Psevdonaključna števila in generatorji

Knuth:

Random numbers should not be generated with a method chosen at random.

Uvod

- **Uporaba:** simulacije, vzorčenje, numerična analiza, računalniško programiranje, odločanje, zabava, *kriptografija*
- **Generiranje:** s formulo (naključnost?), važen je izgled
- **Kriptografija** pogosto zahteva še nepredvidljivost (tekoče šifre in seme, asimetrični ključi).

Vsebina predstavitve

- Linearni generatorji
- Sistemski in kompleksnostni pristop h gradnji generatorjev in primeri
- Razlikovalci porazdelitev in napovedovalci
- Statistični testi
- Linearna kompleksnost
- Primeri, razprava, naloge

Linearni generatorji

Linearni kongruenčni generator

$s_i=(a*s_{i-1} + b) \bmod M$

$z_i=s_i \bmod 2$

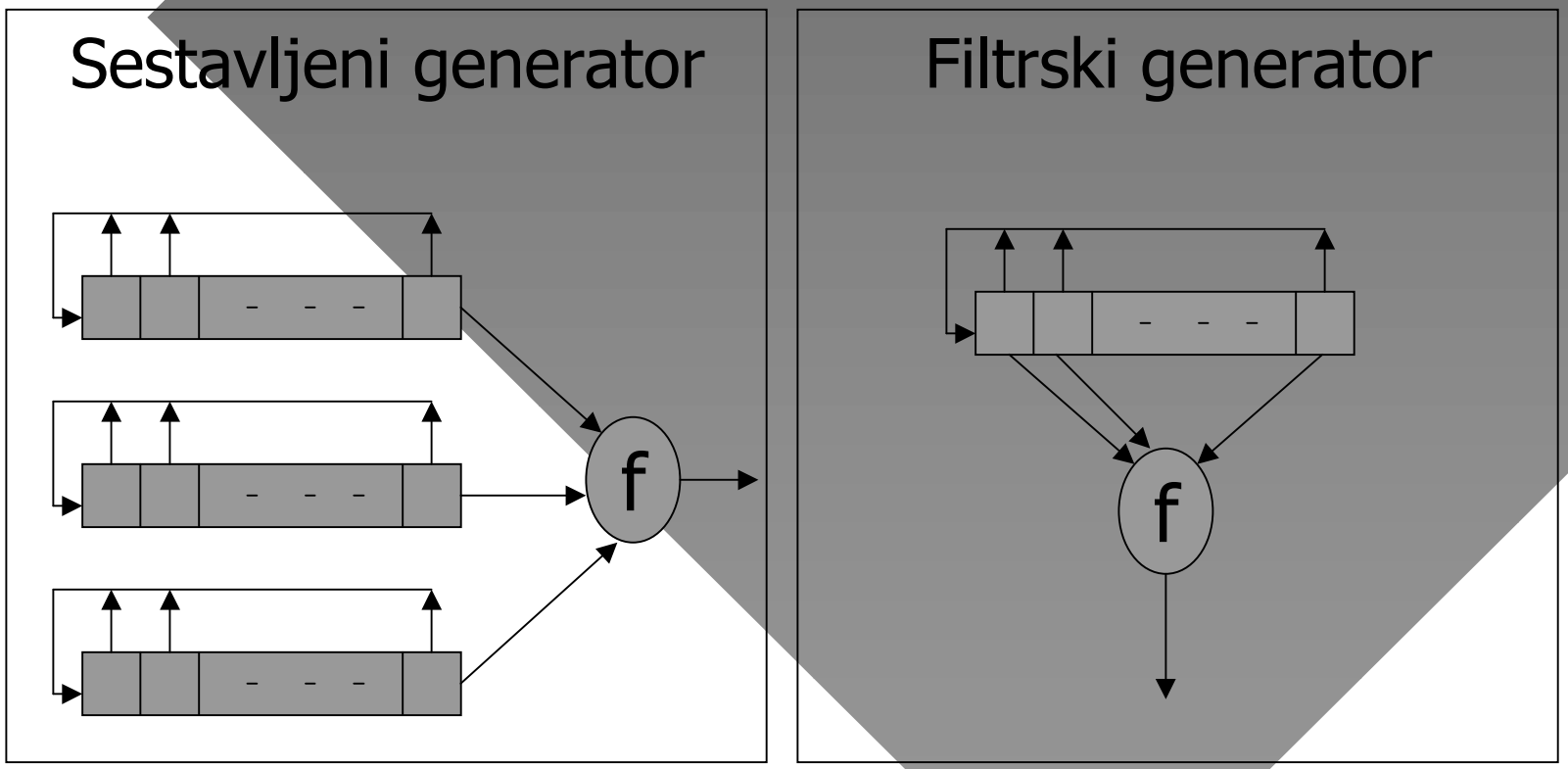
perioda=M $\Leftrightarrow$ b tuj M,
(a-1) večkratnik vsakega prafaktorja M,
če je M večkratnik 4$\Rightarrow$(a-1) tudi

LFSR

Sistemski pristop 1

- gradniki z dokazljivo ugodnimi lastnostmi:
  - perioda
  - porazdelitvena funkcija
  - linearna kompleksnost
  - razdalja do linearnih struktur

Sistemski pristop 2

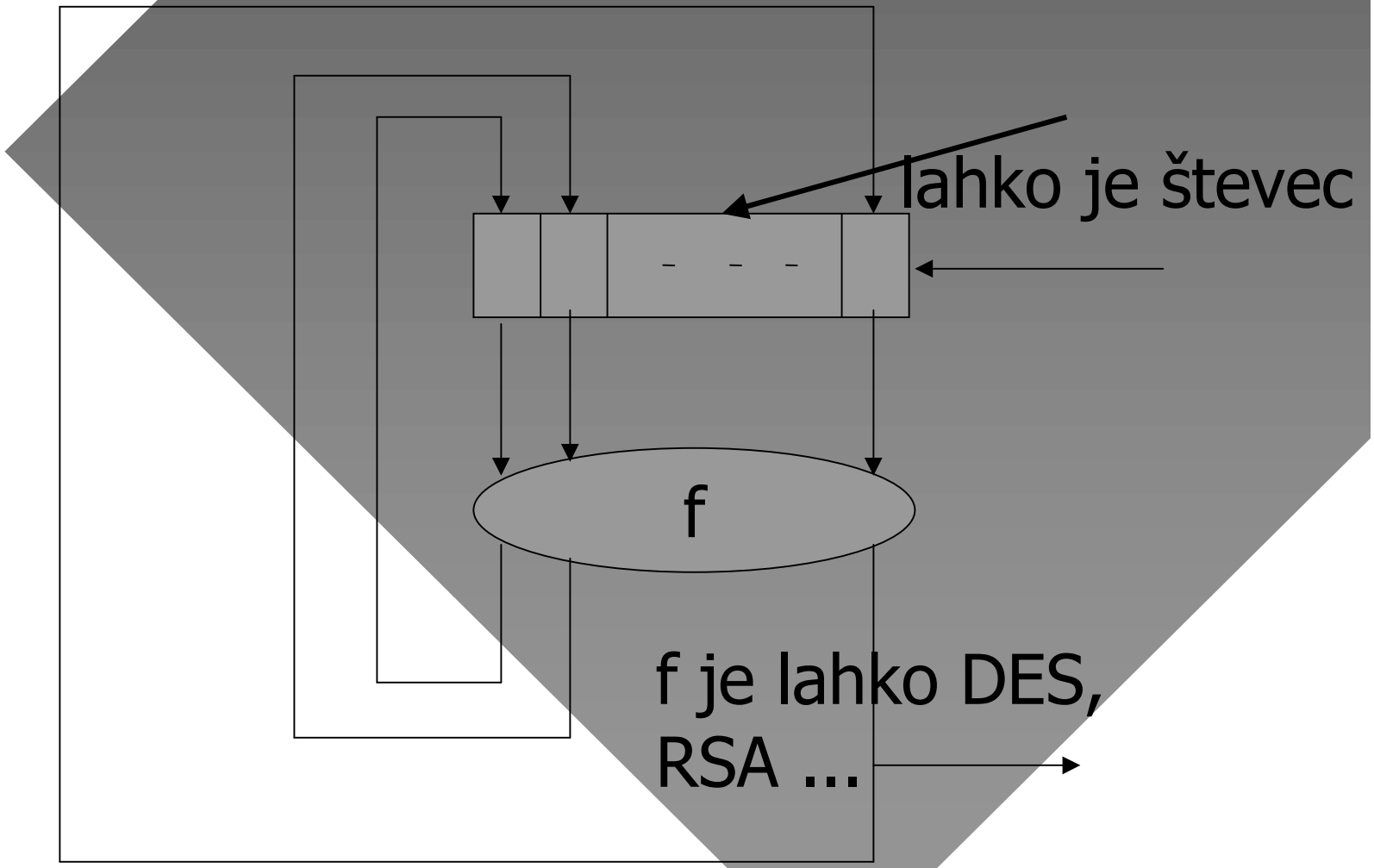


korelacija: k+m<=N

Pristop iz teorije kompleksnosti

- šifra temelji na nekem znanem težkem problemu
- računsko je analiza generatorja neizvedljiva
- BBS generator
  - $s_{i+1}=s_i^2 \bmod n$; $s_0 \in QR(n)$
  - $n=pq$; $p,q = 3 \bmod 4$
  - $z_i=s_i \bmod 2$

Kombinacija pristopov



Razlikovalci porazdelitev in napovedovalci

- želimo, da je v polinomskem času nemogoče razlikovati psevdonaključni vir od naključnega
- k seme in l dožina niza; porazdelitvi $1/2^l$ in 0 ter $1/2^k$
- ali obstaja s pomočjo verjetnostnega algoritma izračunan ε razlikovalec
- napovedovalec bitov iz ε razlikovalca in obratno

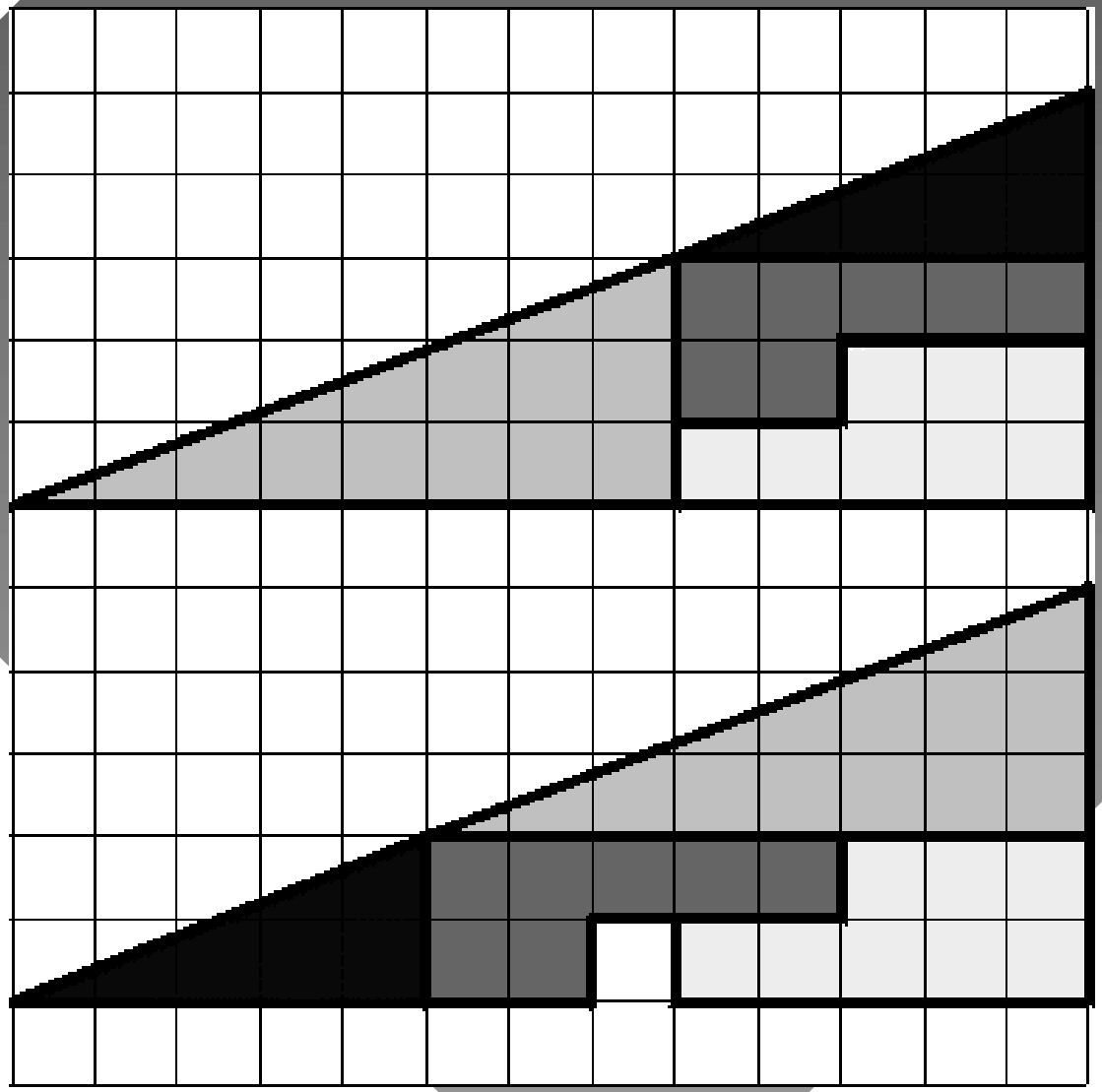
Statistični testi

- stopnja zaupanja
- splošna testa
  - Π ^{2} test
  - Kolmogorov-Smirnov test
- empirični testi
  - frekvenčni in serijski test
  - vrzelni test
  - poker test …
- univerzalni Maurerjev test

Linearna kompleksnost

- Golombovi postulati
- Berlekamp-Massey-ev algoritem
- Oblika linearne kompleksnosti (premica n/2)

Naloge



?