DAV/DGVFM
Herbsttagung
2025

Christian Weiß

State-of-the-Art Techniken für die Erzeugung von Zufallszahlen

Inhalt

Inhalt

Beispiel: Solvency II (1/2)

- Nach der Solvency II Rahmenrichtlinie gilt (Artikel 76): *Die versicherungstechnischen Rückstellungen müssen auf vorsichtige, verlässliche und objektive Art und Weise berechnet werden*.
- In Artikel 121 wird dazu ergänzt: *Die zur Berechnung der Wahrscheinlichkeitsverteilungsprognose verwendeten Methoden basieren auf aktuellen und zuverlässigen Informationen sowie auf realistischen Annahmen.*
- **Konsequenz**: Die Berechnungen nach Solvency II dürfen keine starke Abhängigkeit von frei wählbaren Modellparametern zeigen.
- **Konkret**: Die EIOPA-Guideline für die Berechnung der Technical Provisions fordert deshalb (unter anderem) in **Guideline 59**, dass die Güte der verwendeten Zufallszahlgeneratoren getestet werden muss.

Beispiel: Solvency II (2/2)

- Das **Branchensimulationsmodell** (BSM) wird von vielen kleineren Versicherungsunternehmen zur Berechnung von Own Funds, Best Estimates Liablities (BEL) und Solvency Capital Requirements (SCR) eingesetzt.
- Hierin ist insbesondere der **Random Seed**, der bei der Erzeugung der Zufallszahlen für die stochastischen Berechnungen verwendet wird, ein frei wählbarer Parameter.
- (Echte) Berechnungsergebnisse (nach [1]) für einen deutschen Versicherer mit einem hohen Anteil von Kapitallebensversicherungen zeigen jedoch folgendes Bild zwischen den zwei extremsten (von insgesamt 30) Random Seeds:

Variable	Δ in %
Own Funds	-8,2
SCR	7,2
SII Quote	-14,2

Aktuarielle Anwendungen von Zufallszahlen

Zufallszahlen werden beispielsweise in folgenden aktuariellen Anwendungen eingesetzt:

- Risikokapitalberechnung
- Stochastische Schadenreservierung (z.B. mit Bootstrapping oder MCMC)
- Stochastische Sterblichkeits- und Biometrie-Modelle
- Algorithmen der künstlichen Intelligenz

Inhalt

Bekannte Typen von Zufallszahlengeneratoren

- **Mersenne Twister**: Sehr häufig verwendet seit dessen Erfindung im Jahr 1998.
- **Xorshift**: Generator mit geringen Anforderungen an Speicher und Prozessor, für den Einsatz auf Systemen mit geringen Ressourcen, z. B. Eingebettete Systeme, besonders geeignet.
- **Arc4Random**: Kryptografisch sicherer Zufallszahlengenerator von 1997, der sich ohne manuelles Setzen des Seeds aus der Systementropie initialisiert.

Warnung

Alle diese Zufallszahlengeneratoren können relativ leicht von echten Zufallszahlen (z.B. von Zerfallsprozess eines Atomts) unterschieden werden.

Gütekriterien für Zufallszahlengeneratoren (1/3)

Permutationstest

- Wir wählen eine beliebige ganze Zahl $2 \leq k \ll N-1$ und betrachten die Tupel $(x_n, x_{n+1}, \ldots, x_{n+k-1})$ für $n = 1, \ldots, N-k$.
- Alle $k!$ relativen Anordnungen der Einträge eines allgemeinen k-Tupels sollten gleich wahrscheinlich sein, d. h. eine Wahrscheinlichkeit von $\frac{1}{k!}$ haben.
- Hierzu wird ein statistischer Anpassungstest durchgeführt.

Zum Beispiel ist die relative Anordnung des 4-Tupels $(0{,}8, 0{,}1, 0{,}2, 0{,}05)$ gleich $(4, 2, 3, 1)$.

Gütekriterien für Zufallszahlengeneratoren (2/3)

Serientest

- Eine gleichverteilte Folge auf $[0,1]$ ist überall gleich dicht.
- Auch l-Tupel aufeinanderfolgender Zahlen sollten unabhängig und gleichverteilt auf $[0,1]^l$ sein.
- Wir unterteilen zunächst jede Kopie von $[0,1]$ in d gleich lange Intervalle für eine ganze Zahl $d \geq 2$.
- Durch diese Konstruktion erhalten wir d^l Unterwürfel mit Volumen $\frac{1}{d^l}$, und jeder Unterwürfel sollte daher im Mittel $\lambda := \frac{N}{d^l}$ Elemente der endlichen Folge enthalten.
- Der Serientest misst die Abweichung zwischen den empirischen Häufigkeiten Y_j der Unterwürfel und dem Erwartungswert λ.
- Das Testverfahren beruht dann letztendlich auf einem Chi-Quadrat-Anpassungstest.

TestU01 Software

Softwareempfehlung

- **TestU01** ist eine in C geschriebene Softwarebibliothek zur Durchführung statistischer Tests zur Qualitätsbewertung von Zufallszahlengeneratoren (RNGs), entwickelt von Pierre L'Ecuyer und Richard Simard.
- Die Software bietet **strukturierte Testbatterien** (SmallCrush, Crush, BigCrush, Rabbit etc.), die eine Vielzahl statistischer Eigenschaften von RNGs unter standardisierten Bedingungen evaluieren.
- TestU01 gilt als **de-facto-Standard in der wissenschaftlichen Bewertung von RNGs** und wird häufig in der Literatur zur Verifikation und zum Vergleich von Zufallszahlengeneratoren verwendet.
- Link: https://github.com/umontreal-simul/TestU01-2009.

Lineare Kongruenzmethode

- Die **lineare Kongruenzmethode** (LCG) erzeugt eine Folge von Pseudozufallszahlen in einer Dimension mittels der Rekursion:

$$x_{n+1} = ax_n \mod m,$$

  wobei x_0 der Startwert ist. Wir bezeichnen m als **Modulus** und a als **Multiplikator**.
- Teilt man alle erzeugten Zahlen durch m, so erhält man eine Folge y_n in $[0, 1]$.
- Die Qualität hängt stark von der Wahl der Parameter ab; insbesondere beeinflussen sie die Periodenlänge und Gleichverteilung der Folge, siehe [6].
- Oft betrachtet man anstelle der Folge (y_n), die Folge von k-dimensionalen Tupeln $(y_1, \ldots, y_k), (y_{k+1}, \ldots, y_{2k}), \ldots$.
- Es gibt zahlreiche Verallgemeinerungen der Methode, beispielsweise **multiple recursive generators**

$$x_n = (a_1 x_{n-1} + \ldots + a_k x_{n-k}) \mod m.$$

Vor- und Nachteile

Vorteile

- extrem schnell; Reproduzierbarkeit durch Bekanntgabe von Modulus und Multiplikatoren; geringer Speicherbedarf
- Verknüpfung zur Theorie von Gittern

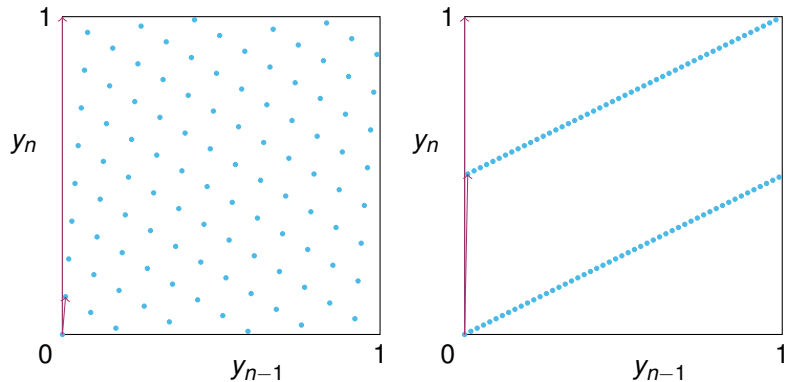
$$\Lambda_t = \left\{ v = zV = \sum_{j=1}^{t} z_j v_j \ \text{ mit } \ z = (z_1, \ldots, z_t) \in \mathbb{Z}^t \right\}.$$

Nachteile

- Durch TestU01 identifizierbar.
- Parametrisierung ist entscheidend.

Inhalt

Beispiel



Gitterstruktur eines LCGs für $m = 101$ und $a = 12$ (links) sowie $a = 51$ (rechts).

Gütekriterien für Zufallszahlengeneratoren (3/3)

Spektral Test

- Am vorherigen Beispiel sehen wir, dass der Zufallszahlengenerator um so besser ist, je größer der kürzeste Vektor ist beziehungsweise je kleiner der Abstand zwischen den Hyperebenen (den Linien im Beispiel) ist, was wiederum der *reziproken* **Länge des kürzesten Vektor** im sogenannten zu Λ_t dualen Gitter Λ_t^* entspricht.
- Die Bestimmung der Länge ℓ_t^* des kürzesten Vektors in Λ_t^* nennt man auch **Spektral Test** - je größer desto besser.
- Zusätzlich ist noch eine dimensionsabhängige Normalisierung notwendig, q_t^*.
- Zufallszahlen (auch echte) auf Computern sind **immer** endlich genau darstellbar, da Computer nur eine endliche Anzahl an Bitmustern speichern können. Dadurch liegen die generierten Punkte im mehrdimensionalen Raum nicht kontinuierlich verteilt, sondern immer nur auf **einem Gitter**, das sich in Hyperebenen anordnet.

DAV Deutsche Aktuarvereinigung e.V.

DGVFM Deutsche Gesellschaft für Versicherungs- und Finanzmathematik e.V.

Inhalt

Suche nach Zufallszahlengeneratoren

Aufgabe

- Der Spektral Test sollte nicht nur gute Werte liefern, wenn der zwei-dimensionale Output eines LCGs betrachtet wird, sondern auch für möglichst viele andere und höhere Dimensionen.
- Deswegen betrachtet man sogenannte **Figures of Merit**, die den Spektral-Test für viele Dimensionen durchführen und das Minimum der q_t^* ausgeben.
- **Problem**: Einerseits sollen sehr viele Seeds getestet werden, um einen guten Zufallszahlengenerator zu finden, andererseits ist die **exakte** Berechnung von q_t^* sehr aufwändig (branch-and-bound Algorithmus).

Bedeutung von Pre Reduction

- Idee: **Reduziere die Basisvektoren** eines Gitters, so dass diese bereits möglichst kurz und möglichst orthogonal sind. Diese Aufgabe nennt sich Pre Reduction und sollte in vertretbarer Rechenzeit durchgeführt werden.
- In $\mathbb{R}^n$ kann eine Basis mithilfe des **Gram-Schmidt-Orthogonalisierungsverfahrens** orthogonalisiert werden. Dabei werden Basisvektoren durch Linearkombinationen (mit reellen Koeffizienten) anderer Basisvektoren modifiziert. Auch können die Basisvektoren beliebig kurz gemacht werden.
- Für eine Gitterbasis hingegen dürfen nur Linearkombinationen mit **ganzzahligen Koeffizienten** verwendet werden, und die Basisvektoren können nicht beliebig kurz gemacht werden.
- Der bekannteste Algorithmus für diese Aufgabe sind der **LLL Algorithmus** (Arjen Lenstra, Hendrik Lenstra und Laszlo Lovasz) beziehungsweise seine Verallgemeinerungen wie der **BKZ Algorithmus** (Block Korkine-Zolotarev).

Numerische Ergebnisse

$m = 1099511627791$	Λ_t		Λ_t^*	
Methode	Laufzeit	Best FOM	Laufzeit	Best FOM
1. BKZ+BB, naive	1025.8	0.241259	700.6	0.223998
2. BKZ+BB, mit Ausschluss	7.6	0.264833	9.2	0.269388
3. LLL only, mit Ausschluss	5.5	0.264833	7.3	0.269388

Es wurden jeweils 100.000 Multiplikatoren getestet. Die Figures of Merit wurden jeweils bis hin zur Dimension 32 berechnet mit jeweils 446 Projektionen.

Aktuelle Umsetzung in Software

Softwareempfehlung

- Alle notwendigen Funktionen zur Analyse von Gittern wurden in der Software **LatticeTester** umgesetzt. Mit dieser können zum Beispiel die kürzesten Vektoren eines Gitters berechnet werden sowie Pre Reductions durchgeführt werden.
- Link: https://github.com/pierrelecuyer/latticetester
- In **LatMRG** wird ein Framework geschaffen werden, um gute Zufallszahlengeneratoren zu finden. Derzeit werden verschiedene Typen von Zufallszahlengeneratoren implementiert. Perspektivisch soll eine User Schnittstelle entwickelt werden.
- Link: https://github.com/pierrelecuyer/LatMRG

Literatur

1 Q. Culver, D. Heitmann, C. Weiß. The Influence of Seed Selection on the Solvency II Ratio.*Der Aktuar*, 2018(1): 15–18, 2018.

2 P. L'Ecuyer, R. Simard. TestU01: A C Library for Empirical Testing of Random Number Generators. *ACM Transactions on Mathematical Software*, 33 (4), Article 22 (2007).

3 P. L'Ecuyer und C. Weiß. Lattice Tester: A Software Tool to Analyze Integral Lattices. *erscheint in: Monte Carlo and Quasi-Monte Carlo Methods*, Springer Verlag, 2025.

4 EIOPA, *Guidelines on the Valuation of Technical Provisions*, EIOPA-BoS-14/166, 2014.

5 D. Knuth. *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*. Addison-Wesley, Reading, MA, third edition, 1998.

6 Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25. November 2009 über die Aufnahme und Ausübung der Versicherungs- und Rückversicherungstätigkeit (Solvabilität II), ABl. L 335 vom 17.12.2009, S. 1–155.

Vielen Dank für Ihre Aufmerksamkeit!

Christian Weiß