ON TERNARY ADDITION CHAINS

TAKAHIRO HAYATA AND MASAYA WAGATUMA

1. Introduction

In this paper we introduce a notion of p-addition chains for $p \geq 2$. It is a straightforward generalization of usual addition chains (we call them as *binary* addition chains). The main requirement for the p-chain of n is that the every term should be the sums of p former terms. The most of the notions for binary addition chains have corresponding p-chain version, such as small steps, star steps, $\nu(n)$, $\lambda(n)$, etc. Statements and properties about binary addition chains also have anologous generalization. Some statements are simplifed when generalizing to p. Others get involved. We are going to show two of them: to show pruning bounds discussed in [H], and to announce results about chains with a small step in [W].

Firstly we explain pruning bounds. The backtracking algorithm to find minimal chains explained in [T] works also for p-chains with no modification. To speed up the algorithm we need pruning bounds. Theorems 3.5, 3.6 are our main result. These clarify pruning bounds for general p-chains. In §4, we show some numerical examples when $p = 3$ by using this algorithm.

Secondly, we investigate chains with small steps. Unlike $p = 2$, things get involved in this point; we should take care of digits not necessarily 0, 1.

In §5, we discuss the length of chains of n with few standing bits. In general if the top digit of n appears not to be 1, it requires additional treatment. If $p = 3$, classification result for chains with only one small step claims the length of 3-chains of integers with two and three standing bits [W]. Unlike $p = 2$, this classification results obtained needs pages to describe and is not easy to verify. We hope to prove the statement for the length of n with $\nu_3(n) = 3$ without classification.

2. addition chains with base number p

Let $(S, +)$ be a commutative semi-group and p be a positive integer. Choose S_0 as a subset of S as an *initial set*. For given $n \in S$, the sequence $\{a_1, a_2, \ldots, a_r\}$ of S is called *an addition chain of n with base number p and initial set* S_0 or shortly (p, S_0)*-chain of n*, when

Date: Apr. 20, 2006.

(a) $a_r = n$
(b) For any $1 \leq j \leq r$, a_j is expressed as the sum of p former terms, *i.e.*, $a_j = a_{i_1} + a_{i_2} + \cdots + a_{i_p}$ with $j > i_1 \geq i_2 \geq \cdots \geq i_p \geq 0$. If $i_k = 0$, we understand that a_0 would be any element of S_0.

Typically a_1 is understood as an element of $S_0 + S_0 + \cdots + S_0$ (p times). If $\{a_k\}$ is a (p, S_0)-chain of n, r is called its (p, S_0)-*length*. The (p, S_0)-length of n is the minimal length of p-chains and is denoted by $\ell_{p,S_0}(n)$. We note that $\ell_{p,S_0}(n)$ could be infinity. The addition chain in usual sense is obtained by $p = 2$, $S = \mathbb{Z}$ (the set of integers) and $S_0 = \{0, 1\}$.

In this paper, we concentrate on the case $S = \mathbb{Z}$ and $S_0 = \{0, 1\}$. For simplicity, we omit S_0 from the notation, *i.e.*, p-chain, $\ell_p(n)$, *etc* and understand $a_{-\infty} = 0$, $a_0 = 1$. Because we are interested in $\ell_p(n)$, we always assume that the p-chain is strictly increasing.

If $i_1 = i_2 = \cdots = i_k = j - 1$, the step a_j is called *k-star step*. 1-star step is simply called star step. On the other hand, if $k = p$ we call them as *full step*. Doubling (resp. tripling) are just the full step for $p = 2$ (resp. $p = 3$). A chain consisting of the (k-)star steps is called a *(k−)star p-chain*. We denote by $\ell_p^*(n)$ the minimal length of star p-chains.

The basic functions $\lambda_p(n)$, $\nu_p(n)$ for addition chains can be imported directly;

$$\lambda_p(n) = \lfloor \log_p(n) \rfloor$$
$$\nu_p(n) = \text{the number of non zero entries in } p\text{-ary expression of } n$$

where $\lfloor x \rfloor$ means the biggest integer which does not exceed x. Considering p-adic "power multiplication method", it is not difficult to find this 1-st stage evaluation of the length

$$\lceil \log_p(n) \rceil \leq \ell_p(n) \leq \lambda_p(n) + \nu_p(n) - \delta_p(n), \tag{1}$$

where $\lceil x \rceil$ denotes the smallest integer no less than x and $\delta_p(n) = 1$ if $\lfloor n/p^{\lambda_p(n)} \rfloor = 1$, $\delta_p(n) = 0$ otherwise.

3. Pruning bounds

Because we are interested in $\ell_p(n)$ we need an algorithm to calculate a minimal p-chain of n. The backtracking algorithm described in [T, §4] works well with no modification for this generalization. To speed up the algorithm in practical sense we need better pruning bounds. The idea to calculate pruning bounds in [T, §§5–7] works exactly the same way, even simpler for general p-chain case.

3.1. **Class 1 bounds.** Let us start with class 1 pruning bounds. Since the full step is the biggest step, we have

$$a_j \leq p a_{j-1} \quad (j > 0) \qquad (\textbf{elementary inequality}).$$

It implies that the lower bound for a_j would be $\lceil n/p^{r-j} \rceil$. The next proposition shows there is some improvement.

Proposition 3.1. *Suppose that $\{a_j\}_{j=1}^r$ be a p-chain of $n = a_r$. Assume $p \nmid n$. Then it holds*

$$a_{r-1} \geq \left\lceil \frac{n}{p} \right\rceil \tag{2}$$

$$a_{r-k} \geq \left\lceil \frac{n}{(p^2 - p + 1)p^{k-2}} \right\rceil \quad (2 \leq k \leq r). \tag{3}$$

Proof. (2) is clear. Let $r \geq 3$. Since $p \nmid n$, a_r is not a full step. We have

$$n \leq (p-1)a_{r-1} + a_{r-2} \leq (p-1)pa_{r-2} + a_{r-2},$$

which shows (3) when $k = 2$. Now (3) for $k > 2$ is clear by the elementary inequality. □

We say e is the *p-exponent of n* when e be a nonnegative integer such that $n = p^e m$ with $p \nmid m$. The general form of class 1 bound is found straightforwardly.

Theorem 3.2. *Suppose that $\{a_j\}_{j=1}^r$ be a p-chain of $n = a_r$. Let e be the p-exponent of n. Then it holds*

$$a_j \geq \left\lceil \frac{n}{p^{r-j}} \right\rceil \qquad (r - e - 1 \leq j \leq r) \tag{4}$$

$$a_j \geq \left\lceil \frac{n}{(p^2 - p + 1)p^{r-2-j}} \right\rceil \qquad (0 \leq j \leq r - e - 2). \tag{5}$$

Proof. Because (4) is clear, assume $0 \leq j \leq r - e - 2$. By the assumption of the theorem, there exists a non full step between a_{r-e} and a_r, say a_s. We have

$$a_s \leq (p-1)a_{s-1} + a_{s-2} \leq (p(p-1)+1)a_{s-2} \leq (p^2 - p + 1)p^{s-2-j}a_j.$$

On the other hand, one has $n \leq p^{r-s}a_s$. These inequalities indicate (5). □

3.2. **Class 2 bounds.** Class 2 bounds are inequalities between succeeding two terms a_j and a_{j-1} under the existence of non full step. We already have a class-2-bound candidate, so to speak, by adding class 1 bounds

$$(p-1)a_j + a_{j-1} \geq \begin{cases} \left(1 - \dfrac{1}{p} + \dfrac{1}{p^2}\right)\dfrac{n}{p^{r-j-1}}, & (r - e \leq j \leq r); \\ \left(1 - \dfrac{(p-1)^2}{p(p^2-p+1)}\right)\dfrac{n}{p^e}, & (j = r - e - 1); \\ \dfrac{n}{p^{r-j-1}}, & (1 \leq j \leq r - e - 2). \end{cases} \tag{6}$$

The aim of this section is to achieve some improvement.

Before stepping into the class 2 pruning bounds, we prepare the next lemma, which will be used in the proof of Theorem repeatedly.

Lemma 3.3. *Let $\{a_j\}_{j=1}^r$ be a p-chain of $n = a_r$. Suppose that it holds for $3 \leq j_0 \leq r$,*

$$(p-1)a_{j_0-2} + a_{j_0-3} < \frac{n}{(p^2-1)p^{r-j_0-1}}. \tag{7}$$

Assume there is a non full step a_s between $j_0 \leq s \leq r$. Then the following inequalities hold

$$a_s > p^{s-j_0-1}(p^2-1)((p-1)a_{j_0-2} + a_{j_0-3}) \tag{8}$$

$$a_s > p^{s-j_0-2}(p^4-p^3+p-1)a_{j_0-2}. \tag{9}$$

Proof. If (9) does not hold, one sees

$$\begin{aligned} a_s &\leq p^{s-j_0-2} \cdot (p^4-p^3+p-1)a_{j_0-2} \\ &\leq p^{s-j_0-2} \cdot ((p^4-p^3+p-1-(p^2-1))a_{j_0-2} + p(p^2-1)a_{j_0-3}) \\ &= p^{s-j_0-1} \cdot (p^2-1)((p-1)a_{j_0-2} + a_{j_0-3}). \end{aligned} \tag{10}$$

By the assumption, (10) implies $a_s < p^{s-r}n$, which contradicts to the elementary inequality. The right hand side of (8) is found in the proof, thus shown already. □

The next lemma describes which kind of restriction the inequality (7) actually gives.

Lemma 3.4. *Under the assumption* (7)*,*

(a) All steps a_s for $j_0 \leq s \leq r$ should be at least $(p-1)$-star steps.
(b) If $p \geq 3$, at most one step between j_0 and r can be a non full step.

Proof. Put $a_s = a_{s_1} + a_{s_2} + \cdots + a_{s_p}$ $(s_1 \geq \cdots \geq s_p)$. Assume that $s-2 \geq s_{p-1} \geq s_p$. Then

$$a_s \leq (p-2)a_{s-1} + 2a_{s-2} \leq (p^2-2p+2)a_{s-2} \leq p^{s-j_0}(p^2-2p+2)a_{j_0-2}.$$

The inequality $p^2(p^2-2p+2) < p^4-p^3+p-1$ for $p = 2, 3, \ldots$ and Lemma 3.3(9) shows the contradiction. Hence (a). Let assume a_s and a_t would be non full steps ($j_0 \leq s < t \leq r$). By (a), both are $(p-1)$-star.

$$\begin{aligned} a_t &\leq (p-1)a_{t-1} + a_{t-2} \leq p^{t-1-s}((p-1)a_s + a_{s-1}) \\ &\leq p^{t-1-s}(((p-1)^2+1)a_{s-1} + (p-1)a_{s-2}) \leq p^{t-1-s}(p^3-2p^2+3p-1)a_{s-2} \\ &\leq p^{t-1-s+s-2-(j_0-2)}(p^3-2p^2+3p-1)a_{j_0-2} \end{aligned}$$

The inequality $p(p^3-2p^2+3p-1) < p^4-p^3+p-1$ for $p \geq 3$ causes a contradiction to Lemma 3.3(9). □

We remark that if $p = 2$ the lemma holds if we modify it to "at most two".

The next theorem describes "Region 1" case.

Theorem 3.5. *Let $\{a_j\}_{j=1}^r$ be a p-chain of $n = a_r$. Let e be a p-exponent of n such that $n = p^e m$. The inequality*

$$(p-1)a_j + a_{j-1} \geq \frac{n}{p^{r-j-1}}, \tag{11}$$

holds for $1 \leq j \leq r-1$ if a_j is not of the form n/p^{r-j}.

Proof. Assume $n \neq p^{r-j}a_j$. Then there exists a non full step, say a_s between j and r. We have

$$n \leq p^{r-s}a_s \leq p^{r-s}((p-1)a_{s-1} + a_{s-2}) \leq p^{r-s}p^{s-j-1}((p-1)a_j + a_{j-1})$$

which shows (11). □

Theorem 3.6. *Let $\{a_j\}_{j=1}^r$, $n = p^e m$ be as in Theorem 3.5. Assume further that*

$$p^3 - p^2 + 1 \nmid m. \tag{12}$$

Then it holds

$$(p-1)a_j + a_{j-1} \geq \frac{n}{(p^2-1)p^{r-j-3}} \quad (1 \leq j \leq r-e-3). \tag{13}$$

Remark 3.7. We proceed the proof when $p \geq 3$ because the theorem for $p = 2$ is known ([T, Theorem 4]). Though most of the part works well for general p, there needs a special care for $p = 2$, for example to treat (15); eventually these are found to reduce to the condition $5 \mid n$, which contradicts the assumption in Theorem 3.6(12).

Proof. Suppose that $j = r - e - 3$. We assume

$$(p-1)a_{r-e-3} + a_{r-e-4} < \frac{n}{(p^2-1)p^e} \tag{14}$$

and try to deduce contradiction. By (14) and class 1 bound (5) with $j = r - e - 2$, the step a_{r-e-2} should be necessarily a full step: $a_{r-e-2} = pa_{r-e-3}$. We do a case study on the step a_{r-e-1}. By Lemma 3.4, a_{r-e-1} is $(p-1)$-star step. Put $a_{r-e-1} = (p-1)a_{r-e-2} + a_i$ $(i \leq r-e-2)$.

Case $i \leq r-e-3$: If every step from a_{r-e} to a_r is a full step, it follows $n = p^{e+1}a_{r-e-1}$ which contradicts $p^{e+1} \nmid n$. So there is a non full step, say a_s $(r-e \leq s \leq r)$. One has

$$\begin{aligned} a_s &\leq (p-1)a_{s-1} + a_{s-2} \leq p^{s-r+e}((p-1)a_{r-e-1} + a_{r-e-2}) \\ &\leq p^{s-r+e}((p-1)((p-1)a_{r-e-2} + a_{r-e-3}) + a_{r-e-2}) \\ &\leq p^{s-r+e}(p^3 - 2p^2 + 3p - 1)a_{r-e-3}. \end{aligned}$$

Lemma 3.3(9) with $j_0 = r - e - 1$ and the inequality

$$p(p^3 - 2p^2 + 3p - 1) < p^4 - p^3 + p - 1 \text{ for } p \geq 3 \tag{15}$$

cause a contradiction.

Case $i = r - e - 2$: In this case we have $a_{r-e-1} = p^2 a_{r-e-3}$. If $p \geq 3$, there are exactly one non full step, say a_s for $r - e \leq s \leq r$. Since a_s is $(p-1)$-star, we put $a_s = (p-1)a_{s-1} + a_{s_0}$. If $s_0 \leq s - 4$,

$$\begin{aligned} a_s &\leq (p-1)a_{s-1} + a_{s-4} \\ &\leq p^{s-r+e}((p-1)a_{r-e-1} + a_{r-e-4}) = p^{s-r+e}((p-1)p^2 a_{r-e-3} + a_{r-e-4}) \end{aligned}$$

Then,

$$a_s \leq p^{s-r+e}(((p-1)p^2 - t)a_{r-e-3} + (pt+1)a_{r-e-4})$$

for $t = (p^2-1)(p-1)/(p^2-p+1) > 0$. It turns out

$$a_s \leq p^{s-r+e}\frac{p^4 - p^3 + 1}{p^2 - p + 1}((p-1)a_{r-e-3} + a_{r-e-4}).$$

The inequality $(p^4 - p^3 + 1)/(p^2 - p + 1) \leq p^2 - 1$ shows contradiction to Lemma 3.3(8).

The only possibility is either $s_0 = s - 2, s - 3$. In both cases, we have

$$\begin{aligned} n = p^{r-s}a_s = p^{r-s}((p-1)a_{s-1} + a_{s-2-\epsilon}) \\ = p^{r-s}p^{s-r+e}((p-1)a_{r-e-1} + a_{r-e-2-\epsilon}) = \begin{cases} p^e(p^3 - p^2 + 1)a_{r-e-3}, & (\epsilon = 1); \\ p^{e+1}(p^2 - p + 1)a_{r-e-3}, & (\epsilon = 0). \end{cases} \end{aligned}$$

So, n is divided by either $p^3 - p^2 + 1$ or p^{e+1}, but both are impossible.

The assertion for $j < r - e - 3$ can be deduced easily from the case $j = r - e - 3$ by the elementary inequality. □

Remark 3.8. Both bounds do not require the assumption that the given p-chain has to be minimal.

4. NUMERICAL EXAMPLES FOR $p = 3$

By suitable implementation of backtracking algorithm using pruning bounds we have just proved, we can obtain numerical examples for general p. In this section we take $p = 3$ and show several examples for ternary addition chains.

There are several questions which was already answered to binary addition chains [K, 4.6.3]. We show a few answers to its ternary version.

- For an integer r ($7 \leq r \leq 17$), the smallest number n which attains the minimal length $r = \ell_3(n)$ are listed in Table 1. Unlike binary case [S], no efficient lower bound for the length of ternary addition chains are available at this moment. So we used the trivial bound (1)

TABLE 1. numerical examples for ternary addition chain

$\ell_3(n)$	n	runtime(sec.)	# of nodes	class 1	class 2
7	232	0.00	1226	60.4%	43.4%
8	580	0.00	6611	48.1%	29.9%
9	1402	0.02	50763	49.5%	29.8%
10	3880	0.06	205871	45.2%	25.9%
11	9638	1.16	2.26×10^6	58.3%	42.0%
12	25828	2.65	7.87×10^6	44.5%	35.0%
13	65608	60.75	1.13×10^8	60.0%	42.3%
14	189296	150.09	3.05×10^8	55.1%	37.2%
15	506600	250.25	8.36×10^8	39.9%	21.8%
16	1377736	1139.79	3.79×10^9	38.8%	21.2%
17	3649318	5286.13	1.98×10^{10}	35.9%	18.3%

as a start point. The number of nodes indicates how many nodes are used to run down searching trees in general. The ratio shows to how extent the nodes are valid in sight of pruning bounds (class 1/class 2). Actually what the running time indicated are under the search with both pruning bounds.

- $\ell_3(5251) = \ell_3(3 \cdot 5251) = 10$ is the first example for "$\ell_3(3n) \le \ell_3(n)$".
- $\ell_3(30754) = 11$, but $\ell_3^*(30754) = 12$. This is the first n with the property: $\ell_3(n) \neq \ell_3^*(n)$.

5. CHAINS FOR INTEGERS WITH FEW STANDING BITS

Let $\{a_j\}$ be a p-chain of length r. If $\lambda_p(a_j) = \lambda_p(a_{j-1})$, a_j is called a *small step*. Non small step is sometimes called a *large step*. The number of the large steps is equal to $\lambda_p(n)$. Because steps are whether small or large, the number of small steps is computed to $r - \lambda_p(n)$.

Lemma 5.1. *For* $1 \le k \le p-1$,

$$\ell_p(kp^\alpha) = \begin{cases} \alpha & (k = 1) \\ \alpha + 1 & (1 < k \le p-1) \end{cases}$$

Proof. Clear. □

Lemma 5.2. *If* $\nu_p(n) = 2$, $\lambda_p(n) + 1 \le \ell_p(n) \le \lambda_p(n) + 2$.

Proof. Clear by Equation (1). □

Lemma 5.3. *Let* $p \ge 3$. *For integers* $\alpha > \beta$, $2 \le \gamma \le p-1$, *let* $n = (p-1)p^\alpha + \gamma p^\beta$. *Then*

$$\ell_p(n) = \alpha + 2$$

Proof. Assume that $\ell_p(n) = \alpha + 1$ and $\{a_j\}$ is the p-chain of n with length $\alpha + 1$. Let a_r be the first and the only small step. That is, $a_k = p^k$ $(1 \leq k \leq r-1)$, $a_r < p^r$, $\lambda_p(a_k) = k - 1$ $(r < k \leq \alpha + 1)$. We have $a_r \leq (p-1)p^{r-1} + p^{r-2}$. Because $\gamma \geq 2$, we see that r cannot be $\alpha + 1$, and that there is a non-full step after a_r. Let a_s be the first non-full step after a_r. Then $a_{r+k} \leq (p-1)p^{r-1+k} + p^{r-2+k}$ $(k = 1, 2, \ldots, s-r-1)$. So we have

$$\begin{aligned} a_s &\leq (p-1)a_{s-1} + a_{s-2} \\ &\leq (p-1)((p-1)p^{s-2} + p^{s-3}) + (p-1)p^{s-3} + p^{s-4} \\ &= (p-2)p^{s-1} + 2p^{s-2} + (p-2)p^{s-3} + p^{s-4} \end{aligned}$$

On the other hand,

$$a_s \geq \lceil n/p^{\alpha+1-s} \rceil = \lceil (p-1)p^{s-1} + (p-1)p^{s-1+\beta-\alpha} \rceil,$$

a contradiction. □

Corollary 5.4. *Let $p = 3$, $\nu_3(n) = 2$. Then for $\alpha > \beta$,*

$$\ell_3(a3^\alpha + b3^\beta) = \begin{cases} \alpha + 2 & (a, b) = (2, 2) \\ \alpha + 1 & (a, b) = (1, 1), (1, 2), (2, 1) \end{cases}$$

Proof. When $(a, b) = (2, 2)$, Lemma 5.3 yields that its length is $\alpha + 2$. We can find a length $\alpha + 1$ p-chain of $ap^\alpha + bp^\beta$ $(a + b \leq p)$ easily, thus the corollary. □

Remark 5.5. By Table 2, we also claim the statement on the length of n with $\nu_3(n) = 3$. It holds $\ell_p(n) = \lambda_3(n) + 1$ iff $n = 3^\alpha + 3^\beta + 3^\gamma$, $3^\alpha + 3^\beta + 2 \cdot 3^\gamma$ $(\beta \geq \alpha - 3)$, $3^\alpha + 2 \cdot 3^{\alpha-2} + 2 \cdot 3^{\alpha-3}$, $3^\alpha + 2 \cdot 2 \cdot 3^\beta + 2 \cdot 3^\gamma$ for $\alpha > \beta > \gamma$. Others have length $\lambda_3(n) + 2$, for they are obtained by chains having successive small steps.

6. CHAINS WITH ONLY ONE SMALL STEP

First we claim on boundedness of the number of standing bits among integers achieved by a chain having fixed number of small steps. The basic idea to obtain Inequality 6.3 is found in [S] when $p = 2$.

Lemma 6.1.

$$\nu_p(x + y) \leq \nu_p(x) + \nu_p(y).$$

Proof. Without loss of generality, we assume $\lambda_p(x) \geq \lambda_p(y)$, $x \neq 0$, $y \neq 0$. If $\lambda_p(x) = 0$, the assertion is clear since $\lambda_p(x + y)$ is at most 2. Suppose that $\lambda_p(x) > 0$. Write $x = \sum x_i p^i$, $y = \sum y_i p^i$. If $x_0 = y_0 = 0$, $\nu_p(x + y) = \nu_p((x + y)/p) \leq \nu_p(x/p) + \nu_p(y/p) = \nu_p(x) + \nu_p(y)$. If $x_0 = 0$, $y_0 = 0$, $\nu_p(x+y) = \nu_p(x/p + \lfloor y/p \rfloor) + 1$. The assertion follows since $\nu_p(\lfloor y/p \rfloor) + 1 = \nu_p(y)$.

If $x_0 \neq 0$, $y_0 \neq 0$, $x_0 + y_0 < p$, the assertion is clear. Assume that $x_0 \neq 0$, $y_0 \neq 0$, $x_0 + y_0 \geq p$. Put $x_0 + y_0 = p + z_0$. Then we have

$$\nu_p(x+y) = \nu_p(x-x_0+y-y_0+p+z_0) = \nu_p((x-x_0)/p+(y-y_0)/p+1)+\nu_p(z_0).$$

If $\lambda_p((x - x_0)/p + 1) < \lambda_p(x)$, then, by induction hypothesis,

$$\begin{aligned}\nu_p(x + y) &\leq \nu_p((x - x_0)/p + 1) + \nu_p((y - y_0)/p) + \nu_p(z_0)\\ &\leq \nu_p((x - x_0)/p) + 1 + \nu_p((y - y_0)/p) + \nu_p(z_0)\\ &\leq \nu_p(x) - 1 + 1 + \nu_p(y) - 1 + \nu_p(z_0) \leq \nu_p(x) + \nu_p(y)\end{aligned}$$

The remaining case is $\lambda_p((x - x_0)/p + 1) = \lambda_p(x)$ and $\lambda_p((y - y_0)/p + 1) = \lambda_p(y)$. This means $(x - x_0)/p = p^{\lambda_p(x)} - 1$ so that $\nu_p((x - x_0)/p + 1) = 1$ and $\nu_p(x) = \lambda_p(x) + 1$ (similar for y). Since

$$\nu_p(x) + \nu_p(y) = \lambda_p(x) + \lambda_p(y) + 2 \geq \lambda_p(x + y) + 1 \geq \nu_p(x + y),$$

we have the lemma. □

Lemma 6.2. *Let N be the number of the non-full steps of $\{a_i\}$, a given addition chain of $n > 1$ of length r. Then $N \geq \log_p(\nu_p(n))$.*

Proof. If $r = 1$, then the assertion holds since $\nu_p(n) = 1$. Suppose $r > 1$. If a_r is a full step, then $\nu_p(a_r) = \nu_p(a_{r-1})$ and the number of the non-full steps remains equal. So this case is settled by induction hypothesis. Assume a_r is a non-full step. Put N_{r-1} the number of non-full steps in subchain of a_{r-1}. Then $N_{r-1} = N - 1$. By Lemma 6.1

$$\nu_p(a_r) = \nu_p(a_{i_1}+a_{i_2}+\cdots+a_{i_p}) \leq \nu_p(a_{i_1})+\nu_p(a_{i_2})+\cdots+\nu_p(a_{i_p}) \leq p\cdot p^{N_{r-1}} = p^N,$$

hence the lemma. □

Lemma 6.3. *For an addition chain $\{a_i\}$ of n of length r, one has*

$$r \geq \log_p(n) + (1 - \log_p(\gamma_p)) \log_p \nu_p(n).$$

Here γ_p is a positive solution of $x^2 = (p - 1)x + 1$.

Proof. Let N be the number of non-full steps. Define a sequence $\{c_i\}$ by

$$\begin{aligned}&c_0 = 1\\ &c_i = pc_{i-1} \quad \text{when } a_i \text{ is a full step}\\ &c_i = \gamma_p c_{i-1} \quad \text{when } a_i \text{ is a non-full step}\end{aligned}$$

Clearly $c_i \geq a_i$. One has $n \leq c_r = \gamma_p^N p^{r-N}$. Taking a log,

$$\log_p(n) \leq r - N + N \log_p(\gamma_p).$$

This inequality and Lemma 6.2 yield the lemma. □

TABLE 2. List of $3 \nmid n \in \mathrm{S}_p(1)$ in base 3 representation

$\nu_3(n)$	n
1	(10), 2
2	10^a1, 10^a2, 20^a1.
3	10^a10^b1, 110^a2, 1010^a2, 10010^a2 1021 10^a20^b2
4	1010^a11, 110^a10^b2, 10^a110^b2, 101010^a2, 1010^a12, 1010^a102, 10010^a10^b2, $1010^a10^{a+4}2$, 110^a20^b1, 1010^a21, 101201, 10010^a20^b1, 100010^a21, 100010^a201, $1010^a20^{a+2}1$, 10122, 10210^a1, 100^a20^b11, 1000020101, 100212, 10220^a2, 100222, 1002022, 1000222, 10001012, 10002202.
5	$1010^a110^{a+1}1$, 1010^a10^b11, 1010^a110^b1, 10010^a111, $1010^a1010^{a+1}1$, $110^a110^{a+1}1$, 10010^a112, 1010^a120^b2, 10010^a122, 10010^a1022, 100010^a122, 1010^a20^b12, 10010^a210^b2, $1010^a2010^{a+1}2$, 100012102, $110^a20^b20^a1$, 101220^a1, 10010^a20^b21, $10010^a2020^{a+1}1$, 101000221, 10020^a112, 1000020^a112, 10002112, 10210^a21, 1002120^a1, 10020121, 1002001021, 10200211, 1002211, 10022101, 102222.
6	101010^a112, 10010^a10^b112, 100010^a1112, 1000110^a1102, 10110121, $1010^a110^b20^{a+1}1$, 10010^a1120^b1, 100110^a1021, $10010^a10010^{a+2}21$, $10010^a10120^{a+1}1$, 10010^a1211, $10010^a1210^{a+2}1$, $1010^a1220^{a+1}2$, $1010^a20^b110^a1$, 100012122, 10010^a2212, 101220^a21, $10010^a20020^{a+1}21$, 1021111, 10210^a122, 1000020^a10122, 1002120^a21, 1002120^a201, 10220^a112.
7	$1010^a110^b120^{a+1}2$, 10010^a1120^b21, $10010^a1120^b20^{a+2}1$, $1010^a120^b110^{a+1}2$, 10010^a210^b112, $10010^a20^b1120^a1$, 1002201222.
8	101220^a1211, $10010^a120120^{a+1}21$.
9	1002120^a11221.
10	$10010^a1120^b11120^{a+1}21$.

0^a means 0 is repeated a times ($a \geq 0, b \geq 0$).

Corollary 6.4. *Let $\mathrm{S}_p(k)$ be the set of positive integers which is achieved by an addition chain having just k small steps. Then $\nu_p(n)$ ($n \in \mathrm{S}_p(k)$) is bounded.*

Proof. This follows from Lemma 6.3 if we consider the length r is the sum of the number of small steps and $\lambda_p(n)$. □

Next step is to classify addition chains and $\mathrm{S}_p(k)$ for given k. We show $\mathrm{S}_p(1)$ when $p = 3$ in Table 2. In this case Lemma 6.3 says $3^{1/(1-\log_3(\gamma_3))} \sim 259$ is a bound whereas the actual upper bound is 10.

One can find a concrete chains for each of $n \in \mathrm{S}_p(1)$ [W]. In particular one has $\ell_3(n) = \lambda_3(n) + 1$ when $\nu_3(n) > 1$, $n \in \mathrm{S}_p(1)$.

References

[H] Takahiro Hayata, *Ternary addition chains and pruning bounds*, preprint, 2005.

[K] Donald E. Knuth, *The Art of Computer Programming Vol. 2*, third ed., Addison-Wesley, 1997.

[S] Arnold Schönhage, *A lower bound for the length of addition chains*, Theor. Comput. Sci. **1** (1975), 1–12.

[T] Edward G. Thurber, *Efficient generation of minimal length addition chains*, SIAM J. Comput. **28** (1999), 1247–1263.

[W] Masaya Wagatuma, *Classification of ternary addition chains having few small steps (in Japanese)*, master thesis, Yamagata University, 2006.

Department of Informatics, Yamagata University, 4-3-16 Jyonan, Yonezawa, 992-8510, Japan