă $f : \mathbf{N} \longrightarrow \mathbf{N}$ prin $string(f(n)) = a_p^{l(string(n))}$ şi funcţia parţial recursivă $\phi : X^* \times \mathbf{N} \xrightarrow{\circ} X^*$,

$$\phi(x, n) = a_p^{n \dot{-} l(x)} x, \text{ în cazul } n \geq l(x).$$

Fie $i > t + c$, unde c este constanta din Teorema de Invarianţă aplicată lui ψ şi ϕ. Să notăm că $string(n) \preceq_m string(f(n))$; orice cuvânt $w \in U_{string(f(n))}$ cu $l(string(n)) > i$, poate fi scris ca $w = xstring(f(n))$, $x \in X^*$.

Avem

$$K(w|l(w)) \leq K_\phi(w|l(w)) + c \leq l(w) - l(string(f(n))) + c =$$

$$l(w) - l(string(n)) + c < l(w) - l(string(n)) + i - t < l(w) - t;$$

deci $w \notin RAND_t^K$, adică $U_{string(f(n))} \cap RAND_t^K = \emptyset$. Utilizînd Propoziţia 3.7 obţinem rezultatul dorit. □

Propoziţia 4.7 *Pentru orice $t \geq 0$, $RAND_t^K$ este recursiv rară în $\tau(\preceq_{pm})$.*

Demonstraţie. Utilizăm funcţia parţial recursivă $\phi : X^* \times \mathbf{N} \xrightarrow{\circ} X^*$,

$$\phi(x, n) = a_p^{n - l(x)} x, \text{ în cazul } n \geq l(x),$$

într-o construcţie similară cu cea din Propoziţia 4.6. □

Lema 4.8 *(Calude, Câmpeanu [5]) Presupunem că $\preceq$ este o relaţie de ordine recursivă pe X^*. Fie $A \subseteq X^*$. Dacă pentru orice $x \in X^*$ putem găsi un număr natural m şi un cuvânt w, astfel ca*

$$x \preceq w \text{ şi } card\{y \in X^* \mid l(y) = m, \, w \preceq y\} > card\{z \in X^* \mid l(z) = m, z \notin A\},$$

atunci A este densă.

Demonstraţie. Fiind dat un cuvânt x putem găsi m şi w cu proprietăţile de mai sus. Deci există $y \in A$, cu $w \preceq y$. Deoarece $x \preceq w$, rezultă că $x \preceq y$, adică $x \in \overline{A}$. □

Corolar 4.9 *(Calude, Câmpeanu [5]) Fie $t \geq 0$. Dacă pentru orice cuvânt x există un m şi un cuvânt w astfel încât*

$$x < w \text{ şi } card\{y \in X^* | l(y) = m, \, w \preceq y\} \cdot (p-1) \geq p^{m-t},$$

atunci $\overline{RAND_t^K} = X^*$.

Demonstraţie. Este cunoscut (v. Calude [2]) că

$$\text{card}\{y \in X^* | l(y) = m, K(y|m) < m - t\} \leq (p^{m-t} - 1)/(p-1). \,\square$$

Un cuvânt $x \in X^*$ se numeşte nebordurat dacă nu se poate scrie sub forma $x = yzy$, cu $y \in X^*$, $y \neq \lambda$.

Fapt 4.10 *(Calude, Chiţescu [7]) Fie x un cuvânt nebordurat de lungime $n \geq 3$. Fie $m \in \mathbf{N}$. Notăm*

$$R(m, x) = p^m \cdot card\{y \in X^* | l(y) = m, \, x \preceq_i y\}.$$

Atunci avem

$$\begin{array}{ll} R(m, x) = p^m, & 0 \leq m < n, \\ R(m+1, x) = p \cdot R(m, x) - R(m+1-n, x), & m \geq n. \end{array}$$

Fapt 4.11 *(Calude, Chiţescu [7]) Pentru orice cuvânt nebordurat x de lungime $n \geq 3$, există $M \in \mathbf{N}$, astfel încât pentru orice $m \geq M$,*

$$R(m^2, x) < \frac{p^{m^2-m}}{p-1}.$$

Teorema 4.12 *(Calude, Câmpeanu [5]) Mulţimea $RAND_t^K$ este densă în raport cu ordinea infix, în cazul în care $t > 0$ sau alfabetul conţine cel puţin trei elemente.*

Demonstraţie. Fie $x \in X^*$. Construim cuvântul nebordurat

$$v(x) = a_1^{l(x)} x a_2^{l(x)},\ x \preceq_i v(x).$$

Vom arăta că există un număr natural m astfel încât

$$\text{card}\{y \in X^* | l(y) = m,\ y \preceq_i v(x)\} \cdot (p-1) \geq p^{m-t},$$

adică, exact condiţia din Corolarul 4.9 pentru ca $RAND_t^K$ să fie densă.

Din Faptul 4.11 rezultă că, pentru orice $i \geq M$,

$$R(i^2, v(x)) < \frac{p^{i^2-i}}{p-1}.$$

Luăm $m \geq \max(M, t)$. Inegalitatea cerută devine

$$\frac{p^{m^2-m}}{p-1} \leq p^{m^2} \cdot \left(1 - \frac{1}{p^t \cdot (p-1)}\right),$$

care este adevărată în cazul $p > 2$ sau $t > 0$. $\square$

Problema dacă Teorema 4.12 este sau nu adevărată în cazul binar pentru $t = 0$, a fost soluţionată de G. Chaitin (v. Calude [3]). În continuare vom schiţa soluţia lui Chaitin în general, menţionînd că nu avem cunoştinţă de o demonstraţie topologică uniformă. Este de remarcat faptul că această soluţie pare, la prima vedere, foarte simplă. Ea însă se bazează pe proprietatea de normalitate Borel a cuvintelor aleatoare (Calude [3]), rezultat care se obţine cu o demonstraţie foarte lungă şi tehnică. Mai mult, demonstraţia care urmează este "indirectă", ascunzînd fenomenul topologic descris mai sus.

Teorema 4.13 *Mulţimea $RAND_t^K$ este densă în raport cu ordinea infix.*

Demonstraţie. Folosim Definiţia 2.3 şi Teorema 2.6. Fixăm $x \in X^*$, $l(x) = i$. Aproape toate cuvintele $z \in RAND_t^K$ sunt Borel normale (Teorema 2.6), adică ele satisfac inegalitatea

$$\left| \frac{N_j^m(z)}{\lfloor n/m \rfloor} - p^{-m} \right| \leq \sqrt{\frac{\log_p n}{n}},$$

oricare ar fi $1 \leq j \leq p^m, 1 \leq m \leq \log_p \log_p n$; $n = l(z)$.

Luăm $m = i$, x al j-lea cuvânt de lungime i şi un cuvânt $z \in RAND_t^K$ de lungime $n = p^{p^{2i+1}}$. Rezultă că

$$\left| \frac{N_j^i(z)}{\lfloor n/i \rfloor} - p^{-i} \right| \leq \sqrt{\frac{\log_p n}{n}},$$

în particular,

$$p^{-i} - \sqrt{\frac{\log_p n}{n}} \leq \frac{N_j^i(z)}{\lfloor n/i \rfloor}.$$

Pentru a arăta că $N_j^i(z) > 0$, este suficient să arătăm că

$$p^{-i} > \sqrt{\frac{\log_p n}{n}},$$

care este adevărat, deoarece avem implicaţiile:

$$4^i + 4 > 4i + 1 \Rightarrow p^{2i+1} > 4i + 1 \Rightarrow p^{2i+1-2i} > 2i + 1 \Rightarrow$$

$$p^{p^{2i+1}} \cdot p^{-2i} > p^{2i+1} \Rightarrow n \cdot p^{-2i} > \log_p n \Rightarrow p^{-i} > \left(\frac{\log_p n}{n} \right)^{\frac{1}{2}}. \square$$

Corolar 4.14 *(Calude, Câmpeanu [5]) Pentru orice $t \geq 0$, $RAND_t^K$ este densă în raport cu topologiile generate de ordinea uniformă şi de ordinea hipercod.*

Demonstraţie. Dacă $w \preceq_i v$, atunci $w \preceq_u v$ ($w = v$ sau $l(w) < l(v)$) şi $w \preceq_h v$. $\square$

Teorema 4.15 *(Câmpeanu [12]) Considerăm $\preceq$ relaţie de ordine recursivă şi nemărginită. Atunci mulţimea non $- R_t^C$ este densă în X^*, în raport cu $\tau(\preceq)$.*

Demonstraţie. Fie $x \in X^*$ şi considerăm următorul calculator Chaitin:

$$C(a_2^n a_1, \lambda) = string(q(n)),$$

unde

$$q(n) = \min\{m \in \mathbf{N} | l(string(m)) \geq l(x) + 2 \cdot (n+1), x \preceq string(m),$$
$$string(m) \neq string(q(i)), \text{ pentru toţi } i < n\}.$$

Este uşor de văzut că

$$H_C(string(q(n)) = l(a_2^n a_1) < l(string(q(n))) - l(x) - n.$$

Utilizînd Teorema de Invarianţă, obţinem un număr natural $sim(C)$, astfel încât $H(z) \leq H_C(z) + sim(C)$ pentru toţi $z \in X^*$, deci

$$H(string(q(n))) < l(string(q(n))) - l(x) - n + sim(C).$$

Luînd $n > t + sim(C)$, rezultă că

$$H(string(q(n))) < l(string(q(n))) - l(x) - t - sim(C) + sim(C) \leq$$

$$l(string(q(n))) - t - l(x) \leq l(string(q(n))) - t,$$

deci

$$string(q(n)) \in non - R_t^C \text{ şi } x \preceq string(q(n)). \square$$

Corolar 4.16 *(Calude [3]) Dacă $\preceq$ este o relaţie de ordine recursivă şi nemărginită, atunci mulţimea $non - RAND_t^C$ este densă în raport cu $\tau(\preceq)$.*

Demonstraţie. Deoarece

$$non - R_t^C \subseteq non - RAND_t^C$$

şi $non - R_m^C$ este densă în $\tau(\preceq)$ pentru orice $m \geq 0$ (din Teorema 4.15), rezultă $non - RAND_t^C$ este densă în raport cu $\tau(\preceq)$. $\square$

Teorema 4.17 *(Câmpeanu [12]) Fie $\preceq$ o relaţie de ordine parţială recursivă, cu următoarea proprietate:*

$$\sum_{x \preceq w} p^{-l(w)} > 1, \text{ pentru orice } w \in X^*. \tag{4.1}$$

Atunci R^C este densă în raport cu topologia $\tau(\preceq)$.

Demonstraţie. Presupunem că R^C nu este densă. Atunci există $x \in X^*$, astfel ca $U_x \cap R^C = \emptyset$. Deoarece $l(v) > l(v^*)$ pentru toţi $x \preceq v$, avem:

$$\sum_{x \preceq v,\, l(v^*) \geq l(v)} p^{-l(v)} = 0. \tag{4.2}$$

(Suma este peste mulţimea vidă.)

Deoarece

$$\sum_{w \in \mathrm{dom} U_\lambda} p^{-l(w)} \leq 1,$$

avem inegalitatea:

$$S = \sum_{x \preceq v,\, l(v^*) < l(v)} p^{-l(v^*)} \leq 1. \tag{4.3}$$

Din $l(v^*) < l(v)$, deducem că

$$p^{-l(v^*)} < p^{-l(v)},$$

deci

$$S = \sum_{x \preceq v,\, l(v^*) < l(v)} p^{-l(v^*)} \geq \sum_{x \preceq v,\, l(v^*) < l(v)} p^{-l(v)} = \sum_{x \preceq v} p^{-l(v)} > 1,$$

în contradicţie cu (4.3). □

Corolar 4.18 *(Câmpeanu [12]) R_t^C este densă în X^* în raport cu toate topologiile generate de relaţiile din Exemplul 3.1.*

Demonstraţie. Deoarece $\preceq_d \subseteq \preceq_x$ pentru $x \in \{p, s, i, h, pm, l\}$ şi $R^C \subseteq R_t^C$ oricare ar fi $t \in \mathbf{N}$, este suficient să verificăm condiţia 4.1 din Teorema 4.15 doar pentru $\preceq_d$ şi $\preceq_m$:

$$\sum_{x \preceq_d w} p^{-l(w)} \geq \sum_{v \in X^*} p^{-l(xvx)} = \left(\sum_{v \in X^*} p^{-l(v)} \right) / p^{2 \cdot l(x)} = \infty$$

$$\sum_{x \preceq_m w} p^{-l(w)} \geq \sum_{v \in X^*} p^{-l(v a_p x)} = \left(\sum_{v \in X^*} p^{-l(v)} \right) / p^{l(x)+1} = \infty. \ \square$$

Teorema 4.19 *(Câmpeanu [12]) a) Mulţimea $non - RAND_t^K$ este aproape densă $\tau(\preceq_t)$ în X^*.*

b) Mulţimea $non - R_t^C$ este aproape densă $\tau(\preceq_t)$ în X^*.

Demonstraţie. a) Fie funcţia parţial recursivă $\phi : X^* \times \mathbf{N} \overset{\circ}{\longrightarrow} X^*$, definită prin $\phi(x, n) = a_p^n$.

$$K_\phi(x|l(x)) = 0, \text{ dacă } x = a_p^{l(x)} \text{ şi } K_\phi(x|l(x)) = \infty, \text{ altfel.}$$

Utilizînd Teorema de Invarianţă, obţinem o constantă c cu proprietatea:

$$K_(a_p^n|n) \leq K_\phi(a_p^n|n) + c.$$

De aici, dacă $l(x) > c + m$, atunci

$$x \preceq_t a_p^{l(x)} \text{ şi } a_p^{l(x)} \in non - RAND_m^K.$$

b) Considerăm următorul calculator Chaitin $C(a_2^n a_1, \lambda) = w_n$, unde

$$w_n = a_p^{2n+2+m}.$$

Evident,

$$H_C(w_n) = n + 1 < l(w_n) - n - m.$$

Utilizînd Teorema de Invarianţă, găsim o constantă naturală c astfel încât

$$H(w_n) \leq H_C(w_n) + c < l(w_n) - n - m + c \text{ pentru toţi } n \in \mathbf{N}.$$

De aici, dacă $n > c + 1$, pentru orice $x \in X^n$, $x \preceq_t w_n$ şi $w_n \in non - R_m^C$. $\square$

Teorema 4.20 *(Câmpeanu [12]) a) Mulţimea $RAND_m^K$ este aproape recursiv rară $\tau(\preceq_t)$ în X^*, dar nu este rară.*

b) Mulţimea R_m^C este aproape recursiv rară $\tau(\preceq_t)$ în X^*, dar nu este rară.

Demonstraţie. Am demonstrat deja că există un număr natural n_0, astfel încât pentru orice $n \geq n_0$, $a_p^n \notin RAND_m^K$ şi $a_p^n \notin R_m^C$.

Considerăm acum că funcţia recursivă $r : \mathbf{N} \longrightarrow \mathbf{N}$,

$$string(r(n)) = a_p^{n_0+n}.$$

Deci, $string(n) \preceq_t string(r(n))$ pentru orice $n > 0$.

Deoarece
$$U_{string(r(n))} = \{string(r(n))\},$$
rezultă că
$$U_{string(r(n))} \cap RAND_m^K = \emptyset \text{ şi } U_{string(r(n))} \cap R_m^C = \emptyset \text{ pentru orice } n > 0;$$
prin urmare, atât $RAND_m^K$ cât şi R_m^C sunt $\tau(\preceq_t)$ recursiv rare în X^*. Deoarece
$$RAND_m^K \cap \{a_p^n | n \geq 0\} \neq \emptyset,$$
nu există $w \in X^*$, astfel ca $U_w \cap RAND_m^K = \emptyset$, cu $a_p^n \preceq_t w$ şi $a_p^n \in RAND_m^K$, deci $RAND_m^K$ nu este rară.

O demonstraţie asemănătoare arată că R_m^C nu este rară. □

4.2 Extensii pentru numere

Teorema 4.21 *(Câmpeanu [14]) Fie $\preceq$ recursivă şi nemărginită. Atunci există o constantă naturală $c > 0$, astfel încât pentru orice numere naturale m şi d, cu $d \geq c$, mulţimea*
$$A^p(m,d) = \{x \in \mathbf{N} |\, l_p(x) \geq m,\ K(x|l(x)) \leq d\}$$
este densă.

Demonstraţie. Demonstraţia urmează aceiaşi paşi ca în Teorema 4.1; aici luăm $f : \mathbf{N} \to \mathbf{N}$,
$$f(n) = min\{i \geq 0 | l_p(i) \geq n, n \preceq i\},$$
în loc de $B(m)$, vom avea
$$B^p(m) = \{number_p(f(n)|n \geq m\}$$
şi $\phi : X^* \times \mathbf{N} \overset{\circ}{\to} \mathbf{N}$,
$$\phi(x, l_p(f(n))) = f(n), \text{ pentru toţi } x \in \mathbf{N} \text{ şi } n \geq m. \, \square$$

Corolar 4.22 *(Câmpeanu [14]) Mulţimea non$-RAND_t^p$ este densă în orice topologie generată de relaţii de ordine recursive nemărginite pe* $\mathbf{N}$.

Demonstraţie. Pentru orice $d \geq 0$,

$$A^p(1+d+t,d) \subseteq non - RAND_t^p.$$

(aici $A^p(1+d+t,d)$ este mulţimea din Teorema 4.21). Luăm $d \geq c$, unde c este cel din Teorema 4.21. □

Observaţia 4.23 *a) Un rezultat mai puternic decât cel de mai sus este: Pentru orice funcţie* $f : \mathbf{N} \longrightarrow \mathbf{N}$, *crescătoare şi nemărginită, nu neapărat recursivă, mulţimea* $T_p(f) = \{x \in \mathbf{N} | K^p(x|l_p(x)) \leq f(l_p(x))\}$ *este densă.*

Lema 4.24 *(Câmpeanu [14]) O mulţime* $A \subseteq \mathbf{N}$ *este rară (recursiv rară, densă) în* $\tau(\preceq)$, *dacă şi numai dacă* $f(A) = \{f(x)|x \in A\}$ *este rară (recursiv rară, densă) în* $\tau(\preceq_f)$, *unde* $f : \mathbf{N} \longrightarrow \mathbf{N}$ *este o funcţie recursivă şi bijectivă.*

Teorema 4.25 *(Câmpeanu [14]) Pentru orice* $t \geq 0$, $RAND_t^p$ *este recursiv rară în* $\tau(\preceq_p)$, $\tau(\preceq_s)$, $\tau(\preceq_d)$.

Demonstraţie. Mai întâi vom demonstra teorema pentru $\tau(\preceq_p)$. Deci, considerăm funcţia recursivă $r : \mathbf{N} \longrightarrow \mathbf{N}$,

$$r(n) = min\{m \in \mathbf{N} | n \preceq m \text{ şi } l_p(m) \geq n\},$$

pentru orice $n \in \mathbf{N}$. Vom arăta că există i cu $U_{r(n)} \cap RAND_t = \emptyset$, oricare ar fi $n > i$. Fie $\phi : \mathbf{N} \times \mathbf{N} \stackrel{\circ}{\longrightarrow} \mathbf{N}$ funcţia recursivă definită prin

$$\phi(z,m) = number_p^{-1}(number_p(r(m \dot{-} l_p(z))z).$$

Deoarece este recursivă, există o constantă c astfel încât pentru toate numerele naturale m avem

$$K^p(m|l_p(m)) \leq K_\phi^p(m|l_p(m)) + c.$$

Luăm $i > t + c$. Aratăm că dacă $n > i$, atunci $RAND_t^p \cap U_{r(n)} = \emptyset$. Întradevăr, fie $m = number_p^{-1}(number_p(r(n))z)$, unde $n > i$. Evident

$$\phi(z, l_p(m)) = m$$

şi

$$K_\phi^p(m|l_p(m)) \le l_p(z) = l_p(m) - l_p(r(n)) \le$$
$$l_p(m) - l_p(n) < l_p(m) - i < l_p(m) - (t+c).$$

De aici rezultă că

$$K^p(m|l_p(m)) \le K_\phi^p(m|l_p(m)) + c < l_p(m) - (t+c) + c = l_p(m) - t.$$

Deci $RAND_t^p \cap U_{r(n)} = \emptyset$, de unde conform cu Propoziţia 3.26, mulţimea $RAND_t^p$ este recursiv rară în $\tau(\preceq_p)$.

Pentru $\tau(\preceq_s)$ demonstraţia este similară. Pentru $\tau(\preceq_d)$ se utilizează aceeaşi idee ca în Corolarul 4.5, luînd

$$r(n) = \{k \in \mathbf{N} | rp(n) \preceq_p k \text{ şi } rs(n) \preceq_s k\}. \ \Box$$

Teorema 4.26 *(Câmpeanu [14]) Pentru orice $t \in \mathbf{N}$, mulţimea $RAND_t^p$ este recursiv rară în $\tau(\preceq_m)$ şi $\tau(\preceq_{pm})$.*

Demonstraţie. Pentru $\tau(\preceq_m)$, definim funcţia recursivă $f : \mathbf{N} \longrightarrow \mathbf{N}$ prin

$$number_p(f(n)) = a_p^{n \dot{-} l_p(n)}$$

şi funcţia parţial recursivă $\phi : \mathbf{N} \times \mathbf{N} \stackrel{\circ}{\longrightarrow} \mathbf{N}$,

$$\phi(x,n) = number_p^{-1}(number_p(x) a_p^{n \dot{-} l_p(n)}), \text{ în cazul } n \ge l_p(x).$$

Fie $i > t + c$, unde c este cel din Teorema 1.13 b), aplicată funcţiilor ϕ şi U. Să notăm că $n \preceq_m f(n)$; orice $w \in U_{f(n)}$ cu $l_p(n) > i$, poate fi scris ca

$$number_p(w) = number_p(x) number_p(f(n)), \ x \in \mathbf{N}.$$

Avem

$$K^p(w|l_p(w)) \le K_\phi^p(w|l_p(w)) + c \le l_p(w) - l_p(f(n)) + c =$$
$$l_p(w) - l_p(n) + c < l_p(w) - l_p(n) + i - t < l_p(w) - t;$$

deci $w \notin RAND_t^p$, adică $U_{f(n)} \cap RAND_t^p = \emptyset$. Rezultatul se obţine aplicînd Propoziţia 3.26.

Pentru $\tau(\preceq_{pm})$, utilizăm funcţia parţial recursivă $\phi : \mathbf{N} \times \mathbf{N} \stackrel{\circ}{\longrightarrow} \mathbf{N}$,

$$\phi(x,n) = number_p^{-1}(a_p^{n \dot{-} l_p(n)} number_p(x)), \text{ dacă } n \ge l_p(x),$$

într-o construcţie similară cu cea de înainte pentru $\tau(\preceq_m)$. $\Box$

Teorema 4.27 *(Câmpeanu [14]) a) Mulţimea* $non - RAND_m^p$ *este aproape densă în* $\tau(\preceq_t)$.

b) Mulţimea $RAND_m^p$ *este aproape recursiv rară în* $\tau(\preceq_t)$, *dar nu este rară.*

Demonstraţie. a) Fie $\phi : \mathbf{N} \times \mathbf{N} \overset{\circ}{\longrightarrow} \mathbf{N}$, funcţia parţial recursivă definită prin:

$$\phi(x, n) = a_p^n.$$

Deci

$$K_\phi^p(x|l_p(x)) = 1, \text{ dacă } x = number_p^{-1}(a_p^{l_p(x)}) \text{ şi } K_\phi^p(x|l_p(x)) = \infty, \text{ altfel.}$$

Utilizînd Teorema 1.13 obţinem o constantă c astfel încât

$$K^p(a_p^n|n) \leq K_\phi^p(a_p^n|n) + c = c + 1.$$

De aici, dacă $l_p(x) > c + m + 1$, $x \preceq_t a_p^{l_p(x)}$ şi $a_p^{l_p(x)} \in non - RAND_m^p$.

b) Din a) rezultă că funcţia recursivă $r : \mathbf{N} \longrightarrow \mathbf{N}$, definită prin

$$r(x) = a_p^{l_p(x)+m+c+1}$$

şi $RAND_m^p$ satisfac condiţiile c1) şi c2) din Definiţia 3.31

$$(x < r(x),\ U_{r(x)} \cap RAND_m^p = \emptyset, \text{ dacă } l_p(x) > c + m + 1).$$

Mulţimea $RAND_m^p$ nu este rară în $\tau(\preceq_t)$ deoarece

$$RAND_m^p \cap \{a_p^n | n \geq 0\} \neq \emptyset. \ \square$$

5

Codificări binare şi nebinare

În acest capitol arătăm că nu există calculatoare Chaitin şi Chaitin-Kolmogorov, care să fie universale pentru calculatoarele definite pe un alfabet cu mai multe elemente decât alfabetul peste care este considerat domeniul lor de definiţie (Teorema 5.1 şi Teorema 5.2). În secţiunea a doua, studiem comportarea mulţimii cuvintelor aleatoare, faţă de modificarea complexităţii descriptive (înmulţirea sa cu o constantă egală cu logaritmul în baza doi a numărului de litere al alfabetului , pentru a "compensa" diferenţa de baze) (Corolarul 5.5, Corolarul 5.6 şi Corolarul 5.10). Aceste rezultate întăresc argumentele ce arată că există diferenţe esenţiale între complexităţile descriptive în cazul binar şi cazul nebinar. Secţiunea a treia intitulată "Sunt codificările binare universale?", este o concluzie a acestui capitol. Această întrebare a fost formulată de C. Rackhoff [33] şi are un răspuns negativ. Aparent, impresia generală este că este suficient să considerăm că întreaga arie de generalitate a codificării, cel puţin din punctul de vedere algoritmic, este acoperită de cazul binar. Această idee apare în cea mai puternică formă în Li şi Vitányi [30], p. 147:

> *măsura tratată în textul principal este universală în sensul că nici restricţia la descrirea obiectelor binare, nici restricţia la descrierile binare (programe), rezultă fară a se pierde în nici un fel generalitatea.*

Noi credem că, dimpotrivă *există diferenţe esenţiale pentru complexitatea descriptivă în cazul binar şi cel ne-binar;* unele dintre acestea au fost studiate în Calude [2], Calude şi Chiţescu [7], şi în special, Calude, Jürgensen şi

Salomaa [11] (v. de asemenea [3]). Aceste rezultate sunt compatibile cu fapte din teoria clasică a informaţiei; vezi, spre exemplu, Rissanen ([34], p 27) sau analiza din Fenwick [17].

5.1 Inexistenţa calculatoarelor universale de rang inferior

Teorema 5.1 *(Câmpeanu [15]) Fie* $U : V^* \overset{\circ}{\longrightarrow} V^*$ *un calculator. Nu există nici un calculator* $C : X^* \overset{\circ}{\longrightarrow} V^*$ *şi nici o constantă* $c \in \mathbf{N}$*, astfel încât pentru orice* $(x, y) \in V^* \times V^*$ *cu* $U(x) = y$ *există un* $z \in X^*$ *astfel încât următoarele două condiţii sunt adevărate:*

(1) $C(z) = y$ *şi*

(2) $l(z) \leq l(x) + c$*.*

Demonstraţie. Presupunem prin absurd că există un calculator C satisfacînd proprietăţile (1) şi (2). Utilizînd calculatorul $C_0(x) = x$, obţinem o constantă c_0 astfel încât pentru fiecare $x \in V^*$,

$$K(x) \leq K_{C_0}(x) + c_0 = l(x) + c_0.$$

De aici:

$$\min\{l(z) \,|\, z \in X^*, C(z) = y\} \leq K(y) + c \leq l(y) + c_0 + c = l(y) + c_1,$$

pentru orice $y \in V^*$, $(c_1 = c_0 + c)$.

Deoarece

$$\mathrm{card}\{y \in V^* | l(y) = i\} = p^i,$$

$$\mathrm{card}\{z \in X^* \,|\, l(z) \leq i + c_1\} = q^0 + q^1 + \ldots + q^{i+c_1} = \frac{q^{i+c_1+1} - 1}{q - 1},$$

şi pentru orice y există z cu $l(z) \leq l(y) + c_1$ şi $C(z) = y$, va rezulta că, pentru orice număr natural i :

$$\frac{q^{i+c_1+1} - 1}{q - 1} \geq p^i,$$

ceea ce este absurd $(p > q)$, deoarece

$$\lim_{i \to \infty} \left(\frac{q}{p}\right)^i \cdot \frac{q^{c_1+1}}{q - 1} = 0. \,\square$$

Teorema 5.2 *(Câmpeanu [15]) Fie $U : V^* \overset{\circ}{\longrightarrow} V^*$ un calculator Chaitin. Nu există nici un calculator Chaitin $C : X^* \overset{\circ}{\longrightarrow} V^*$ şi nici o constantă $c \in \mathbf{N}$, astfel încât pentru orice $(x, y) \in V^* \times V^*$ cu $U(x) = y$ există un $z \in X^*$ astfel încât următoarele două condiţii sunt adevărate*
(1) $C(z) = y$ şi
(2) $l(z) \leq l(x) + c$.

Demonstraţie. Presupunem, fără a micşora generalitatea, că $X \subset V$. Fie $U : V^* \overset{\circ}{\longrightarrow} V^*$ un calculator universal Chaitin. Presupunem că există o constantă c şi un calculator Chaitin $C : X^* \overset{\circ}{\longrightarrow} V^*$ astfel încât pentru orice $(x, y) \in V^* \times V^*$ cu $U(x) = y$ există un $z \in X^*$ astfel încât $C(z) = y$ şi $l(z) \leq l(x) + c$.

Definim $C_0 : V^* \overset{\circ}{\longrightarrow} V^*$ prin $C_0(z) = C(z)$, deci

$$H_{C_0}(x) = H_C(x) \leq H(x) + c.$$

Din

$$\sum_{z \in domC_0} q^{-l(z)} = \sum_{z \in domC} q^{-l(z)} \leq 1$$

rezultă că

$$\sum_{x \in domU} q^{-l(x)} < \infty. \tag{5.1}$$

Într-adevăr,

$$1 \geq \sum_{z \in domC_0} q^{-l(z)} \geq \sum_{x \in domU} q^{-l(x)-c} = q^{-c} \cdot \sum_{x \in domU} q^{-l(x)}.$$

Luăm funcţia $f : N \longrightarrow N$, definită prin: $f(0) = 2$, $f(1) = 2, \ldots, f(p-2) = 2$, $f(p) = 3$, $\ldots$, $f(p-2+(p-1)^2) = 3$, $f(p-2+(p-1)^2+1) = 4$, $\cdots$, adică funcţia recursivă nedecrescătoare care are primele $p-1$ valori 2, apoi următoarele $(p-1)^2$ valori egale cu 3, ş.a.m.d. Avem relaţiile:

$$\sum_{n \in N} p^{-f(n)} = \sum_{k=0}^{\infty} p^{-k} \cdot \mathrm{card}\{n \in \mathbf{N} | f(n) = k\} = \sum_{k=2}^{\infty} p^{-k} \cdot (p-1)^{k-1} =$$

$$\sum_{n=1}^{\infty} \frac{(p-1)^n}{p^{n+1}} \leq \sum_{n=0}^{\infty} \frac{(p-1)^n}{p^{n+1}} = 1,$$

adică

$$\sum_{n\in\mathbf{N}} p^{-f(n)} \leq 1. \tag{5.2}$$

În virtutea relaţiilor:

$$\sum_{n=0}^{\infty} q^{-f(n)} = \sum_{k=0}^{\infty} q^{-k} \cdot \mathrm{card}\{n \in \mathbf{N} | f(n) = k\} =$$

$$\sum_{k=2}^{\infty} q^{-k} \cdot \mathrm{card}\{n \in \mathbf{N} | f(n) = k\} =$$

$$\sum_{k=1}^{\infty} q^{-k-1} \cdot \mathrm{card}\{n \in \mathbf{N} | f(n) = k+1\} = \sum_{k=1}^{\infty} \frac{(p-1)^k}{q^{k+1}} = \frac{1}{q}\sum_{k=1}^{\infty} \left(\frac{p-1}{q}\right)^k = \infty,$$

deducem:

$$\sum_{n=0}^{\infty} q^{-f(n)} = \infty. \tag{5.3}$$

Utilizînd Teorema Kraft-Chaitin va rezulta că există o mulţime recursiv enumerabilă liberă de prefixe $W \subseteq V^*$ şi o funcţie recursivă $g : \mathbf{N} \longrightarrow V^*$, astfel ca $W = g(\mathbf{N})$ şi $l(g(n)) = f(n)$, pentru orice $n \in \mathbf{N}$.

Definim acum calculatorul Chaitin $C_1 : V^* \overset{\circ}{\longrightarrow} V^*$ prin

$$C_1(g(n)) = string(p, n),$$

deci există $c_1 \in \mathbf{N}$ cu

$$H(x) \leq H_{C_1}(x) + c_1.$$

Avem:

$$\sum_{x\in domU} q^{-l(x)} \geq \sum_{z\in domC_1} q^{-l(z)-c_1} \geq$$

$$\sum_{n\in N} q^{-f(n)-c_1} \geq q^{-c_1} \sum_{n\in N} q^{-f(n)} = \infty.$$

Evident am obţinut o contradicţie, deci nu există calculatoare Chaitin cu asemenea proprietaţi. $\square$

5.2 Codificări nebinare

Notăm
$$R_t^p = \{x \in X^* |\, log_2 p \cdot K(x|m) \geq l(x) - t\},$$

$$non - R_t^p = X^* - R_t^p.$$

Lema 5.3 *(Câmpeanu [16]) Avem relaţiile:*
(1) $RAND_t^K \subseteq R_t^p$,
(2)$card\ X^n \cap non - R_t^p \leq \frac{p \cdot 2^{n-t}-1}{p-1} < \frac{p \cdot 2^{n-t}}{p-1}$.

Demonstraţie. (1) Evident.
(2) Avem:

$$\text{card} X^n \cap non - R_t^p \leq \sum_{k=0}^{[\frac{n-t}{log_2 p}]} p^k \leq$$

$$\frac{p^{1+\left[\frac{n-t}{log_2 p}\right]} - 1}{p-1} \leq \frac{p \cdot p^{\frac{n-t}{log_2 p}} - 1}{p-1} =$$

$$\frac{p \cdot (p^{log_2 p})^{n-t} - 1}{p-1} = \frac{p \cdot 2^{n-t} - 1}{p-1} < \frac{p \cdot 2^{n-t}}{p-1}.$$

Corolar 5.4 *(Câmpeanu [16]) Mulţimea* $non - R_t^p$ *este densă în orice topologie generată de relaţii recursive şi nemărginite de ordine parţială pe* X^*.

Demonstraţie. Rezultă din relaţia

$$A(1 + d + t, d \cdot log_2 p) \subseteq non - R_t,$$

unde mulţimea $A(m, d)$ este cea definită în Teorema 4.1. □

Corolar 5.5 *(Câmpeanu [16]) Fie* $t \geq 0$. *Dacă pentru orice cuvânt* x *există un număr natural* m *şi un cuvânt* w, *astfel încât* $x \preceq w$ *şi*

$$card\{y \in X^* |\, l(y) = m,\ w \preceq y\} \cdot (p-1) > p \cdot 2^{n-t} - 1,$$

atunci R_t^p *este densă.*

Demonstraţie. Deoarece

$$\text{card } X^n \cap non - R_t^p \leq \frac{p \cdot 2^{n-t} - 1}{p-1} < \frac{p \cdot 2^{n-t}}{p-1},$$

rezultă din relaţia:

$$\text{card}\{z \in X^* |\, l(z) = n,\, z \notin R_t^p\} \cdot (p-1) \leq p \cdot 2^{n-t} - 1 \,\square$$

Corolar 5.6 *(Câmpeanu [16]) R_t^p este densă în raport cu toate topologiile generate de relaţiile de ordine parţială din Exemplul 3.1, dacă $p > 2$.*

Demonstraţie. Avem relaţiile:

$$\text{card}\{y \in X^* |\, l(y) = m,\, w \preceq_d y\} \cdot (p-1) \geq p^{m-2 \cdot l(w)} \cdot (p-1) > p \cdot 2^{m-t},$$

$$\text{card}\{y \in X^* |\, l(y) = m,\, w \preceq_l y\} \cdot (p-1) \geq p^{m-l(w)-1} \cdot (p-1) > p \cdot 2^{m-t},$$

$$\text{card}\{y \in X^* |\, l(y) = m,\, w \preceq_m y\} \cdot (p-1) \geq p^{m-l(w)} \cdot (p-1) > p \cdot 2^{m-t},$$

care sunt adevărate pentru m suficient de mare. Luăm, spre exemplu, m astfel încât: $(\frac{p}{2})^m > p \cdot \frac{p^{2 \cdot l(w)+2}}{2^t}$; amintim că $p > 2$.

Deoarece $\preceq_d \subseteq <_s$, $\preceq_d \subseteq <_p$, $\preceq_d \subseteq <_i$, $\preceq_d \subseteq <_h$, $\preceq_d \subseteq <_p m$, rezultă ca R_t^p este densă pentru toate topologiile din Exemplul 3.1. $\square$

Lema 5.7 *(Câmpeanu [16]) Pentru orice $\varepsilon > 0$:*

$$card\{x \in X^n |\, x \text{ nu este } \varepsilon\text{-limiting}\} \geq$$

$$max \left(\sum_{k=\lceil \frac{n \cdot (p \cdot \varepsilon + 1)}{p} \rceil}^{n} \binom{n}{k} \cdot (p-1)^{n-k}, \sum_{k=0}^{\lfloor \frac{n \cdot (1 - p \cdot \varepsilon)}{p} \rfloor} \binom{n}{k} \cdot (p-1)^{n-k} \right).$$

Demonstraţie. Avem:

$$\text{card}\{x \in X^n | \, x \text{ nu este } \varepsilon\text{-limiting } \} =$$

$$\text{card}\{x \in X^n | \, \text{există } 1 \le i \le p, \left| \frac{N_i(x)}{l(x)} - \frac{1}{p} \right| \ge \varepsilon\} \ge$$

$$\text{card}\{x \in X^n |, \left| \frac{N_i(x)}{l(x)} - \frac{1}{p} \right| \ge \varepsilon\} =$$

$$\sum_{\substack{k=0 \\ \left|\frac{k}{n} - \frac{1}{p}\right| \ge \varepsilon}}^{n} \text{card}\{x \in X^n | N_i(x) = k\} =$$

$$\sum_{\substack{k=0 \\ \left|\frac{k}{n} - \frac{1}{p}\right| \ge \varepsilon}}^{n} \binom{n}{k} \cdot (p-1)^{n-k} =$$

$$\sum_{\substack{k=0 \\ |p \cdot k - n| \ge \varepsilon \cdot p \cdot n}}^{n} \binom{n}{k} \cdot (p-1)^{n-k} \ge$$

$$max\left(\sum_{k=\lceil \frac{n\cdot(p\cdot\varepsilon+1)}{p} \rceil}^{n} \binom{n}{k} \cdot (p-1)^{n-k}, \sum_{k=0}^{\lfloor \frac{n\cdot(1-p\cdot\varepsilon)}{p} \rfloor} \binom{n}{k} \cdot (p-1)^{n-k} \right). \square$$

Corolar 5.8 *(Câmpeanu [16]) Dacă $\varepsilon < 1/(2 \cdot p)$, atunci*

$$card\{x \in X^n | \, x \text{ este } \varepsilon\text{-limiting}\} \le p^n - \sum_{k=0}^{\left[\frac{n}{2\cdot p}\right]} \binom{n}{k} \cdot (p-1)^{n-k}.$$

Demonstraţie. Dacă $\varepsilon < 1/(2 \cdot p)$, atunci

$$\left\lfloor \frac{n \cdot (1 - p \cdot \varepsilon)}{p} \right\rfloor > \left\lfloor \frac{n \cdot (1 - p \cdot \frac{1}{2 \cdot p})}{p} \right\rfloor = \left[\frac{n}{2 \cdot p} \right]$$

şi utilizăm lema precedentă. $\square$

Lema 5.9 *Următoarea formulă este adevărată:*

$$\lim_{n\to\infty}\left(\frac{p-1}{2}\right)^n \sum_{k=0}^{\left[\frac{n}{2\cdot p}\right]} \binom{n}{k}\cdot(p-1)^{-k}=\infty,$$

pentru $p>2$.

Demonstraţie. Putem lua fără a micşora generalitatea $n=2\cdot p\cdot q$, $q\in\mathbf{N}$. Deci:

$$\left(\frac{p-1}{2}\right)^{2pq}\sum_{k=0}^{q}\binom{2pq}{k}\cdot(p-1)^{-k}>\left(\frac{p-1}{2}\right)^{2pq}\sum_{k=0}^{q}\binom{q}{k}\cdot(p-1)^{-k}=$$

$$\left(\frac{p-1}{2}\right)^{2pq}\left(1+\frac{1}{p-1}\right)^{q}\to\infty,$$

pentru $q\to\infty$.
(Am utilizat $\binom{2pq}{k}>\binom{q}{k}$ dacă $k\le q$).
Concluzia este evidentă. □

Corolar 5.10 *(Câmpeanu [16]) Există* $x\in R_t^p$ *care nu sunt* ε*-limiting, pentru* $\varepsilon<1/(2\cdot p)$ *şi* $p>2$.

Demonstraţie. În virtutea lui 5.8 şi 5.9 există un număr natural n asfel ca

$$\left(\frac{p-1}{2}\right)^n \sum_{k=0}^{\left[\frac{n}{2\cdot p}\right]}\binom{n}{k}\cdot(p-1)^{-k}>\frac{p}{2^t\cdot(p-1)},$$

deci

$$\sum_{k=0}^{\left[\frac{n}{2\cdot p}\right]}\binom{n}{k}\cdot(p-1)^{n-k}>\frac{p\cdot 2^{n-t}}{p-1}.$$

De aici

$$p^n-\sum_{k=0}^{\left[\frac{n}{2\cdot p}\right]}\binom{n}{k}\cdot(p-1)^{n-k}<p^n-\frac{p\cdot 2^{n-t}-1}{p-1}.$$

ceea ce înseamnă că în X^n sunt mai multe cuvinte în R_t^p decât ε-limiting. □

Corolar 5.11 *Dacă* $p > 2$, *există* $x \in RC_t^p$ *care nu sunt* ε*-limiting, pentru* $\varepsilon < 1/(2 \cdot p)$, *unde*

$$RC_t^p = \{x \in X^* | \log_2 p \cdot H_C(x) \geq \Sigma(l(x)) - t\}.$$

Demonstraţie. Demonstraţia urmează aceiaşi paşi ca în cazul complexităţii Chaitin-Kolmogorov, utilizînd faptul că, există $c \in \mathbf{N}$, cu

$$\Sigma(n) \leq n + c \cdot \log_p n. \, \Box$$

5.3 Sunt codificările binare universale?

Pentru $p \geq 2$ vom nota $X_p = \{0, 1, \ldots, p-1\}$.

O funcţie $f : A \longrightarrow \mathbf{N}$ (unde A este X_p^* sau $\mathbf{N}_+$) este semi-calculabilă superior dacă mulţimea $\{(x, m) \mid x \in X, m \in \mathbf{N}, f(n) \leq m\}$ este recursiv enumerabilă. De exemplu, complexitatea Chaitin este semi-calculabilă superior (dar nu este calculabilă). Vom nota cu $H_p(x)$ complexitatea Chaitin a cuvântului $x \in X_p$.

Un şir $\mathbf{x} = x_1 x_2 \cdots x_n \cdots \in X_p^\omega$ este *aleator* dacă $\lim_{n\to\infty}(H_p(\mathbf{x}(n)) - n) = \infty$; unde $\mathbf{x}(n) = x_1 x_2 \cdots x_n$ este prefixul de lungime n al lui $\mathbf{x}$.

Pentru $f, g : \mathbf{N} \longrightarrow \mathbf{R}$ spunem că $f = \mathrm{O}(g)$, dacă

$$\overline{\lim_{n\to\infty}} \frac{f(n)}{g(n)} < \infty.$$

5.3.1 Complexitatea numerelor naturale

Dacă vrem să comunicăm rapid şi neambiguu un şir infinit de numere naturale unui calculator (de exemplu intrucţiunile), pentru a garanta o comunicaţie rapidă, trebuie să folosim coduri de lungime cât mai mică. Pentru a evita ambiguitatea trebuie să ne asigurăm că acel calculator *cunoaşte* unde se termină un număr şi unde începe următorul. Vom considera coduri libere de prefix pentru *toate numerele naturale.*

Domeniul unui calculator binar universal Chaitin este un cod binar optimal pentru toate numerele naturale. El nu este calculabil. Cerînd calculabilitate pierdem optimalitate; oricum, îmbunătăţirea asimptotică pe care o obţinem nu este esenţială, în sensul că există o codificare "aproape optimă" şi nici o alta calculabilă nu poate fi "mult mai bună"; vezi Knuth [26].

O diferenţă esenţială apare atunci când comparăm codificări avînd alfabete de mărimi diferite. În sistemul uzual (poziţional) avem nevoie de mai puţine cifre pentru a codifica numere în ternar decât în binar. Îmbunătăţirea nu este lineară, [1] ci este cam de $\log_3 2$ ori mai bună. Vom demonstra că acest fapt nu este o consecinţă a faptului că am utilizat o codificare particulară ci este un fenomen general.

Începem prin a îmbunătăţii câteva rezultate datorate lui Chaitin [19].

Lema 5.12 *Fie $f : \mathbf{N}_+ \longrightarrow X_p^*$ o funcţie injectivă (nu neapărat recursivă) avînd codomeniul liber de prefixe. Atunci pentru orice m natural următoarea inegalitate*

$$l(f(n)) > \log_p n + m,$$

este adevărată pentru o infinitate de n.

Demonstraţie. Presupunem prin absurd că există $m \in \mathbf{N}$ astfel încât inegalitatea $l(f(n)) \leq \log_p n + m$ este adevărată pentru aproape toţi n. Atunci, rezultă că seria divergentă

$$\sum_{n\geq 1} p^{-\log_p n - m}$$

va converge:

$$\sum_{n\geq 1} p^{-\log_p n - m} \leq \sum_{n\geq 1} p^{-l(f(n))} + c < \infty.$$

□

Corolar 5.13 *Avem:*

$$H_p(string_p(n)) > \log_p n,$$

pentru o infinitate de n.

Rezultă că pentru orice m, nu există o codificare liberă de prefixe a tuturor numerelor naturale — peste alfabetul X_p — ce poate fi micşorată sub $\log_p n + m$, pentru aproape toţi n. Lucrînd cu un alfabet mai bogat se obţine o

[1] Pentru un alfabet fixat, Teorema de Invarianţă nu poate fi îmbunătăţită; v. secţiunile anterioare din acest capitol.

îmbunătăţire chiar cu un cod recursiv banal. De exemplu, luăm codul $F : \mathbf{N}_+ \longrightarrow X_{p+1}^*$ definit prin

$$F(n) = number_p(n)(p),$$

concatenarea între $number_p(n)$ şi noua literă p. Evident,

$$l(F(n)) = l_p(n) + 1 \leq \log_p n + 2.$$

Lema 5.14 *(Calude, Câmpeanu [6]) Fie* $F : \mathbf{N}_+ \longrightarrow X_p^*$ *recursivă şi injectivă, şi fie* $g : \mathbf{N}_+ \longrightarrow \mathbf{N}_+$ *o funcţie semi-calculabilă superior astfel încât*

$$\sum_{n \geq 1} p^{-g(n)} < \infty.$$

Atunci există $c \in \mathbf{N}$ *astfel încât*

$$H_p(F(n)) \leq g(n) + c.$$

Demonstraţie. Mai întâi să notăm că

$$\begin{aligned} \sum_{n \geq N} \sum_{m \geq g(n)} p^{-m} &= \sum_{n \geq N} \sum_{m=0}^{\infty} p^{-(g(n)+m)} \\ &= \sum_{n \geq N} p^{-g(n)} \sum_{m=0}^{\infty} p^{-m} \\ &= \frac{p}{p-1} \sum_{n \geq N} p^{-g(n)} \leq 1, \end{aligned}$$

în cazul

$$\sum_{n \geq N} p^{-g(n)} < p/(p-1).$$

În virtutea Teoremei Kraft-Chaitin, există un calculator Chaitin $C : X_p^* \stackrel{\circ}{\longrightarrow} X_p^*$ astfel încât pentru orice $n \geq N$ şi $m \geq g(n)$ există un cuvânt x de lungime m astfel încât $C(x) = F(n)$. În particular, există un cuvânt x_n de lungime $g(n)$ astfel încât $C(x_n) = F(n)$, pentru orice $n \geq N$; utilizînd Teorema de Invarianţă deducem formula:

$$H_p(F(n)) \leq g(n) + c. \ \square$$

Exemplul 5.15 *Pentru orice* $p \geq 2$, $\alpha > 1$, *există* $c \in \mathbf{N}$ *astfel încât*

$$H_p(string_p(n)) \leq \alpha \cdot \log_p(n) + c.$$

În cazul $p > 2$ *se poate obţine o inegalitate mai tare:*

$$H_p(string_p(n)) \leq \log_{p-1}(n) + c.$$

Următorul rezultat va evidenţia şi mai mult diferenţa între codificari peste alfabete cu un numar diferit de elemente. Vom demonstra că *nu există codificare optimală liberă de prefixe pentru toate numerele naturale*, şi *codificarea binară este cea mai slabă posibilă.* Pentru alfabete din ce în ce mai mari obţinem codificări din ce în ce mai bune; în contrast cu situaţia în care alfabetul era fixat, unde îmbunătăţirea se putea face indefinit, dar foarte puţin semnificativ (a se vedea Knuth [26]).

Teorema 5.16 *(Calude, Câmpeanu [6]) Fie* $2 \leq q < p$ *numere naturale şi considerăm două funcţii recursive bijective* $F : \mathbf{N}_+ \longrightarrow X_p^*$, $f : \mathbf{N}_+ \longrightarrow X_q^*$. *Atunci, există* $c \in \mathbf{N}$ *astfel încât*

$$H_p(F(n)) < (\log_p q)H_q(f(n)) + c.$$

Demonstraţie. Luăm funcţia $g(n) = \lfloor (\log_p q)H_q(f(n)) \rfloor$. Avem:

$$\begin{aligned} \sum_{n \geq 1} p^{-g(n)} &\leq \sum_{n \geq 1} p^{1-(\log_p q)H_q(f(n))} \\ &= p \sum_{n \geq 1} q^{-H_q(f(n))} \\ &\leq p < \infty. \end{aligned}$$

Deoarece g este semi-calculabilă superior putem utiliza Lema 5.14 pentru a obţine inegalitatea căutată. $\square$

Corolar 5.17 *(Calude, Câmpeanu [6]) Fie* $2 \leq q < p$ *numere naturale. Există* $c \in \mathbf{N}$ *astfel încât, pentru orice cuvânt* $x \in X_q^*$ *avem*

$$H_p(x) \leq (\log_p q)H_q(x) + c.$$

Demonstraţie. Considerăm funcţia recursivă bijectivă $F : \mathbf{N}_+ \longrightarrow X_p^*, f : \mathbf{N}_+ \longrightarrow X_q^*$ definite prin:

$$F(n) = f(n) = string_q(n),$$

şi utilizăm Lema 5.14. □

Corolar 5.18 *(Calude, Câmpeanu [6]) Pentru orice $2 \leq q \leq p$, există $c \in \mathbf{N}$ astfel încât*

$$H_p(string_p(n)) \leq (\log_p q) H_q(string_q(n)) + c.$$

5.3.2 Măsuri ale hazardului

Aici vom analiza rolul mărimii alfabetului pentru definirea cuvintelor şi şirurilor aleatoare. [2]

Mai întâi să notăm relaţiile:

Teorema 5.19 *(Calude, Câmpeanu [6]) Fie $2 \leq q < p$. Atunci, există o constantă α (care depinde de q şi p) astfel încât pentru orice $x \in X_q^*$ avem:*

$$|H_q(x) - (\log_q p) H_p(x)| \leq \alpha.$$

Demonstraţie. Utilizăm Corolarul 5.17 şi Lema 5.14, luând $F : \mathbf{N}_+ \longrightarrow X_q^*$,

$$F(n) = string_q(n), g(n) = \lfloor (\log_q p) H_p(F(n)) \rfloor. \; \square$$

Vrem să calculăm complexitatea cuvintelor $x \in X_q^*$ considerate cuvinte în X_p^*.

Propoziţia 5.20 *(Calude, Câmpeanu [6]) Pentru orice $2 \leq q < p$ şi orice $x \in X_q^*$, există $c \in \mathbf{N}$ astfel încât*

$$H_p(x) < l(x) + c.$$

[2]Teoria algoritmică a informaţiei a fost dezvoltată în special în cazul binar, cu puţine excepţii şi anume Knuth [25], Calude [2, 3], Calude şi Chiţescu [7], Kramosil [28], şi Calude şi Jürgensen [10].

Demonstraţie. Într-adevăr, din Propoziţia 5.20 avem:

$$\begin{aligned} H_p(x) &\leq (\log_p q)H_q(x) + c_1 \\ &\leq (\log_p q)\Sigma_q(l(x)) + c \\ &\leq (\log_p q)(l(x) + \mathrm{O}(\log_q l(x))) \\ &= (\log_p q)l(x) + \mathrm{O}(\log_q l(x)) \\ &< l(x) + c. \end{aligned}$$

□

Corolar 5.21 *(Calude, Câmpeanu [6]) Nici un cuvânt $x \in X_q^*$ nu este aleator peste X_p^*.*

În cazul binar nu avem decât două astfel de cuvinte şi anume

$$00\ldots0 \text{ şi } 11\ldots1,$$

care evident nu sunt aleatoare. În cazul ne-binar avem

$$\sum_{i=2}^{p-1} i^n \binom{p}{i}$$

cuvinte peste alfabetul X_p care nu sunt aleatoare deoarece ele nu conţin toate cele p litere. De exemplu, pentru $p = 3$ sunt 3×2^n astfel de cuvinte, unele dintre ele (de fapt, urmîndu-l pe Chaitin [22], mai mult de $3 \times 2^{n-c_2}$, unde c_2 este o constantă ce depinde de mărimea alfabetului dar nu de lungimea n) sunt aleatoare ca şi cuvinte *binare* .

Distincţia de mai sus este mai mare pentru şiruri aleatoare: trecem de la două şiruri în cazul binar la o infinitate (de puterea continuului) în cazurile ne-binare:

Corolar 5.22 *(Calude, Câmpeanu [6]) Nici un şir $\mathbf{x} \in X_q^\omega$ nu este aleator peste alfabetul A_p în cazul $p > q \geq 2$.*

Bibliografie

[1] Cristian Calude, Topological size of sets of partial recursive function *Z. Math. Logik Gründlag. Math.*, **32** (1982) 81-88.

[2] Cristian Calude, *Theories of Computational Complexity*, North-Holland, Amsterdam, 1988.

[3] Cristian Calude, *Information and Randomness - An Algorithmic Perspective*, Springer-Verlag, Berlin, 1994.

[4] Cristian Calude. Borel normality and algorithmic randomness, in G. Rozenberg, Arto Salomaa (eds.). *Developments in Language Theory*, World Scientific, Singapore, 1994, 113-129. (with a note by G. J. Chaitin)

[5] Cristian Calude, Cezar Câmpeanu, Note on the topological structure of random strings. *Theoretical Computer Science*, **112** (1993) 383-390.

[6] Cristian Calude, Cezar Câmpeanu, Are Binary Codes Universal ? *Report No.98 Dept. of Computer Science School of Mathematical & Information Sciences The University of Auckland*, July 1994, 1-11.

[7] Cristian Calude, Ion Chiţescu, Random strings according to A. N. Kolmogorov and P. Martin-Löf. Classical approach, *Found. Control. Engrg.*, **3** (1982), 73-85.

[8] Cristian Calude, Ion Chiţescu, Qualitative properties of P. Martin-Löf random sequences, *Bolletino Un. Mat. Ital. B*, **3** (1989), 229-240.

[9] Cristian Calude, Ion Chiţescu, L. Staiger, P. Martin-Löf tests: representability and embeddability, *Revue Roumanie Math. Pures Appl.*, **30** (1985), 719-732.

[10] C. Calude, H. Jürgensen. Randomness as an invariant for number representations, in H. Maurer, J. Karhumäki, G. Rozenberg (eds.). *New Results and Trends in Theoretical Computer Science*, Springer-Verlag, Berlin, 1994, 44-66.

[11] C. Calude, Helmut Jürgensen, Arto Salomaa. *Coding without Tears*, manuscript, February 1994, 15 pp.

[12] Cezar Câmpeanu. Note on Kolmogorov and Chaitin random strings *Salodays in Computer Science*, A. Atanasiu, C. Calude (eds.), Hyperion Press, 1992, 8pp.

[13] Cezar Câmpeanu. Chaitin's Representability of Martin-Löf Tests *Analele Univ. Buc.,* 1994 (to appear), 5pp.

[14] Cezar Câmpeanu. Random numbers, *Procedings of ROSYCS'93* 1993, 10p.

[15] Cezar Câmpeanu. Note on codding universal computers *St. Cerc. Mat.*, (submitted) 4p.

[16] Cezar Câmpeanu. Note on Kolmogorov Complexity *Manuscript* , 1994, 7p.

[17] P. Fenwick. Huffman code efficiency for extensions of sources, *IEEE Trans. Comm.* (in press)

[18] G. J. Chaitin, *Algorithmic Information Theory*, Cambridge University Press, Cambridge, 1987.

[19] G. J. Chaitin. A theory of program size formally identical to information theory, *J. Assoc. Comput. Mach.,* 22(1975), 329-340.(retiparită in Chaitin [20], 197-223.)

[20] G. J. Chaitin. *Information, Randomness and Incompletness, Papers on Algorithmic Information Theory,* Word Scientific, Singapore, New Jersey, Hong Kong, 1987.(ed. 2 1990)

[21] G. J. Chaitin. Randomness in arithmetic, *Scientific American* 259(1988), 80-85(retiparită în Chaitin [20], 14-19.)

[22] G. J. Chaitin. On the number of N-bit strings with maximum complexity, *Applied Mathematics and Computation* 59(1993), 97-100.

[23] H. Jürgensen, S.S. Yu. Relations on free monoids, their independent sets and codes, *Report no. 257, Dept. of Computer Science, Univ. of Western Ontario*, 1989.

[24] J. Kelley, *General Topology*, Van Nostrand, Princeton, **NJ**, 1968.

[25] D. E. Knuth. *The Art of Computer Programming*, Vol. 2, *Seminumerical Algorithms*, Addison-Wesley, Reading, MA, 2nd ed., 1981.

[26] D. E. Knuth. Supernatural numbers, in D. A. Klarner (ed.). *The Mathematical Gardner,* Prindle, Weber & Schmidt, Wadsworth, Boston, MA, 1981, 310-325.

[27] A. N. Kolmogorov. Three approaches for defining the concept of "information quantity", *Problems Inform. Transmission* 1(1965), 3-11.

[28] I. Kramosil. Recursive classification of pseudo-random sequences, *Kybernetika (Prague)* 20(1984), 1-34. (supplement)

[29] L. A. Levin. Randomness conservation inequalities: information and independence in mathematical theories, *Problems Inform. Transmission,* 10(1974), 206-210.

[30] M. Li, P. M. Vitányi. *An Introduction to Kolmogorov Complexity and Its Applications*, Springer-Verlag, Berlin, 1993.

[31] P. Martin-Löf, The definition of random sequences, *Inform. and Control*, **19** (1966), 602-619.

[32] I.P. Natanson. *Theory of Functions of Real Variable,* Nauka, Moscova, 1974 (în Lb. Rusa)

[33] C. Rackhoff, *Personal Communication to C. Calude*, November 1993.

[34] J. Rissanen, *Stochastic Complexity in Statistical Inquiry*, World Scientific, Singapore, 1989.

[35] G. Rozenberg, A. Salomaa, *Cornerstones of Undecidability,* Prentice-Hall, 1994.

[36] C. P. Schnorr. A survey of the theory of random sequences, in R.E. Butts, J. Hintikka (eds.). *Basic Problems in Metodology and Linguistics,* Reidel, Dordrecht, 1977, 193-210.

[37] R.M.Solovay, *Draft of a paper (or series of papers) on Chaitin's work ... done for the most part during the period of Sept.-Dec. 1974*, unpublished manuscript, IBM Thomas J. Watson Research Center, Yorktown Heights, New York, May 1975, 215pp.

[38] Marius Zimand, On the topological size of random strings, *Zeitschr. f. math. Logik und Grundlagen d. Math.* Bd. 32, S. 81-88(1986)