Construction of uniformly distributed linear recurring sequences modulo powers of 3

Tamás Herendi

University of Debrecen

June 25 - June 29, 2012
Smolenice

Definition

Let $a_0, \ldots, a_{d-1} \in \mathbb{Z}$ *and* $u = \{u_n\}_{n=0}^{\infty}$ *be a sequence in* $\mathbb{Z}$ *satisfying the* **recurrence relation**

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

Definition

Let $a_0, \ldots, a_{d-1} \in \mathbb{Z}$ *and* $u = \{u_n\}_{n=0}^{\infty}$ *be a sequence in* $\mathbb{Z}$ *satisfying the* **recurrence relation**

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

– u *is a* **linear recurring sequence** *(***LRS***) with* **defining coefficients** $a_0, \ldots, a_{d-1}$ *and* **initial values** $u_0, \ldots, u_{d-1}$.

Definition

Let $a_0, \ldots, a_{d-1} \in \mathbb{Z}$ *and* $u = \{u_n\}_{n=0}^{\infty}$ *be a sequence in* $\mathbb{Z}$ *satisfying the* **recurrence relation**

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

- u *is a* **linear recurring sequence** *(***LRS***) with* **defining coefficients** $a_0, \ldots, a_{d-1}$ *and* **initial values** $u_0, \ldots, u_{d-1}$.
- d *is the* **order** *of the recurrence*

Definition

Let $a_0, \dots, a_{d-1} \in \mathbb{Z}$ *and* $u = \{u_n\}_{n=0}^{\infty}$ *be a sequence in* $\mathbb{Z}$ *satisfying the* **recurrence relation**

$$u_{n+d} = a_{d-1}u_{n+d-1} + \cdots + a_0 u_n \quad \text{for} \quad n = 0, 1, \dots \quad .$$

- u *is a* **linear recurring sequence** *(***LRS***) with* **defining coefficients** $a_0, \dots, a_{d-1}$ *and* **initial values** $u_0, \dots, u_{d-1}$.
- d *is the* **order** *of the recurrence*
- $P(x) = x^d - a_{d-1}x^{d-1} - \cdots - a_0$ *is a* **characteristic polynomial** *of* u.

Remarks

Let $P(x), Q(x) \in \mathbb{Z}[x]$ *and* $m, n \in \mathbb{Z}$.

Remarks

Let $P(x), Q(x) \in \mathbb{Z}[x]$ *and* $m, n \in \mathbb{Z}$.

- *If* $P(x)$ *is a characteristic polynomial of* u, *then the same is true for* $P(x) \cdot Q(x)$.

Remarks

Let $P(x), Q(x) \in \mathbb{Z}[x]$ *and* $m, n \in \mathbb{Z}$.

- *If* $P(x)$ *is a characteristic polynomial of* u, *then the same is true for* $P(x) \cdot Q(x)$.
- $u \mod m$ *is* **periodic**.

Remarks

Let $P(x), Q(x) \in \mathbb{Z}[x]$ *and* $m, n \in \mathbb{Z}$*.*

- *If* $P(x)$ *is a characteristic polynomial of* u*, then the same is true for* $P(x) \cdot Q(x)$*.*
- $u \mod m$ *is* **periodic***.*
- *If* u *is* **uniformly distributed** *(***UD***)* $\mod m \cdot n$ *then it is UD* $\mod m$*, too.*

Question

Assume $m, n \in \mathbb{Z}$ *and* u *is UD both* $\mod m$ *and* $\mod n$.

$$\text{Is it UD} \mod m \cdot n?$$

Question

Assume $m, n \in \mathbb{Z}$ *and* u *is UD both* $\mod m$ *and* $\mod n$.

$$\text{Is it UD} \mod m \cdot n?$$

Answer

It depends.

Question

Assume $m, n \in \mathbb{Z}$ *and* u *is UD both* $\mod m$ *and* $\mod n$.

$$\textit{Is it UD} \mod m \cdot n?$$

Answer

It depends.

- *If the period lengths* $\mod m$ *and* $\mod n$ *are coprime, then yes.*

Question

Assume $m, n \in \mathbb{Z}$ *and* u *is UD both* $\mod m$ *and* $\mod n$.

$$\textit{Is it UD} \mod m \cdot n?$$

Answer

It depends.

- *If the period lengths* $\mod m$ *and* $\mod n$ *are coprime, then yes.*
- *If* m *and* n *are coprime, but the period lengths are not, then need some additional observations.*

Theorem

Let $p \in \mathbb{N}$ be a prime, $d \geq 2$ be an integer, u be a dth-order LRS of integers and let $\sigma = \frac{3d^2+9d}{2} + 1$.

If u is UD modulo p^σ, then it is also UD modulo p^s for any $s \in \mathbb{N}$.

Theorem

Let $p \in \mathbb{N}$ be a prime, $d \geq 2$ be an integer, u be a dth-order LRS of integers and let $\sigma = \frac{3d^2+9d}{2} + 1$.

If u is UD modulo p^σ, then it is also UD modulo p^s for any $s \in \mathbb{N}$.

The theorem is proven in a more general settings in [H 2004].

Theorem

Let $p \in \mathbb{N}$ be a prime, $d \geq 2$ be an integer, u be a dth-order LRS of integers and let $\sigma = \frac{3d^2+9d}{2} + 1$.

If u is UD modulo p^σ, then it is also UD modulo p^s for any $s \in \mathbb{N}$.

The theorem is proven in a more general settings in [H 2004].

If d is large (> 1000), then it is practically useless.

Theorem

Let $p \in \mathbb{N}$ be a prime, $d \geq 2$ be an integer, u be a dth-order LRS of integers and let $\sigma = \frac{3d^2+9d}{2} + 1$.

If u is UD modulo p^σ, then it is also UD modulo p^s for any $s \in \mathbb{N}$.

The theorem is proven in a more general settings in [H 2004].

If d is large (> 1000), then it is practically useless.

With some - not difficult to fulfill - assumptions, we can set $\sigma = 2$, independently of d.

Theorem

Let $p \in \mathbb{N}$ be a prime, $d \geq 2$ be an integer, u be a dth-order LRS of integers and let $\sigma = \frac{3d^2+9d}{2} + 1$.

If u is UD modulo p^σ, then it is also UD modulo p^s for any $s \in \mathbb{N}$.

The theorem is proven in a more general settings in [H 2004].

If d is large (> 1000), then it is practically useless.

With some - not difficult to fulfill - assumptions, we can set $\sigma = 2$, independently of d.

Remains: find (construct) a UD sequence $\mod p^2$.

Theorem

Let $P, Q, P_i \in \mathbb{Z}[x]$ where $i = 1, 2, 3, 4$,

a. *Q be monic irreducible modulo 2 of degree k*
b. $P(x) \equiv (x^2 - 1)Q(x) \mod 2$
c. $P_1(x) = P(x)$
   $P_2(x) = P(x) - 2$
   $P_3(x) = P(x) - 2x$
   $P_4(x) = P(x) - 2x - 2$
d. *$u^{(i)}$ are LRS corresponding to P_i, with the greatest minimal period length modulo 2.*

Then at least one of the $u^{(i)}$'s is UD modulo 2^s with minimal period length $2^s ord(Q)$ for any $s \in \mathbb{N}$. [H 201?]

A similar result can be found for the case $p = 3$.
Crucial point is finding the characteristic polynomial $P(x)$ of the sequence.

A similar result can be found for the case $p = 3$.
Crucial point is finding the characteristic polynomial $P(x)$ of the sequence.

Lemma

Let $\mathbb{F}$ be a finite field and let u be a LRS over $\mathbb{F}$. If u is UD, then the characteristic polynomial of u has a multiple factor.

A similar result can be found for the case $p = 3$.
Crucial point is finding the characteristic polynomial $P(x)$ of the sequence.

Lemma

Let $\mathbb{F}$ be a finite field and let u be a LRS over $\mathbb{F}$. If u is UD, then the characteristic polynomial of u has a multiple factor.

We search in the form $P(x) \equiv (x+1)^2 Q(x) \mod 3$, assuming $Q(x)$ is irreducible with maximal order.

Lemma

Let

a. $Q(x)$ *be irreducible modulo* 3,

b. $P(x) \equiv (x+1)^2 Q(x) \mod 3$,

c. u *be a sequence having characteristic polynomial* P *and minimal period length modulo* 3 *equal to* $ord(P)$.

Then u *is uniformly distributed modulo* 3.

Lemma

Let

a. $Q(x)$ *be irreducible modulo* 3,

b. $P(x) \equiv (x+1)^2 Q(x) \mod 3$,

c. u *be a sequence having characteristic polynomial* P *and minimal period length modulo* 3 *equal to* $ord(P)$.

Then u *is uniformly distributed modulo* 3.

Remark

If $(x+1)Q(x)$ *and* $(x+1)^2$ *is not a characteristic polynomial of* u *then condition* **c.** *holds.*

Lemma

Let

a. $Q(x)$ *be irreducible modulo* 3,

b. $P(x) \equiv (x+1)^2 Q(x) \mod 3$,

c. u *be a sequence having characteristic polynomial* P *and minimal period length modulo* 3 *equal to ord*(P).

Then u *is uniformly distributed modulo* 3.

The proof based on the fact that the period length divides $\mathrm{ord}(P)$. The sequences classified by shifting (cyclic permutation) and the sequences in the maximal classes contains all numbers with equal frequency.

Theorem

Let

a. $Q \in \mathbb{Z}[x]$ *be monic irreducible modulo* 3 *of degree* k

b. $P(x) \equiv (x+1)^2 Q(x) \mod 3$,

c. $P_1(x) = P(x)$
$P_2(x) = P(x) - 3$
$P_3(x) = P(x) - 6$

d. $u^{(i)}$ *be LRS corresponding to* P_i, *with greatest minimal period length modulo* 3.

Then at least one of the $u^{(i)}$*'s is UD modulo* 3^s *with period length* $3^s ord(Q)$ *for any* $s \in \mathbb{N}$.

Theorem

- $P(x) \equiv (x+1)^2 Q(x) \mod 3$,
- $P_1(x) = P(x) \rightarrow u^{(1)}$
  $P_2(x) = P(x) - 3 \rightarrow u^{(2)}$
  $P_3(x) = P(x) - 6 \rightarrow u^{(2)}$

$\Rightarrow$ *one of $u^{(i)}$'s is UD modulo 3^s.*

Theorem

- $P(x) \equiv (x+1)^2 Q(x) \mod 3$,
- $P_1(x) = P(x) \rightarrow u^{(1)}$
  $P_2(x) = P(x) - 3 \rightarrow u^{(2)}$
  $P_3(x) = P(x) - 6 \rightarrow u^{(2)}$

$\Rightarrow$ *one of $u^{(i)}$'s is UD modulo 3^s.*

Proof:

Theorem

- $P(x) \equiv (x+1)^2 Q(x) \mod 3$,
- $$\begin{aligned} P_1(x) &= P(x) &\to\ u^{(1)} \\ P_2(x) &= P(x) - 3 &\to\ u^{(2)} \\ P_3(x) &= P(x) - 6 &\to\ u^{(2)} \end{aligned} \quad \Rightarrow \quad$$ *one of $u^{(i)}$'s is UD modulo 3^s.*

Proof:

1. In one of the cases the period length increases by a factor of 3, as the exponent of 3 increases.

Theorem

- $P(x) \equiv (x+1)^2 Q(x) \mod 3$,
- $$\begin{array}{lcl} P_1(x) = P(x) & \to & u^{(1)} \\ P_2(x) = P(x) - 3 & \to & u^{(2)} \\ P_3(x) = P(x) - 6 & \to & u^{(2)} \end{array} \quad \Rightarrow \quad \textit{one of } u^{(i)}\textit{'s is UD modulo } 3^s.$$

Proof:

1. In one of the cases the period length increases by a factor of 3, as the exponent of 3 increases.

2. In that case, the period modulo 3^2 is divided into 3 equal part and the parts can be additively shifted to each other $\Rightarrow$ the sequence is UD.

Theorem

- $P(x) \equiv (x+1)^2 Q(x) \mod 3$,
- $$\begin{array}{lcl} P_1(x) = P(x) & \to & u^{(1)} \\ P_2(x) = P(x) - 3 & \to & u^{(2)} \\ P_3(x) = P(x) - 6 & \to & u^{(2)} \end{array} \quad \Rightarrow \quad \textit{one of } u^{(i)}\textit{'s is UD modulo } 3^s.$$

Proof:

1. In one of the cases the period length increases by a factor of 3, as the exponent of 3 increases.

2. In that case, the period modulo 3^2 is divided into 3 equal part and the parts can be additively shifted to each other $\Rightarrow$ the sequence is UD.

3. By a general theorem of [H 2004] this implies the UD for any exponent.

Algorithm for constructing UD sequence

Step 1 Choose modulo 3 irreducible $Q(x) \in \mathbb{Z}[x]$ of degree k.

Algorithm for constructing UD sequence

Step 1 Choose modulo 3 irreducible $Q(x) \in \mathbb{Z}[x]$ of degree k.
Step 2 Calculate $P(x) \equiv (x+1)^2 Q(x) \mod 3$,
$P'(x) \equiv (x+1)Q(x) \mod 3$ and
$P_1(x) = P(x)$, $P_2(x) = P_1(x) - 3$, $P_3(x) = P_1(x) - 6$.

Algorithm for constructing UD sequence

Step 1 Choose modulo 3 irreducible $Q(x) \in \mathbb{Z}[x]$ of degree k.
Step 2 Calculate $P(x) \equiv (x+1)^2 Q(x) \mod 3$,
$P'(x) \equiv (x+1)Q(x) \mod 3$ and
$P_1(x) = P(x)$, $P_2(x) = P_1(x) - 3$, $P_3(x) = P_1(x) - 6$.
Step 3 Calculate the companion matrices $M_{(i)}$ corresponding to the characteristic polynomials $P_i(x)$.

Algorithm for constructing UD sequence

Step 1 Choose modulo 3 irreducible $Q(x) \in \mathbb{Z}[x]$ of degree k.
Step 2 Calculate $P(x) \equiv (x+1)^2 Q(x) \mod 3$,
$P'(x) \equiv (x+1)Q(x) \mod 3$ and
$P_1(x) = P(x)$, $P_2(x) = P_1(x) - 3$, $P_3(x) = P_1(x) - 6$.
Step 3 Calculate the companion matrices $M_{(i)}$ corresponding to the characteristic polynomials $P_i(x)$.
Step 4 Compute $\varrho = \mathrm{ord}(Q)$ modulo 3 and $M_1^{3\varrho}$ modulo 9. If $M_1^{3\varrho} \not\equiv E \mod 9$ then set $M = M_1$ else do the same with M_2. If it is still not good then $M = M_3$.

Algorithm for constructing UD sequence

Step 1 Choose modulo 3 irreducible $Q(x) \in \mathbb{Z}[x]$ of degree k.
Step 2 Calculate $P(x) \equiv (x+1)^2 Q(x) \mod 3$,
$P'(x) \equiv (x+1)Q(x) \mod 3$ and
$P_1(x) = P(x),\ P_2(x) = P_1(x) - 3,\ P_3(x) = P_1(x) - 6.$
Step 3 Calculate the companion matrices $M_{(i)}$ corresponding to the characteristic polynomials $P_i(x)$.
Step 4 Compute $\varrho = \mathrm{ord}(Q)$ modulo 3 and $M_1^{3\varrho}$ modulo 9. If $M_1^{3\varrho} \not\equiv E \mod 9$ then set $M = M_1$ else do the same with M_2. If it is still not good then $M = M_3$.
Step 5 Initial values: we want to have s digits random numbers, choose random $u_0, u_1, \ldots, u_k \in [0, 3^s - 1]$. Set these values as initial values of the linear recurring sequence with characteristic polynomial $P'(x)$. Compute the next element of the sequence u'_{k+1}. Find a random number $u_{k+1} \in [0, 3^s - 1]$ satisfying $u_{k+1} \not\equiv u'_{k+1} \mod 3$. The set $u_0, u_1, \ldots, u_k, u_{k+1}$ are suitable initial values for the sequence.

References

- T. Herendi, *Uniform distribution of linear recurrences modulo prime powers* J. Finite Fields And Applications 10 (2004), 1-23.
- T. Herendi, *Construction of uniformly distributed linear recurring sequences modulo powers of 2* (201?)
- T. Herendi, R.S. Major, *Modular exponentiation of matrices on FPGA-s* Acta Univ. Sapientiae, Informatica, 3, 2 (2011) 172 - 191