Asian Research Journal of Mathematics

17(3): 134-153, 2021; Article no.ARJOM.69077
ISSN: 2456-477X

Connections on Valuated Binary Tree and Their Applications in Factoring Odd Integers

Xingbo Wang[1*], Jinfeng Luo[1], Ying Tian[1] and Li Ma[2]

[1]*Department of Mechatronic Engineering, Foshan University, Foshan City, China.*
[2]*Department of Electronic and Information Engineering, Foshan University, Foshan City, China.*

Authors' contributions

This work was carried out in collaboration among all authors. Author XW is in charge of theory and proof. Authors JL and YT are in charge of programming test. Author LM is in charge of other work. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/ARJOM/2021/v17i330287
Editor(s):
(1) Dr. Nikolaos D. Bagis. Aristotle University of Thessaloniki, Greece.
Reviewers:
(1) A. Rizwana, V. H. N. Senthikumara Nadar College (Autonomous), India.
(2) Simon Joseph, Bahr El-Ghazal University, South Sudan.
(3) Dhanapal P. Basti, Visvesvaraya Technological University, India.
Complete Peer review History: http://www.sdiarticle4.com/review-history/69077

Original Research Article

Received 25 March 2021
Accepted 31 May 2021
Published 01 June 2021

Abstract

This paper makes an investigation on geometric relationships among nodes of the valuated binary trees, including parallelism, connection and penetration. By defining central lines and distance from a node to a line, some intrinsic connections are discovered to connect nodes between different subtrees. It is proved that a node out of a subtree can penetrate into the subtree along a parallel connection. If the connection starts downward from a node that is a multiple of the subtree's root, then all the nodes on the connection are multiples of the root. Accordingly composite odd integers on such connections can be easily factorized. The paper proves the new results with detail mathematical reasoning and demonstrates several numerical experiments made with Maple software to factorize rapidly a kind of big odd integers that are of the length from 59 to 99 decimal digits. It is once again shown that the valuated binary tree might be a key to unlock the lock of the integer factorization problem.

Keywords: Integer factorization; valuated binary tree; parallel lines; connection.

**Corresponding author: Email: 153668@qq.com;*

2020 Mathematics Subject Classification: 11A51, 11Y99.

1 Introduction

The idea using binary tree to study odd integers bigger than 1 was first put forward in WANG's paper [1]. In that paper and its following studies, many new properties were discovered. For example, articles [2] and [3] discovered the properties of symmetric nodes and symmetric common divisors, article [4] disclosed the genetic properties of odd integers, and article [5] demonstrated the periodical divisibility traits along the leftmost path or the left side-path of the tree. All these new properties enable people to know the integers in a different point of view, as stated and investigated in paper [6].

Based on the new properties, fast approaches to factorize odd integers are disclosed. For example, article [7] presented an algorithm of $O(\log_2 N)$ searching steps (or $O((\log_2 N)^4)$ bit operations) to factorize an odd integer $N = pq$ with the divisor q being of the form $2^a u+1$ or $2^a u-1$ and the divisor p satisfying $1 < p \le 2^a+1$ or $2^{a+1} < p \le 2^{a+1}-1$, article [8] exhibited a fast approach to factorized big Fermat numbers, and article [9] introduced a method to estimate the divisors' bounds for semiprimes or RSA numbers. Thereby, it is reasonable to believe that valuated binary tree might be a key to unlock the lock of the integer factorization problem.

It is undoubted that knowing the distribution of all the multiples of an odd integer p bigger than 1 is surely helpful to factorize a composite odd integer that has p as a divisor. Under description of the valuated binary tree, say T_p, the distribution of the multiples of the root p is critically important, as investigated in articles [4,5,6] and [7]. When a multiple, say $m = \alpha p$ with odd integer $\alpha > 1$ and $(\alpha, p) = 1$, lies in the tree T_p, m is very easy to be factorized by $p = \gcd(m, p)$ because tracing upwards from m by $\log_2 \alpha$ steps reaches p. Since unfortunately m is out of T_p in most cases, the research topic is naturally brought out on how to make m be related with an inner descendant of T_p. This paper does such a research. The paper first defines several metric relations on the valuated binary tree from the point of view of geometry, then finds out the converting relations from an outer node to an inner node of a tree, and in the end the paper proves that there are a special kind of odd integers that can be factorized in $O(\log_2 N)$ searching steps.

The paper is composed of five parts. The first is this introductory part, the second cites some old related preliminaries, the third gives some new definitions, the fourth presents new theorems together with their proof, and the last part introduces factorization of the special kind of odd integers.

2 Preliminaries

This section cites some definitions, notations and lemmas that have been defined, introduced or proved in the related previous publications that are necessary for later descriptions. Also, some new conclusions with their simple proofs are placed here.

2.1 Definitions and notations

A valuated binary tree T is a perfect full binary tree that each of its nodes is assigned a value. The terms binary tree and its root, nodes, father, left-son, right-son as well as subtrees can be seen in school-books of data structure, for example, Dinesh's handbook [10] (Dinesh P. Mehta, Sartaj Sahni, 2005). Let N be an odd integer bigger than 1; an N-rooted tree, denoted by T_N is a recursively constructed valuated binary tree whose root is the odd number N with $2N-1$ and $2N+1$ being the root's left and right sons, respectively. Each son is connected with its father with a path, but there is no path between the two sons. The father, grandfather and so forth are called direct ancestors; accordingly a path connecting a node with its direct ancestor or descendant is called a direct path, and it either starts or ends at the root. The number of nodes on a path is the length of the path. Nodes on the same level are brothers. T_3 tree is the case N=3. For convenience, symbol $N_{(k,j)}$ is by default the node at position j on level k of T_3, where $k \ge 0$ and $0 \le j \le 2^k - 1$. An odd integer bigger than 1 is regarded to be a node of a certain valuated binary tree. Symbol $N_{(k,j)}^X$ is to denote the node at position j on level k of T_X, where $k = 0,1,...$ and $j = 0,1,...,2^k - 1$. When the index j is out of the range $0 \le j \le 2^k - 1$, for example, $j = -2,-1$ or $j = 2^k, 2^k + 1$, $N_{(k,j)}^X$ is called an outer-node of T_X. Symbol $x \in T_X$ means node x is a node of T_X while symbol $x \notin T_X$ means x is not a node of T_X. Symbol $x \in l(T_X)$ means node x is in the left branch of T_X while symbol $x \in r(T_X)$ means node x is in the right branch of T_X. Symbol A_X^α is X's direct ancestor that is α levels over X. A walk of a node $N_{(k,j)}^X$ means an operation on either the index k or j, for example, $N_{(k+\sigma,j)}^X$, $N_{(k,j+\omega)}^X$ and $N_{(k+\sigma,j+\omega)}^X$ are all results from the walk of $N_{(k,j)}^X$. A tracing step or a searching step is the computation of a father based on a son or vice versa, or a node to its adjacent brother.

Symbol $A \Rightarrow B$ means result B is derived from condition A or A can derive B out. In this whole article, symbol $\lfloor x \rfloor$ denotes the floor function, an integer function of the real number x such that $x-1 < \lfloor x \rfloor \le x$ or equivalently $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$. Article [11] collected most necessary properties to refer. An odd interval $[a,b]$ is a set of consecutive odd numbers that take a as lower bound and b as upper bound. Intervals in this whole article are by default the odd ones unless particularly mentioned. Symbol Z^+ is the set of positive integers.

2.2 Lemmas

Lemma 1. [1,5,12]. The T_3 Tree has the following fundamental properties.

(P1). Every node is an odd integer and every odd integer bigger than 1 must be a node of the tree. Odd integer N with N>1 lies on level $\lfloor \log_2 N \rfloor - 1$. On the same level, there is not a node that is a multiple of another one.

(P2). $N_{(k,j)}$ is calculated by

$$N_{(k,j)} = 2^{k+1} + 1 + 2j, j = 0,1,...,2^k - 1$$

(P3) Nodes $N_{(k+1,2j)}$ and $N_{(k+1,2j+1)}$ on the $(k+1)^{\text{th}}$ level are respectively left son and right son of node $N_{(k,j)}$ on the k^{th} level. The descendants of $N_{(k,j)}$ on the $(k+i)^{\text{th}}$ level with $i \ge 0$ are $N_{(k+i,2^i j+\omega)}$ ($0 \le \omega \le 2^i - 1$), which are

$$N_{(k+i,2^i j)}, N_{(k+i,2^i j+1)}, N_{(k+i,2^i j+2)}, ..., N_{(k+i,2^i j+\omega)}, ..., N_{(k+i,2^i j+2^i-1)}$$

(P4) For given $N_{(k,j)} \in T_3$, it holds

$$N_{(k,j)} + 2^{k+1}(2^\sigma - 1) + 2\omega = N_{(k+\sigma,j+\omega)}$$

and

$$N_{(k,j)} + 2^{k+1}(2^\sigma - 1) - 2\theta = N_{(k+\sigma,j-\theta)}$$

where integers $\sigma \ge 0$, ω and θ satisfy $0 \le \omega \le 2^{k+\sigma} - 1 - j$ and $0 \le \theta \le j$.

Lemma 2. [1,5,12]. Let T be X-rooted binary tree. Then

(P1) On level k with $k = 0,1,...$, there are 2^k nodes. On the same level, there is not a node that is a multiple of another one.

(P2) Node $N_{(k,j)}^{X}$ is computed by

$$N_{(k,j)}^{X} = 2^k X - 2^k + 2j + 1; k = 0,1,2,...; j = 0,1,...,2^k - 1$$

(P3) Let p be an odd integer bigger than 1 and $p = N_{(k,j)}$; then $N_{(i,\omega)}^{p}$ of T_p $(0 \le i; 0 \le \omega \le 2^i - 1)$ is corresponding to node $N_{(k+i,2^i j+\omega)}$ of T_3, namely, $N_{(i,\omega)}^{N_{(k,j)}} = N_{(k+i,2^i j+\omega)}$.

(P4) For T_x and integer $k \ge 0$, it holds

$$N_{(k+1,2^k-1\pm\omega)}^{X} = N_{(k,2^{k-1}-1\pm\omega)}^{X} \pm 2^k X$$

and

$$N_{(k+1,2^k\pm\omega)}^{X} = N_{(k,2^{k-1}\pm\omega)}^{X} \pm 2^k X$$

where ω is an integer satisfying $0 \le \omega \le 2^{\lfloor \log_2 X \rfloor - 1 + k}$ and the $\pm$ symbols are mandatory to be the same in the corresponding terms, namely, one term taking + requires the other terms to take +, or vice versa.

Lemma 3. Suppose $N > 1$ is an odd integer; then $N = N_{(k,j)}$ in T_3 with $k = \lfloor \log_2 N \rfloor - 1$ and $j = \frac{N-1}{2} - 2^{\lfloor \log_2 N \rfloor - 1}$. Accordingly, $n = \alpha N$ with $\alpha \ge 1$ being an odd integer lies on $k + \lfloor \log_2 \alpha \rfloor$ or $k + \lfloor \log_2 \alpha \rfloor + 1$.

Proof. By Lemma 1(P1), p lies on level $\lfloor \log_2 p \rfloor - 1$. Let $p = 2^{k+1} + 2j + 1$; then $j = \frac{p-1}{2} - 2^k$. Thereby, $n = \alpha N$ lies on level $k_n = \lfloor \log_2 \alpha N \rfloor - 1$. By properties of the floor function it holds

$$k + \lfloor \log_2 \alpha \rfloor = \lfloor \log_2 \alpha \rfloor + \lfloor \log_2 N \rfloor - 1 \le k_{\alpha N} \le \lfloor \log_2 \alpha \rfloor + \lfloor \log_2 N \rfloor = k + 1 + \lfloor \log_2 \alpha \rfloor$$

3 Geometric Relationships on a Tree

By definition, a valuated binary tree consists of nodes and paths connecting sons with fathers and so forth with the direct ancestors. Geometrically, nodes are considered to place with rows and columns. For example, the first five rows of a valuated binary tree *T* can be either one of the two layouts illustrated in Fig. 1.

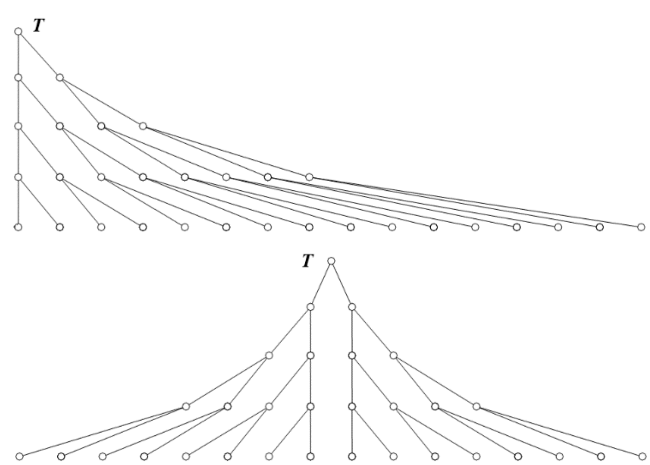

Fig. 1. Different layouts of a tree

A row is conventionally called a level while a column has no alternative new name. By definition, there is a gap between two nodes. When the gap between arbitrary two adjacent levels is the same as that between arbitrary two adjacent columns, the tree is an equal-distanced tree. The equal-distanced tree is by default supposed in scientific research however it is usually drawn to layout in an isosceles triangle, as seen in Fig. 2. It can be seen that nodes are in parallel distribution from level to level and from column to column. Except for the parallelism, there are other geometric relationships on a valuated binary tree, as introduced next.

3.1 Central lines and connections

Suppose p>1 is an odd integer and T_p is the p-rooted valuated binary tree; let $C_l=\{N^p_{(1,0)},N^p_{(2,1)},N^p_{(3,3)},...,N^p_{(k,2^{k-1}-1)},...\}$ and $C_r=\{N^p_{(1,1)},N^p_{(2,2)},N^p_{(3,4)},...,N^p_{(k,2^{k-1})},...\}$; then the path connecting nodes in C_l is defined to be a ***left central line*** and the path connecting nodes in C_r is defined to be a ***right central line***, as shown in Fig. 2(a). In T_p, the root $p=N^p_{(0,0)}$ is regarded to be the end of both C_l and C_r. On a level k>0, the number of nodes between node $N^p_{(k,j)}$ and $N^p_{(k,2^{k-1}-1)}$ is defined to be the ***distance*** from $N^p_{(k,j)}$ to C_l. Statement that A is d away from B means d is the distance between node A and B. The number of nodes on an entire level is a ***span*** of the tree on the level. A ***connection*** is a virtual (imaginary) path (line) to connect two nodes between which there is no direct path. For example, connect two nodes that have the same distance to C_l, as shown in Fig. 2(*b*). Connections can connect nodes both inside and outside of a tree. A connection on which all the nodes have the same distance to C_l is a parallel connection of C_l. Distance to C_r and parallel connections of C_r can be defined likewise. Fig. 2 illustrates C_l, C_r and a connection. The number of nodes on a connection is the length of the connection.

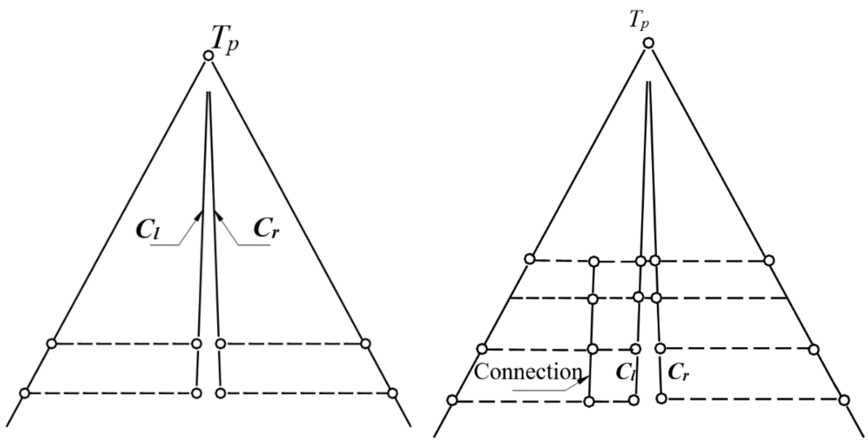

Fig. 2. Left-center line and right-center line

3.2 Trace and penetration

Lemma 1 (P1) indicates that, for an arbitrary odd integer N≥3,T_N is a subtree of T_3. Obviously, T_X and T_Y are two distinct subtrees if two odd integers X and Y satisfying X>3, Y>3 and X≠Y. Accordingly, for a subtree T_X with X>3, a node $x\in T_3$ might be $x\in T_X$ or $x\notin T_X$. When $x\notin T_X$, it can walk into T_X. For this reason, in later statements of the paper, the root of a subtree is by default bigger than 3 unless it is particularly declared. By definition, a walk can go along a path, a connection, or a combination of them. The ordered array of all paths and connections for a walk forms a trace and the number of non-repeat nodes on a trace is the length of the trace. For example, if walking into subtree $T_{N_{1,1}}$, illustrated in Fig. 3, node $N_{1,0}$ can have at least four selective decisions:

(1) Along trace $N_{1,0}\to N_{0,0}\to N_{1,1}$ that is combined of path $N_{1,0}\to N_{0,0}$ and path $N_{0,0}\to N_{1,1}$;
(2) Along trace (connection) $N_{1,0}\to N_{1,1}$;

(3) Along trace (connection) $N_{1,0} \rightarrow N_{2,1}$;
(4) Along trace $N_{1,0} \rightarrow N_{2,1} \rightarrow N_{2,1}$ that is combined of path $N_{1,0} \rightarrow N_{2,1}$ and connection $N_{2,1} \rightarrow N_{2,1}$.

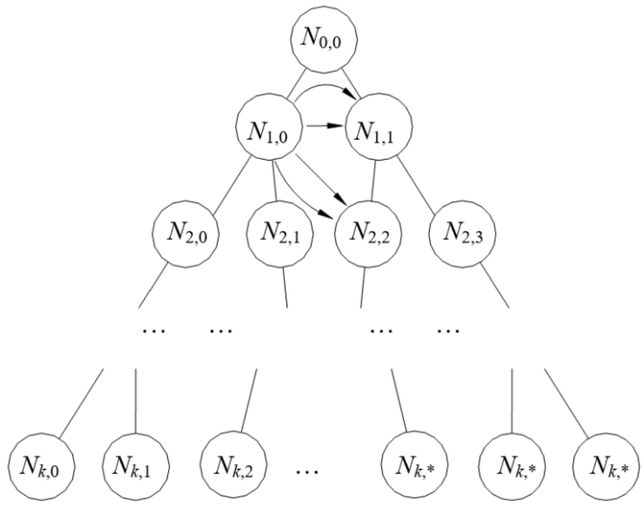

Fig. 3. Traces of a walk

If the trace of a walk is parallel to C_l or C_r of a tree, the walk is a parallel walk. A penetration is a walk whose trace has the shortest length. Obviously the penetration of a node into a tree is worth to investigate because it concerns something with the optimal problems of finding a shortest path.

4 Main Results and Proofs

Property 1. In any valuated binary tree, C_l and C_r are in perpetuity parallel to each other.

Proof. By definition, the distance between C_l and C_r is in perpetuity 2.

Property 2. In $\boldsymbol{T}_3$, a connection that starts downwards from $N_{(k,j)}$ ($k>0, 0 \le j \le 2^k - 1$) and connects the node $N_{(k+i, 2^{k-1}(2^i-1)+j)}$ with $i \ge 0$ is parallel to C_l and C_r.

Proof. The condition $k>0$ and $0 \le j \le 2^k - 1$ is mandatory because C_l starts downwards from $N_{(1,0)}$. Now consider the case that $N_{(k,j)}$ is on the left of C_l. Direct calculation shows that, the distances from $N_{(k,j)}$ to C_l and C_r are respectively

$$d_k^l = \frac{N_{(k,2^{k-1}-1)} - N_{(k,j)}}{2} + 1 = 2^{k-1} - j$$

and

$$d_k^r = \frac{N_{(k,2^{k-1})} - N_{(k,j)}}{2} + 1 = 2^{k-1} - j + 1$$

Since the distances from $N_{(k+i, 2^{k-1}(2^i-1)+j)}$ to C_l and C_r are respectively

$$d_{k+i}^{l} = \frac{N_{(k+i,2^{k+i-1}-1)} - N_{(k+i,2^{k-1}(2^{i}-1)+j)}}{2} + 1$$
$$= 2^{k-1} - j$$

and

$$d_{k+i}^{r} = \frac{N_{(k+i,2^{k+i-1})} - N_{(k+i,2^{k-1}(2^{i}-1)+j)}}{2} + 1$$
$$= 2^{k-1} - j + 1$$

the property surely holds.

For the case $N_{(k,j)}$ is on the right of C_l, it holds

$$d_{k}^{l} = \frac{N_{(k,j)} - N_{(k,2^{k-1}-1)}}{2} + 1 = j - 2^{k-1} + 1$$
$$d_{k}^{r} = \frac{N_{(k,j)} - N_{(k,2^{k-1})}}{2} + 1 = j - 2^{k-1}$$
$$d_{k+i}^{l} = \frac{N_{(k+i,2^{k-1}(2^{i}-1)+j)} - N_{(k+i,2^{k+i-1}-1)}}{2} + 1$$
$$= j - 2^{k-1} + 1$$
$$d_{k+i}^{r} = \frac{N_{(k+i,2^{k-1}(2^{i}-1)+j)} - N_{(k+i,2^{k+i-1})}}{2} + 1$$
$$= j - 2^{k-1}$$

Thereby the property holds.

Property 3. Let p>3 be an odd integer and T_p be the p-rooted valuated binary tree with C_l and C_r being the left and right central lines respectively; the connection that starts downwards from $N_{(k,j)}^{p}$ ($k > 0$, $0 \le j \le 2^{k} - 1$) and connects the node $N_{(k+i,2^{k-1}(2^{i}-1)+j)}^{p}$ with $i \ge 0$ is parallel to C_l and C_r, as illustrated in Fig. 4.

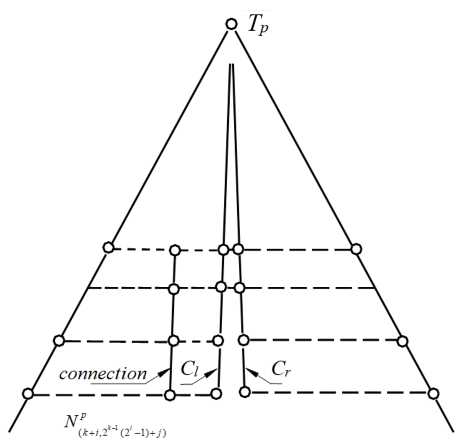

Fig. 4. Connection parallel to C_l and C_r

Proof. Referring to the proof of Property 2, there are two cases to be considered. One is the case that $N^p_{(k,j)}$ is on the left of C_l and the other is the case $N^p_{(k,j)}$ is on the right of C_l. For the case that $N^p_{(k,j)}$ is on the left of C_l, direct calculation shows that, the distances from $N^p_{(k,j)}$ to C_l and C_r are respectively

$$d^l_k = \frac{N^p_{(k,2^{k-1}-1)} - N^p_{(k,j)}}{2} + 1 = 2^{k-1} - j$$

$$d^r_k = \frac{N^p_{(k,2^{k-1})} - N^p_{(k,j)}}{2} + 1 = 2^{k-1} - j + 1$$

and the distances from $N^p_{(k+i,2^{k-1}(2^i-1)+j)}$ to C_l and C_r are respectively

$$\begin{aligned} d^l_{k+i} &= \frac{N^p_{(k+i,2^{k+i-1}-1)} - N^p_{(k+i,2^{k-1}(2^i-1)+j)}}{2} + 1 \\ &= 2^{k-1} - j \\ d^r_{k+i} &= \frac{N^p_{(k+i,2^{k+i-1})} - N^p_{(k+i,2^{k-1}(2^i-1)+j)}}{2} + 1 \\ &= 2^{k-1} - j + 1 \end{aligned}$$

Likewise, the case $N^p_{(k,j)}$ is on the right of C_l can be shown by following calculations.

$$\begin{aligned} d^l_k &= \frac{N^p_{(k,j)} - N^p_{(k,2^{k-1}-1)}}{2} + 1 = j - 2^{k-1} + 1 \\ d^r_k &= \frac{N^p_{(k,j)} - N^p_{(k,2^{k-1})}}{2} + 1 = j - 2^{k-1} \\ d^l_{k+i} &= \frac{N^p_{(k+i,2^{k-1}(2^i-1)+j)} - N^p_{(k+i,2^{k+i-1}-1)}}{2} + 1 \\ &= j - 2^{k-1} + 1 \\ d^r_{k+i} &= \frac{N^p_{(k+i,2^{k-1}(2^i-1)+j)} - N^p_{(k+i,2^{k+i-1})}}{2} + 1 \\ &= j - 2^{k-1} \end{aligned}$$

Hence the property holds.

Remark 1. Property 2 and Property 3 are of the same essence because taking *p*=3 in Property 3 immediately yields Property 2.

Property 4. Let *p*>3 be an odd number and T_p be the p-rooted valuated binary tree with C_l and C_r being the left and right central lines respectively; suppose $n = N_{(k,j)} \in T_3$ such that $\lfloor \log_2 n \rfloor - \lfloor \log_2 p \rfloor \geq 0$ and is $d_l(n)$ away from C_l. Then the connection L_n starting downwards from n and parallel to C_l, as is illustrated with Fig. 5, passes through $N^p_{(i,2^{i-1}+d_l(n))}$ if *n* is on the left of C_l whereas it passes through $N^p_{(i,2^{i-1}+d_l(n)-2)}$ if *n* is on the right of C_r, where integer $i \geq 1$ and the node $N^p_{(i,2^{i-1}+d_l(n))}$ or $N^p_{(i,2^{i-1}+d_l(n)-2)}$ might be a virtual one.

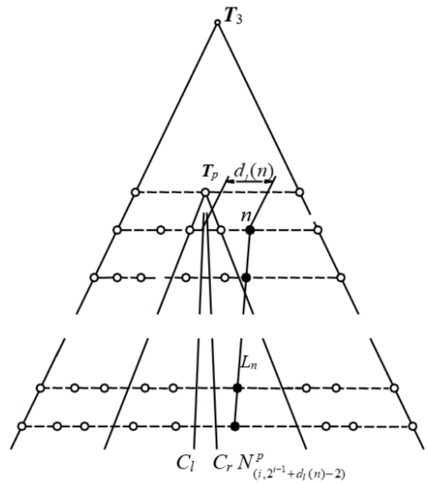

Fig. 5. Nodes of T_p on connection from T_3 to T_p

Proof. Let $k_n = \lfloor \log_2 n \rfloor - 1$ and $k_p = \lfloor \log_2 p \rfloor - 1$ be respectively the levels of T_3 where n and p lie. The condition $\lfloor \log_2 n \rfloor - \lfloor \log_2 p \rfloor \geq 0$ means n lies on the same level as p lies or on a lower level.

Since L_n starts downwards from level k_n of T_3, it is sure $i \geq 1$ if node $N^p_{(i,*)} \in T_p$ is on L_n.

Now referring to the proof of Property 3, it is seen that, for the case n is on the left of C_l, the node $x \in T_p$ that is on level i and is $d_l(n)$ away from C_l satisfies

$$\frac{N^p_{(i,2^{i-1}-1)} - x}{2} + 1 = d_l(n)$$

That is

$$x = N^p_{(i,2^{i-1}-1)} - 2(d_l(n) - 1) = N^p_{(i,2^{i-1}-d_l(n))}$$

Likewise, for the case n is on the right of C_l, the node $y \in T_p$ that is $d_l(n)$ away from C_l satisfies

$$\frac{y - N^p_{(i,2^{i-1}-1)}}{2} + 1 = d_l(n)$$

Namely

$$y = N^p_{(i,2^{i-1}-1)} + 2(d_l(n) - 1) = N^p_{(i,2^{i-1}+d_l(n)-2)}$$

Property 5. Let p>3 be an odd number and T_p be the p-rooted valuated binary tree with C_l and C_r being the left and right central lines respectively; Given a node n of T_3 satisfying $\lfloor \log_2 n \rfloor - \lfloor \log_2 p \rfloor \geq 0$; suppose L_n is the connection starting downward from n and parallel to C_l and C_r, as is illustrated with Fig. 6; then after penetrating at most $\lfloor \log_2 n \rfloor - 1$ levels, L_n goes into T_p.

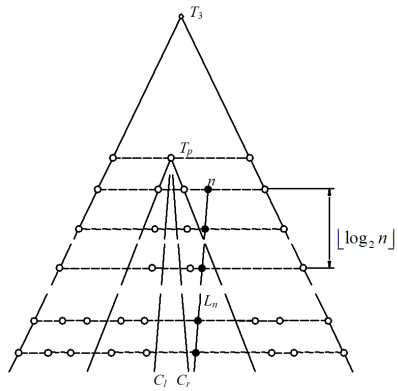

Fig. 6. Connection goes from T_3 into T_p

Proof. Let k_p and k_n be the levels where *p* and *n* lies in T_3; denote $d_l(n)$ and $d_r(n)$ to be the distances from *n* to C_l and C_r respectively. Consider the case n is on the right of C_r. The proof is based on the fact that L_n goes into T_p when the span on a level of the right branch of T_p is bigger than $d_r(n)$. Obviously, the Property is surely true if $n \in r(T_p)$. If $n \notin T_p$, let $k_n - k_p = \sigma$. Then *n* lies on the level matching to level σ of T_p. Take an arbitrary level $\sigma + i$ of T_p with $i \geq 0$; then there are $2^{\sigma+i-1}$ nodes from C_r to the rightmost node on the level. Thereby, if $2^{\sigma+i-1} \geq d_r(n)$, namely, $i \geq \lfloor \log_2 d_r(n) \rfloor + 1 - \sigma$, L_n goes into T_p. Take $i_0 = \lfloor \log_2 d_r(n) \rfloor + 1 - \sigma$ to be the critical case; then $i_0 < \lfloor \log_2 d_r(n) \rfloor + 2 - \sigma$. Since n lies on level k_n in T_3, it knows $d_l(n) \leq 2^{k_n} - 1$ and $d_r(n) \leq 2^{k_n} - 2$. Thereby,

$$i_0 < \lfloor \log_2 d_r(n) \rfloor + 2 - \sigma \leq \log_2 d_r(n) + 1 - \sigma < k_n + 2 - \sigma \leq k_n + 1 = \lfloor \log_2 n \rfloor$$

that is

$$i_0 \leq \lfloor \log_2 n \rfloor - 1$$

Similarly, the conclusion holds when *n* is on the left side of C_l.

Example 1. Take in T_3 a node *p*=27 and *n*=61, as shown in Fig. 7; then $\lfloor \log_2 n \rfloor = 5$, $\lfloor \log_2 p \rfloor = 4$, C_r of T_{27} is $C_r = \{55, 109, 217, 433, 865, ...\}$ and $d_l(n) = 5$ by Property 4. Construct a connection L_n by Property 4; then L_n passes through $N^{27}_{(1,4)} = 61$, $N^{27}_{(2,5)} = 115$, $N^{27}_{(3,7)} = 223$ and $N^{27}_{(4,11)} = 439$, among which $N^{27}_{(3,7)} = 223 \in T_{27}$ and $N^{27}_{(4,11)} = 439 \in T_{27}$. It is sure L_n goes into T_{23} by penetrating at most $\lfloor \log_2 n \rfloor - 1 = 4$ levels.

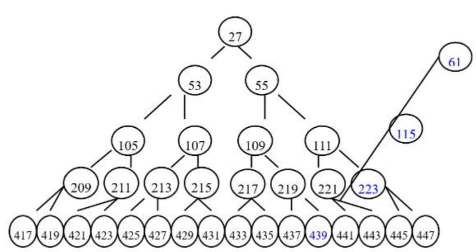

Fig. 7. Penetration of a node into a tree

Theorem 1. Let *m* and *n* be two odd integers bigger than 3; then there always a trace that leads *m* to walk into T_n or *n* to walk into T_m.

Proof. Without loss of generality, assume $m < n$. Then by Properties 4 and 5, *n* is surely able to walk into T_m. By Lemma 2, *m* can first walk along a parallel connection to the level where *n* lies, then penetrates into T_n.

Property 6. Let *p*>3 be an odd number, T_p be the *p*-rooted valuated binary tree with C_l and C_r being the left-center and right-center lines respectively; suppose $n \in T_3$ is a node that is $d_l(n)$ and $d_r(n)$ away from C_l and C_r, respectively; assume s_l and s_r are *n*'s left son and right son respectively, as illustrated in Fig. 8; then $s_r + 2(d_l(n)-1)$ and $s_r + 2(d_r(n)-1)$ are respectively $d_l(n)$ and $d_r(n)$ away from C_l and C_r if *n* lies on the left of C_l, whereas $s_l - 2(d_l(n)-1)$ and $s_l - 2(d_r(n)-1)$ are respectively $d_l(n)$ and $d_r(n)$ away from C_l and C_r if *n* lies on the right of C_l.

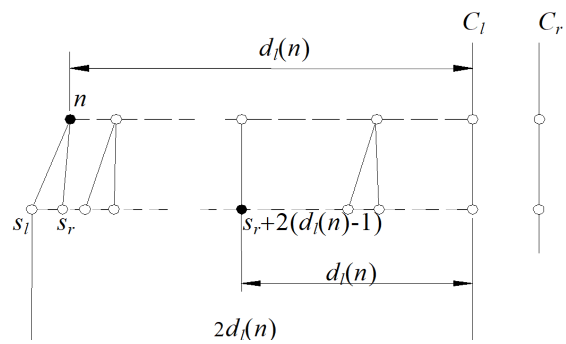

Fig. 8. ***n*** **and** $s_r + 2(d_l(n)-1)$ **are equal-distanced from** C_l

Proof. Here the proof is for the case *n* lies on the left of C_l. Assume $n = N_{(k_n,J_n)} - 2(d_l(n)-1)$, where $N_{(k_n,J_n)} \in C_l$; then $2N_{(k_n,J_n)} + 1 = N_{(k_n+1,2J_n+1)} \in C_l$, s_l and s_r are on level $k_n + 1$. Considering

$$\begin{aligned} s_r &= 2n+1 \Rightarrow s_r + 2(d_l(n)-1) = 2n+1+2(d_l(n)-1) \\ &= 2(N_{(k_n,J_n)} - 2(d_l(n)-1)) + 1 + 2(d_l(n)-1) \\ &= 2N_{(k_n,J_n)} - 2(d_l(n)-1)) + 1 \\ &= N_{(k_n+1,2J_n+1)} - 2(d_l(n)-1)) \end{aligned}$$

it knows that $s_r + 2(d_l(n)-1)$ is $d_l(n)$ away from C_l.

Similarly, other cases can be proved.

Remark 2. There is a more geometric proof for Property 6 shown here. *n*'s being $d_l(n)$ away from C_l leads to s_l being $2d_l(n)$ away from C_l. Accordingly, from s_l to C_l, there is one that is $d_l(n)$ taway from C_l. That one is sure $d_l(n)-1$ away from s_r and is expressed by $s_r + 2(d_l(n)-1)$.

Property 7. Let *m* be an odd integer and $\beta = \lfloor \log_2 m \rfloor$; suppose integer α satisfies $\alpha > \beta$; then $m + 2^{\alpha-\beta}(2^{\alpha+\chi}-1)m = N^m_{(2\alpha-\beta+\chi+1,J)} \in l(T_m)$, where integer $\chi \geq 0$.

Proof. First, $\alpha > \beta$ is mandatory because $m+2^{\alpha-\beta}(2^{\alpha+\chi}-1)m = 2^{\alpha+\chi}m \notin T_m$ in the case $\alpha=\beta$. Now let $n = m+2^{\alpha-\beta}(2^{\alpha+\chi}-1)m$ and $J = 2^{2\alpha-\beta+\chi-1} - 2^{\alpha-\beta-1}m + \frac{m-1}{2}$; then

$$\begin{aligned} n &= 2^{2\alpha-\beta+\chi}m - 2^{2\alpha-\beta+\chi} + 2^{2\alpha-\beta+\chi} - 2^{\alpha-\beta}m + m \\ &= 2^{2\alpha-\beta+\chi}(m-1) + 2(2^{2\alpha-\beta+\chi-1} - 2^{\alpha-\beta-1}m + \frac{m-1}{2}) + 1 \\ &= 2^{2\alpha-\beta+\chi}(m-1) + 2J + 1 \end{aligned}$$

Now it is to show $0 \le J \le 2^{2\alpha-\beta+\chi}-1$ and $n = N^m_{(2\alpha-\beta+\chi,J)}$. In fact, $\beta = \lfloor \log_2 m \rfloor$ yields $2^\beta + 1 \le m \le 2^{\beta+1}-1$, namely, $-2^{\beta+1}+1 \le -m \le -2^\beta - 1$. Multiplying each term of this inequality by $2^{\alpha-\beta-1}$ yields

$$-2^\alpha + 2^{\alpha-\beta-1} \le -2^{\alpha-\beta-1}m \le -2^{\alpha-1} - 2^{\alpha-\beta-1}$$

Since $2^{\beta-1} \le \frac{m-1}{2} \le 2^\beta - 1$, it is sure

$$2^{2\alpha-\beta+\chi-1} - 2^\alpha + 2^{\alpha-\beta-1} + 2^{\beta-1} \le J \le 2^\beta - 1 - 2^{\alpha-1} - 2^{\alpha-\beta-1} + 2^{2\alpha-\beta+\chi-1}$$

Subtracting $2^{2\alpha-\beta+\chi}-1$ from the right side term yields

$$\begin{aligned} &2^\beta - 1 - 2^{\alpha-1} - 2^{\alpha-\beta-1} + 2^{2\alpha-\beta+\chi-1} - (2^{2\alpha-\beta+\chi}-1) \\ &= 2^\beta - 2^{\alpha-1} - 2^{\alpha-\beta-1} - 2^{2\alpha-\beta+\chi-1} \le 0 \end{aligned}$$

Next is to show $2^{2\alpha-\beta+\chi-1} - 2^\alpha + 2^{\alpha-\beta-1} + 2^{\beta-1} \ge 0$ by using proof of contradiction. In fact, assume $2^{2\alpha-\beta+\chi-1} - 2^\alpha + 2^{\alpha-\beta-1} + 2^{\beta-1} < 0$; then

$$\begin{aligned} &2^{2\alpha-\beta+\chi-1} + 2^{\alpha-\beta-1} + 2^{\beta-1} < 2^\alpha \\ &\Rightarrow 2^{\alpha-\beta+\chi-1} + 2^{-\beta-1} + 2^{\beta-\alpha-1} < 1 \end{aligned}$$

which is contradictory to $\alpha \ge \beta+1$ and $\chi \ge 0$.

As a result,

$$0 \le J \le 2^{2\alpha-\beta+\chi}-1$$

which shows

$$m + 2^{\alpha-\beta}(2^{\alpha+\chi}-1)m = N^m_{(2\alpha-\beta+\chi+1,J)} \in l(T_m)$$

Property 7*. Let m be an odd integer and $\beta = \lfloor \log_2 m \rfloor$; then $m + 2^\sigma(2^{\sigma+\beta+\chi}-1)m \in l(T_m)$, where $\sigma > 0$ and $\chi \ge 0$ are integers. Particularly, $m+2(2^\beta-1)m \in T_m$, $m+2(2^{\beta+1}-1)m \in T_m$ and $m+2(2^{\beta+\delta}-1)m \in T_m$ with $\delta \ge 0$.

Proof. Taking $\sigma = \alpha - \beta$ in Property 7 immediately turns $m+2^{\alpha-\beta}(2^{\alpha+\chi}-1)m$ into $m+2^\sigma(2^{\sigma+\beta+\chi}-1)m$. The particular case $m+2(2^\beta-1)m \in T_m$, is shown in the following reasoning.

$$\begin{aligned}
& m+2(2^{\beta}-1)m = 2^{\beta+1}m - m \\
& = 2^{\beta+1}m - 2^{\beta+1} + 2^{\beta+1} - m \\
& = 2^{\beta+1}(m-1) + 2(2^{\beta} - \frac{m+1}{2}) + 1
\end{aligned}$$

Obviously, if $0 \le 2^{\beta} - \frac{m+1}{2} \le 2^{\beta+1} - 1$ then $m+2(2^{\beta}-1)m = N^{m}_{(\beta+1, 2^{\beta}-\frac{m+1}{2})} \in T_m$. Note that

$$\begin{aligned}
& \beta = \lfloor \log_2 m \rfloor \\
& \Rightarrow 2^{\beta} + 1 \le m \le 2^{\beta+1} - 1 \\
& \Rightarrow 2^{\beta-1} + 1 \le \frac{m+1}{2} \le 2^{\beta} \\
& \Rightarrow -2^{\beta} \le -\frac{m+1}{2} \le -2^{\beta-1} - 1 \\
& \Rightarrow 0 \le 2^{\beta} - \frac{m+1}{2} \le 2^{\beta-1} - 1
\end{aligned}$$

Consequently, it follows

$$m+2(2^{\beta}-1)m = N^{m}_{(\beta+1, 2^{\beta}-\frac{m+1}{2})} \in T_m$$

Actually, $N^{m}_{(\beta+1, 2^{\beta}-\frac{m+1}{2})}$ lies on level $\beta+1$ in the left branch of T_m .

The particular case $m+2(2^{\beta+1}-1)m \in T_m$ is shown as follows

$$\begin{aligned}
& \beta = \lfloor \log_2 m \rfloor \\
& \Rightarrow -2^{\beta} \le -\frac{m+1}{2} \le -2^{\beta-1} - 1 \\
& \Rightarrow 2^{\beta+1} - 2^{\beta} \le 2^{\beta+1} - \frac{m+1}{2} \le 2^{\beta+1} - 2^{\beta-1} - 1 \\
& \Rightarrow 2^{\beta} \le 2^{\beta+1} - \frac{m+1}{2} < 2^{\beta+1} - 1 \\
& m+2(2^{\beta+1}-1)m = 2^{\beta+2}m - 2m + m \\
& = 2^{\beta+2}m - m = 2^{\beta+2}m - 2^{\beta+2} + 2^{\beta+2} - m \\
& = 2^{\beta+2}(m-1) + 2(2^{\beta+1} - \frac{m+1}{2}) + 1 \\
& = N^{m}_{(\beta+2, 2^{\beta+1}-\frac{m+1}{2})} \in T_m
\end{aligned}$$

It can be seen that, $N^{m}_{(\beta+2, 2^{\beta+1}-\frac{m+1}{2})}$ lies on level $\beta+2$ in the right branch of T_m .

The case $m+2(2^{\beta+\delta}-1)m \in T_m$ is shown as follows.

$$
\begin{aligned}
&2^{\beta-1}+1\le \frac{m+1}{2}\le 2^{\beta}\\
&\Rightarrow -2^{\beta}\le -\frac{m+1}{2}\le -2^{\beta-1}-1\\
&\Rightarrow 2^{\beta+\delta}-2^{\beta}\le 2^{\beta+\delta}-\frac{m+1}{2}\le 2^{\beta+\delta}-2^{\beta-1}-1\\
&\Rightarrow 2^{\beta}(2^{\delta}-1)\le 2^{\beta+\delta}-\frac{m+1}{2}\le 2^{\beta+\delta}-2^{\beta-1}-1<2^{\beta+\delta}-1\\
&m+2(2^{\beta+\delta}-1)m=2^{\beta+\delta+1}m-m\\
&=2^{\beta+\delta+1}m-2^{\beta+\delta+1}+2^{\beta+\delta+1}-m\\
&=2^{\beta+\delta+1}(m-1)+2(2^{\beta+\delta}-\frac{m+1}{2})+1\\
&=N^{m}_{(\beta+\delta+1,2^{\beta+\delta}-\frac{m+1}{2})}\in T_m
\end{aligned}
$$

It can be seen that, the bigger δ is, the closer $N^{m}_{(\beta+\delta+1,2^{\beta+\delta}-\frac{m+1}{2})}$ is to the right branch of T_m .

Property 8. Let p>3 be an odd integer and T_p be the p-rooted valuated binary tree with C_l and C_r being the left and right central lines respectively; suppose $n=\alpha p$ with $\alpha>1$ being an odd integer is a node of T_3, L_n is the connection starting downwards from n and parallel to C_l ; then each node on L_n is a multiple of p.

Proof. By Lemma 3, p lies at position $J_p=\frac{p-1}{2}-2^{k_p}$ on level $k_p=\lfloor\log_2 p\rfloor-1$ of T_3. Assume n lies at position J_n on level k_n of T_3, namely, $n=N_{(k_n,J_n)}$. Then by $\alpha>1$ and Lemma 1(P1), $k_n\ge k_p+1$ and $J_n=\frac{n-1}{2}-2^{k_n}$. By Lemma 2(P3), C_l and C_r are represented in T_3 by

$$
\begin{aligned}
C_l&=\{N_{(k_p+1,2J_p)},N_{(k_p+2,4J_p+1)},N_{(k_p+2,8J_p+3)},\ldots,N_{(k_p+i,2^iJ_p+2^{i-1}-1)},\ldots\}\\
C_r&=\{N_{(k_p+1,2J_p+1)},N_{(k_p+2,4J_p+2)},N_{(k_p+3,8J_p+4)},\ldots,N_{(k_p+i,2^iJ_p+2^{i-1})},\ldots\}
\end{aligned}
$$

Assume $k_p+\sigma=k_n$; then the node on C_l and on level k_n is $N_{(k_n,2^\sigma J_p+2^{\sigma-1}-1)}$ and its distance to $n=N_{(k_n,J_n)}$ is given by

$$d=|\frac{N_{(k_n,2^\sigma J_p+2^{\sigma-1}-1)}-N_{(k_n,J_n)}}{2}|+1$$

That is

$$d=|2^\sigma J_p+2^{\sigma-1}-1-J_n|+1$$

$$d=\begin{cases}2^\sigma J_p+2^{\sigma-1}-J_n \quad ,N_{(k_n,2^\sigma J_p+2^{\sigma-1}-1)}>N_{(k_n,J_n)}\\ J_n-2^\sigma J_p-2^{\sigma-1}+2,N_{(k_n,2^\sigma J_p+2^{\sigma-1}-1)}<N_{(k_n,J_n)}\end{cases}$$

Now take an arbitrary node on C_l , say $N_{(k_p+i,2^iJ_p+2^{i-1}-1)}$ with $i>\sigma$; it can be seen that, when $N_{(k_n,2^\sigma J_p+2^{\sigma-1}-1)}>N_{(k_n,J_n)}$, the node $N_{(k_p+i,2^iJ_p+2^{i-1}-1)}-2(d-1)$ is the node on L_n that has distance d to

$N_{(k_p+i,2^i J_p+2^{i-1}-1)}$, whereas when $N_{(k_n,2^\sigma J_p+2^{\sigma-1}-1)} < N_{(k_n,J_n)}$, the node $N_{(k_p+i,2^i J_p+2^{i-1}-1)}+2(d(k_n)-1)$ is the node on L_n that has distance d to $N_{(k_p+i,2^i J_p+2^{i-1}-1)}$.

Note that, for the case $N_{(k_n,2^\sigma J_p+2^{\sigma-1}-1)} > N_{(k_n,J_n)}$, it holds

$$\begin{aligned}
&N_{(k_p+i,2^i J_p+2^{i-1}-1)}-2(d-1)\\
&=N_{(k_p+i,2^i J_p+2^{i-1}-1)}-2(2^\sigma J_p+2^{\sigma-1}-J_n-1)\\
&=2^{k_p+i+1}+2(2^i J_p+2^{i-1}-1)+1-2^{\sigma+1}J_p-2^\sigma+2J_n+2\\
&=2^{k_p+i+1}+2^{i+1}J_p+2^i-2+1-2^{\sigma+1}J_p-2^\sigma+2J_n+2\\
&=2^{k_p+i+1}+2^{i+1}J_p+2^i-2^{\sigma+1}J_p-2^\sigma+2J_n+1\\
&=2^i(2^{k_p+1}+2J_p+1)-2^{k_p+\sigma+1}+2^{k_p+\sigma+1}-2^{\sigma+1}J_p-2^\sigma+2J_n+1\\
&=2^i(2^{k_p+1}+2J_p+1)-2^\sigma(2^{k_p+1}+2J_p+1)+2^{k_p+\sigma+1}+2J_n+1\\
&=2^i(2^{k_p+1}+2J_p+1)-2^\sigma(2^{k_p+1}+2J_p+1)+(2^{k_n+1}+2J_n+1)\\
&=(2^i-2^\sigma)p+\alpha p
\end{aligned}$$

while for the case $N_{(k_n,2^\sigma J_p+2^{\sigma-1}-1)} < N_{(k_n,J_n)}$ it holds

$$\begin{aligned}
&N_{(k_p+i,2^i J_p+2^{i-1}-1)}+2(d-1)\\
&=N_{(k_p+i,2^i J_p+2^{i-1}-1)}+2((J_n-2^\sigma J_p-2^{\sigma-1}+2)-1)\\
&=2^{k_p+i+1}+2(2^i J_p+2^{i-1}-1)+1+2J_n-2^{\sigma+1}J_p-2^\sigma+2\\
&=2^{k_p+i+1}+2^{i+1}J_p+2^i-2+1+2J_n-2^{\sigma+1}J_p-2^\sigma+2\\
&=2^{k_p+i+1}+2^{i+1}J_p+2^i-2^{\sigma+1}J_p-2^\sigma+2J_n+1\\
&=2^i(2^{k_p+1}+2J_p+1)-2^{k_p+\sigma+1}+2^{k_p+\sigma+1}-2^{\sigma+1}J_p-2^\sigma+2J_n+1\\
&=2^i(2^{k_p+1}+2J_p+1)-2^\sigma(2^{k_p+1}+2J_p+1)+2^{k_p+\sigma+1}+2J_n+1\\
&=2^i(2^{k_p+1}+2J_p+1)-2^\sigma(2^{k_p+1}+2J_p+1)+(2^{k_n+1}+2J_n+1)\\
&=(2^i-2^\sigma)p+\alpha p
\end{aligned}$$

It is seen that, either $N_{(k_n,2^\sigma J_p+2^{\sigma-1}-1)} > N_{(k_n,J_n)}$ or $N_{(k_n,2^\sigma J_p+2^{\sigma-1}-1)} < N_{(k_n,J_n)}$ leads to that a node on L_n is of the form $(2^i-2^\sigma)p+\alpha p$, which is a multiple of *p*.

Property 8*. Let *p*>3 be an odd integer; then there are always odd integers of the form $(2^i-2^\sigma)p+\alpha p$ that are descendant nodes of T_p, where $\alpha>1$ is an odd integer and $i>\sigma\ge\lfloor\log_2 p\rfloor$.

Proof. Property 4 ensures $n=\alpha p$ reaches a descendant of T_p after penetrating downwards along a parallel connection by $\lfloor\log_2 \alpha p\rfloor-1=\lfloor\log_2\alpha+\log_2 p\rfloor-1\ge\lfloor\log_2 p\rfloor$ steps. The reasoning processes in proving property 8 show that the descendant is of the form $(2^i-2^\sigma+\alpha)p$ and $i>\sigma\ge\lfloor\log_2 p\rfloor$.

5 Applications in Integer Factorization

Property 7, Property 7*, and Property 8* indicate that an odd integer of the form $(2^{\alpha}-2^{\beta}+\gamma)p$ must be a descendant of the p-rooted tree, where $\gamma \ge 1$ and $p>3$ are positive odd integers, $\alpha>\beta$. This on the other hand mean that an odd integer *m* that has a divisor of the form $2^{\alpha}-2^{\beta}+\gamma$ can be factorized very soon. This section proves the related results.

5.1 Corollaries

Corollary 1. The divisor *p* of odd positive composite integer $m=pq$ can be found out in at most $O(1+\log_2 q)$ searching steps provided that $q=2^{\alpha}-1$ with integers $\alpha \ge \left\lfloor \frac{\log_2 m}{2} \right\rfloor +1$.

Proof. Referring to the particular cases in Property 7* knows that, an arbitrary positive odd integer $n>1$ results in $n+2(2^{\beta+\delta}-1)n=(2^{\beta+\delta+1}-1)n \in T_n$, where $\beta=\lfloor \log_2 n \rfloor$ and $\delta \ge 0$. This is equivalent to $(2^{\chi}-1)n \in T_n$ with integer $\chi \ge \lfloor \log_2 n \rfloor +1$. By $m=pq$, $q=2^{\alpha}-1$ and $\alpha \ge \left\lfloor \frac{\log_2 m}{2} \right\rfloor +1$, it follows

$$q \ge 2^{\left\lfloor \frac{\log_2 m}{2} \right\rfloor +1}-1 > 2^{\frac{\log_2 m}{2}}-1=\sqrt{m}-1 \Rightarrow q \ge \lfloor \sqrt{m} \rfloor \ge p \Rightarrow \left\lfloor \frac{\log_2 m}{2} \right\rfloor \ge \lfloor \log_2 p \rfloor$$

Let $\left\lfloor \frac{\log_2 m}{2} \right\rfloor = \lfloor \log_2 p \rfloor + \delta$ with $\delta \ge 0$; then it is known

$$\begin{cases} m=pq \\ q=2^{\alpha}-1 \\ \alpha \ge \lfloor \log_2 p \rfloor +\delta+1 \\ \delta \ge 0 \end{cases} \Rightarrow m \in T_p$$

Since *m* and *p* lie respectively on level $\lfloor \log_2 m \rfloor -1$ and level $\lfloor \log_2 p \rfloor -1$ of T_3, the difference is

$$\lfloor \log_2 q \rfloor \le \lfloor \log_2 m \rfloor - \lfloor \log_2 p \rfloor \le \lfloor \log_2 q \rfloor +1$$

Namely, it takes at most $\lfloor \log_2 q \rfloor +1$ searching steps for *m* to trace up to *q*.

Remark 3. The conclusion $q \ge \lfloor \sqrt{m} \rfloor \ge p$ in the reasoning process is the key. Accordingly, Corollary 1still holds if the condition $\alpha \ge \left\lfloor \frac{\log_2 m}{2} \right\rfloor +1$ is substituted with $\alpha \ge \lfloor \log_2 p \rfloor +1$ because

$$\alpha \ge \lfloor \log_2 p \rfloor +1 \Rightarrow q=2^{\alpha}-1 \ge 2^{\lfloor \log_2 p \rfloor +1}-1 > 2^{\log_2 p}-1=p-1 \Rightarrow q \ge p$$

Corollary 2. The divisor *p* of odd positive composite integer $m=pq \ge 9$ can be found out in at most $O(1+\lfloor \log_2 q \rfloor)$ searching steps provided that $q=2^{2\alpha+\beta}-2^{\alpha}+1$ with integers $\alpha \ge 1, \beta \ge \left\lfloor \frac{\log_2 m}{2} \right\rfloor$.

Proof. The given conditions yield

$$
\begin{aligned}
q &= 2^{2\alpha+\beta} - 2^{\alpha} + 1 \\
&\geq 2^{\left\lfloor \frac{\log_2 m}{2} \right\rfloor + 2\alpha} - 2^{\alpha} + 1 = 2^{\alpha}(2^{\left\lfloor \frac{\log_2 m}{2} \right\rfloor + \alpha} - 1) + 1 \\
&\geq 2^{\alpha}(2^{\left\lfloor \frac{\log_2 m}{2} \right\rfloor + 1} - 1) + 1 > 2^{\alpha}(2^{\frac{\log_2 m}{2}} - 1) + 1 = 2^{\alpha}(\sqrt{m} - 1) + 1 \\
\Rightarrow \frac{q}{\sqrt{m}} &> 2^{\alpha}(1 - \frac{1}{\sqrt{m}}) + \frac{1}{\sqrt{m}} \geq 2^{\alpha}(1 - \frac{1}{3}) + \frac{1}{\sqrt{m}} > 1
\end{aligned}
$$

which means

$$
p < q \Rightarrow p \leq \sqrt{m} \Rightarrow \log_2 p \leq \frac{\log_2 m}{2} \Rightarrow \lfloor \log_2 p \rfloor \leq \left\lfloor \frac{\log_2 m}{2} \right\rfloor
$$

Let $\beta = \left\lfloor \frac{\log_2 m}{2} \right\rfloor + \delta = \lfloor \log_2 p \rfloor + \omega$; then integers $\omega \geq 0$, $\delta \geq 0$ and $2^{2\alpha+\beta} - 2^{\alpha} + 1 = 2^{\lfloor \log_2 p \rfloor + \omega + 2\alpha} - 2^{\alpha} + 1$. By Property 7 it follows

$$
m = pq = (2^{\lfloor \log_2 p \rfloor + \omega + 2\alpha} - 2^{\alpha} + 1)p \in l(T_p)
$$

Since *m* and *p* lie respectively on level $\lfloor \log_2 m \rfloor - 1$ and $\lfloor \log_2 p \rfloor - 1$, it takes $\lfloor \log_2 m \rfloor - \lfloor \log_2 p \rfloor \leq \lfloor \log_2 q \rfloor + 1$ steps for *m* to trace up to *q*.

Remark 4. By substituting the condition $\beta \geq \left\lfloor \frac{\log_2 m}{2} \right\rfloor$ with $\beta \geq \lfloor \log_2 p \rfloor$, Corollary 2 still holds because

$$
\begin{aligned}
q &= 2^{2\alpha+\beta} - 2^{\alpha} + 1 \\
&\geq 2^{\lfloor \log_2 p \rfloor + 2\alpha} - 2^{\alpha} + 1 = 2^{\alpha}(2^{\lfloor \log_2 p \rfloor + \alpha} - 1) + 1 \\
&\geq 2^{\alpha}(2^{\lfloor \log_2 p \rfloor + 1} - 1) + 1 > 2^{\alpha}(2^{\log_2 p} - 1) + 1 = 2^{\alpha}(p - 1) + 1 \geq 2p - 1
\end{aligned}
$$

Corollary 3. The divisor *p* of odd positive composite integer $m = pq$ can be found out in at least $O(\log_2 q)$ and at most $O(\lfloor \log_2 m \rfloor)$ searching steps provided that $q = 2^{\alpha} - 2^{\beta} + \gamma$ with integers $\alpha > \beta > \lfloor \log_2 p \rfloor$ and odd integer $\gamma \geq 1$.

Proof. By Property 8*, an arbitrary odd integer of the form $m = (2^{\alpha} - 2^{\beta})p + \gamma p$ must be a descendant node of T_p. By $\alpha > \beta > \lfloor \log_2 p \rfloor$, it follows $q \geq 2^{\beta+1} - 2^{\beta} + \gamma = 2^{\beta} + \gamma > p$. Since obviously $q < \frac{m}{3}$, it yields

$$
\lfloor \log_2 q \rfloor \leq \left\lfloor \log_2 \frac{m}{3} \right\rfloor = \lfloor \log_2 m - \log_2 3 \rfloor \leq \lfloor \log_2 m \rfloor - 1
$$

Note that, *p* and *m* lie respectively on level $\lfloor \log_2 p \rfloor - 1$ and level $\lfloor \log_2 m \rfloor - 1$ of T_3, the difference between the two levels satisfies

$$
\lfloor \log_2 p \rfloor \leq \lfloor \log_2 q \rfloor \leq \lfloor \log_2 m \rfloor - \lfloor \log_2 p \rfloor \leq \lfloor \log_2 q \rfloor + 1 \leq \lfloor \log_2 m \rfloor
$$

and the corollary is validated.

5.2 Numerical experiments

Numerical experiments are made with Maple software. Table 1 lists the experimental results. In the table, the column ‘Big Number N’ is the big odd composite number to be factorized, the column ‘nDigits’ is the number of decimal digits, the column ‘sDivisor’ is the found divisor of N, the column ‘Tsteps’ is the number of searching steps calculated theoretically from the previous corollaries and the column ‘Rsteps’ is the real searching steps recorded by the computer. It can be seen that the real searching steps are exactly match to the theoretical steps. For readers to know the algorithms more deeply, the Maple programs are list in the appendix section. Readers can test them with the programs.

Table 1.

Big Number N	nDigits	sDivisor	Tsteps	Rsteps
13611294676837538749339910604792106573720569303980406995753	59	80000000000000001239	126	126
100433627766186892221372630609062766858404681029709092356097	59	618970019642690137449562111	106	106
36970860646792246757344801116631819016393505518278570670458580224861	68	217295189176711542778874311843	126	126
15591554295920093644358232049377238142052981863686538114062107392351	68	91638919976965192288826967713	126	126
215679573337205118357336031493686674815718346332418321765033807708157	69	1267650600228229401496702681091	126	126
27606985387162255149739023449107931668458716142620601169954803000803329	71	162259276829213363391578010288127	126	126
101345312745982312287461852810916277139253536353869833593151553211936321	71	595654213076100889780265054949823	126	126
260740604970814219042361048116398797676543695397537050426636276215371946505523582892895109067	93	162259276829213363391578010288127	200	199
273406340597876490546562778389702670667539240815895986601061536603385793897980093024134417319198667	99	170141183460469231731687303715884105727	200	199
467998186686678582633448624213918602485092274227885458664761758295410611935326445796738078604349487	99	4659775785220018543264560743076778192897	196	195

6 Conclusions and Future Work

By means of defining connection and penetration in a valuated binary tree, nodes out of a tree can be related with those in a tree and some outer properties are brought into the tree so that more properties of nodes are discovered. This broadens the studies on a tree. Research in this paper validates such means. It is seen from previous research and the research in this paper that, there is always a proper approach to factorize rapidly a certain kind of special odd integers. The theoretical analysis and numerical experiments in this paper once again demonstrate this point of view. However something is still very rough and there is still work to make it refinery. For example, the traits of α, β in the three corollaries still need further investigating to make their limits more accurate. This remains future studies to make them clear. Meanwhile, this paper merely draws a rough outline in studying the connections and penetrations, more subtle contents need further studying. Hope more young to join the work.

Acknowledgement

The research work is supported Natural Science Foundation of Guangdong Province under Grant No. 2018A0303130082.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Wang X. Valuated binary tree: A new approach in study of integers. International Journal of Scientific and Innovative Mathematical Research. 2016;4(3),63-67.
DOI: http://dx.doi.org/10.20431/2347-3142.0403008

[2] Wang X. Amusing properties of odd numbers derived from valuated binary tree. IOSR Journal of Mathematics. 2016;12(6 Ver5):53-57.

[3] Wang X. Two more symmetric properties of odd numbers. IOSR Journal of Mathematics. 2017;13(3 Ver.II):37-40.
DOI: https://dx.doi.org/10.9790/5728-1303023740

[4] Wang X. Genetic traits of odd numbers with applications in factorization of integers. Global Journal of Pure and Applied Mathematics. 2017;13(2):493-517.
DOI: http://www. ripublication.com/gjpam17/gjpamv13n2_29.pdf

[5] Wang X. T3 tree and its traits in understanding integers. Advances in Pure Mathematics. 2018;8(5):494-507.
DOI: https://doi.org/10.4236/apm.2018.85028

[6] Wang X, Guo H. Some divisibility traits on valuated binary trees. International Journal of Applied Physics and Mathematics. 2019;9(1):1-15.
DOI: https://doi:org/10.17706/ijapm.2019.9.4.173-181

[7] Wang X. Fast approach to factorize odd integers with special divisors. Journal of Mathematics and Statistics. 2020;16(1):24-34.
DOI: https://doi.org/10.3844/jmssp.2020.24. 34

[8] Wang X. Algorithm available for factoring big Fermat numbers. Journal of Software. 2020;15(3):86-97.
DOI: 10.17706/jsw.15.3.86-97

[9] Wang X. Bound estimation for divisors of RSA modulus with small divisor-ratio. International Journal of Network Security. 2021;23(3):412-425

[10] Dinesh PM, Sahni S. Handbook of data structures and applications. Chapman & Hall/CRC; 2005.

[11] Wang X. Frequently-used properties of the floor function. International Journal of Applied Physics and Mathematics. 2020;10(4):135-142.
DOI: http://doi.org/ 10.17706/ijapm. 2020.10.4.135-142

[12] Wang X, Zheng S. Some miscellaneous properties of valuated binary tree. Journal of Mathematics Research. 2021;13(3):1-12.
DOI: https://doi.org/10.5539/jmr.v13n3p1

Appendix

Maple Source Codes

SubRoutine Father (Calculate the father of a node Son)

```
Father:=proc( Son)
 local X, r;
 r:=modp(Son,4);
   if r=1 then X:= (Son+1)/2;
   else    X:= (Son -1)/2;
   fi
End proc
```

MainRoutine FactIt (Calculate the small divisor of N)

```
FactIt:=proc(N)
    local X, AA, g, p, q, Tsteps, Rsteps:=0, len;
  AA:=Father(N);
  g:=gcd(AA,N);
  while g=1 do
   Rsteps:=Rsteps+1;
   X:=AA;
   AA:=Father(X);
   g:=gcd(AA,N);
  od;
   p:=g;
  q:=N/p;
 Tsteps:=floor(evalf(log2(q))
 lprint("Find p=", p , " Tsteps=", Tsteps, "Rsteps=", Rsteps);
End proc
```


Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://www.sdiarticle4.com/review-history/69077