Construction of Uniformly Distributed Linear Recurring Sequences Over Dedekind Domains

Tamás Herendi

University of Debrecen

July 4 - July 8, 2022, Debrecen

Pseudo Random Number Generation

Pseudo random sequences with uniform distribution have several applications:

Pseudo Random Number Generation

Pseudo random sequences with uniform distribution have several applications:

- Monte Carlo methods

Pseudo Random Number Generation

Pseudo random sequences with uniform distribution have several applications:

- Monte Carlo methods
- simulations

Pseudo Random Number Generation

Pseudo random sequences with uniform distribution have several applications:

- Monte Carlo methods
- simulations
- cryptography

Pseudo Random Number Generation

Pseudo random sequences with uniform distribution have several applications:

- Monte Carlo methods
- simulations
- cryptography
- ...

Pseudo Random Number Generation

Pseudo random sequences with uniform distribution have several applications:

- Monte Carlo methods
- simulations
- cryptography
- ...

Sequences can be

Pseudo Random Number Generation

Pseudo random sequences with uniform distribution have several applications:

- Monte Carlo methods
- simulations
- cryptography
- ...

Sequences can be

- theoretical
  e.g. real sequences:

$$\alpha \cdot n \mod 1$$

Pseudo Random Number Generation

Pseudo random sequences with uniform distribution have several applications:

- Monte Carlo methods
- simulations
- cryptography
- ...

Sequences can be

- theoretical
  e.g. real sequences:
  $$\alpha \cdot n \mod 1$$
- practical e.g. sequences over finite structures:
  $$n \mod M.$$

Pseudo Random Number Generation

In practical applications we need:

Pseudo Random Number Generation

In practical applications we need:

known distribution (usually uniform)

Pseudo Random Number Generation

In practical applications we need:

- known distribution (usually uniform)
- easy computation

Pseudo Random Number Generation

In practical applications we need:

- known distribution (usually uniform)
- easy computation
- long period

Pseudo Random Number Generation

In practical applications we need:

- known distribution (usually uniform)
- easy computation
- long period
- good statistical properties, e.g.
  - good approximation to the distribution
  - low correlation of consecutive elements

Main result

If D is Dedekind domain, $\mathcal{I} \subseteq D$ is a particular prime ideal, u is a linear recurring sequence in D

- with a recurrence relation satisfying some simple condition,
- and having maximal period length $\mod \mathcal{I}$,

then u is uniformly distributed $\mod \mathcal{I}^s$ for all positive integers s.

Dedekind domains

D: a Dedekind domain, $\mathcal{I} \subseteq D$: an ideal

Definition (Norm)

$$\begin{aligned} \text{Norm: } & \mathbf{N}(\mathcal{I}) = |D/\mathcal{I}| \\ \text{Finite norm: } & \mathbf{N}(\mathcal{I}) < \infty \end{aligned}$$

Dedekind domains

D: a Dedekind domain, $\quad \mathcal{I} \subseteq D$: an ideal

Definition (Norm)

$$\text{Norm: } \mathbf{N}(\mathcal{I}) = |D/\mathcal{I}|$$

$$\text{Finite norm: } \mathbf{N}(\mathcal{I}) < \infty$$

$u \in D^\infty$ a sequence in D

Definition (Uniform distribution)

$\mathcal{I}$ has finite norm: u is **uniformly distributed** *modulo $\mathcal{I}$, if*

$$\lim_{m\to\infty} \frac{1}{m} \left|\{n < m \mid u_n \equiv r \mod \mathcal{I}\}\right| = \frac{1}{\mathbf{N}(\mathcal{I})} \quad \textit{for all } r \in D$$

Dedekind domains

Lemma (Semi GCD domain)

$Q_1, Q_2 \in D[x]$, $\quad Q_1$ *is monic.*

Then there exist unique $\gcd(Q_1, Q_2)$ *and* $\operatorname{lcm}(Q_1, Q_2)$*.*
The gcd *is monic.*

If both Q_1, Q_2 *are monic:* lcm *is monic.*

Dedekind domains

Lemma (Semi GCD domain)

$Q_1, Q_2 \in D[x]$, Q_1 *is monic.*

Then there exist unique $\gcd(Q_1, Q_2)$ *and* $\operatorname{lcm}(Q_1, Q_2)$.
The gcd *is monic.*

If both Q_1, Q_2 *are monic:* lcm *is monic.*

Definition (Generating function)

$u \in D^\infty$, $G_u \in D[[x]]$.

Generating function *of* u: $$G_u(x) = \sum_{n=0}^{\infty} u_n \cdot x^n$$

Linear Recurring Sequences

D: a Dedekind domain, $u \in D^\infty$ a sequence in D

Definition (LRS)

$a_0, \ldots, a_{d-1} \in D$, *$u$ satisfies the* ***recurrence relation***

$$u_{n+d} = a_{d-1} u_{n+d-1} + \cdots + a_0 u_n \qquad n = 0, 1, \ldots$$

u: ***linear recurring sequene***
$a_0, \ldots, a_{d-1}$: ***coefficients***
$u_0, \ldots, u_{d-1}$: ***initial values***.

Linear Recurring Sequences

D: a Dedekind domain, $u \in D^\infty$ a sequence in D

Definition (LRS)

$a_0, \dots, a_{d-1} \in D$, *$u$ satisfies the* ***recurrence relation***

$$u_{n+d} = a_{d-1}u_{n+d-1} + \cdots + a_0 u_n \qquad n = 0, 1, \dots$$

u: ***linear recurring sequene***
$a_0, \dots, a_{d-1}$: ***coefficients***
$u_0, \dots, u_{d-1}$: ***initial values***.

$P \in D[x]$

Definition (Characteristic polynomial)

characteristic polynomial: $P(x) = x^d - a_{d-1}x^{d-1} - \cdots - a_0$.

Linear Recurring Sequences

Lemma (LRS and Generating function)

$u \in D^\infty$, $G_u \in D[[x]]$ the generating function of u.

$$u \text{ is a LRS} \iff \exists P \in D[x], \text{ s.t. } P^* \cdot G_u \in D[x].$$

P^* is the reciprocal polynomial of P.

Remark

Technically: P is a characteristic polynomial of u.

Module structure of LRSs

Lemma

$P \in D[x]$ *is monic,* $\quad d = \deg(P)$,
$\mathcal{U}(D,P) = \{u \mid u \in D^\infty,\ \deg(P^* \cdot G_u) < d\}$

$$\textit{Then} \quad \mathcal{U}(D,P) \;\cong\; D[x]/x^d D[x] \;\cong\; D^d.$$

Module structure of LRSs

Lemma

$P \in D[x]$ is monic, $\quad d = \deg(P)$,
$\mathcal{U}(D,P) = \{u \mid u \in D^\infty,\ \deg(P^* \cdot G_u) < d\}$

$$\textit{Then} \quad \mathcal{U}(D,P) \ \cong\ D[x]/x^d D[x] \ \cong\ D^d .$$

Lemma

$P, Q \in D[x]$ are monic, then

$$\mathcal{U}(D,P) \subseteq \mathcal{U}(D, P \cdot Q)$$
$$\mathcal{U}(D,P) \cap \mathcal{U}(D,Q) = \mathcal{U}(D, \gcd(P,Q))$$

Module structure of LRSs

Lemma (Linear combination of LRSs)

$$\mathcal{U}(D) = \bigcup_{\substack{P \in D[x] \\ monic}} \mathcal{U}(D, P) \quad \textit{is a module.}$$

Module structure of LRSs

Lemma (Linear combination of LRSs)

$$\mathcal{U}(D) = \bigcup_{\substack{P \in D[x] \\ \text{monic}}} \mathcal{U}(D,P) \quad \textit{is a module.}$$

Definition (Linear complexity)

$u \in D^\infty$, *s.t.* $G_u \in \mathcal{U}(D)$.
*The **linear complexity** of u:*

$$d(u) = \min\left\{\dim\left(\mathcal{U}(D,P)\right) \mid P \in D[x] \text{ monic, } u \in \mathcal{U}(D,P)\right\}$$

Module structure of LRSs

Lemma (Linear combination of LRSs)

$$\mathcal{U}(D) = \bigcup_{\substack{P \in D[x] \\ \textit{monic}}} \mathcal{U}(D,P) \quad \textit{is a module.}$$

Definition (Linear complexity)

$u \in D^\infty$, s.t. $G_u \in \mathcal{U}(D)$.
*The **linear complexity** of u:*

$$d(u) = \min \left\{ \dim \left(\mathcal{U}(D,P) \right) \mid P \in D[x] \ \textit{monic},\ u \in \mathcal{U}(D,P) \right\}$$

Lemma (Minimal characteristic polynomial)

If u is a LRS, then there exists a unique $P \in D[x]$ monic polynomial, s.t.

$$d(u) = \dim \left(\mathcal{U}(D,P) \right)$$

Periodicity

Definition

*$u \in D^\infty$ is **(ultimately) periodic**, if $\exists \varrho \in \mathbb{Z}^+$, s.t.*

$$G_u \in \mathcal{U}(D, x^\varrho - 1)$$

*ϱ is a **period length**;*

*The smallest such a ϱ is the **minimal period length**, denoted by $\varrho(u)$.*

Periodicity

Definition

*$u \in D^\infty$ is **(ultimately) periodic**, if $\exists \varrho \in \mathbb{Z}^+$, s.t.*

$$G_u \in \mathcal{U}(D, x^\varrho - 1)$$

*ϱ is a **period length**;*

*The smallest such a ϱ is the **minimal period length**, denoted by $\varrho(u)$.*

Lemma

$u \in D^\infty$ is a LRS, $\quad \mathcal{I} \subseteq D$ is an ideal with finite norm.

Then u is periodic $\mod \mathcal{I}$.

Periodicity

Definition (Impulse response sequence (IRS))

$u \in D^\infty$, $\;$ *s.t.* $G_u \in \mathcal{U}(D)$, $\quad d = d(u)$.
u is an ***impulse response sequence****, if*

$$u_0 = \cdots = u_{d-2} = 0,\; u_{d-1} = 1\ .$$

Periodicity

Definition (Impulse response sequence (IRS))

$u \in D^\infty$, s.t. $G_u \in \mathcal{U}(D)$, $d = d(u)$.
u is an ***impulse response sequence****, if*

$$u_0 = \cdots = u_{d-2} = 0,\ u_{d-1} = 1\ .$$

Remark

If u is an IRS, then

$$G_u(x) \equiv x^{d-1} \mod x^d\ .$$

Periodicity

Definition (Impulse response sequence (IRS))

$u \in D^\infty$, s.t. $G_u \in \mathcal{U}(D)$, $d = d(u)$.

u *is an* ***impulse response sequence***, *if*

$$u_0 = \cdots = u_{d-2} = 0, \; u_{d-1} = 1 \; .$$

Remark

If u is an IRS, then

$$G_u(x) \equiv x^{d-1} \mod x^d \; .$$

Lemma (Periodicity of LRS)

$u \in D^\infty$ *is a LRS,* $\mathcal{I} \subseteq D$ *is an ideal with finite norm.*

Then u is periodic $\mod \mathcal{I}$.

Uniform distribution

Lemma (Maximal period length)

$\mathbb{F}$ is a finite field, $P \in \mathbb{F}[x]$ monic, and $u, v \in \mathbb{F}^\infty$, s.t $G_u, G_v \in \mathcal{U}(\mathbb{F}, P)$.

$$\textit{Then } u, v \textit{ are periodic, and if } u \textit{ is an IRS, then } \varrho(v) | \varrho(u).$$

Uniform distribution

Lemma (Maximal period length)

$\mathbb{F}$ is a finite field, $P \in \mathbb{F}[x]$ monic, and $u, v \in \mathbb{F}^\infty$, s.t $G_u, G_v \in \mathcal{U}(\mathbb{F}, P)$.

Then u, v are periodic, and if u is an IRS, then $\varrho(v) | \varrho(u)$.

Lemma (Shifted sequence)

*Let $Q, P \in D[x]$, s.t Q is monic and $P(x) = (x-1)^2 Q(x)$,
$a \in D$ and $u, v \in D^\infty$, s.t. $v_n = u_n + a$ for all $n \geq 0$.*

$$\text{Then} \quad G_u \in \mathcal{U}(D, P) \implies G_v \in \mathcal{U}(D, P)$$

Uniform distribution

Theorem (Uniform distribution)

$P, P', Q \in D[x]$ monic, s.t

$$P(x) = (x-1)^2 Q(x) \text{ and } P'(x) = (x-1)Q(x)$$

$u, v \in D^\infty$, s.t. $G_u, G_v \in \mathcal{U}(D, P)$, and v is an IRS,
$\mathcal{I} \subset D$ is a prime ideal with $\mathbf{N}(\mathcal{I}) = p$,
Q is irreducible $\mod \mathcal{I}$,
$\varrho(\mathcal{I}, u)$ and $\varrho(\mathcal{I}, v)$ are the period lengths $\mod \mathcal{I}$.

If $\varrho(\mathcal{I}, u) = \varrho(\mathcal{I}, v)$, then u uniformly distributed $\mod \mathcal{I}$.

Uniform distribution

Theorem (Uniform distribution)

$P, P', Q \in D[x]$ monic, s.t

$$P(x) = (x-1)^2 Q(x) \text{ and } P'(x) = (x-1)Q(x)$$

$u, v \in D^\infty$, s.t. $G_u, G_v \in \mathcal{U}(D, P)$, and v is an IRS,
$\mathcal{I} \subset D$ is a prime ideal with $\mathbf{N}(\mathcal{I}) = p$,
Q is irreducible $\mod \mathcal{I}$,
$\varrho(\mathcal{I}, u)$ and $\varrho(\mathcal{I}, v)$ are the period lengths $\mod \mathcal{I}$.

If $\varrho(\mathcal{I}, u) = \varrho(\mathcal{I}, v)$, then u uniformly distributed $\mod \mathcal{I}$.

The proof is based on the observation of the structure of $\mathcal{U}(D/\mathcal{I}, P)/\mathcal{U}(D/\mathcal{I}, P')$.

Uniform distribution

Theorem (Uniform distribution)

$P, Q \in D[x]$ monic, s.t $P(x) = (x-1)^2 Q(x)$,
$u, v \in D^\infty$, s.t. $G_u, G_v \in \mathcal{U}(D, P)$, and v is an IRS,
$p \in \mathbb{N}$ is a prime,
$\mathcal{I} \subset D$ is a prime ideal with $\mathbf{N}(\mathcal{I}) = p$,
Q is irreducible $\mod \mathcal{I}$,
$s \in \mathbb{Z}^+$, and $\varrho(\mathcal{I}^s, u)$ and $\varrho(\mathcal{I}^s, v)$ are the period lengths $\mod \mathcal{I}^s$.

$$\text{If } \varrho(\mathcal{I}, u) = \varrho(\mathcal{I}, v), \quad \text{then} \quad \varrho(\mathcal{I}^{s+1}, u) = p \cdot \varrho(\mathcal{I}^s, u).$$

Uniform distribution

Theorem (Uniform distribution)

$P, Q \in D[x]$ monic, s.t $P(x) = (x-1)^2 Q(x)$,
$u, v \in D^\infty$, s.t. $G_u, G_v \in \mathcal{U}(D, P)$, and v is an IRS,
$p \in \mathbb{N}$ is a prime,
$\mathcal{I} \subset D$ is a prime ideal with $\mathbf{N}(\mathcal{I}) = p$,
Q is irreducible $\mod \mathcal{I}$,
$s \in \mathbb{Z}^+$, and $\varrho(\mathcal{I}^s, u)$ and $\varrho(\mathcal{I}^s, v)$ are the period lengths $\mod \mathcal{I}^s$.

$$\text{If } \varrho(\mathcal{I}, u) = \varrho(\mathcal{I}, v), \quad \text{then} \quad \varrho(\mathcal{I}^{s+1}, u) = p \cdot \varrho(\mathcal{I}^s, u).$$

The proof is based on the observation of the structure of $\mathcal{U}(D/\mathcal{I}^{s+1}, P)/\mathcal{U}(D/\mathcal{I}^s, P)$.

Uniform distribution

Theorem (Uniform distribution)

$P, Q \in D[x]$ monic, s.t $P(x) = (x-1)^2 Q(x)$,
$u, v \in D^\infty$, s.t. $G_u, G_v \in \mathcal{U}(D, P)$, and v is an IRS,
$p \in \mathbb{N}$ is a prime,
$\mathcal{I} \subset D$ is a prime ideal with $\mathbf{N}(\mathcal{I}) = p$,
Q is irreducible $\mod \mathcal{I}$.

If $\varrho(\mathcal{I}, u) = \varrho(\mathcal{I}, v)$, then

$$u \text{ is uniformly distributed } \mod \mathcal{I}^s, \text{ for all } s \in \mathbb{Z}^+.$$

Furthermore,

$$\varrho(\mathcal{I}^s, u) = ord(Q) \cdot p^s.$$

$ord(Q) | p^{\deg(Q)} - 1$, is the order of Q.

Thanks

The research was supported by the SETIT Project (no. 2018-1.2.1-NKP-2018-00004), which has been implemented with the support provided by the National Research, Development and Innovation Fund of Hungary, financed under the 2018-1.2.1-NKP funding scheme.