

3x + 1 予想検証回路の改良と評価

指導教官：市川周一

学籍番号：033701 秋中昌訓

1 はじめに

L. Collatz は、任意の自然数 n に対し、式 (1) の操作を繰り返すと必ず 1 になるという予想を立てた ($3x + 1$ 予想)。

$$H(n) = \begin{cases} 3n + 1, & \text{if } n \equiv 1 \pmod{2}, \\ n/2, & \text{if } n \equiv 0 \pmod{2}. \end{cases} \quad (1)$$

しかし、 $3x + 1$ 予想は未解決である [1]。そのためソフトウェアによる検証が行われており、2004 年 7 月現在、 $n = 9 \times 2^{55} (\pm 324 \times 10^{15})$ まで予想の成立が確認されている [2]。

本研究では、Field Programmable Gate Array (FPGA) を用いて、 $3x + 1$ 予想を高速で検証するための専用回路を設計・評価する。先行研究 [3] を基に Composite Polynomial の bit 幅を調整し (2 節)、回路のパイプライン化を施す (3 節) ことで改良を試みる。 $3x + 1$ 予想の検証はデバイス上で並列処理が可能であるため、評価尺度には AT 積を用いる。AT 積とは、回路規模 (Area) × 実行時間 (Time)、即ち単位性能当たりの必要面積である。

2 3x + 1 予想のアルゴリズム

自然数 m 以下で $3x + 1$ 予想が確認されているとする。 $m + 1$ の検証中に途中結果が n より小さくなれば、1 まで計算を続けなくとも数学的帰納法により n について検証が成立する。この他にも $3x + 1$ 予想を効率よく解く手法が提案されている [4]。

• Composite Polynomial (CP)

下位 k bit の値に応じて、複数ステップ分の $H(n)$ をまとめて計算する。例えば 2-bit CP は式 (2) のようになる。

$$CP_2(n) = \begin{cases} 3\lfloor \frac{n}{4} \rfloor + 1, & \text{if } n \equiv 1 \pmod{4}, \\ 3\lfloor \frac{n}{4} \rfloor + 2, & \text{if } n \equiv 2 \pmod{4}, \\ 9\lfloor \frac{n}{4} \rfloor + 8, & \text{if } n \equiv 3 \pmod{4}, \\ \frac{n}{4}, & \text{if } n \equiv 0 \pmod{4}. \end{cases} \quad (2)$$

• Cutoff

CP を用いて複数ステップ分計算した後に入力値よりも小さくなるのが明らかであれば、最初から計算を省略する。

これらのアルゴリズムを GMP (多倍長精度数値計算ライブラリ) を用いて C 言語で実装し、CP の bit 幅を変えながら実行時間を測定した。測定環境は Vine Linux 2.6r1, Athlon XP 2600+, コンパイラは gcc 2.95.3 でオプションは -O2 である。入力値の範囲は $3 \leq n < 2^{20}$ とし、100 回の平均実行時間を測定した。その結果、16-bit CP の実行時間 6.80×10^{-2} [sec.] が最短で、CP を使用しない場合に比べて 7.53 倍高速になった。

3 設計

提案回路 1 Altera 社の積和演算モジュール (lpm_mult) を用いて k -bit CP ($2 \leq k \leq 10$) を実装した回路 (図 1)。値の下位 k bit に応じて定数 (乗算値: a_i , 加算値: b_i) が選択される。

提案回路 2 提案回路 1 で最も AT 積の良い 5-bit CP をパイプライン化して、スループットを改善した回路。lpm_mult のパラメータである lpm_pipeline を設定することで実現する。パイプラインの段数 x は $2 \leq x \leq 5$ とした。

提案回路 3 定数の乗算を多段の加算器で構成した回路。CP の bit 幅 k は $2 \leq k \leq 4$ とした。

提案回路 4 提案回路 3 で最も AT 積の良い 2-bit CP をパイプライン化した回路。実装を容易にするため加算モジュール (lpm_add) を使用し、そのパラメータ lpm_pipeline を設定することで実現する。パイプラインの段数 x は $2 \leq x \leq 5$ とした。

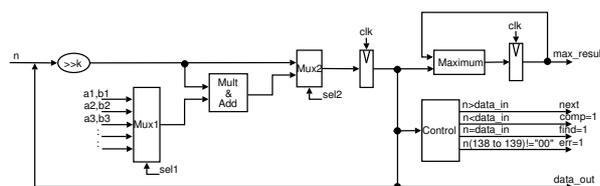


図 1: 提案回路 1 のブロック図

4 評価

Altera 社の Quartus II 4.0 を用いて、提案回路の Analysis & Synthesis, Fitter, Assembler, Timing Analyzer を実行し、回路規模 (LE 数) と動作周波数を見積もった。ターゲットデバイスは Stratix EP1S10F780C7ES とした。各設計のサイクルシミュレータで計算終了までのサイクル数を計り、動作周波数とサイクル数から実行時間を求め、そこから AT 積を算出した。入力値を $3 \leq n < 2^{20}$ としたとき、提案回路 1, 3 の評価結果を図 2 に、提案回路 2, 4 の評価結果を図 3 に示す。

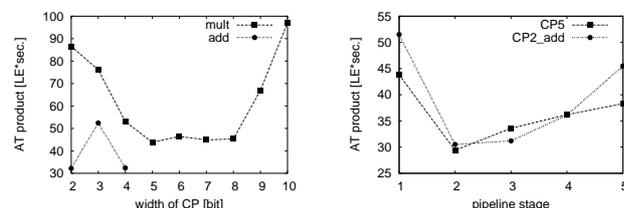


図 2: 提案回路 1, 3 の評価 図 3: 提案回路 2, 4 の評価

提案回路 1 (mult) では CP の bit 幅を 5 bit としたものが最も AT 積が良く、提案回路 2 (CP5) では 2 段にパイプライン化したものが最も AT 積が良い。同様に、提案回路 3 (add) では 2-bit CP としたものが最も AT 積が良く、提案回路 4 (CP2.add) では 2 段にパイプライン化したものが最も AT 積が良い。

5 おわりに

提案回路 2 (パイプライン 2 段) では、AT 積が小林の回路 (1.08×10^2 [LE×sec.]) の約 27% となった。ただし、積和演算器は DSP ブロックを多く消費するため、複数ユニットを 1 つのデバイスに実装することが難しい。これに対し提案回路 4 (パイプライン 2 段) は、AT 積が小林の回路の約 30% となった。この回路の場合、EP1S80F1508C7 (79,040LE) 上に最大 55 ユニット実装できる。このとき $3 \leq n < 2^{20}$ の検証時間は 3.85×10^{-4} [sec.] である。先行研究 [5] のソフトウェアでは、同じ検証を 3.3×10^{-3} [sec.] で実行できるので、1 チップの FPGA で先行研究 [5] よりも 8.57 倍高速な検証が可能と思われる。また、GMP を用いた 16-bit CP よりも約 177 倍高速な検証が可能と思われる。

今後は実チップ上での動作確認を行っていきたい。

参考文献

- [1] R. K. Guy: *Unsolved Problems in Number Theory*, 2nd ed., ch. E16, Springer (1994).
- [2] Eric Roosendaal: "On the $3x + 1$ problem," <http://personal.computrain.nl/eric/wondrous/>.
- [3] S. Ichikawa, N. Kobayashi: "Preliminary Study of Custom Computing Hardware for the $3x+1$ Problem," *Proceedings of IEEE TENCON2004*, Vol. D, pp. 387-390 (2004).
- [4] G. T. Leavens, M. Vermeulen: "3x+1 Search Programs," *Computers Math. Applic.*, Vol. 24, No. 11, pp. 79-99 (1992).
- [5] T. Oliveira e Silva: "Maximum Excursion and Stopping Time Record-Holders for the Problem: Computational Results," *Math. Comput.*, Vol. 68, No. 225, pp. 371-384 (1999).