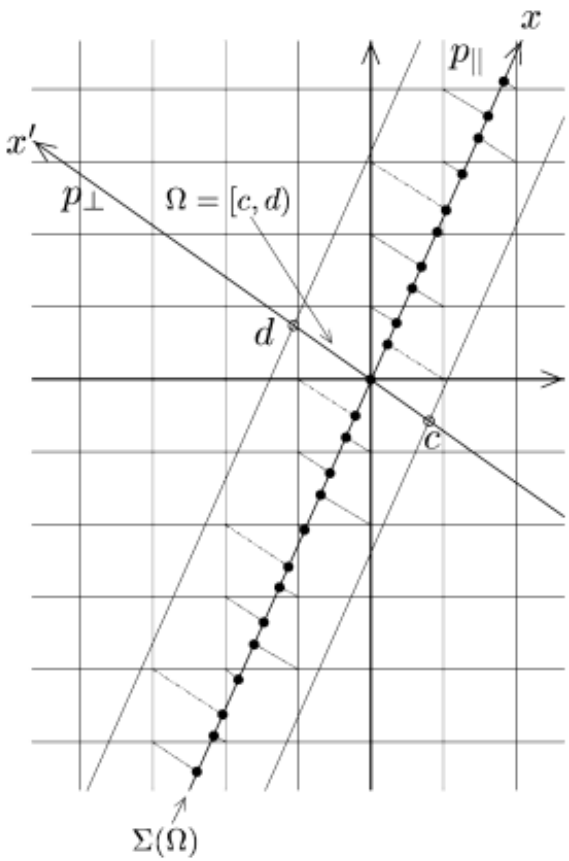
Generátory pseudonáhodných čísel II - využití kombinatoriky na slovech

Karel Břinda
karel.brinda@fjfi.cvut.cz

Theoretical **I**nformatics **Gr**oup
FJFI ČVUT v Praze

Combinatorics on Words 2011
Fryšava, 18. května 2011

Stručně o kvazikrystalech



Modelovány pomocí cut and project množin - projekce m-dimenzionální mřížky do n-dimenzionálního prostoru
$x^2 = x + 1$, kořeny β, β'; pro názornost budem používat τ

Stručně o kvazikrystalech

Automorfismus $' : \mathbb{Q}[\tau] \to \mathbb{Q}[\tau]$

$$(a + b\tau)' = a + b\tau'$$

Definice

Jednodimenzionální cut and project kvazikrystal je množina

$$\Sigma(\Omega) = \{x \in \mathbb{Z}[\tau'] \mid x' \in \Omega\},^a$$

kde Ω je omezený interval v $\mathbb{R}$ s neprázdným vnitřkem. Ω se nazývá „okýnko“.

$^a\mathbb{Z}[\tau] = \{a + b\tau \mid a, b \in \mathbb{Z}\}$

Stručně o kvazikrystalech

Věta

Nechť $\Sigma(\Omega)$ je kvazikrystal. Potom má $\Sigma(\Omega)$ následující vlastnosti:

i) *Posun*

$$\Sigma(\Omega + \lambda') = \Sigma(\Omega) + \lambda$$

ii) *Zvětšení/zmenšení*

$$\Sigma(\tau^i \Omega) = (\tau')^i \Sigma(\Omega)$$

Věta

Nechť $\Sigma(\Omega)$ je kvazikrystal. Až na zvětšení/zmenšení a posun můžeme předpokládat $0 \in \Omega = [c, d)$ a $d - c \in [1, \tau)$. Dále můžeme volit počáteční bod kvazikrystalu $x_0 = 0$.

Stručně o kvazikrystalech

Věta

Nechť $\Sigma(\Omega)$ je kvazikrystal s „okýnkem“ $\Omega = [c, d)$, kde $d - c \in [1, \tau)$. Nechť $(x_i)_{i \in \mathbb{Z}}$ je uspořádaná posloupnost bodů množiny $\Sigma(\Omega)$. Potom $\Sigma(\Omega)$ splňuje jednu z podmínek:

i) *Pokud $d - c = 1$, pak $\Sigma(\Omega)$ je dvoudlaždicový kvazikrystal, konkrétně pro každé i*

$$x_{i+1} - x_i \in \{\tau, \tau^2\}$$

a každá z těchto vzdáleností se nabývá nekonečněkrát.

ii) *Pokud $d - c \neq 1$, pak $\Sigma(\Omega)$ je třídlaždicový kvazikrystal, konkrétně pro každé i*

$$x_{i+1} - x_i \in \{1, \tau, \tau^2\}$$

a každá z těchto vzdáleností se nabývá nekonečněkrát.

Stručně o kvazikrystalech

Věta

Nechť $\Sigma(\Omega) = \Sigma[c, d), d - c =\in [1, \tau)$ *je kvazikrystal. Nechť* $\Sigma_S, \Sigma_M, \Sigma_L$ *jsou množiny bodů z* $\Sigma(\Omega)$ *takové, že*

i) $\Sigma_S = \{x_i \in \Sigma(\Omega) \mid x_{i+1} - x_i = 1\}$,

ii) $\Sigma_M = \{x_i \in \Sigma(\Omega) \mid x_{i+1} - x_i = \tau\}$,

iii) $\Sigma_L = \{x_i \in \Sigma(\Omega) \mid x_{i+1} - x_i = \tau^2\}$.

Pak platí

i) $\Sigma_S = \{x \in \mathbb{Z}[\tau] \mid x' \in \Omega_S = [c, d - 1)\}$,

ii) $\Sigma_M = \{x \in \mathbb{Z}[\tau] \mid x' \in \Omega_M = [c + \frac{1}{\tau}, d)\}$,

iii) $\Sigma_L = \{x \in \mathbb{Z}[\tau] \mid x' \in \Omega_L = [d - 1, c + \frac{1}{\tau})\}$.

Stručně o kvazikrystalech

Definice

Nechť $\Sigma(\Omega) = \Sigma[c, d)$, *kde* $d - c \in [1, \tau)$. *Potom definujeme krokovací funkci* $f : \Omega \to \Omega$ *jako*

$$f(x) = \begin{cases} x + 1 & \text{pro } x \in \Omega_S = [c, d - 1), \\ x - \frac{1}{\tau} & \text{pro } x \in \Omega_M = [c + \frac{1}{\tau}, d), \\ x - \frac{1}{\tau^2} & \text{pro } x \in \Omega_L = [d - 1, c + \frac{1}{\tau}). \end{cases}$$

Stručně o kvazikrystalech

Věta

Nechť $\Sigma(\Omega) = \Sigma[c, c+d)$ je takový kvazikrystal, že $1 \leq d < \tau$. Potom jsou hustoty dlaždic S, M a L následující: $\frac{1}{d}(d-1), \frac{1}{d}(d-\frac{1}{\tau}), \frac{1}{d}(\tau-d)$.

Malé shrnutí z minula

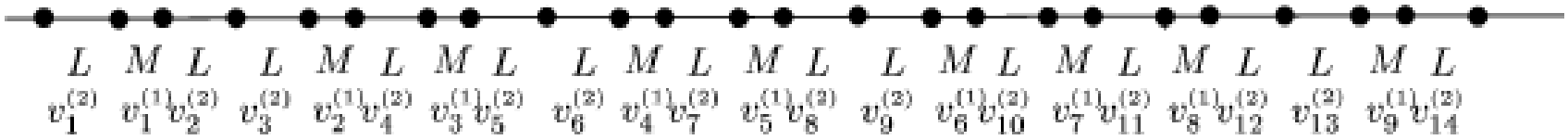
LCG:

- $X_{n+1} = (aX_n + c) \mod m$
- c a m jsou nesoudělné; $a - 1$ je násobkem každého prvočísla, které dělí m; $a - 1$ je násobkem 4, pokud je i m násobkem 4.

MCG:

- LCG, kde $c = 0$

Konstrukce aperiodických generátorů

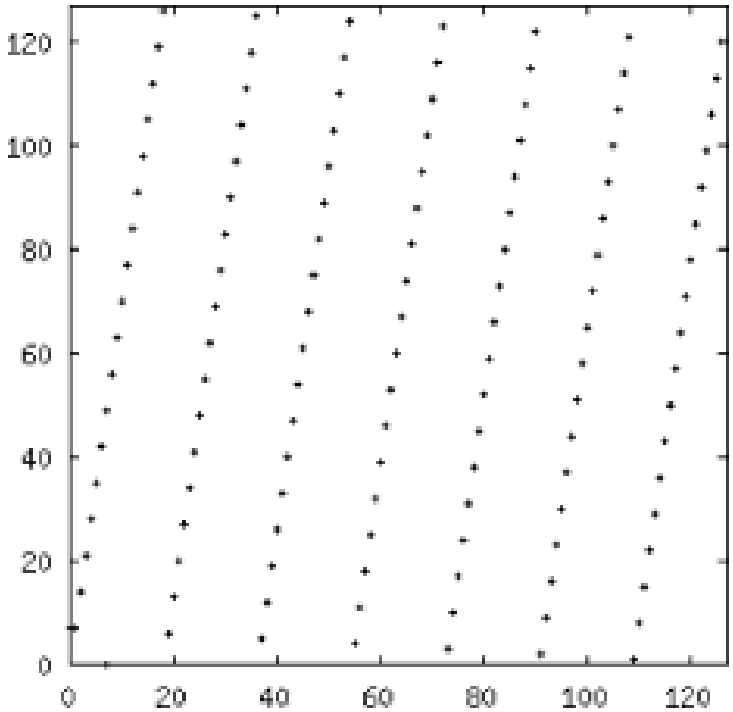


Konstrukce aperiodických generátorů

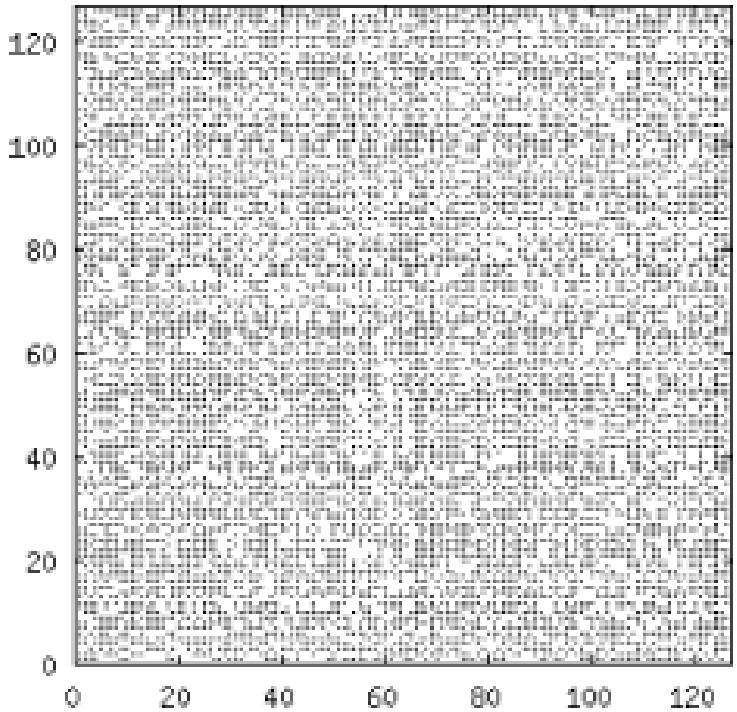
Věta (!!!)

Nechť Z je pseudonáhodná posloupnost generovaná APRNG použitím dvoudlaždicového kvazikrystalu kombinování 2 periodických PRNG. Pokud mají stejnou množinu Γ racionálních výstupních hodnot, potom dostatečně dlouhý segment ze Z nemá žádnou mřížkovou strukturu. (Jinými slovy - libovolná rodina nadrovin pokrývajících všechny t-tice v dostatečně dlouhém segmentu Z pokrývá také všechny t-tice $(a_1, \ldots, a_t) \in \Gamma$.)

Konstrukce aperiodických generátorů



(a)



(b)

Konstrukce aperiodických generátorů

Nutné implementovat

- LCG
- Generování kvazikrystalu
  - Symbolicky
  - Numericky

Generování pomocí substituce

- Prostorová složitost $\Omega(\log n)$ - na dnešních počítačích můžeme procházet neuvěřitelně dlouhý prefix
- Možnost dalšího prodloužení možného generovaného slova změnou substituce (pro každý kvazikrystal existuje spočetně mnoho substitucí)

Generování pomocí substituce

Příklad

Generování prefixu $u = \varphi^3(0)$ Fibonacciho slova $\lim_{n\to+\infty} \varphi^n(0)$, kde $\varphi(0) = 010,\ \varphi(1) = 01$.

1) Konstrukce zásobníku

Patro	Uložené faktory
0.	**0**
1.	
2.	
3.	

$u = \varphi^3(0)$

Generování pomocí substituce

Příklad

Generování prefixu $u = \varphi^3(0)$ Fibonacciho slova $\lim_{n\to+\infty} \varphi^n(0)$, kde $\varphi(0) = 010,\ \varphi(1) = 01$.

1) Konstrukce zásobníku

Patro	Uložené faktory
0.	~~0~~
1.	**010**
2.	
3.	

$u = \varphi^2(010)$

Generování pomocí substituce

Příklad

Generování prefixu $u = \varphi^3(0)$ Fibonacciho slova $\lim_{n\to+\infty} \varphi^n(0)$, kde $\varphi(0) = 010,\ \varphi(1) = 01$.

1) Konstrukce zásobníku

Patro	Uložené faktory
0.	
1.	~~0~~**10**
2.	**010**
3.	

$u = \varphi(010)\varphi^2(10)$

Generování pomocí substituce

Příklad

Generování prefixu $u = \varphi^3(0)$ Fibonacciho slova $\lim_{n\to+\infty} \varphi^n(0)$, kde $\varphi(0) = 010,\ \varphi(1) = 01$.

1) Konstrukce zásobníku

Patro	Uložené faktory
0.	
1.	**10**
2.	~~**0**~~**10**
3.	**010**

$u = 010\varphi(10)\varphi^2(10)$

Generování pomocí substituce

Příklad

Generování prefixu $u = \varphi^3(0)$ Fibonacciho slova $\lim_{n\to+\infty} \varphi^n(0)$, kde $\varphi(0) = 010,\ \varphi(1) = 01$.

1) Konstrukce zásobníku

Patro	Uložené faktory
0.	
1.	**10**
2.	**10**
3.	**010**

$u = 010\varphi(10)\varphi^2(10)$

Generování pomocí substituce

Příklad

Generování prefixu $u = \varphi^3(0)$ Fibonacciho slova $\lim_{n\to+\infty} \varphi^n(0)$, kde $\varphi(0) = 010,\ \varphi(1) = 01$.

2) Samotné generování prefixu

Patro	Uložené faktory
0.	
1.	**10**
2.	**10**
3.	~~010~~

Zbývá ke zpracování: $\varphi(10)\varphi^2(10)$

Získaný prefix: 010

Generování pomocí substituce

Příklad

Generování prefixu $u = \varphi^3(0)$ Fibonacciho slova $\lim_{n\to+\infty} \varphi^n(0)$, kde $\varphi(0) = 010,\ \varphi(1) = 01$.

2) Samotné generování prefixu

Patro	Uložené faktory
0.	
1.	**10**
2.	**0**
3.	**01**

Zbývá ke zpracování: $01\varphi(0)\varphi^2(10)$

Získaný prefix: 010

Generování pomocí substituce

Příklad

Generování prefixu $u = \varphi^3(0)$ Fibonacciho slova $\lim_{n\to+\infty} \varphi^n(0)$, kde $\varphi(0) = 010,\ \varphi(1) = 01$.

2) Samotné generování prefixu

Patro	Uložené faktory
0.	
1.	**10**
2.	**0**
3.	~~01~~

Zbývá ke zpracování: $\varphi(0)\varphi^2(10)$

Získaný prefix: 01001

Generování pomocí substituce

Příklad

Generování prefixu $u = \varphi^3(0)$ Fibonacciho slova $\lim_{n\to+\infty} \varphi^n(0)$, kde $\varphi(0) = 010,\ \varphi(1) = 01$.

2) Samotné generování prefixu

Patro	Uložené faktory
0.	
1.	**10**
2.	
3.	**010**

Zbývá ke zpracování: $010\varphi^2(10)$

Získaný prefix: 01001

Generování pomocí substituce

Příklad

Generování prefixu $u = \varphi^3(0)$ Fibonacciho slova $\lim_{n\to+\infty} \varphi^n(0)$, kde $\varphi(0) = 010,\ \varphi(1) = 01$.

2) Samotné generování prefixu

Patro	Uložené faktory
0.	
1.	
2.	
3.	**010**

Zbývá ke zpracování: 010

Získaný prefix: 0100101001001010 01

Generování pomocí substituce

Příklad

Generování prefixu $u = \varphi^3(0)$ Fibonacciho slova $\lim_{n\to+\infty} \varphi^n(0)$, kde $\varphi(0) = 010,\ \varphi(1) = 01$.

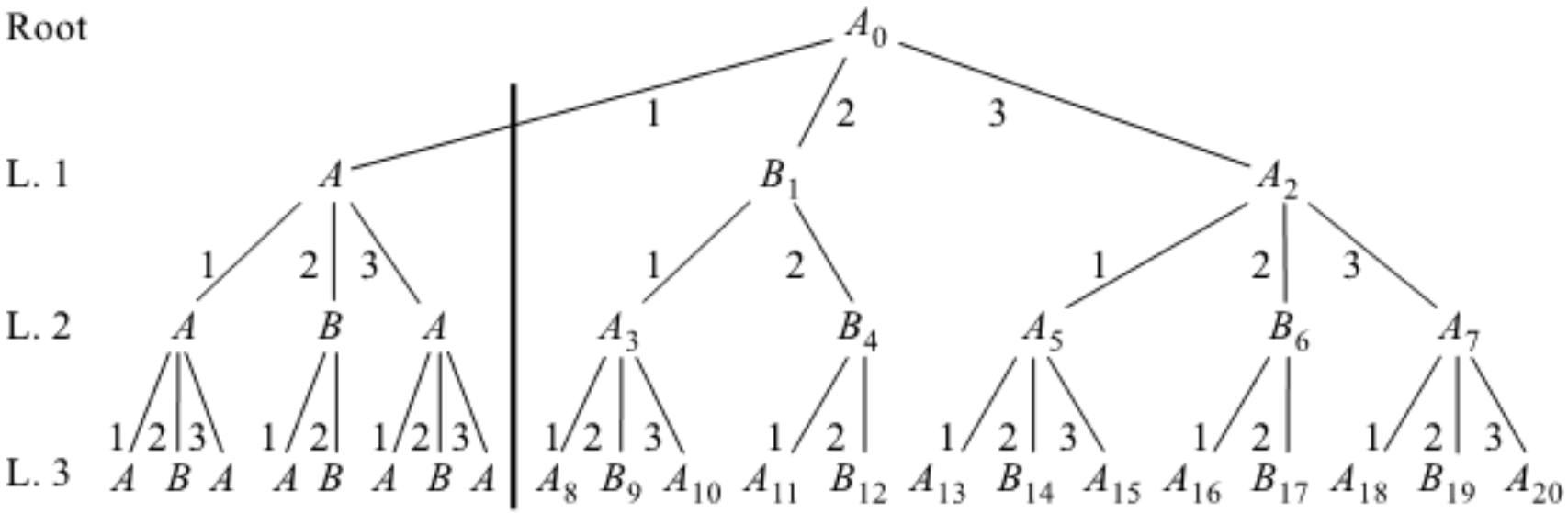
2) Samotné generování prefixu

Patro	Uložené faktory
0.	
1.	
2.	
3.	~~010~~

Zbývá ke zpracování:

Získaný prefix: $01001010010010100 1010 = \varphi^3(0)$

Generování pomocí substituce



Děkuji za pozornost :-)

Literatura

 .-S. Guimond, Ji. Patera, Ja. Patera: **Combining random number generators using cut and project sequences**

 a. Patera: **Generating the Fibonacci chain in $\mathcal{O}(\log n)$ SPACE and $\mathcal{O}(n)$ TIME**