EVOLUȚIA ȘI PERSPECTIVA GENERATOARELOR DE NUMERE PSEUDOALEATORII: DE LA ORIGINI LA CUANTUM

Gabriela CEBOTAR

Departamentul Ingineria Software și Automatică, TI-231M, Facultatea de Calculatoare, Informatică și Microelectronică, Universitatea Tehnică a Moldovei, Chișinău, Republica Moldova

Autorul corespondent: Cebotar Gabriela, cebotar.gabriela@isa.utm.md

Coordonatorul științific **Alexei LEAHU**, doctor, profesor universitar, Universitatea Tehnică a Moldovei

Rezumat. *Această lucrare efectuează o explorare a traiectoriei evolutive a generatoarelor de numere pseudo-aleatorii, evidențiind transformările tehnologice și metodologice de-a lungul timpului, stadiul actual al tehnologiei și predicții pentru viitor. Prin implementarea unei analize comparative a algoritmilor, de la cei istorici la cei moderni, studiul subliniază progresele în securitatea și eficiența acestor sisteme. De asemenea, studiul efectuează o analiză asupra creșterii varietății domeniilor de aplicare de-a lungul timpului, de la criptografie la arta generativă. Rezultatele studiului indică o creștere continuă a complexității generatoarelor cercetate, alături de provocările persistente în asigurarea unei generări autentic aleatorii. Analizele sugerează că dezvoltările viitoare vor depinde în mare măsură de inovațiile din domeniul calculatoarelor cuantice. În concluzie, această lucrare stabilește o bază pentru dialoguri ulterioare privind direcțiile de cercetare și implementarea practică a generatoarelor de numere pseudo-aleatorii.*

Cuvinte cheie: *generatoare, pseudoaleatorii, numere aleatorii.*

Introducere

Numerele aleatorii sunt esențiale în simulările statistice, criptografie, modelarea proceselor stocastice și în multe alte domenii. Ele sunt utilizate pentru a reprezenta evenimente aleatorii în modele matematice, pentru a testa ipoteze statistice și pentru a asigura securitatea în comunicațiile criptografice.

Generatoarele de numere aleatorii se împart în generatoare de numere aleatorii veritabile și generatoare de numere pseudo-aleatorii. Astfel, componenta cheie a generatoarele de numere aleatorii veritabile constă în extragerea entropiei din mediul înconjurător, un element ce nu poate fi simulat sau recreat artificial. De exemplu, *Random.org* utilizează entropia colectată din zgomotul atmosferic pentru a produce secvențe aleatorii [1].

Generatoarele de numere pseudo-aleatorii produc secvențe de numere folosind algoritmi matematici. În ciuda naturii lor deterministe, acești algoritmi sunt proiectați să ofere secvențe care par a fi aleatorii. Aspectele principale ale acestui tip de generatoare sunt:

- generarea numerelor cu o distribuție uniformă;
- producerea aceleași secvențe de numere dintr-o sursă inițială, asigurând reproductibilitate și posibilitate de testare;
- imprevizibilitatea, dacă sursa inițială nu este cunoscută, secvența următoare trebuie să fie imprevizibilă, chiar dacă secvențele anterioare sunt cunoscute.

Fiecare categorie are avantajele și limitările sale, iar alegerea între ele depinde de cerințele specifice ale aplicației în cauză. Primul tip de generatoare sunt esențiale în aplicații cu cerințe stricte de securitate datorită imprevizibilității înalte a secvențelor generate. Pe când al doilea tip, este considerat eficient și rapid, fiind preferat pentru volume mari de date sau în scenarii unde reproductibilitatea este utilă. Înțelegerea principiilor și metodologiilor asociate acestui concept este esențială pentru progresul în multe domenii de cercetare și dezvoltare.

Evoluția generatoarelor de numere pseudo-aleatorii

Evoluția generatoarelor de numere pseudo-aleatorii a fost profund influențată de progresul tehnologic și de necesitățile în continuă schimbare ale domeniilor lor de aplicare. Inițial, în a doua jumătate a secolului al XX-lea, clasa standard de algoritmi folosiți pentru generatoare era compusă din generatoare liniare congruente. Calitatea acestora era considerată inadecvată din cauza limitărilor în termeni de perioadă și distribuției secvențelor generate, dar metode mai bune nu erau disponibile.

O inovație semnificativă în dezvoltarea generatoarelor pseudo-aleatorii a fost adoptarea tehnicilor care utilizează recurențe liniare în cadrul unui câmp format din două elemente. Un punct de cotitură a fost atins în 1997 cu introducerea Mersenne Twister [2], un algoritm care a depășit limitările predecesorilor săi prin excelența sa în testele de aleatorietate și aplicabilitatea în scenarii complexe, precum simulările statistice și generarea lumilor virtuale.

Standardele rigide din criptografiei au fost un factor decisiv în diversificarea și specializarea algoritmilor [3]. Necesitatea unei securități robuste a determinat dezvoltarea generatoarelor precum algoritmul Yarrow și succesorul său, Fortuna [4]. Aceste sisteme utilizează surse de entropie externă pentru a îmbunătăți aleatorietatea și sunt esențiale pentru generarea cheilor criptografice și a altor elemente în securitatea informației.

În domeniul artei generative, spre deosebire de criptografie, se preferă utilizarea unor algoritmi precum Perlin Noise și Simplex Noise, care permit un control fin asupra secvențelor generate. Aceste tehnici nu sunt generatoare de numere pseudo-aleatorii în sensul tradițional, ci mai degrabă algoritmi de generare a zgomotului care produc modele vizuale complexe.

Astfel, evoluția generatoarelor de numere pseudo-aleatorii nu reprezintă doar un traseu al avansului tehnologic, ci reflectă și modul în care cerințele specifice ale diverselor domenii de aplicare formează noi direcții ale dezvoltării tehnologice. Selectarea unui generator de numere pseudo-aleatorii este importantă și trebuie să corespundă necesităților și obiectivelor specifice ale fiecărui proiect.

Testarea generatoarelor de numere pseudo-aleatorii

Testarea generatoarelor de numere pseudo-aleatorii ocupă un rol crucial în asigurarea calității și fiabilității acestor sisteme, având un impact direct asupra domeniilor lor aplicative. Pe măsură ce tehnologiile au avansat, și metodele de testare au evoluat, devenind tot mai sofisticate pentru a detecta slăbiciunile potențiale ale algoritmilor. Inițial, testele se concentrau pe evaluarea uniformității distribuției și a independenței statistice, însă cu trecerea timpului, au fost dezvoltate suite de teste complexe, precum cele propuse de Diehard și NIST care evaluează o gamă largă de proprietăți statistice ale secvențelor generate [5,6].

Este importantă testarea generatoarelor utilizate în cercetările proprii, având în vedere varietatea resurselor oferite de limbaje de programare precum Python, R, C++ și Java. Aceste limbaje includ biblioteci standard cu generatoare integrate și framework-uri pentru testarea proprietăților statistice a secvențelor generate. O evaluare meticuloasă a generatoarelor asigură integritatea științifică și sporește încrederea în aplicabilitatea și reproductibilitatea studiilor.

Posibilități în limbajul R

Investigația realizată în limbajul R a avut ca obiectiv evaluarea și testarea unui set de algoritmi generatori de numere pseudo-aleatorii, selectați pentru diversitatea lor și relevanța în practică. Algoritmii analizați includ Wichmann-Hill, Super-Duper, Marsaglia-Multicarry, Mersenne-Twister și o versiune simplificată a generatorului liniar congruențial (LGC).

Pentru a evalua performanța acestor algoritmi, s-au aplicat mai multe metode de testare, prezentate în Tabelul 1. Unul dintre teste este testul Kolmogorov-Smirnov, care măsoară gradul de conformitate al distribuției numerelor generate cu o distribuție uniformă teoretică, fiind esențial pentru a asigura echidistribuția numerelor generate. Testul Bartels verifică aleatorietatea secvențelor de numere, evaluând absența unor modele sau tendințe predefinite. Testul de

corelație este utilizat pentru a examina independența statistică între numerele consecutive. În cele din urmă, testul de secvențe (Runs) este folosit pentru a detecta non-aleatorietatea, identificând structuri repetitive sau anomalii în secvențele de numere.

Rezultatele testelor statistice au arătat o variație a performanței algoritmilor. De exemplu, algoritmii Super-Duper și Wichmann-Hill au avut rezultate satisfăcătoare în unele teste, dar au prezentat rezultate mixte în altele. Această variație subliniază faptul că un generator de numere pseudo-aleatorii poate satisface criteriile unor teste de aleatorietate, în timp ce eșuează în a îndeplini parametrii altor teste. Acest lucru indică importanța aplicării unui set diversificat de teste pentru a obține o evaluare cuprinzătoare a calității unui generator.

Este important de menționat că niciun test de aleatorietate nu poate furniza o garanție absolută a aleatorietății. În schimb, aceste teste pot indica dacă există suficiente motive pentru a suspecta non-aleatorietatea în secvențele generate de diverși algoritmi. Prin urmare, interpretarea rezultatelor testelor necesită o abordare prudentă și o analiză detaliată a comportamentului generatorilor în diverse contexte de utilizare.

Tabelul 1

Performanța în cadrul testelor statistice

	Testul Kolmogorov-Smirnov	**Testul Bartels**	**Testul Corelației**	**Testul Runs**
LGC	bună	slabă	bună	bună
Super-Duper	Bună	slabă	bună	foarte bună
Marsaglia-Multicarry	bună	bună	bună	slabă
Wichmann-Hill	bună	bună	bună	bună
Mersenne-Twister	foarte bună	bună	bună	bună

Inovații contemporane și perspective viitoare

Inovațiile contemporane în domeniul generării de numere aleatorii sunt profund influențate de progresul tehnologiei cuantice, dând naștere unei noi clase de generatoare cunoscute sub denumirea de generatoare de numere aleatorii cuantice (Quantum Random Number Generators - QRNG). Aceste generatoare exploatează principiile mecanicii cuantice pentru a produce secvențe de numere cu un grad de aleatorietate superior celui obținut prin metodele tradiționale.

QRNG-urile bazate pe fotonica cuantică exploatează proprietățile fundamentale ale mecanicii cuantice, cum ar fi superpoziția și încălcarea inegalităților Bell, pentru a genera numere cu un grad de aleatorietate ce nu poate fi atins prin metode clasice. Pe de altă parte, QRNG-urile care se bazează pe fluctuațiile de vid cuantic se folosesc de variațiile aleatorii ale câmpurilor cuantice la scara microscopică, o resursă omniprezentă și inepuizabilă de aleatorietate. În plus, există QRNG-uri care se fundamentează pe procese nucleare, cum ar fi descompunerea radioactivă, care este un fenomen cuantic intrinsec aleatoriu. Prin măsurarea intervalului de timp dintre două evenimente de descompunere succesive, se poate genera un șir de valori aleatorii.

În ceea ce privește progresul actual în acest domeniu, există deja pe piață diverse exemple de QRNG-uri comerciale, care demonstrează viabilitatea și aplicabilitatea acestor tehnologii. Companiile precum ID Quantique [7] oferă QRNG-uri care utilizează procese optice pentru a produce numere aleatorii, încorporându-le în sisteme de securitate.

Progresul în domeniul generatoarelor de numere aleatorii cuantice deschide noi orizonturi pentru securitatea și fiabilitatea sistemelor criptografice, oferind perspective promițătoare pentru viitorul tehnologiilor bazate pe principiile mecanicii cuantice.

Concluzii

Studiul subliniază importanța evaluării meticuloase a generatoarelor de numere pseudo-aleatorii și alegerea acestora în funcție de necesitățile specifice ale diferitelor aplicații. Analiza algoritmilor din limbajul R a evidențiat rolul crucial al testărilor statistice în asigurarea fiabilității și calității surselor de aleatorietate.

Progresul în domeniul generatoarelor cuantice de numere aleatorii deschide noi perspective pentru dezvoltarea tehnologiilor de generare a numerelor aleatorii. Avansul tehnologic în acest domeniu promite o îmbunătățire semnificativă a calității și siguranței numerelor generate, oferind oportunități pentru aplicații inovatoare în criptografie, simulări statistice și alte domenii critice.

Surse bibliografice:

[1] "What's this fuss about true randomness?" [Online]. Available: https://www.random.org/
[2] M. Makoto, N. Takuji, "Mersenne twister: a 623-dimensionally equi-distributed uniform pseudo-random number generator", *ACM Transactions on Modeling and Computer Simulation*, doi:10.1145/272991.272995.
[3] W. Schindler, "Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators", *Anwendungshinweise und Interpretationen (AIS)*, pp. 5–11, 19 August 2013.
[4] N. Ferguson, B. Schneier, "Chapter 9: Generating Randomness", *Cryptography Engineering: Design Principles and Practical Applications*, Wiley Publishing, 2010.
[5] "The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness", Florida State University, 1995.
[6] *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, National Institute of Standards and Techology, 2010.
[7] "Use Quantum random numbers" [Online]. Available: https://www.idquantique.com/random-number-generation/overview/