Przegląd wybranych generatorów liczb pseudolosowych

Mateusz Sołtysik, Andrzej Kwak, Wiktor Dyngosz

Politechnika Wrocławska, Wydział Podstawowych Problemów Techniki

mateusz@soltysik.org andrzej@kwak.re wiktor.dyngosz@gmail.com

Prowadzący: dr Krzysztof Majcher.

Streszczenie

W pracy dokonano przeglądu generatorów liczb losowych oraz zaprezentowano ich implementację w języku JAVA.
Abstrakt pisze się na końcu. `http://texterbooks.com/do/content/jak_napisac_dobry_abstrakt`

I. Wstęp

Termin generator liczb pseudolosowych odnosi się do układu elektronicznego lub programu komputerowego, który na podstawie niewielkiej ilości informacji (ziarna, ang. seed) generuje deterministycznie ciąg bitów. Ciąg ten pod pewnymi względami jest nieodróżnialny od ciągu uzyskanego z prawdziwie losowego źródła. W pracy będziemy chcieli przedstawić 16 algorytmów, służących generowaniu liczb pseudolosowych:

- Blum Blum Shub (Mateusz)
- Wichmann-Hill (Andrzej)
- Complementary-multiply-with-carry (Wiktor)
- Inversive congruential generator (Mateusz)
- ISAAC (cipher) (Andrzej)
- Lagged Fibonacci generator (Wiktor)
- Linear congruential generator (Mateusz)
- Linear feedback shift register (Andrzej)
- Maximal periodic reciprocals (Wiktor)
- Mersenne twister (Mateusz)
- Multiply-with-carry (Andrzej)
- Naor-Reingold Pseudorandom Function (Wiktor)
- Park–Miller random number generator (Mateusz)
- RC4 PRGA (Andrzej)
- Well Equidistributed Long-period Linear (Wiktor)
- Xorshift (Mateusz)

II. Methods

Maecenas sed ultricies felis. Sed imperdiet dictum arcu a egestas.

- Donec dolor arcu, rutrum id molestie in, viverra sed diam
- Curabitur feugiat
- turpis sed auctor facilisis
- arcu eros accumsan lorem, at posuere mi diam sit amet tortor
- Fusce fermentum, mi sit amet euismod rutrum
- sem lorem molestie diam, iaculis aliquet sapien tortor non nisi
- Pellentesque bibendum pretium aliquet

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor

vitae risus porta vehicula.

III. Results

Tabela 1: *Example table*

Name		
First name	Last Name	Grade
John	Doe	7.5
Richard	Miles	2

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

$$e = mc^2 \tag{1}$$

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

IV. Discussion

I. Subsection One

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

II. Subsection Two

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet, egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, consectetuer at, consectetuer sed, eleifend ac, lectus. Nulla facilisi. Pellentesque eget lectus. Proin eu metus. Sed porttitor. In hac habitasse platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet, placerat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu, malesuada ac, dui. Mauris nibh leo, facilisis non, adipiscing quis, ultrices a, dui.

Literatura

[Figueredo and Wolf, 2009] Figueredo, A. J. and Wolf, P. S. A. (2009). Assortative pairing and life history strategy - a cross-cultural study. *Human Nature*, 20:317–330.