关于加法链的 Scholz 猜想在$n = 2^m(23) + 7, m \in \mathbb{N}^*$时成立

Amadou TALL[1]

达喀尔谢赫·安塔·迪奥普大学数学与计算机科学系
amadou7.tall@ucad.edu.sn

arXiv:2302.02143v1 [math.NT] 4 Feb 2023

摘要。关于加法链的 Scholz 猜想指出，对于所有整数 n， $\ell(2^n - 1) \leq \ell(n) + n - 1$ 成立，其中 $\ell(n)$表示整数 n的所有加法链中的最小长度。已证明该猜想对无穷多个整数成立。本文将证明，该猜想对 $n = 2^m(23) + 7$也成立。这是 Thurber [8] 给出的第一组整数，用以证明存在无穷多个整数满足 $\ell(2n) = \ell(n)$。后来，Thurber [4] 又给出了具有相同性质的第二组整数（$n = 2^{2m+k+7} + 2^{2m+k+5} + 2^{m+k+4} + 2^{m+k+3} + 2^{m+2} + 2^{m+1} + 1$）。我们也将证明该猜想对这些整数成立。

关键词：加法链、Scholz-Bauer猜想、最小长度、因子法

引言

幂运算是数学中的一项关键运算。它通常被视为若干次乘法。设 x 为一个整数，对于给定的 n，求出 x^n 似乎很容易。我们需要进行 n 次乘法。但如果 n 变得非常大呢？幂运算在密码学等许多领域都是一项非常重要的运算。已知最快速进行幂运算的最佳工具是加法链。

定义 1. 对于整数 n，其加法链是一个集合 $\mathcal{C} = \{a_0 = 1, a_1, a_2, \ldots, a_r\}$，满足最后一个元素 a_r 为 n，且每个元素 a_k 都是两个前面元素 a_i 和 a_j之和。整数 r 是该链的长度，记作 $\ell(c)$。

容易看出，同一个整数 n可以有许多长度不同的加法链；求出 n 的所有加法链的最小长度（记作 $\ell(n)$）是一个 NP完全问题。举例来说，可以认为，达到 $2n$ 最快的方法是先达到 n，再将其加倍，这意味着 $\ell(2n) = \ell(n) + 1$。已证明，有无穷多个整数不符合这一规律。我们有 $\ell(382) = \ell(191) = 11$。关于加法链，最著名的猜想为二进制展开中仅含“1”的整数（对于某个 a，$n = 2^a - 1$）的加法链长度给出了一个上界。

猜想 2. Scholz 加法链猜想指出：

$$\ell(2^n - 1) \leq \ell(n) + n - 1, \ \forall n \in \mathbb{N}$$

经过数十年的研究，该猜想已被证明对 $n < 5784689$成立。它已被证明对若干整数集合成立。我们知道，如果它对 n成立，且 $\ell(2n) = \ell(n) + 1$，那么它对 $2n$也成立。我们想知道，当 $\ell(2n) = \ell(n)$时，该猜想是否成立。一般情形目前尚无答案。

在本文中，我们将研究这两种情形 es.

1. 我们将给出一个非常简单的证明：如果猜想对 n成立，且 $\ell(2n) = \ell(n)+1$，那么它对 $2n$也成立。2. 我们还将证明，该猜想对整数 $n = 2^m(23) + 7$ 成立；据悉，这些整数属于最早验证 $\ell(2n) = \ell(n)$的无限整数集合之一。

Thurber 的主要结果是 [8]

定理 3. 设 m 是一个大于 5 的整数。那么

$$\ell(2^m(23) + 7) = m + 8 = \ell(2 \times (2^m(23) + 7))$$

我们回顾一下因子法，这是一种基于 n 和 m 的链来构造乘积 nm 的链的方法。

定义4. 设 c_1 和 c_2 分别是 n_1 和 n_2 的加法链。那么， $c_1 \times c_2$ 是 $n_1 \times n_2$ 的加法链，其长度为 $\ell(c_1) + \ell(c_2)$，其中 $\times$ 定义如下:

若 $c_1 = \{a_0,\ a_1,\ \ldots,\ a_r\}$ 和 $c_2 = \{b_0,\ b_1,\ \ldots,\ b_l\}$，则

$$c_1 \times c_2 = \{a_0,\ a_1,\ \ldots,\ a_r,\ a_r \times b_1,\ a_r \times b_2,\ \times,\ a_r \times b_l\}.$$

长　　度是新链中各链长度之和，即 $\ell(mn) \leq \ell(n)+\ell(m)$。

1 我们的贡献

定理5. 设 n 是满足 $\ell(2n) = \ell(n)+1$的正整数。若 Scholz 猜想对n成立，则对 $2n$也成立。

证明. 设 n 是满足 $\ell(2n) = \ell(n) + 1$ 且 $\ell(2^n - 1) \leq \ell(n) + n - 1$的正整数。设$n_0 = 2n$ 是另一个正整数，我们有

$$2^{n_0} - 1 = (2^n - 1)(2^n + 1),$$

利用因子法，我们可以推出一个长度为 的 $2^{n_0} - 1$ 链

$$\ell(n) + n - 1 + n + 1 = \ell(n) + 2n = \ell(n_0) + n_0 - 1.$$

定理6. 对所有形如 $U_m = 2^m(23) + 7$的整数，Scholz 猜想均成立。

将通过对 m进行归纳法证明

证明. 1. 由计算结果可知，Scholz 猜想对 U_m, $m \in \{1, 2, 3, 4, 5\}$成立。2. 一个长度为 $m + 7$ 的链（其中 $X_m + 3$ （满足 $X_m = 2^m(23)$））可如下构造

$$\mathcal{C}_{\mathcal{X}_{\Updownarrow}} = \{1, 2, 3, 5, 10, 20, 23, 2 \times 23, \cdots, 2^m \times 23, 2^m \times 23 + 3\}$$

3. 我们知道

$$U_{m+1} = 2^{m+1}(23) + 7$$

so,

$$X_m = U_m - 7 = \frac{U_{m+1} - 1}{2} - 3$$

这会导出

$$\begin{aligned} 2^{U_{m+1}} - 1 &= 2^{2(X_m+3)+1} - 1 \\ &= 2(2^{2(X_m+3)} - 1) + 1 \\ &= 2(2^{X_m+3} - 1)(2^{X_m+3} + 1) + 1 \end{aligned}$$

From 由（$2^{X_m+3} - 1$）构成的链，并使用因子法，随后我们可以推导出一条链，适用于 $2^{U_{m+1}} - 1$，长度为

$$\begin{aligned} X_m + 3 + 1 + 1 + 1 + \ell(2^{X_m+3} - 1) &= X_m + 6 + \ell(X_m + 3) + X_m + 3 - 1 \\ &= 2X_m + 8 + m \\ &= (2x_m + 7) + (m + 9) - 1 \\ &= U_{m+1} + \ell(U_{m+1}) - 1 \end{aligned}$$

两年后，Thurber 也指出

定理 7. 对每个 $m \geq 1$，具有 $v(n) = 7$ 且 n 为二进制形式 n =$101\cdots m\cdots 11\cdots k\cdots 11\cdots m\cdots 1$（其中 $k \geq 3$）的整数集合，是一个无限整数类，其中 $\ell(2n) = \ell(n)$。

He 证明 $\ell(n) = \lambda(n) + 4$。我们还将证明，Scholz 猜想对这类 n 成立。

定理 8. 加法链上的 Scholz 猜想对 $n = 2^{2m+k+7} + 2^{2m+k+5} + 2^{m+k+4} + 2^{m+k+3} + 2^{m+2} + 2^{m+1} + 1$ 成立。

证明。我们改写

$$\begin{aligned} n &= 2^{2m+k+7} + 2^{2m+k+5} + 2^{m+k+4} + 2^{m+k+3} + 2^{m+2} + 2^{m+1} + 1 \\ &= 2^{m+k+3}(2^{m+4} + 2 + 2^{m+2} + 1) + (2^{m+2} + 1 + 2^{m+1}) \\ &= 2^{m+k+3}(2(2^{m+3} + 1) + (2^{m+2} + 1)) + (2^{m+2} + 1) + 2^{m+1} \end{aligned}$$

n 的最短链为

$$\begin{aligned} \rfloor = \{&1, 2, \ldots, 2^{m+1}, 2^{m+2}, 2^{m+2} + 1, 2^{m+3} + 1, 2^{m+1} + (2^{m+2} + 1) = \beta, \\ &2(2^{m+3} + 1), 2(2^{m+3} + 1) + (2^{m+2} + 1) = \alpha, \\ &2\alpha, 2^2\alpha, \ldots, 2^{m+k+3}\alpha, n = 2^{m+k+3}\alpha + \beta\}. \end{aligned}$$

其长度为

$$m + 2 + 1 + 1 + 1 + 1 + 1 + m + k + 3 + 1 = 2m + k + 11 = \lambda(n) + 4.$$

使用以下规则：

1. 若 $A = 2B$，则在 $2^B - 1$ 的链上增加 $B + 1$ 步，即可得到 $2^A - 1 = (2^B - 1)(2^B + 1)$ 的链。
2. 若 $A = B + 1$，则我们将增加两步（$2^A - 1 = 2(2^B - 1) + 1$）3. $2^{m+3} + 1 = 2^{m+2} + 2^{m+2} + 1$，因此

$$2^{2^{m+3}+1} - 1 = 2^{2^{m+2}}(2^{2^{m+2}+1} - 1) + (2^{2^{m+2}} + 1)$$

4. $2^{m+2} + 2^{m+1} + 1 = (2^{m+2} + 1) + 2^{m+1}$，因此

$$2^{2^{m+2}+2^{m+1}+1} - 1 = 2^{2^{m+1}}(2^{2^{m+2}+1} - 1) + (2^{2^{m+1}} - 1)$$

于是，我们可以为 $2^n - 1$ 构造一条长度为 $\mathcal{C}$ 的链

值	step	额外步骤	注释
1	DBL		
2	DBL		
$\ldots$	DBL		
2^{m+1}	DBL		
2^{m+2}	DBL	$2^{m+2} + m + 2 - 1$	
$2^{m+2} + 1$	$+1$	2	
$2^{m+3} + 1$	$+2^{m+2}$	$2^{m+2} + 1$	
$2^{m+2} + 2^{m+1} + 1 = \beta$	2^{m+1}	1	$2^{2^{m+1}}(2^{2^{m+2}+1} - 1) \in \mathcal{C}$
$2(2^{m+3} + 1)$	DBL	$2^{m+3} + 1 + 1$	
$2(2^{m+3} + 1) + (2^{m+2} + 1) = \alpha$	$+2^{m+2} + 1$	$2^{m+2} + 1 + 1$	
2α	DBL	$\alpha + 1$	
$2^2\alpha$	DBL	$2\alpha + 1$	
$\ldots$	DBL	$\ldots$	
$2^{m+k+3}\alpha$	DBL	$2^{m+k+3}\alpha + 1$	
$n = 2^{m+k+3}\alpha + \beta$	$+\beta$	$\beta + 1$	
总计	4 个小步		$\ell(n) + n - 1 =$

$$\begin{aligned} \ell &= 2^{m+2} + m + 2 - 1 + 2 + 2^{m+2} + 1 + 2 + 2^{m+3} + \\ &+ 1 + 1 + 2^{m+2} + 1 + 1 + (m + k + 3) + \alpha(2^{m+k+3} - 1) + \beta = 2m + k + 13 + 2^{m+4} + 2^{m+2} + (\\ &2^{m+4} + 2^{m+2} + 2 + 1)(2^{m+k+3} - 1) + 2^{m+2} + 2^{m+1} + 1 \\ &= 2m + k + 14 + 2^{m+4} + 2^{m+3} + 2^{m+1} + 2^{2m+k+7} + 2^{2m+k+5}2^{m+k+4} + 2^{m+k+3} - 2^{m+4} - 2^{m+2} - 2 - 1 \\ &= (2m + k + 11) + (2^{2m+k+7} + 2^{2m+k+5}2^{m+k+4} + 2^{m+k+3} + 2^{m+2} + 2^{m+1}) = \ell(n) + n - 1. \end{aligned}$$

结论

我们不知道 Scholz 猜想是否对所有满足 $\ell(2n) = \ell(n)$ 的整数都成立。研究 $\ell(2n) < \ell(n)$ 的情况肯定更加困难。

致谢

Th作者谨向 IHES 致谢。该工作是在其访问学者奖学金期间完成的。

参考文献

1. D.E. Knuth, *The Art of Computer Programming*, 第 2 卷（Addison-Wesley，马萨诸塞州雷丁，1969）398-422。2. Tall Amadou, *A generalization of Lucas addition chains*, Bulletin Math´ematique de la Roumanie, 第 55 卷（103）（1）（2012）79 - 93。3. Maurice Mignotte, Amadou Tall, *A note on addition chains.* 5,《国际代数杂志》, 第 274 卷。4. Thurber, Edward G., *The Scholz-Brauer problem on addition chains*,《太平洋数学杂志》, 第 49 卷第 1 期, 1973 年, 第 229-242 页。5. Sch¨ *A Lower Bound for the Length of Addition Chains* 1 onhage, A.,《理论计算机科学》, 第 页。6. A. T. Brauer, *On addition chains*,《美国数学会通报》45（1939）, 736-739。7. W. R. Utz, *A note on the Scholz-Brauer problem in addition chains*,《美国数学会会刊》4（1953）, 462-463。8. Thurber, Edward G., *On additions chains and solutions of* $\ell(2n) = \ell(n)$ *and* $\ell(2^n - 1) = \ell(n) + n - 1$,《离散数学》16（1976）279-289。9. Cliff, N., *Calculating optimal addition chains*,《计算》2011, 265-284。