Losowość algorytmiczna

Podstawowe idee i problemy

Łukasz Dębowski
ldebowsk@ipipan.waw.pl

Instytut Podstaw Informatyki PAN

Pierwsza obserwacja

Rozważamy słowa i sekwencje nad skończonym alfabetem:

$$x_1^n = (x_1, x_2, \ldots, x_n), \qquad x_k \in \{0, 1, \ldots, D-1\},$$
$$x_1^\infty = (x_1, x_2, x_3, \ldots),$$

równoważnie także liczby rzeczywiste $x := \sum_{k=1}^{\infty} x_k D^{-k}$.

Niektóre z nich można wygenerować prostym programem:

$$0 = 0.000000000000\ldots$$
$$\frac{1}{7} = 0.142857142857\ldots$$
$$\pi = 3.141592653589\ldots$$

Ale wiele innych nie, np. $0.00787499699\ldots$

Programów jest przeliczalnie wiele, sekwencji jest kontinuum.

Druga obserwacja

Obserwujemy pewien empiryczny szereg czasowy:

$$\mathbf{01010101010101...}$$

Jaka będzie następna cyfra? **0**?

A skąd wiemy, że nie jest to wynik rzutów uczciwą monetą?

Przecież wszystkie słowa są równie prawdopodobne!

Trzecia obserwacja

Niech X_i będą rzutami uczciwą monetą,
tzn. niezależnymi zmiennymi losowymi o $P(X_i = \frac{1}{2} \pm \frac{1}{2}) = \frac{1}{2}$.

Wiemy, że z p-stwem 1 zachodzi

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} X_i = \frac{1}{2}.$$

Choć wszystkie słowa są równie prawdopodobne,
to prawdopodobieństwo skupione jest na podzbiorze sekwencji.

Czy możemy scharakteryzować, jaki jest to podzbiór?
Czy należą do niego liczby 0, $1/7$, π?

Kody bezprefiksowe

- Niech $\{0,1\}^*$ oznacza zbiór słów binarnych.
- Funkcję $C : A \to \{0,1\}^*$ nazywamy kodem bezprefiksowym, gdy

$$C(u) = C(v)z \implies u = v.$$

- Symbol $|C(u)|$ będzie oznaczać długość słowa kodowego.

Istnieją proste kody bezprefiksowe takie, że

$$|C_1(w)| = |w| + |C_2(|w|)|, \qquad w \in \{0,1\}^*,$$
$$|C_2(n)| \leq \log n + 2 \log\log n, \qquad n \in \mathbb{N}.$$

Jeżeli istnieje program generujący sekwencję x_1^∞, to istnieje (obliczalny) kod bezprefiksowy C taki, że

$$\left|C(x_1^n)\right| = |C_2(n)| \leq \log n + 2 \log\log n.$$

Nierówności Krafta i Barrona

Nierówność Krafta: (dla kodu bezprefiksowego)

$$\sum_{w \in \{0,1\}^*} 2^{-|C(w)|} \leq 1.$$

Nierówność Barrona: (dla semirozkładu)

$$\sum_x Q(x) \leq 1, \quad P(x) := P(X = x)$$

$$\Longrightarrow \; P\left(\frac{Q(X)}{P(X)} \geq q\right) \leq \frac{1}{q}.$$

Biorąc $Q(x_1^n) = 2^{-|C(x_1^n)|}$ oraz $P(x_1^n) = 2^{-n}$, otrzymujemy

$$P(\left|C(X_1^n)\right| \leq n - m) \leq 2^{-m}.$$

Losowość I: Złożoność prefiksów

- Niech X_1^∞ będzie dowolnym procesem stochastycznym.

Twierdzenie Barrona:
Z nierówności Krafta i Barrona oraz z lematu Borela-Cantellego, z p-stwem $\mathbf{1}$ zachodzi

$$\inf_{n\in\mathbb{N}} \left[\left|C(X_1^n)\right| + \log P(X_1^n)\right] > -\infty.$$

Definicja I

Niech $\mathcal{C}$ będzie przeliczalną klasą kodów bezprefiksowych. Sekwencję x_1^∞ nazwiemy $\mathcal{C}$-losową, jeżeli

$$\forall_{C\in\mathcal{C}} \quad \inf_{n\in\mathbb{N}} \left[\left|C(x_1^n)\right| + \log P(x_1^n)\right] > -\infty.$$

Proces X_1^∞ jest $\mathcal{C}$-losowy z p-stwem $\mathbf{1}$.

Martyngały względem σ-ciał cylindrów

- Niech X_1^∞ będzie dowolnym procesem stochastycznym.
- Funkcję $M : \mathbb{X}^* \to \mathbb{R}$ nazywamy P-martyngałem, gdy

$$P(x_1^n) \cdot M(x_1^n) = \sum_{x_{n+1} \in \mathbb{X}} P(x_1^{n+1}) \cdot M(x_1^{n+1}).$$

- Martyngał obrazowo reprezentuje kapitał w uczciwej grze.
- Funkcja $M : \{0,1\}^* \to \mathbb{R}$ jest P-martyngałem dla $P(x_1^n) = 2^{-n}$, gdy

$$2M(x_1^n) = M(x_1^n 0) + M(x_1^n 1).$$

- Jeżeli umiemy policzyć x_1^∞, to biorąc $M(x_1^{n+1}) := 2M(x_1^n)$, gromadzimy nieskończony kapitał: $\lim_{n\to\infty} M(x_1^n) = \infty$.

Losowość II: Martyngały

- Niech X_1^∞ będzie dowolnym procesem stochastycznym.

Twierdzenie Dooba:
Z p-stwem 1 dla dowolnego P-martyngału istnieje granica

$$\lim_{n\to\infty} M(X_1^n) \in (-\infty, \infty).$$

Definicja II

Niech $\mathcal{M}$ będzie przeliczalną klasą P-martyngałów.
Sekwencję x_1^∞ nazwiemy $\mathcal{M}$-losową, jeżeli

$$\forall_{M\in\mathcal{M}} \quad \limsup_{n\to\infty} M(x_1^n) < \infty.$$

Proces X_1^∞ jest $\mathcal{M}$-losowy z p-stwem 1.

Losowość III: Zbiory miary zero

- Niech X_1^∞ będzie dowolnym procesem stochastycznym.

Definicja III

Niech $\mathcal{N}$ będzie przeliczalną klasą podzbiorów sekwencji.
Sekwencję x_1^∞ nazwiemy $\mathcal{N}$-losową, jeżeli

$$\forall_{N\in\mathcal{N}} \quad P(X_1^\infty \in N) = 0 \implies x_1^\infty \notin N.$$

— Łatwiej jest badać zbiory miary 0 niż miary 1.

Proces X_1^∞ jest $\mathcal{N}$-losowy z p-stwem 1.

Problem: Równoważność definicji

Definicja I: kody bezprefiksowe

Sekwencję x_1^∞ nazwiemy $\mathcal{C}$-losową, jeżeli

$$\forall_{C \in \mathcal{C}} \quad \inf_{n \in \mathbb{N}} \left[\left| C(x_1^n) \right| + \log P(x_1^n) \right] > -\infty.$$

Definicja II: P-martyngały

Sekwencję x_1^∞ nazwiemy $\mathcal{M}$-losową, jeżeli

$$\forall_{M \in \mathcal{M}} \quad \limsup_{n \to \infty} M(x_1^n) < \infty.$$

Definicja III: zbiory miary zero

Sekwencję x_1^∞ nazwiemy $\mathcal{N}$-losową, jeżeli

$$\forall_{N \in \mathcal{N}} \quad P(X_1^\infty \in N) = 0 \implies x_1^\infty \notin N.$$

Maszyna z rejestrami

Maszyna składa się z rejestrów $R_1, R_2, \ldots \in \mathbb{N}$.

Interpretuje ona programy składające się ze skończonej liczby instrukcji postaci:

- $R_j := 1$;
- $R_j := R_j + 1$;
- $R_j := R_k$;
- IF $R_j = R_k$ GO TO m;

Stan maszyny: $(x_0, x_1, \ldots, x_k)$ — $x_0 =$ nr instrukcji, $R_j = x_j$.

Funkcja częściowa obliczana przez program π:

$$\pi(x_{11}, \ldots, x_{k1}) := x_{1M} \iff$$
$$(1, x_{11}, \ldots, x_{k1}) \to \ldots \to (|\pi| + 1, x_{1M}, \ldots, x_{kM})$$

lub jeżeli obliczenie się nie kończy: $\pi(x_{11}, \ldots, x_{k1}) := \perp$.

Funkcje całkowite i częściowe rekurencyjne

Funkcja całkowita: $f : A \to B$

Funkcja częściowa: $f : A \xrightarrow{o} B \iff f : A \to B \cup \{\perp\}$

Definicja

Funkcja $f : \mathbb{N}^k \xrightarrow{o} \mathbb{N}$ jest rekurencyjna, jeżeli istnieje program π taki, że

$$\forall_{x_1,..,x_k \in \mathbb{N}} \quad f(x_1, x_2, .., x_k) = \pi(x_1, x_2, ..., x_k, 1, ..., 1)$$

— z uwzględnieniem wartości $\perp$.

Obierając kanoniczne bijekcje $\phi : \mathbb{X}^* \to \mathbb{N}$ i $\psi : \mathbb{Q} \to \mathbb{N}$ definiujemy rekurencyjne funkcje słów i liczb wymiernych, kładąc jako argumenty lub wartości kody $\phi(w)$ i $\psi(q)$.

Zbiory rekurencyjne i rekurencyjnie przeliczalne

Definicja

- Zbiór $A \subseteq \mathbb{N}^k$ jest rekurencyjny, jeżeli istnieje całkowita funkcja rekurencyjna $f : \mathbb{N}^k \to \mathbb{N}$ taka, że

$$(n_1, ..., n_k) \in A \iff f(n_1, ..., n_k) = 1.$$

- Zbiór $A \subseteq \mathbb{N}^k$ jest rekurencyjnie przeliczalny (r.p.), jeżeli istnieje częściowa funkcja rekurencyjna $f : \mathbb{N}^k \xrightarrow{o} \mathbb{N}$ taka, że

$$(n_1, ..., n_k) \in A \iff f(n_1, ..n_k) = 1.$$

Zbiory $A_1, A_2, ...$ są jednostajnie rekurencyjne lub r.p., gdy zbiór $\bigcup_{n\in\mathbb{N}} \{n\} \times A_n$ jest rekurekcyjny lub r.p.

Jeżeli A i $\mathbb{N} \setminus A$ są r.p., to A jest rekurencyjny.

Problem stopu i funkcja uniwersalna

- Zbiór częściowych funkcji rekurencyjnych jest przeliczalny.
- Niech $f_1, f_2, \ldots$ będzie wyliczeniem częściowych funkcji rekurencyjnych z jednym argumentem w ich kanonicznym porządku (zadanym przez porządek programów).
- Funkcja U nazywana jest uniwersalną, gdy $U(n, m) = f_n(m)$ dla wszystkich n i m (z uwzględnieniem wartości $\perp$).

Twierdzenie

Funkcja uniwersalna jest rekurencyjna.

Twierdzenie

Zbiór $\{n : U(n, n) \neq \perp\}$ jest r.p., ale nie jest rekurencyjny.

Funkcje i liczby rzeczywiste

Definicja

- Funkcja $f : \mathbb{N} \xrightarrow{o} \mathbb{R}$ jest rekurencyjna, jeżeli zbiory $A_n := \{q \in \mathbb{Q} : q < f(n)\}$ są jednostajnie rekurencyjne.
- Funkcja $f : \mathbb{N} \xrightarrow{o} \mathbb{R}$ jest r.p., jeżeli zbiory $A_n := \{q \in \mathbb{Q} : q < f(n)\}$ są jednostajnie r.p.

Jeżeli f i $-f$ są r.p., to f jest rekurencyjna.

Funkcje bezprefiksowe (komputery)

- Funkcja częściowa $f : \{0,1\}^* \xrightarrow{o} B$ nazywa się bezprefiksowa, jeżeli jej dziedzina

$$\mathbf{dom}\, f := \left\{p \in \{0,1\}^* : f(p) \neq \perp\right\}$$

  jest bezprefiksowa, tzn $\forall_{p,q \in \mathbf{dom}\, f}\, [p = qr \implies p = q]$.
- Niech $f_1, f_2, \ldots$ będzie wyliczeniem częściowych funkcji rekurencyjnych bezprefiksowych w ich kanonicznym porządku.
- Niech $C : \mathbb{N} \to \{0,1\}^*$ będzie kanonicznym kodem bezprefiksowym.
- Funkcja $U : \{0,1\}^* \xrightarrow{o} B$ nazywana jest bezprefiksowo uniwersalną, gdy $U(C(n)p) = f_n(p)$ dla wszystkich n i p (z uwzgl. wart. $\perp$), zaś $U(w) = \perp$ dla pozostałych w.

Twierdzenie

Funkcja bezprefiksowo uniwersalna jest bezprefiksowa rekurencyjna.

Bezprefiksowa złożoność Kołmogorowa

- Niech $U : \{0,1\}^* \xrightarrow{o} B$ będzie funkcją bezprefiksowo uniwersalną.
- Niech $x \in B$.
- Kod Kołmogorowa to odwzorowanie $x \mapsto x^*$, gdzie

$$x^* := \operatorname*{arg\,min}_{p \in \{0,1\}^* : U(p) = x} |p| .$$

  Kod Kołmogorowa jest bezprefiksowy.
- Złożoność Kołmogorowa to funkcja

$$K(x) := |x^*| .$$

  Funkcja $x \mapsto -K(x)$ jest r.p., ale nie jest rekurencyjna.

Problem: Równoważność definicji

Definicja I: złożoność Kołmogorowa

Sekwencję x_1^∞ nazwiemy K-losową, jeżeli

$$\inf_{n\in\mathbb{N}} \left[K(x_1^n) + \log P(x_1^n)\right] > -\infty.$$

Definicja II: P-martyngały

Sekwencję x_1^∞ nazwiemy $\mathcal{M}$-losową, jeżeli

$$\forall_{M\in\mathcal{M}} \quad \limsup_{n\to\infty} M(x_1^n) < \infty.$$

Definicja III: zbiory miary zero

Sekwencję x_1^∞ nazwiemy $\mathcal{N}$-losową, jeżeli

$$\forall_{N\in\mathcal{N}} \quad P(X_1^\infty \in N) = 0 \implies x_1^\infty \notin N.$$

Nierówność Hoeffdinga i lemat Borela-Cantellego

- Niech X_i — rzuty uczciwą monetą.
- Połóżmy: $N_n = \left\{ x_1^n : \left| \frac{1}{n} \sum_{i=1}^{n} x_i - \frac{1}{2} \right| \geq \sqrt{\frac{\log n}{n}} \right\}$.
- Nierówność Hoeffdinga: $P(X_1^n \in N_n) \leq 2n^{-2}$.
- Lemat Borela-Cantellego:

$$\sum_{n \in \mathbb{N}} P(A_n) < \infty \implies P\left(\bigcap_{n \in \mathbb{N}} \bigcup_{k \geq n} A_k \right) = 0.$$

- Zatem

$$P\left(\bigcap_{n \in \mathbb{N}} (X_1^n \in N_n) \right) = P\left(\bigcap_{n \in \mathbb{N}} \bigcup_{k \geq n} (X_1^k \in N_k) \right) = 0.$$

Efektywne zbiory miary zero

- Dla $L \subseteq \{0,1\}^{\mathbb{N}}$ określmy $[L] := \left\{x_1^\infty : \exists_{n\in\mathbb{N}}\, x_1^n \in L\right\}$.
- Zbiór sekwencji $N \subseteq \{0,1\}^{\mathbb{N}}$ nazywamy zbiorem P-Martina-Löfa, jeżeli istnieją zbiory słów $N_n \subseteq \{0,1\}^*$ jednostajnie r.p. oraz całkowita funkcja rekurencyjna $f : \mathbb{N} \to \mathbb{R}$ takie, że

$$P\left(X_1^\infty \in [N_n]\right) \leq f(n)$$

oraz $\lim_{n\to\infty} f(n) = 0$ i $N = \bigcap_{n\in\mathbb{N}}[N_n]$.

- Zbiór sekwencji $N \subseteq \{0,1\}^{\mathbb{N}}$ nazywamy zbiorem P-Solovaya, jeżeli istnieją zbiory słów $N_n \subseteq \{0,1\}^*$ jednostajnie r.p. oraz całkowita funkcja rekurencyjna $f : \mathbb{N} \to \mathbb{R}$ takie, że

$$P\left(X_1^\infty \in [N_n]\right) \leq f(n)$$

oraz $\sum_{n\in\mathbb{N}} f(n) < \infty$ i $N = \bigcap_{n\in\mathbb{N}} \bigcup_{k\geq n} [N_k]$.

- $P(X_1^\infty \in N) = 0$ w obu przypadkach.

Twierdzenie Schnorra i sekwencje Martina-Löfa

Twierdzenie (Schnorr)

Niech:

- P — miara rekurencyjna;
- K — bezprefiksowa złożoność Kołmogorowa;
- $\mathcal{M}$ — klasa r.p. P-martyngałów;
- $\mathcal{N}_{ML}$ — klasa zbiorów P-Martina-Löfa;
- $\mathcal{N}_S$ — klasa zbiorów P-Solovaya.

Zbiory sekwencji K-, $\mathcal{M}$-, $\mathcal{N}_{ML}$- i $\mathcal{N}_S$-losowych są sobie równe.

Definicja

Sekwencje te nazywamy P-losowymi (w sensie Martina-Löfa).

Efektywizacja

Program efektywizacji

Twierdzenie

Zachodzi $\varphi(\omega)$ dla P-prawie wszystkich ω.

$$\Downarrow \Downarrow \Downarrow$$

Twierdzenie

Zachodzi $\varphi(\omega)$ dla wszystkich P-losowych ω.

Trzy źródła twierdzeń „prawie na pewno”

1. Lemat Borela-Cantellego.
2. Zbieżność martyngałów.
3. Twierdzenia ergodyczne.

Lemat Borela-Cantellego i Solovaya

- Lemat Borela-Cantellego:

  $\sum_{n\in\mathbb{N}} P(A_n) < \infty \implies$

  $\omega \notin A_n$ dla prawie wszystkich n dla P-prawie wszystkich ω.

- Lemat Solovaya:

  $P(A_n) \leq f(n)$ rekurencyjna i $\sum_{n\in\mathbb{N}} f(n) < \infty \implies$

  $\omega \notin A_n$ dla prawie wszystkich n dla P-losowych ω.

- Nierówność Hoeffdinga:

  X_i — niezależne rzuty obciążoną monetą, $\mu = P(X_i = 1)$

  $$P\left(\left|\frac{1}{n}\sum_{i=1}^{n} X_i - \mu\right| \geq t\right) \leq 2\exp(-2nt^2).$$

- Mocne prawo wielkich liczb:

  $\lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} X_i = \mu$ na punktach losowych.

Zbieżność martyngałów

Czy istnieje granica $\lim_{n\to\infty} Y_n$ dla $Y_n := P(X_0|X_{-n}^{-1})$?

- Oznaczmy $C_\infty^{[a,b]} := \sup_{t\in\mathbb{N}} C_t^{[a,b]}$, gdzie $C_t^{[a,b]} :=$
$$\max\left\{m \geq 0 : \begin{array}{c} 1 \leq L_1 < U_1 < \ldots < L_m < U_m \leq t, \\ Y_{L_s} \leq a < b \leq Y_{U_s} \text{ dla } 1 \leq s \leq m \end{array}\right\}.$$
- $C_\infty^{[a,b]} = \infty$, jeżeli $\liminf_{n\to\infty} Y_n < a$ i $\liminf_{n\to\infty} Y_n > b$.
- Jeżeli (Y_n) reprezentuje kursy akcji na giełdzie, to oczekiwany zysk ≤ 0. W szczególności $\mathbb{E}\left[(b-a)C_n^{[a,b]} - 2\right] \leq 0$. Stąd
$$P(C_\infty^{[a,b]} \geq n) \leq n^{-1} \sup_{t\in\mathbb{N}} \mathbb{E}\, C_t^{[a,b]} \leq 2n^{-1}(b-a)^{-1}.$$
- Zdarzenia $(C_\infty^{[a,b]} \geq n)$ są jednostajnie r.p. dla $a, b \in \mathbb{Q}$.
- Zdarzenie $(C_\infty^{[a,b]} = \infty)$ jest zbiorem Martina-Löfa.
- Prawo Levy'ego: $\lim_{n\to\infty} Y_n$ istnieje na punktach losowych.

Twierdzenia ergodyczne

- Twierdzenie ergodyczne Birkhoffa:
  Niech P będzie miarą stacjonarną ergodyczną względem T.
  Dla każdej zmiennej losowej Y takiej, że $\int |Y| \, dP < \infty$,

$$\lim_{n\to\infty} \frac{1}{n} \sum_{j=0}^{n-1} Y \circ T^j = \int Y dP \ P\text{-prawie na pewno.}$$

- Dekompozycja ergodyczna:
  Dla każdej miary stacjonarnej P istnieje jedna miara Q na przestrzeni miar stacjonanych ergodycznych, taka że

$$P(A) = \int E(A) dQ(E) \text{ dla każdego zdarzenia } A.$$

- Udowodniono pewne efektywizacje tych twierdzeń dla rekurencyjnych/r.p. miar P, transformacji T i zmiennych Y.

Co z miarami nierekurencyjnymi? $\Longrightarrow$ Relatywizacja

Relatywizacja: Maszyna z rejestrami i wyrocznią

Maszyna składa się z rejestrów $R_1, R_2, \ldots \in \mathbb{N}$ i wyroczni $W \subset \mathbb{N}$.

Interpretuje ona programy składające się ze skończonej liczby instrukcji postaci:

- $R_j := 1$;
- $R_j := R_j + 1$;
- $R_j := R_k$;
- IF $R_j = R_k$ GO TO m;
- IF $R_j \in W$ GO TO m;

Stan maszyny: $(x_0, x_1, \ldots, x_k)$ — $x_0 =$ nr instrukcji, $R_j = x_j$.

Funkcja częściowa obliczana przez program π:

$$\pi(x_{11}, \ldots, x_{k1}|W) := x_{1M} \iff$$
$$(1, x_{11}, \ldots, x_{k1}) \to \ldots \to (|\pi| + 1, x_{1M}, \ldots, x_{kM})$$

lub jeżeli obliczenie się nie kończy: $\pi(x_{11}, \ldots, x_{k1}|W) := \perp$.

Funkcje całkowite i częściowe rekurencyjne (uogóln. I)

Funkcja całkowita: $f : A \to B$

Funkcja częściowa: $f : A \xrightarrow{o} B \iff f : A \to B \cup \{\perp\}$

Definicja

Funkcja $f : \mathbb{N}^k \xrightarrow{o} \mathbb{N}$ jest W-rekurencyjna, jeżeli istnieje program π taki, że

$$\forall_{x_1,..,x_k \in \mathbb{N}} \quad f(x_1, x_2, .., x_k) = \pi(x_1, x_2, ..., x_k, 1, ..., 1 | W)$$

— z uwzględnieniem wartości $\perp$.

Obierając kanoniczne bijekcje $\phi : \mathbb{X}^* \to \mathbb{N}$ i $\psi : \mathbb{Q} \to \mathbb{N}$ definiujemy W-rekurencyjne funkcje słów i liczb wymiernych, kładąc jako argumenty lub wartości kody $\phi(w)$ i $\psi(q)$.

Funkcje całkowite i częściowe rekurencyjne (uogóln. II)

Funkcja całkowita: $f : A \to B$

Funkcja częściowa: $f : A \xrightarrow{o} B \iff f : A \to B \cup \{\perp\}$

Definicja

Funkcja $f : \mathbb{N}^k \times 2^{\mathbb{N}} \xrightarrow{o} \mathbb{N}$ jest rekurencyjna, jeżeli istnieje program π taki, że

$$\forall_{x_1,..,x_k \in \mathbb{N}} \quad f(x_1, x_2, .., x_k | W) = \pi(x_1, x_2, ..., x_k, 1, ..., 1 | W)$$

— z uwzględnieniem wartości $\perp$.

Obierając kanoniczne bijekcje $\phi : \mathbb{X}^* \to \mathbb{N}$, $\psi : \mathbb{Q} \to \mathbb{N}$ oraz $\xi : \mathbb{R} \ni r \mapsto \{q \in \mathbb{Q} : q < r\} \in 2^{\mathbb{Q}}$ definiujemy rekurencyjne funkcje słów, liczb wymiernych oraz liczb rzeczywistych, kładąc jako argumenty lub wartości kody $\phi(w)$, $\psi(q)$ i $\xi(r)$.

Twierdzenie Schnorra z wyrocznią

Rodzina parametryczna miar:

$$P : \mathbb{X}^* \times \mathbb{R} \ni (x_1^n, \theta) \mapsto P_\theta(x_1^n) \in \mathbb{R}.$$

Wyrocznia: $\xi(\theta) = \{q \in \mathbb{Q} : q < \theta\}$.
Niech dla pewnego $\theta \in \mathbb{R}$:

- P_θ — miara $\xi(\theta)$-rekurencyjna;
- $\mathcal{M}$ — klasa $\xi(\theta)$-P_θ-r.p. martyngałów;
- $\mathcal{N}_{ML}$ — klasa zbiorów $\xi(\theta)$-P_θ-Martina-Löfa;
- $\mathcal{N}_S$ — klasa zbiorów $\xi(\theta)$-P_θ-Solovaya.

Wówczas sekwencja x_1^∞ jest P_θ-losowa, gdy równoważnie

- $\inf_{n\in\mathbb{N}} \left[K(x_1^n|\theta) + \log P_\theta(x_1^n)\right] > -\infty$,
- $M \in \mathcal{M} \implies \limsup_{n\to\infty} M(x_1^n) < \infty$,
- $N \in \mathcal{N}_{ML} \cup \mathcal{N}_S \implies x_1^\infty \notin N$.

Zbiór sekwencji P_θ-losowych ma P_θ-miarę 1.

Optymalność wnioskowania bayesowskiego

- Uogólnione twierdzenie van Lambalgena:
  Niech Q — rekurencyjne, P — rekurencyjne, zaś
  $$Y(x_1^n) := \int P_\theta(x_1^n)\, dQ(\theta).$$
  Wówczas sekwencja x_1^∞ jest Y-losowa $\iff$
  istnieje Q-losowy parametr θ taki, że x_1^∞ jest P_θ-losowa.
- Sekwencja x_1^∞ jest Y-losowa $\iff$ $-\log Y(x_1^n)$ jest dobrym przybliżeniem złożoności Kołmogorowa $K(x_1^n)$.
- Załóżmy, że zbiory sekwencji P_θ-losowych są rozłączne. (Tzn. istnieje zgodny estymator parametru θ.)
- Wówczas:
  Wnioskowanie bayesowskie jest optymalną procedurą kompresji $\iff$ parametr jest losowy względem rozkładu Q.

Co z innymi funkcjami straty?

Martin-Löf: Losowość nieasymptotyczna

Czy jeśli złożoność Kołmogorowa skończonego słowa jest duża, to musi ono wykazywać jakieś prawa losowości?

— Tak!

Załóżmy, że $N_n \subseteq \{0,1\}^n$ (j. rekurencyjne zbiory małej miary).

Wówczas z kodowania Shannona-Fano mamy

$$x_1^n \in N_n \implies K(x_1^n) \leq c + K(P) + K(N_n) - \log \frac{P(x_1^n)}{P(N_n)}.$$

Zatem

$$K(x_1^n) > c + K(P) + K(N_n) + \log \frac{P(N_n)}{P(x_1^n)} \implies x_1^n \notin N_n.$$

Poniżej Martina-Löfa: Pseudolosowość

Anyone who attempts to generate random numbers by deterministic means is, of course, living in a state of sin.

John von Neumann

Czy jeśli złożoność Kołmogorowa skończonego słowa jest mała, to może wykazywać ono jakieś prawa losowości?

Liczba Champerowne'a **0.123456789101112...** jest rekurencyjna ale normalna, tzn. dowolne bloki cyfr w jej rozwinięciu dziesiętnym występują równie często.

Hipoteza: liczby π i e są normalne.

Co z innymi prawami losowości? Np. prawo iterowanego logarytmu:

$$\limsup_{n\to\infty} \frac{\sum_{i=1}^{n}(2x_i - 1)}{\sqrt{2n \ln \ln n}} = 1$$

Powyżej Martina-Löfa: Hierarchie obliczalności

Klasyfikacje zbiorów sekwencji ze względu na stopień obliczalności:

- Stopnie Turinga (klasy abstrakcji relacji redukowalności $\equiv_T$).
- Skok Turinga (operator inkrementacji na stopniach Turinga):
  $\emptyset^{(0)} = \emptyset$ (sekwencje rekurencyjne),
  $\emptyset^{(1)}$ (sekwencje równoważne problemowi stopu, np. Ω),
  $\emptyset^{(2)}$ (problem stopu | problem stopu), ...
- Hierarchia arytmetyczna:
  $\Sigma^0_0 = \emptyset$, $\Pi^0_0 = \emptyset$, $\Delta^0_0 := \Sigma^0_0 \cap \Pi^0_0 = \emptyset$,
  Σ^0_1 (r.p.), Π^0_1 (ko-r.p.), $\Delta^0_1 := \Sigma^0_1 \cap \Pi^0_1 = \emptyset$,
  Σ^0_2 (r.p.$|\Pi^0_1$), Π^0_2 (ko-r.p.$|\Sigma^0_1$), $\Delta^0_2 := \Sigma^0_2 \cap \Pi^0_2$, ...

n-losowość $\iff$ losowość względem wyroczni $\in \emptyset^{(n-1)}$
(1-losowość $\iff$ losowość w sensie Martina-Löfa)

Wszystkie zbiory n-losowych sekwencji są miary 1.
"Absolutna" losowość jest silniejsza niż n-losowości.

Niedowodliwość losowości konkretnej sekwencji

system formalny: aksjomaty + reguły wnioskowania

Twierdzenie Gödla

Dla dowolnego zdrowego systemu formalnego M, który zawiera arytmetykę, istnieją zdania wyrażalne w M, które są prawdziwe, ale nie mają dowodu w M.

↑ Paradoks kłamcy: „Ja teraz kłamię.”

Twierdzenie Chaitina

Istnieje stała c taka, że dla dowolnego zdrowego systemu formalnego M, w którym można wyrazić teorię obliczeń, zdania „$K(w) \geq K(M) + c$” nie mają dowodu w M dla żadnego w.

↑ Paradoks Berry'ego: „Najmniejsza liczba naturalna, której nie można określić wyrażeniem o mniej niż dwudziestu słowach.”

Odrobinę ideologii

I would like to able to say that if one has ten pounds of axioms and a twenty-pound theorem, then that theorem cannot be derived from those axioms. And I will argue that this approach to Gödel's theorem does suggest a change in the daily habits of mathematicians, and that Gödel's theorem cannot be shrugged away.

Gregory Chaitin

Prawdopodobieństwo stopu Ω

Nierówność Krafta: (dla zbioru bezprefiksowego $A \subseteq \{0,1\}^*$)

$$\sum_{w \in A} 2^{-|w|} \leq 1.$$

Stała Chaitina: (dla funkcji bezprefiksowo uniwersalnej U)

$$\Omega := \sum_{p \in \{0,1\}^* : U(p) \neq \perp} 2^{-|p|} < 1.$$

Rozwinięcie binarne:

$\Omega_1, \Omega_2, \ldots \in \{0,1\}$ takie, że $\Omega = \sum_{k=1}^{\infty} \Omega_k 2^{-k}$.

Stała Ω rozwiązuje problem stopu

Niech U będzie funkcją bezprefiksowo uniwersalną. Zbiór

$$\mathbf{dom}\, U := \{p \in \{0,1\}^* : U(p) \neq \perp\}$$

jest r.p., ale nie jest rekurencyjny (problem stopu).

Twierdzenie

Istnieje częściowa funkcja rekurencyjna h taka, że

$$h(p, \Omega_1^n) = \begin{cases} 1, & \text{jeżeli } U(p) \neq \perp, \\ 2, & \text{jeżeli } U(p) = \perp, \end{cases}$$

dla każdego $p \in \{0,1\}^*$ takiego, że $|p| \leq n$.

W szczególności mając dostatecznie długie Ω_1^n, możemy policzyć, czy zatrzyma się program szukający kontrprzykładów dla naszej ulubionej hipotezy matematycznej (np. hipotezy Goldbacha).

Losowość stałej Ω w sensie Martina-Löfa

Twierdzenie

Istnieje stała c taka, że $K(\Omega_1^n) \geq n - c$.

Powód: Mając Ω_1^n możemy wyliczyć takie w, że $K(w) > n$.

- Powyższe twierdzenie nie przeczy twierdzeniu Chaitina, gdyż możemy policzyć Ω_1^n tylko dla skończenie wielu n.
- Zbiór $\{q \in \mathbb{Q} : q < \Omega\}$ jest rekurencyjnie przeliczalny, ale zbiór $\{k \in \mathbb{N} : \Omega_k = 1\}$ nie jest rekurencyjnie przeliczalny.
- Dobrzy ludzie policzyli: $\Omega = 0.00787499699...$
- Znając n pierwszych cyfr Ω możemy obliczyć, które hipotezy matematyczne długości mniejszej niż n są prawdziwe, a które są fałszywe (chodzi tu o długość po sformalizowaniu w postaci programu wyszukującego kontrprzykłady).

Podsumowanie

Losowość w sensie Martina-Löfa:

- W statystyce matematycznej do teoretycznej analizy punktowych własności nierandomizowanych procedur wnioskowania powinna wystarczyć losowość Martina-Löfa.
- Program efektywizacji twierdzeń probabilistycznych i statystycznych warto doprowadzić do bliskiego końca.

Wyższe piętra losowości:

- Co się dzieje, gdy stosujemy procedury randomizowane?
- Czym jest "absolutna" losowość, jeżeli istnieje?
- Czy "absolutna" losowość ma jakieś przełożenie praktyczne? (Mechanika kwantowa? Jak dobrze Bóg gra w kości? Czy stała $\mathbf{\Omega}$ ma jakieś znaczenie fizyczne?)

Niższe piętra losowości:

- Jak wiele praw losowości mogą spełniać ciągi pseudolosowe lub rozwinięcia rekurencyjnych liczb niewymiernych?