加法鎖について

On Addition Chains

— Survey and Some New Results —

中村 憲 (一部 バヒグ, M. ハテム と共同研究)
東京都立大学 理学研究科 数学専攻
NAKAMULA, Ken (partly with Bahig, M. Hatem)
Department of Mathematics, Tokyo Metropolitan University

2003年12月1日 (月)

全体の内容と構成

加法鎖の定義・意義・歴史の概観と Scholz 予想に関する新結果.
詳細は [Knu97, § 4.6.3], 及び [BEZN01, BN02] その参考文献.

目的

最短加法鎖の長さ $\ell(n)$ に関する古典的な Scholz 予想

$$\ell\left(2^n - 1\right) \leq n + \ell(n) - 1 \quad (n \in \mathbb{Z}_{>0})$$

が, 次の場合に成立する事を示す.

(i) 理論的に, 二進表示の 1 の個数が 5 以下の n 全てを含む無限族.
(ii) 計算機実験で, 全ての $n \leq 2^{18} = 262144$.

問題の背景, 考察の基本戦略について説明する.
(証明の細部に深くは立ち入らない.)

構成

参考文献

1 定義と問題

2 既知の結果と我々の目標

3 主定理

4 証明の概略

5 結論

参考文献

[AS93] Walter Aiello and M. V. Subbarao. A conjecture in addition chains related to Scholz's conjecture. *Math. Comp.*, Vol. 61, No. 203, pp. 17–23, S1–S6, 1993.

[Bah03] M. Hatem Bahig. *Addition Chains and Efficiency of Cryptosystems*. D.Sc. dissertation, Tokyo Metropolitan University, Tokyo, Japan, 6 March 2003.

[BEZN01] Hatem M. Bahig, Mohamed H. El-Zahar, and Ken Nakamula. Some results for some conjectures in addition chains. In *Combinatorics, computability and logic (Constanţa, 2001)*, Springer Ser. Discrete Math. Theor. Comput. Sci., pp. 47–54, London, July 2001. Springer-Verlag.

[BN02] Hatem M. Bahig and Ken Nakamula. Some properties of

nonstar steps in addition chains and new cases where the Scholz conjecture is true. *J. Algorithms*, Vol. 42, pp. 304–316, 2002. Erratum in [J. Algorithms **47** (2003), no. 1, 60–61].

[Bra39] Alfred Brauer. On addition chains. *Bull. Amer. Math. Soc.*, Vol. 45, pp. 736–739, 1939.

[Han59] Walter Hansen. Zum Scholz-Brauerschen Problem. *J. Reine Angew. Math.*, Vol. 202, pp. 129–136, 1959.

[Knu97] Donald E. Knuth. *The art of computer programming. Vol. 2.* Addison-Wesley Publishing Co., Reading, Mass., third edition, 1997. Seminumerical algorithms, Addison-Wesley Series in Computer Science and Information Processing.

[Sch37] Arnold Scholz. Aufgabe 253. *Jahresbericht der DMV*, Vol. 47, No. 2, pp. 41–42, 1937.

[Thu99] Edward G. Thurber. Efficient generation of minimal length addition chains. *SIAM J. Comput.*, Vol. 28, No. 4, pp. 1247–1263 (electronic), 1999.

1. 定義と問題

加法鎖と冪乗

$n \in \mathbb{Z}_{>0}$ の**長さ** r の**加法鎖**とは $r+1$ 項の数列 $\{a_i\}_{i=0}^{r}$ で

$$1 = a_0 < \cdots < a_r = n$$

を充し, 各 $i = 1, \ldots, r$ に対して, 先行する項 j_i, k_i を

$$a_i = a_{j_i} + a_{k_i} \quad 0 \leq k_i \leq j_i < i$$

となる様に選べるものである.

この時 x^n の計算は

$$x_i = \begin{cases} x & (i = 0), \\ x_{j_i} \times x_{k_i} & (i = 1, \ldots, r), \end{cases}$$

とすれば, 一度計算した x_i $(i = 0, \ldots, r-1)$ は再計算しないで再利用して $x^n = x_r$ と r 回の乗算で求まる.

問題の有用性と困難性

例 1. 素朴な冪乗計算に対応する加法鎖:

$$a_i = a_{i-1} + a_0 = i + 1 \quad (0 < i < n).$$

即ち $j_i = i - 1$, $k_i = 0\,(0 < i < n)$. 長さ $r = n - 1$.

$\lambda(n) = \lfloor \lg n \rfloor$: n の二進表示の桁数 -1.
$\nu(n)$: n の二進表示の 1 の個数.

例 2. 繰返し二倍法, 反復平方法 (1800 B.C., Egypt; 200 B.C., India) に対応する $n = \left(d_{\lambda(n)} \cdots d_0\right)_2$ の加法鎖 (左から右, 右から左もある):

$$b_0 = d_{\lambda(n)} = 1, \quad b_i = \begin{cases} b_{i-1} + b_{i-1} & (2 \nmid i) \\ b_{i-1} + d_{\lambda(n)-(i/2)} & (2 \mid i) \end{cases} \quad (0 < i \leq 2\lambda(n))$$

として, 数列 $\{b_i\}_{i=0}^{2\lambda(n)}$ の重複する項を省いたものを $\{a_i\}_{i=0}^{r}$ とすると, $j_i = i - 1, k_i \in \{i - 1,\, 0\}\,(0 < i \leq r)$. 長さ $r = \lambda(n) + \nu(n) - 1$.

例 3. 積 mn の加法鎖を m, n の加法鎖 $\{a_i\}_{i=0}^{r}$, $\{b_i\}_{i=0}^{s}$ から構成:

$$c_i = a_i \quad (0 < i \leq r) \qquad c_{r+i} = a_r b_i \quad (0 < i \leq s).$$

積 mn の加法鎖 $\{c_i\}_{i=0}^{r+s}$ は長さ $r+s$. 例えば $15 = 3\times 5 = (1111)_2$ の加法鎖は長さ $2+3=5$ で, これは例 2 の $3+4-1=6$ より短い. 例 2 より長い例は $n = 33 = 3\times 11 = (100001)_2$ で $2+5 = 7 > 6 = 5+2-1$.

例 4. 一般の $p \in \mathbb{Z}_{>2}$ でも反復 p 乗法に対応する $n = (d_t \cdots d_0)_p$ の加法鎖がある. 例えば $p=5$ の加法鎖 1, 2, 3, 5 を利用して $23 = (43)_5 = (10111)_2$ の加法鎖 1, 2, 3, 5, 10, 20, 23 が長さ 6 で構成でき, これは例 2 の $4+4-1=7$ より短い. 別の 23 の加法鎖 1, 2, 3, 5, 10, 13, 23 も長さ 6 である.

与えられた n の最短加法鎖を構成する問題は, 加法鎖の場合分けが n が増大するとともに急激に巨大になり, 一般には計算可能な問題の族の中では極めて困難な NP 完全という族に属すると予想されている.

最短加法鎖と一意的構成

なるべく長さ r の小さい加法鎖の構成に取組む事が大切である.

ギャップが大きいステップには, 例えば $a_{i-1}+2 \leq a_i$ なら $a_{i-1} < a_{i-1}+a_0 = a_{i-1}+1 < a_i$ と余分な項 $a_{i-1}+a_0$ を挿入できるが, それは事後未使用で済み r を増すだけなので, 以下, 選んだ先行する項は無駄が無いとする, 即ち $a_i = a_{j_i} + a_{k_i}$, $0 \leq k_i \leq j_i < i \leq r$ に於て

$$\{j_1, \ldots, j_r, k_1, \ldots, k_r\} = \{0, \ldots, r-1\}.$$

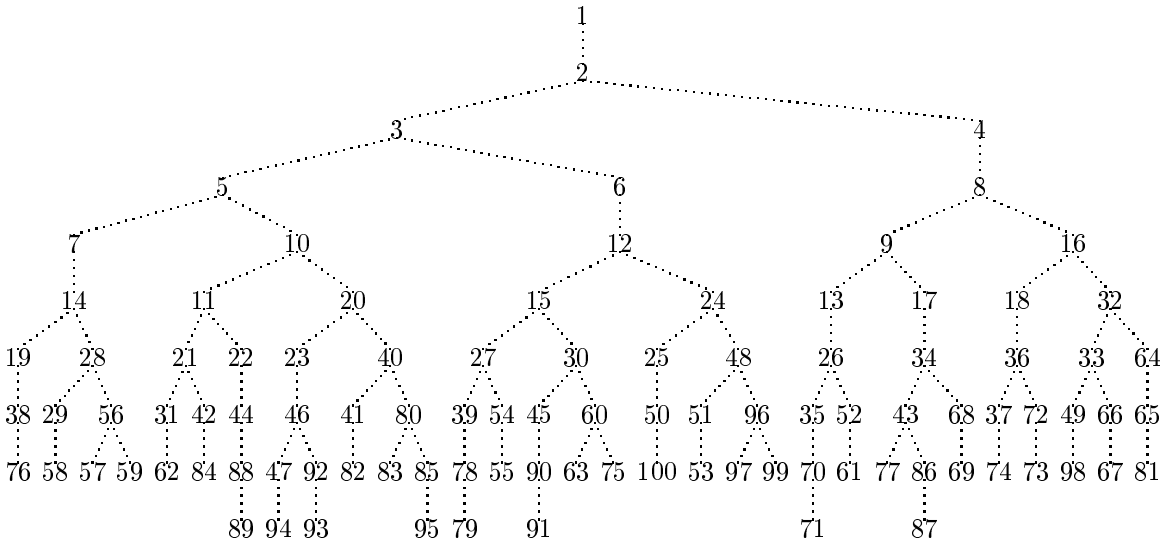
最短加法鎖にも, 例えば

$$\begin{cases} 1<2<3<5 \\ 1<2<4<5 \end{cases} \qquad \begin{cases} 1<2<3<4=3+1<7 \\ 1<2<3<4=2+2<7 \end{cases}$$

の様な異る構成法があるが, これは冪乗計算の効率からみれば今後検討の価値があるかもしれないが, ここでは構成法の一意性は考慮しない.

最短加法鎖の木

各ノードに与えられた $n = 1, \ldots, 100$ に対する $\ell(n)$ の値は, そのノードの深さである. 但し $n > 100$ でも, これより $\ell(n)$ が小さいものもあるが書いてない.



スター鎖と ℓ° 鎖

加法鎖のステップ i, $0 < i \leq r$ について:

ダブル: $j_i = k_i = i - 1$ (選び方は一意的).
スター: $j_i = i - 1$ となる様に選べる.

ダブルステップはスターステップである.

スター鎖: 加法鎖で全てのステップがスター.
ℓ° **鎖**: 加法鎖で $\emptyset \neq \exists H \subseteq \{0, 1, \ldots, r-1\}$ s.t.

$$\max\{t \in H \mid t < i\} \in \{j_i, k_i\} \quad (0 < i \leq r).$$

スター鎖は $H = \{0, 1, \ldots, r-1\}$ とした ℓ° 鎖である.

$\ell^*(n)$: n の最短スター鎖の長さ.
$\ell^\circ(n)$: n の最短 ℓ° 鎖の長さ.
$\ell(n)$: n の最短加法鎖の長さ.

簡単な性質と幾つかの予想

例 2 と定義から容易に,

$$\lambda(n) \leq \ell(n) \leq \ell^{\circ}(n) \leq \ell^{*}(n) \leq \lambda(n) + \nu(n) - 1 \leq 2\lambda(n). \qquad (1)$$

例 2 では $2^n - 1$ の加法鎖は効率悪く, 長さ $2\lambda(2^n - 1) = 2n - 2$.

予想 1 (Schloz [Sch37], 1937). もし $n \in \mathbb{Z}_{>0}$ なら常に

$$\ell(2^n - 1) \leq n + \ell(n) - 1.$$

予想 2 (Hansen [Han59], 1959). もし $n \in \mathbb{Z}_{>0}$ なら常に

$$\ell(n) = \ell^{\circ}(n).$$

予想 3 (Aiello-Subarao [AS93], 1993). もし $n \in \mathbb{Z}_{>0}$ なら常に $2^n - 1$ の加法鎖で長さ $n + \ell(n) - 1$ となるものが存在する.

予想 1 は, 無駄が無い加法鎖を考えているので, 予想 3 より少し弱い.

2. 既知の結果と我々の目標

既知の結果

$$\ell(n) \leq \ell^{\circ}(n) \leq \ell^{*}(n) \leq \lambda(n) + \nu(n) - 1. \qquad (1) \text{ 再録}$$

● [Bra39] $\ell^{*}(2^n - 1) \leq n + \ell^{*}(n) - 1$ より $\ell(n) = \ell^{*}(n) \implies$ 予想 1.
● [Knu97] しかし $\ell(n) = \ell^{*}(n)$ の反例は, 最小 $n = 12509$ 他多く存在.

● [Han59] $2^n - 1$ の加法鎖で長さ $n + \ell^{\circ}(n) - 1$ となるものが存在.
●特に, 予想 2 $\implies$ 予想 3 $\implies$ 予想 1.
●勿論これ迄の上の反例では $\ell(n) = \ell^{\circ}(n) < \ell^{*}(n)$ (予想 2).

● [Knu97] $n < 18269$ なら予想 2 成立.

● [AS93] $\nu(n) < 5$ なら予想 2 成立.

作戦

難関は n の全最短加法鎖が次の何れかの形のステップを含む場合:

- 非スターステップ $i \leq \ell(n)$ で, どう先行する項を選んでも
$$j_i < i - 2. \tag{2}$$
- 非スターステップ $i-1, i \leq \ell(n)$ で, 先行する項の選び方が一意的に決り
$$j_{i-1} = i - 3, \quad j_i = i - 2, k_i \neq i - 3. \tag{3}$$

ℓ' **鎖**: 加法鎖で式 (2) や式 (3) のステップを含まない.
$\ell'(n)$: n の最短 ℓ' 鎖の長さ.

すると ℓ^* 鎖 $\Longrightarrow$ ℓ' 鎖 $\Longrightarrow$ ℓ° 鎖が比較的容易に示され,

$$\ell(n) \leq \ell^\circ(n) \leq \ell'(n) \leq \ell^*(n) \leq \lambda(n) + \nu(n) - 1. \qquad (1) \text{ 再録}$$

●各 n の或最短加法鎖 ℓ' 鎖になる事を確認できれば $\ell(n) = \ell'(n)$.
●式 (2), (3) を集中攻撃し $\ell(n) = \ell^\circ(n)$ (予想 2) かどうか追求する.

3. 主定理

数値実験

アルゴリズムを改良して, 計算機実験により n の最短加法鎖を生成し, それが ℓ' 鎖になる事を確認する.

定理 1 ([BEZN01], [Bah03]). もし

$$0 < n \leq 2^{18} = 262144$$

ならば, 必ず n の最短加法鎖の中に ℓ' 鎖が存在する.

これにより確認された事実から

予想 4 ([BEZN01], 2001). もし $n \in \mathbb{Z}_{>0}$ なら常に

$$\ell(n) = \ell^{\circ}(n) = \ell'(n).$$

を提出する. 当然これは予想 2 より強い.

理論的結果

最短加法鎖が (2) や (3) のステップを含む可能性を考察し, その時に最短加法鎖で ℓ° 鎖となるものを構成する.

定理 2 ([BN02]). もし

$$5 \le \nu(n) \le 8, \quad \ell(n) = \lambda(n) + 3 \tag{4}$$

ならば, 非 ℓ' 鎖となる n の最短加法鎖が存在する場合は, 必ず ℓ° 鎖となる n の別の最短加法鎖が存在し, 予想 2 が正しい.

●もし $\ell(n) < \ell^*(n)$ なら (1) と [Knu97, § 4.6.3, Theorem C] により

$$\nu(n) = 5 \ \Rightarrow \ \lambda(n) + 3 \le \ell(n) < \ell^*(n) \le \lambda(n) + 4 \ \Rightarrow \ \ell(n) = \lambda(n) + 3$$

なので, 予想 2 が $\nu(n) \le 5$ の全ての場合に確認された.

●予想 4 は, 理論的には (4) の下でも部分的にしか確認されていない.

全最短加法鎖の探索

アルゴリズムの改良には以下の命題を利用する必要がある:

命題 1. 次の各場合に $i \leq \ell(n)$ は n の最短加法鎖のスターステップ:

(i) $i = \ell(n)$.
(ii) $i-1$ がダブル.
(iii) $i-2, i-1$ がスターで $k_{i-1} = i-3$.

命題 2. もし $i < \ell(n)$ が n の最短加法鎖の非スターステップならば

$$2 \leq k_i, \quad i - (\ell(n) - \lambda(n)) \leq j_i.$$

- これを n の最短加法鎖全てを生成する既存アルゴリズム [Thu99] に適用して, 範囲 $2^7 \leq n < 2^{16}$ で平均して 25 – 40 % の効率化ができた.
- 特に $n \leq 2^{18}$ の最短加法鎖を一個生成する計算に用いて, それが全て ℓ' 鎖である事を確認した.

非スターステップの性質

非 l' 鎖の考察には以下の命題を利用する必要がある:

命題 3. 加法鎖の先行する項の選び方に関して

$$0 \leq \lambda(a_i) - \lambda(a_{j_i}) \leq 1$$

これにより, スターステップのみならず, 非スターステップ i でも増加列 $a_{j_i} < \cdots < a_i$ に於て二進表示の桁数は高々 1 しか増えない.

命題 4. 非スターステップ i に対して, 全ての $j_i + 1, \ldots, i$ は非ダブルステップである.

これにより, 非スターステップ i では $k_s < j_s \, (j_i < s \leq r)$ である.

命題 3, 4 は, 命題 1, 2 の様に最短加法鎖という制限はなく, 任意の加法鎖のステップについて成立している.

4. 証明の概略

条件 (4) $5 \le \nu(n) \le 8$, $\ell(n) = \lambda(n) + 3$ の下での場合分け
一般に $0 < i \le r$ なら $0 \le \lambda(a_i) - \lambda(a_{i-1}) \le 1$ だから, 二進表示桁数非増加ステップ数は $S(a_i) := \sharp\{t \le i \mid \lambda(a_t) = \lambda(a_{t-1})\} = i - \lambda(a_i)$.

以下 $i < \ell(n)$ を n の最短加法鎖の非スターステップとする.

命題 2 より $j_i \in \{i-2, i-3\}$.

Case $j_i = i - 3$ よって (2) の形.

命題 3 より $3 = S(a_{\ell(n)}) \ge S(a_i) \ge S(a_{i-3})+2$ だから $S(a_{i-3}) \in \{0, 1\}$.

命題 4 よりステップ $i-2, i-1$ の場合分けは四つ:

(I) $i-2, i-1$ は非スター;

(II) $i-2$ は非スター, $i-1$ はスターで非ダブル;

(III) $i-2$ はスターで非ダブル $i-1$ は非スター;

(IV) $i-2, i-1$ はスターで非ダブル.

Case $j_i = i - 2$ よって (3) の形.

命題 3 と, ちょっとした補題より $S(a_{i-3}) \in \{1, 2\}$.

各々の場合

定理 3. 条件 (4) の下で (2) の形の非スターステップを含む n の最短加法鎖は (I), (II), (III) の場合は存在しない.

定理 4. 条件 (4) の下で (2) の形の非スターステップ i を含む n の最短加法鎖が (IV) の場合に存在したとする. この時 $S(a_{i-3}) = 1$ であり, また長さ $\ell(n)$ である n の ℓ° 鎖が構成できる.

同様の, より簡単な議論により

定理 5. 条件 (4) の下で (3) の形の非スターステップ $i-1, i$ を含む n の最短加法鎖が存在したとする. この時 $S(a_{i-2}) = 2$ であり, また長さ $\ell(n)$ である n の ℓ° 鎖が構成できる.

●これにより $j_i = i-3$, $S(a_{i-3}) = 1$ で, しかも $i-2, i-1$ がスターで非ダブルの場合, 及び $j_{i-1} = i-3$, $j_i = i-2$, $k_i \neq i-3$, $S(a_{i-3}) = 2$ の場合を除けば, 予想 4 が条件 (4) の下で証明された事になる.

5. 結論

- 加法鎖の定義, 応用, 構成法, 実例, ℓ^* 鎖, ℓ° 鎖の紹介.
- 予想 $\ell(2^n-1) \le n + \ell(n) - 1$ と強い予想 $\ell(n) = \ell^\circ(n)$ の紹介.
- 予想 $\ell(n) = \ell^\circ(n)$ の $n \le 2^{18}$ に対する ℓ' 鎖の導入による検証と, 更に強い予想 $\ell(n) = \ell^\circ(n) = \ell'(n)$ の提案.
- 特に $5 \le \nu(n) \le 8, \quad \ell(n) = \lambda(n) + 3$ の場合に, 予想 $\ell(n) = \ell^\circ(n)$ の証明, 及び予想 $\ell(n) = \ell^\circ(n) = \ell'(n)$ の部分的証明.

問題

- 予想 $\ell(n) = \ell^\circ(n) = \ell'(n)$ の証明.
- この方法では数値的にも理論的にも限界に近いと思われる. 新手法の開発が必要.