Formal Verification and Code-Generation of Mersenne-Twister Algorithm

Takafumi Saikawa and Kazunari Tanaka and Kensaku Tanaka

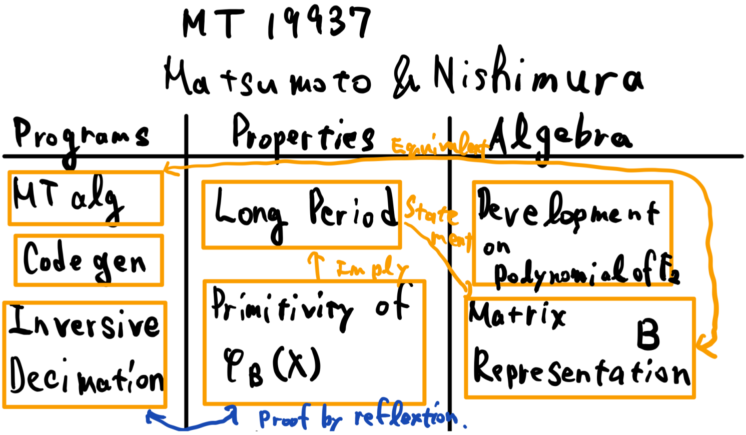
December 7, 2020

Mersenne-Twister (Matsumoto and Nishimura, 1998)

Our work is based on the original work by Matsumoto and Nishimura:

- Mersenne-Twister is a pseudo-random number generator
  - Long-period : $2^{19937} - 1$
  - Good stochastic properties, e.g., 623-distribution
- Two presentations: algebraic and pseudocode
- Their equivalence is implicit
- Proof of long-period property
  - Reduce the property to the irreducibility of a polynomial
  - Use "inversive-decimation" to show the irreducibility

Overview of the project



- Orange: finished formalizations
- Blue: the last remaining part for the long-period property

Formal Verification and Code-Generation of Mersenne-Twister Algorithm

Linear-algebraic presentation

$$A = \left(\begin{array}{c|cccc} & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ \hline a_0 & a_1 & a_2 & \cdots & a_{w-1} \end{array}\right) \qquad S = \left(\begin{array}{c|c} & 1_r \\ \hline 1_{w-r} & \end{array}\right) A$$

$$B = \left(\begin{array}{c|cccccc} & 1_w & & & & & \\ & & 1_w & & & & \\ & & & \ddots & & & \\ 1_w & & & & 1_w & & \\ & & & & & \ddots & \\ & & & & & & 1_{w-r} \\ \hline S & & & & & & \end{array}\right)$$

Linear-algebraic presentation

(`Lemma mulBE` in `cycle.v`)

$$xB = \begin{pmatrix} x_w^n \\ \hline x_w^{n-1} \\ \hline x_w^{n-2} \\ \hline \vdots \\ \hline x_w^2 \\ \hline x_w^1 \\ \hline x_{w-r}^0 \end{pmatrix}^T \left(\begin{array}{c|cccccc} & 1_w & & & & & \\ & & 1_w & & & & \\ & & & \ddots & & & \\ 1_w & & & & 1_w & & \\ & & & & & \ddots & \\ & & & & & & 1_{w-r} \\ \hline S & & & & & & \end{array}\right)$$

$$= \left(\begin{array}{c|c|c|c|c} x_w^m + x_w^1 \left(\begin{array}{c|c} & \\ \hline & 1_r \end{array}\right) A & & & & \\ + \left(\begin{array}{c|c} x_{w-r}^0 & 0 \end{array} \right) A & x_w^n & \ldots & x_w^2 & x_{w-r}^1 \end{array} \right)$$

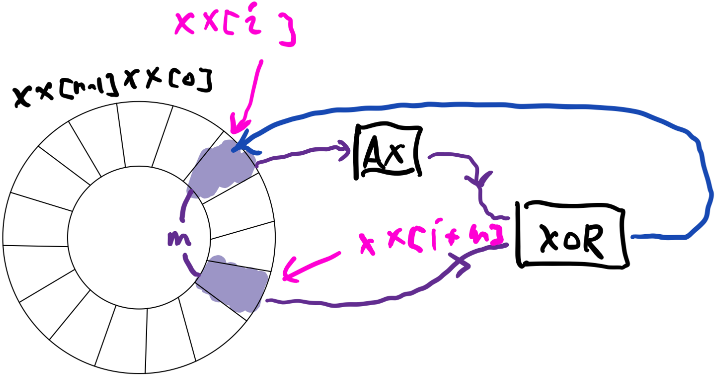
The linear recurrence : $x_w^m + x_w^1 \left(\begin{array}{c|c} & \\ \hline & 1_r \end{array}\right) A + \left(\begin{array}{c|c} x_{w-r}^0 & 0 \end{array} \right) A$.

Pseudocode presentation

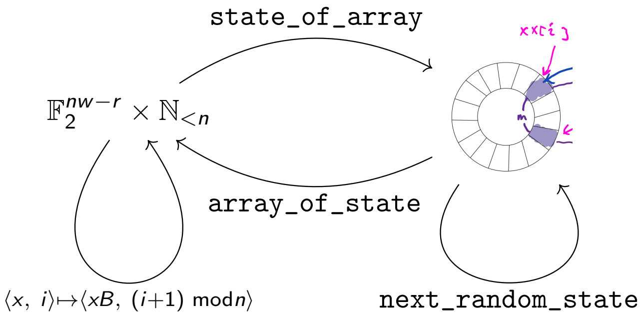
(Definition next_random_state in mt.v)

```
 u      := 1..10..0  ; (w-r) ones and r zeroes
 ll     := 0..01..1  ; (w-r) zeroes and r ones
 i      := 0
 xx[0],..,xx[n-1] := "initial words, not all-zero"
LOOP:
 y      := (xx[i] AND u) OR (xx[(i+1) mod n] AND ll)
 xx[i] := xx[(i+m) mod n] XOR (y >> 1)
                   XOR (if LSB(y) = 0 then 0 else aa)
 OUTPUT xx[i]
 i      := (i+1) mod n
 GOTO LOOP
```

Pseudocode presentation



Equivalence and data structures



- $\mathbb{F}_2^{nw-r} \times \mathbb{N}_{<n} \ni \langle x,\ i\rangle$ is a pair of a state vector and the number of multiplications by B
- `state_of_array` and `array_of_state` are inverses to each other.
- The equivalence (`Lemma next_random_stateE`): for any state σ,

$$\texttt{next\_random\_state}(\sigma) =$$
$$\texttt{state\_of\_array}((\texttt{array\_of\_state}(\sigma))B)$$

Data structures in Coq

$\mathbb{F}_2^{nw-r} \times \mathbb{N}_{<n}$:

Record `vector_with_counter` :=

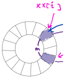
`{`

  `vector` $\in F_2^{nw-r}$;

  `counter` $\in N$;

  `_ : counter < n;`

`}.`

:

Record `valid_random_state` :=

`{`

  $\langle \sigma, k \rangle \in$ (`list` N) $\times N$;

  `_ : size` (σ) `== n;`

  `_ :` k `< n;`

  `_ :` $\forall i < n, i < \texttt{size}(\sigma) \Rightarrow \sigma[i] < 2^w$;

  `_ : The lower` r `bits of` $\sigma[k]$ `are 0;`

`}.`

Irreducibility implies Long-period

Lemma (irreducibleP)

Let $x \in \mathbb{F}_2[X]/\varphi(X)$. If we assume $x^2 \neq x$, the following are equivalent.

1. $\varphi(X)$ *is irreducible (i.e. primitive).*
2. $X^2 \not\equiv_{\varphi(X)} X$ *and* $X^{2^{nw-r}} \equiv_{\varphi(X)} X$.

Lemma (cycleB_dvdP)

Assume that the characteristic polynomial $\varphi_B(X)(= \det(XI - B))$ of B is irreducible. Then for any $q \in \mathbb{N}_{>0}$, the following are equivalent.

1. $B^q = B$.
2. $q - 1$ *is divided by* $2^{nw-r} - 1$.

Lemma (pm)

$2^{624*32-31} - 1 = 2^{19937} - 1$ *is a prime.*

Proof technique: Quotient structure

$$\begin{tikzcd} \mathbb{F}_2[X] \arrow[r, bend left, "\pi"] & \mathbb{F}_2[X]/\varphi_B(X) \arrow[l, bend left, "repr"] \end{tikzcd}$$

- We need to deal with the quotient of the polynomial ring $\mathbb{F}_2[X]$ by the ideal $(\varphi_B(X))$.
- MathComp provides the construction of quotient rings for given ideals.
- We want further structures: of vector space and field.

Proof technique: Quotient structure

$$\begin{tikzcd}
\mathbb{F}_2[X] \arrow[rr, bend left, "\pi"] & & \mathbb{F}_2[X]/\varphi_B(X) \arrow[ll, bend left, "repr"]
\end{tikzcd}$$

We had to prove algebraic facts in addition to MathComp, e.g.:

- Lemma `pi_linear` : the canonical surjection $\mathbb{F}_2[X] \xrightarrow{\pi} \mathbb{F}_2[X]/\varphi_B(X)$ is linear.
- Lemma `QphiI_field` : the quotient $\mathbb{F}_2[X]/\varphi_B(X)$ is a field.
- Lemma `QphiIX_full` and Lemma `QphiIX_free` : $\mathbb{F}_2[X]/\varphi_B(X)$ as a vector space has $1, X, X^2, \ldots, X^{nw-r}$ as its basis.
- Constructivist's note: the explicit form of an inverse element is given by Euclidean algorithm.

Inversive-decimation

Checking that the period is long

V: Vector space of state vectors

The dimension of V is p and p is mersenne exponent i.e. $2^p - 1$ is prime.

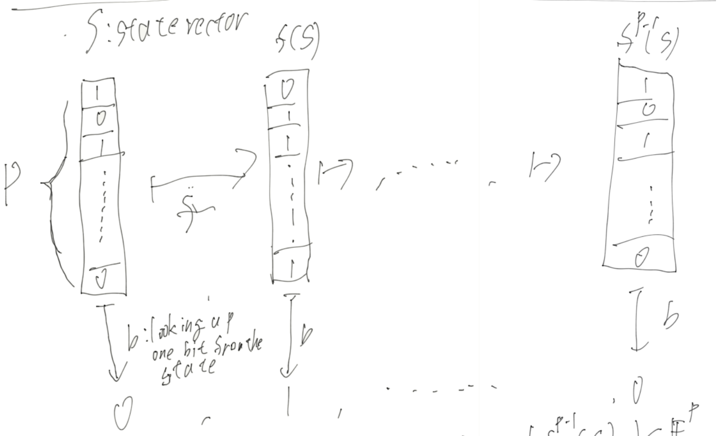
$V \xrightarrow{f} V$: linear state transition map

We want to check that the period of f is $2^p - 1$

computational complexity of simple calculation of f^{2^p-1} is $O(p^3)$

Inversive-decimation

Inversive Decimation Method



$\Phi: V \ni S \longmapsto (b(S), bf(S), \ldots, bf^{p-1}(S)) \in \mathbb{F}_2^p$

We assume that Φ is isomorphism

Inversive-decimation

Inversive Decimation Method

$$s \mapsto \left(b(s), bf(s), \ldots, bf^{p-1}(s), \ldots, bf^{2^p-2}(s)\right)$$

Decimation

$$F(s) \xleftarrow{\Phi^{-1}} \left(b(s), bf^2(s), bf^4(s), \ldots, bf^{2^p-2}(s)\right)$$

chose s s.t. $s \neq F(s)$

[MT] proves that

$F^p(s) = s \Rightarrow$ Group generated by $F \cong Gal(\mathbb{F}_{2^p}/\mathbb{F}_2)$

$\Rightarrow \mathbb{F}_2[t]/\varphi(f) \cong \mathbb{F}_{2^p}$

$\Rightarrow$ period of f is $2^p - 1$

($\varphi(f)$ is characteristic polynomial of f)

Inversive-decimation

Inversive Decimation Method

we assume f and b are computable in $O(1)$ and Φ^{-1} is computable in $O(P)$.
So we check that the period of f is 2^P-1 in $O(P^2)$ by Inversive decimation method.
we formalize Inversive decimation method by Coq. and extract executable and fast enough C code. formalize of the proof is work in progress

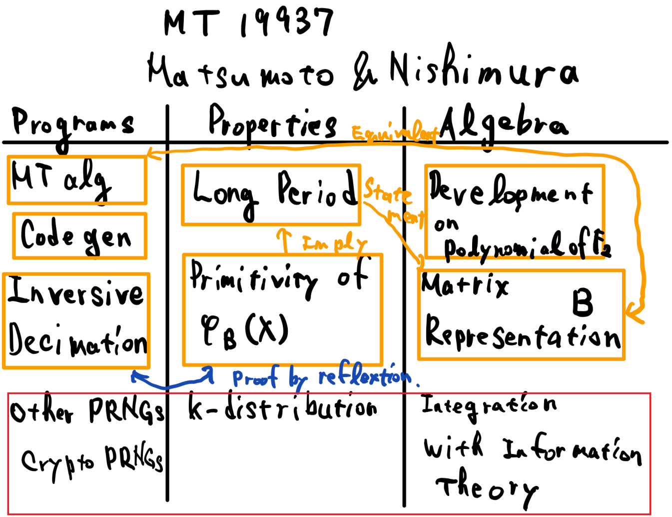
Inversive-decimation

- Remaining tasks:
  - Infinite-dimensional vector space
  - Binding the algorithm and the proof
  - The current version algorithm is not practical in Coq.

Code Generation

- Mersenne-Twister algorithm consists of binary arithmetic operations.
- BinNat library $\to$ a word of C.
- `N.lxor` $\to$ ^ (lxor operation)
- `N.succ` $\to$ _ $+ 1$

Conclusion and future work



- Our next plan is the Blue part, completing the long-period.
- The Red parts are future directions.