疑似乱数生成回路 MT19937 の設計と評価

指導教官：市川 周一　　学籍番号：011703 小沼 士郎

1　背景と目的

計算物理学など多くの分野では，シミュレーションに乱数が必要とされる．多くの場合，高速性や再現性の観点から擬似乱数が用いられ，線型合同法などのアルゴリズムが利用されている．しかし既存の生成法では分布が不均一であるため，シミュレーション結果に深刻な影響を及ぼすことが知られている．

Mersenne Twister (MT)[1] は，1997 年に松本と西村によって開発された疑似乱数生成アルゴリズムである．MT は周期が極めて長く，動作が高速であり，高次元均等分布が証明されているなど多くの長所を持つため，シミュレーション科学に適した擬似乱数生成法として注目されている．

近年，シミュレーションを高速化するために専用ハードウェアが用いられているが，専用ハードウェアでは擬似乱数生成も論理回路として実装しなければならない．そこで本研究では，MT の一種である MT19937 のハードウェアを設計・評価する．MT19937 は $2^{19937}-1$ という長い周期を持ち，623 次元均等分布するため，シミュレーション用には充分な仕様を持っている．

先行研究 [2] では，PCI バスに接続する周辺回路として MT を実現した．実装評価には Xilinx 社の Field Programmable Gate Array (FPGA) を用いているが，1 乱数の生成に 2 クロック要し，乱数生成速度は 0.52〜0.58 Gbps 程度である．それに対し本研究では，高速並列シミュレーションに対応するため，1 クロックに 1〜複数個の乱数を生成する高性能乱数生成回路について検討する．

2　各回路の構成

MT19937 の乱数生成回路は，内部状態を記憶する RAM，現在の内部状態から新しい内部状態を作る生成回路 (Generate)，新しい内部状態から乱数を生成する調律回路 (Temper) から構成される．MT19937 の処理フローは図 1 の通りである．

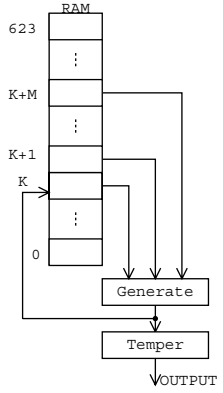

図 1: smt, pmt の構成図

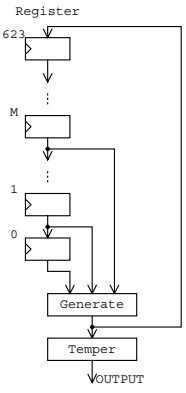

図 2: fmt の構成図

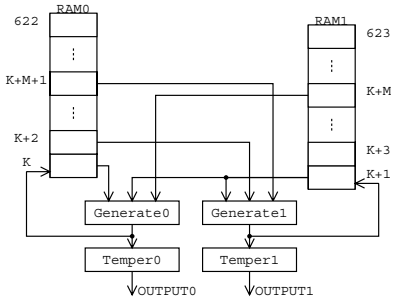

図 3: pmt2 の構成図

図 1 では，1 乱数を生成する毎に RAM を 3 回読んで 1 回書き込む．RAM をデュアルポート RAM で実装し，2 サイクルで 1 乱数生成する回路を以下で **smt** と呼ぶ (先行研究 [2] 相当の回路)．RAM をマルチポート RAM (3R/1W) で実装し，1 サイクルで 1 乱数生成する回路を **pmt** と呼ぶ．さらに RAM をマルチバンク構成にすることにより，1 サイクルに複数乱数を生成することも可能である．1 サイクルで 2 乱数生成する回路 (**pmt2**) を図 3 に示すが，最大で 1 サイクル 52 乱数まで自然に拡張できる．

MT は Generalized Feedback Shift Register という M 系列生成器を基に作られているため [1]，巡回シフトレジスタによる実装が可能である．MT の内部状態格納にレジスタを用いた回路を **fmt** と呼ぶ (図 2)．fmt も pmt と同様に並列出力が可能で，1 サイクルの最大並列出力数は 227 である．

本研究では先行研究 [2] と同様に，内部状態の初期値を外部から与える構成とした．初期化回路を組み込んだ場合の評価結果は，紙数の関係上省略する．

3　評価結果と考察

本研究で設計した回路 (smt，pmt，fmt) を VHDL で記述し，CAD で論理規模 (LE 数，RAM 量) と性能を見積もった．回路の評価には Altera 社の FPGA 用ツール (QuartusII 4.0) を用い，対象デバイスには EP1S10F780C7ES を指定した．比較のため ANSI C の BSD 版 rand 関数を VHDL で記述し (**rand**)，回路規模と性能を見積もった．ちなみに rand のアルゴリズムは線形合同法の一種で，周期は 2^{30} である．さらに西村・松本による MT19937 の C 言語プログラム (**mt19937ar**) を用いて，ソフトウェアの性能を測定した．測定には，Athlon XP 2600+ (2.1 GHz)，Linux 2.4.20-6，gcc 3.2.2 –O2 を用いた．

評価結果を図 4，図 5 にまとめる．rand はメモリを使用しないため，図 5 には現れない．fmt の出力を並列化した回路は，論理規模が大きく EP1S10F780C7ES に実装できないため，ここでは省略する．図示した性能は，回路の最高動作可能周波数における性能である．

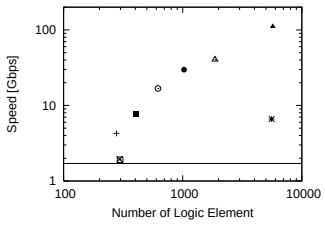

図 4: LE 数と性能

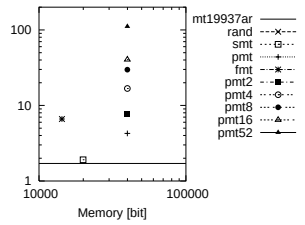

図 5: メモリ量と性能

smt，pmt，fmt の性能は各 1.91 Gbps，4.26 Gbps，6.62 Gbps で，Athlon 上のソフトウェア (1.71 Gbps) よりも高速である．smt，pmt，fmt の動作周波数は各 128 MHz，143 MHz，222 MHz であった．pmt の並列度を上げると動作周波数は漸減するが性能は向上し，pmt2 で 7.65 Gbps，pmt52 では 111 Gbps に達する．このとき pmt2 と pmt52 の動作周波数は各 128 MHz，72 MHz である．FPGA による実装であること，専用計算回路全体の動作可能周波数との比較を考えると，十分な動作周波数と思われる．pmt2〜pmt52 の RAM 量は pmt と同じであるが，LE 数は 1.46〜20.5 倍となる．1 ユニットの pmt2 は 2 ユニットの pmt より論理規模が小さいことが確認された．

参考文献

[1] M. Matsumoto, T. Nishimura : “Mersenne Twister: A 623-Dimensionally Equidistributed Uniform Pseudo-Random Number Generator,” ACM Trans. Model. Comput. Simul., Vol. 8, No. 1, pp. 3–30 (1998).

[2] 黒川 恭一, 梶崎 浩嗣 : “Mersenne Twister の FPGA による実装,” 防衛大学校理工学研究報告, Vol. 40, No. 2, pp. 15–21 (2003).