Mersenne Twister

David Kubát

22. listopadu 2014

Table of contents

Generalized feedback shift register

- The generalized feedback shift register (GFSR) is a pseudorandom number generator introduced in 1973

Definition

Let $n \in \mathbb{N}$, $0 < m < n$, $\mathbf{x}_0, ..., \mathbf{x}_{n-1} \in \mathbb{F}_2^w$. The generalized feedback shift register (GFSR) sequence is the sequence $\{\mathbf{x}_l\}_{l=0}^{\infty}$ defined by the equation

$$\mathbf{x}_{l+n} = \mathbf{x}_{l+m} \oplus \mathbf{x}_l, \quad l = 0, 1, ...$$

.

Generalized feedback shift register

- If $\{\mathbf{x}_l\}_{l=0}^{\infty}$ is a GFSR sequence, then for every $l = 0, 1, ...$

$$(\mathbf{x}_{l+n}|...|\mathbf{x}_{l+1}) = (\mathbf{x}_{l+n-1}|...|\mathbf{x}_l)B,$$

where

$$B = \begin{bmatrix} \mathbf{0} & \mathbf{I}_w & \dots & \mathbf{0} & \dots & \mathbf{0} \\ \vdots & & \ddots & & & \vdots \\ \mathbf{I}_w & \mathbf{0} & \dots & \mathbf{I}_w & \dots & \mathbf{0} \\ \vdots & & & \vdots & & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{I}_w & \mathbf{0} & \dots & \mathbf{0} & \dots & \mathbf{0} \end{bmatrix} \in \mathbb{F}_2^{nw \times nw}$$

and $|$ denotes concatenation of vectors.

Generalized feedback shift register

Observation

Let $\{\mathbf{x}_l\}_{l=0}^{\infty}$ be a GFSR sequence. Then each of the w sequences of bits is a LFRSR sequence with characteristic polynomial $x^n + x^m + 1$.

- m, n are chosen so that $x^n + x^m + 1 \in \mathbb{F}_2[x]$ is primitive. In that case, each of the w sequences of bits induced by $\{\mathbf{x}_l\}_{l=0}^{\infty}$ has a period equal to $2^n - 1$ (and so has the sequence$\{\mathbf{x}_l\}_{l=0}^{\infty}$).
- In other words, each of the w sequences of bits is an m-sequence.

Definition

Binary LFSR sequence with a characteristic polynomial of degree n and period equal to $2^n - 1$ is called m-sequence,

Similarity of GFSR to LFSR

- A sequence of bits $\{a_i\}_{i=0}^{\infty}$ is generated by a linear feedback shift register (LFSR), if there exist bits $c_{n-1}, ..., c_0$ such that

$$(a_{j+n}, ..., a_{j+1}) = (a_{j+n-1}, ..., a_j)A, \ j = 0, 1, ...$$

where

$$A = \begin{bmatrix} c_{n-1} & 1 & 0 & \dots & 0 \\ c_{n-2} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_1 & 0 & 0 & \dots & 1 \\ c_0 & 0 & 0 & \dots & 0 \end{bmatrix} \in \mathbb{F}_2^{n \times n}$$

Drawbacks of GFSR sequences

- The selection of initial seed (the first n vectors) is very critical and influential in the randomness; good initialization is time-consuming

Drawbacks of GFSR sequences

- The selection of initial seed (the first n vectors) is very critical and influential in the randomness; good initialization is time-consuming
- As mentioned before, each bit of a GFSR sequence can be regarded as an m-sequence based on the trinomial $x^n + x^m + 1$, which is known to have poor randomness

Drawbacks of GFSR sequences

- The selection of initial seed (the first n vectors) is very critical and influential in the randomness; good initialization is time-consuming
- As mentioned before, each bit of a GFSR sequence can be regarded as an m-sequence based on the trinomial $x^n + x^m + 1$, which is known to have poor randomness
- The period of a GFSR sequence $2^n - 1$ is far smaller than the theoretical upper bound (i.e. the number of possible states 2^{nw})

Twisted GFSR

- The Twisted generalized feedback shift register (Twisted GFSR) is a pseudorandom number generator introduced in 1992

Definition

Let $n \in \mathbb{N}$, $0 < m < n$, $\mathbf{x}_0, ..., \mathbf{x}_{n-1} \in \mathbb{F}_2^w$. Moreover, let $A \in \mathbb{F}_2^{w \times w}$ be a square $w \times w$ matrix. The twisted generalized feedback shift register (twisted GFSR) sequence is the sequence $\{\mathbf{x}_l\}_{l=0}^{\infty}$ defined by the equation

$$\mathbf{x}_{l+n} = \mathbf{x}_{l+m} \oplus \mathbf{x}_l A, \ \ l = 0, 1, ...$$

We denote this sequence by $\chi(n, m, A)$.

Twisted GFSR

- With suitable choice of n, m, and A, the twisted GFSR generator attains the maximal periond $2^{nw} - 1$. In such case, the inicialization is carefree
- Compared to GFSR, the twisted GFSR requires much less working area in order to attain the same period (note the example on the next next slide)

Twisted GFSR

Definition

Polynomial $f \in \mathbb{F}_2[x]$ of degree n is primitive, if it is irreducible and it's root in $\mathbb{F}_{2^n}$ is a primitive element.

Theorem

Let $\varphi_A(\lambda) \in \mathbb{F}_2[\lambda]$ be the characteristic polynomial of the matrix A. The period of $\chi(n, m, A)$ is $2^{nw} - 1$ if and only if $\varphi_A(t^n + t^m)$ is a primitive polynomial of degree nw.

Twisted GFSR

Example

Consider the trinomial $f(x) = x^n + x^m + 1 = x^2 + x + 1 \in \mathbb{F}_2[x]$. f is a primitive polynomial, so the GFSR based on f has period $2^2 - 1 = 3$ (for any choice of initial seed and w).

Example (Continued)

Consider the 2×2 matrix $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ (so we have $w = 2$). The characteristic polynomial is $\varphi_A(\lambda) = \lambda^2 + \lambda + 1$ and $\varphi_A(t^2 + t) = t^4 + t + 1$ is primitive. So by the previous theorem period of $\chi(2, 1, A) = 2^{2*2} - 1 = 15$

Mersenne Twister

- Suppose we have a polynomial of degree p over $\mathbb{F}_2$
- To test primitivity, one needs to know the factors of $2^p - 1$
- For large p, it would be advantageous that $2^p - 1$ be a (Mersenne) prime
- This is the case of the characteristic polynomial of the Mersenne twister generator

Mersenne Twister

- The Mersenne Twister algorithm is a pseudo random number generator introduced in 1997
- Essentially, it is derived from Twisted GFSR, with a modification allowing us to attain much longer periods

Mersenne Twister

Definition

Let $n \in \mathbb{N}$, $0 < m < n$, $\mathbf{x}_0, ..., \mathbf{x}_{n-1} \in \mathbb{F}_2^w$. Moreover, let $A \in \mathbb{F}_2^{w \times w}$ be a square $w \times w$ matrix and $r \in \{0, ..., w-1\}$. The Mersenne Twister algorithm generates a sequence $\{\mathbf{x}_l\}_{l=0}^{\infty}$ of vectors defined by the equation

$$\mathbf{x}_{l+n} := \mathbf{x}_{l+m} \oplus (\mathbf{x}_l^u | \mathbf{x}_{l+1}^l) A,$$

$l = 0, 1, ...$
$\mathbf{x}_k^u$ and $\mathbf{x}_{k+1}^l$ are defined as the upper $w - r$ bits of $\mathbf{x}_k$ and the lower r bits of $\mathbf{x}_{k+1}$ respectively.

Mersenne Twister

Definition

Let $n \in \mathbb{N}$, $0 < m < n$, $\mathbf{x}_0, ..., \mathbf{x}_{n-1} \in \mathbb{F}_2^w$. Moreover, let $A \in \mathbb{F}_2^{w \times w}$ be a square $w \times w$ matrix and $r \in \{0, ..., w-1\}$. The Mersenne Twister algorithm generates a sequence $\{\mathbf{x}_l\}_{l=0}^{\infty}$ of vectors defined by the equation

$$\mathbf{x}_{l+n} := \mathbf{x}_{l+m} \oplus (\mathbf{x}_l^u | \mathbf{x}_{l+1}^l) A, \tag{1}$$

$l = 0, 1, ...$

- In case $r = 0$, we obtain the defining recurrence of Twisted GFSR
- In case $r = 0$ and $A = I_w$, we obtain the defining recurrence of GFSR

Mersenne Twister

To make computation easy, the matrix A is chosen to be of the form

$$A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ a_{w-1} & a_{w-1} & a_{w-2} & \dots & a_0 \end{bmatrix}$$

So instead of whole matrix A, we only look for the vector $\mathbf{a} = (a_{w-1}, ..., a_0)$

Mersenne Twister

Observation

Let $\{\mathbf{x}_l\}_{l=0}^{\infty}$, $\mathbf{x}_l \in \mathbb{F}_2^w$ be a sequence in $\mathbb{F}_2^w$. It can be shown, that (1) is equivalent to

$$(\mathbf{x}_{i+n}|...|\mathbf{x}_{i+1}^u) = (\mathbf{x}_{i+n-1}|...|\mathbf{x}_i^u)B, \ i = 0, 1, ...$$

for some matrix $B \in \mathbb{F}_2^{(nw-r)\times(nw-r)}$.

- In order to attain the full period $2^{nw} - 1$, we're looking for MT parameters, such that $nw - r$ is a Mersenne exponent and the characteristic polynomial of B is primitive.

Explicit form of B

$$B = \begin{bmatrix} \mathbf{0} & \mathbf{I}_w & \mathbf{0} & \mathbf{0} & & & \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_w & \mathbf{0} & & & \\ \vdots & & & \ddots & & & \\ \mathbf{0} & & & & & & \\ \mathbf{I}_w & & & & & & \\ \mathbf{0} & & & & & & \\ \vdots & & & & \ddots & & \\ \mathbf{0} & & & & \mathbf{0} & \mathbf{I}_w & \mathbf{0} \\ \mathbf{0} & & & & \mathbf{0} & \mathbf{0} & \mathbf{I}_{w-r} \\ \mathbf{S} & & & & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}, \quad S = \begin{bmatrix} \mathbf{0} & \mathbf{I}_r \\ \mathbf{I}_{w-r} & \mathbf{0} \end{bmatrix} A.$$

Characteristic polynomial of B

The characteristic polynomial $\varphi_B(t)$ of B can be computed as

$$\varphi_B(t) = (t^n+t^m)^{w-r}(t^{n-1}+t^{m-1})^r + a_0(t^n+t^m)^{w-r}(t^{n-1}+t^{m-1})^{r-1}$$
$$+ \ldots + a_{r-2}(t^n+t^m)^{w-r}(t^{n-1}+t^{m-1}) + a_{r-1}(t^n+t^m)^{w-r}$$
$$+ a_r(t^n+t^m)^{w-r-1} + \ldots + a_{w-2}(t^n+t^m) + a_{w-1}$$

if $A = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ a_{w-1} & a_{w-1} & a_{w-2} & \ldots & a_0 \end{bmatrix}$.

MT19937

- Usually, the parameters are set as follows

$$(w, n, m, r) = (32, 624, 397, 31), \ \mathbf{a} = (9908B0DF)$$

- Then the MT generates a sequence with period equal to $2^{19937} - 1$

Randomness measure

Definition

A pseudorandom sequence $\mathbf{x}_i$ of w-bit integers of period P satisfying the following condition is said to be k-distributed to a v-bit accuracy: let $trunc_v(\mathbf{x})$ denote the number formed by the leading v bits of $\mathbf{x}$, and consider P of the kv-bit vectors

$$(trunc_v(\mathbf{x}_i), trunc_v(\mathbf{x}_{i+1}), ..., trunc_v(\mathbf{x}_{i+k-1})),\ 0 \leq i < P.$$

Then, each of the 2^{kv} possible combinations of bits occurs the same number of times in a period, except for the all-zero combination that occurs once less often.

Randomness measure

- Possible interpretation: Assume that the sequence is k-distributed to v-bit accuracy, and that all the bits in the seed are randomly given. Then, knowledge of the most significant v bits of the first l words does not allow the user to make any statement about the most significant v bits of the next word, if $l < k$.
- With parameters suggested above, the MT is k-distributed to 32-bit accuracy for every $1 \leq k \leq 623$ (after so called tempering)

Suitability for use in cryptography

- In its native form, it isn't suitable for use in cryptography.

Thank you for your attention!