Construction of Uniformly Distributed Linear Recurring Sequences Over Dedekind Domains

Tamás Herendi

University of Debrecen

July 4 - July 8, 2022, Debrecen
Pseudo random sequences with uniform distribution have several applications:
Pseudo random sequences with uniform distribution have several applications:

- Monte Carlo methods
Pseudo random sequences with uniform distribution have several applications:

- Monte Carlo methods
- simulations
Pseudo random sequences with uniform distribution have several applications:

- Monte Carlo methods
- simulations
- cryptography
Pseudo random sequences with uniform distribution have several applications:

- Monte Carlo methods
- simulations
- cryptography
- ...
Pseudo random sequences with uniform distribution have several applications:

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

Sequences can be
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:
  \[ n \mod M \]
In practical applications we need:
In practical applications we need:

known distribution (usually uniform)
In practical applications we need:

- known distribution (usually uniform)
- easy computation
In practical applications we need:

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

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

Finite norm: $N(\mathcal{I}) < \infty$
Dedekind domains

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

**Definition (Norm)**

- **Norm:** $N(\mathcal{I}) = |D/\mathcal{I}|$
- **Finite norm:** $N(\mathcal{I}) < \infty$

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

**Definition (Uniform distribution)**

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

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

\[
Q_1, Q_2 \in D[x], \quad Q_1 \text{ is monic.}
\]

Then there exist unique \( \gcd(Q_1, Q_2) \) and \( \lcm(Q_1, Q_2) \).

The \( \gcd \) is monic.

\textit{If both} \( Q_1, Q_2 \) \textit{are monic:} \( \lcm \) \textit{is monic.}
Lemma (Semi GCD domain)

\( Q_1, Q_2 \in D[x], \quad Q_1 \text{ is monic.} \)

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

If both \( Q_1, Q_2 \) are monic: \( \text{lcm} \) is monic.

Definition (Generating function)

\( u \in D^\infty, \quad G_u \in D[[x]]. \)

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

$$u_{n+d} = a_{d-1}u_{n+d-1} + \cdots + a_0u_n \quad n = 0, 1, \ldots$$

$u$: **linear recurring sequence**

$a_0, \ldots, a_{d-1}$: **coefficients**

$u_0, \ldots, u_{d-1}$: **initial values**.
$D$: 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**

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

$u$: **linear recurring sequence**

$a_0, \ldots, a_{d-1}$: **coefficients**

$u_0, \ldots, u_{d-1}$: **initial values**.

$P \in D[x]$

**Definition (Characteristic polynomial)**

**characteristic polynomial**: $P(x) = x^d - a_{d-1}x^{d-1} - \cdots - a_0$. 
Lemma (LRS and Generating function)

\[ u \in D^\infty, \quad G_u \in D[[x]] \] 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 \( u \).
Lemma

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

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

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

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

Lemma

\[ P, Q \in D[x] \text{ are monic, then} \]
\[ \mathcal{U}(D, P) \subseteq \mathcal{U}(D, P \cdot Q) \]
\[ \mathcal{U}(D, P) \cap \mathcal{U}(D, Q) = \mathcal{U}(D, \gcd(P, Q)) \]
Lemma (Linear combination of LRSs)

\[ \mathcal{U}(D) = \bigcup_{P \in D[x]} \mathcal{U}(D, P) \text{ is a module.} \]
Module structure of LRSs

Lemma (Linear combination of LRSs)

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

Definition (Linear complexity)

\[ u \in D^\infty, \text{ s.t. } G_u \in \mathcal{U}(D). \]

The linear complexity of \( u \):

\[ d(u) = \min \{ \dim (\mathcal{U}(D, P)) \mid P \in D[x] \text{ monic, } u \in \mathcal{U}(D, P) \} \]
Module structure of LRSs

Lemma (Linear combination of LRSs)

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

Definition (Linear complexity)

\[ u \in D^\infty, \text{ s.t. } G_u \in \mathcal{U}(D). \]

The **linear complexity** of \( u \):

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

Lemma (Minimal characteristic polynomial)

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

\[ d(u) = \dim (\mathcal{U}(D, P)) \]
Definition

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

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

\( \varrho \) is a \textit{period length};

The smallest such a \( \varrho \) is the \textit{minimal period length}, denoted by \( \varrho(u) \).
Definition

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

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

$\varrho$ is a period length;

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

Lemma

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

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

**Definition (Impulse response sequence (IRS))**

\[ u \in D^\infty, \text{ s.t. } G_u \in \mathcal{U}(D), \quad d = d(u). \]

u is an impulse response sequence, if

\[ u_0 = \cdots = u_{d-2} = 0, \quad u_{d-1} = 1. \]
Periodicity

**Definition (Impulse response sequence (IRS))**

\[ u \in D^\infty, \text{ s.t. } G_u \in \mathcal{U}(D), \quad d = d(u). \]

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

\[ u_0 = \cdots = u_{d-2} = 0, \quad u_{d-1} = 1. \]

**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. \( G_u \in U(D), \) \( d = d(u). \)

\( u \) is an **impulse response sequence**, if

\[
    u_0 = \cdots = u_{d-2} = 0, \quad u_{d-1} = 1.
\]

**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 \( \mod \mathcal{I}. \)
Lemma (Maximal period length)

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

Then \( u, v \) are periodic, and if \( u \) is an IRS, then \( \vartheta(v) \mid \vartheta(u) \).
Lemma (Maximal period length)

Let $\mathbb{F}$ be 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 $n \geq 0$.

Then $G_u \in \mathcal{U}(D, P) \implies G_v \in \mathcal{U}(D, P)$.
Theorem (Uniform distribution)

\[ P, P', Q \in D[x] \text{ monic, s.t.} \]
\[ P(x) = (x - 1)^2 Q(x) \text{ and } P'(x) = (x - 1)Q(x) \]

\[ u, v \in D^\infty, \text{ s.t. } G_u, G_v \in \mathcal{U}(D, P), \text{ and } v \text{ is an IRS}, \]

\[ \mathcal{I} \subset D \text{ is a prime ideal with } \mathbf{N}(\mathcal{I}) = p, \]

\[ Q \text{ is irreducible } \mod \mathcal{I}, \]

\[ \varrho(\mathcal{I}, u) \text{ and } \varrho(\mathcal{I}, v) \text{ are the period lengths } \mod \mathcal{I}. \]

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

\( P, P', Q \in D[x] \) monic, s.t.
\[ P(x) = (x - 1)^2 Q(x) \quad \text{and} \quad P'(x) = (x - 1)Q(x) \]

\( u, v \in D^\infty \), 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 \( N(\mathcal{I}) = p \),
\( Q \) is irreducible \( \text{mod} \ \mathcal{I} \),
\( \varrho(\mathcal{I}, u) \) and \( \varrho(\mathcal{I}, v) \) are the period lengths \( \text{mod} \ \mathcal{I} \).

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

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

Let $P, Q \in D[x]$ be monic, such that $P(x) = (x - 1)^2 Q(x)$.

Let $u, v \in D^\infty$, such that $G_u, G_v \in \mathcal{U}(D, P)$, and $v$ is an IRS.

Let $p \in \mathbb{N}$ be a prime,

Let $\mathcal{I} \subset D$ be a prime ideal with $\mathcal{N}(\mathcal{I}) = p$,

Let $Q$ be irreducible modulo $\mathcal{I}$,

Let $s \in \mathbb{Z}^+$, and let $\varrho(\mathcal{I}^s, u)$ and $\varrho(\mathcal{I}^s, v)$ be the period lengths modulo $\mathcal{I}^s$.

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

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

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

The proof is based on the observation of the structure of \( \mathcal{U}(D/\mathcal{I}^{s+1}, P)/\mathcal{U}(D/\mathcal{I}^s, P) \).
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,
$I \subset D$ is a prime ideal with $\mathbb{N}(I) = p$,
$Q$ is irreducible mod $I$.

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

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

Furthermore,

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

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

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.