69-19,065

POGORZELSKI, Henry Andrew, 1922-
GOLDBACH SENTENCES IN ABSTRACT ARITHMETICS ak (A).

The City University of New York, Ph.D., 1969
Mathematics

University Microfilms, Inc., Ann Arbor, Michigan

GOLDBACH SENTENCES IN ABSTRACT ARITHMETICS $\mathcal{A}^k(A)$

by

H. A. Pogorzelski

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

GOLDBACH SENTENCES IN ABSTRACT ARITHMETICS $\mathcal{A}^k(A)$

by

H. A. Pogorzelski

This manuscript has been read and accepted for the University Committee in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

April 29, 1969
date

Raymond Smullyan
Chairman of Examining Committee
Professor Raymond Smullyan

April 29, 1969
date

Eldon Dyer
Executive Officer
Professor Eldon Dyer

Professor Louis Auslander

Dr. Charles Barton

Supervisory Committee

PREFACE

There are presently three main ways of attacking the celebrated Goldbach conjecture: (i) the approach introduced by Euler and Sylvester [3, 12], involving partitions and asymptotic formulas leading to various other analytic techniques; (ii) the approach introduced by Brun [1], involving generally the so-called elementary techniques; (iii) the latest approach introduced by Kemeny [6], involving model-theoretic techniques. It is the purpose of this work to introduce a fourth approach to the Goldbach conjecture, namely, one involving abstract word-theoretic techniques concerning Goldbach sentences in abstract arithmetics $\mathcal{A}^k(A)$ $(k \geq 0)$ on commutative free monoids with an infinite number of generators. To a degree, our approach has contacts with each of the above-mentioned approaches. Goldbach sentences in arithmetic $\mathcal{A}^k(A)$ $(k \geq 0)$ correspond exactly to the usual Goldbach conjecture in certain arithmetizations of $\mathcal{A}^k(A)$.

Among various other results, we show the following. (1) For any $k \geq 0$, if a Goldbach sentence is a theorem in arithmetic $\mathcal{A}^k(A)$, then the Goldbach conjecture is true. (2) For any $k \geq 0$, if all Goldbach sentences in an arithmetic $\mathcal{A}^k(A)$ are independent of $\mathcal{A}^k(A)$, then the Goldbach conjecture is independent of arithmetic $\mathcal{A}^k(A)$. (3) For any $k \geq 0$, there are an infinite number of different Goldbach sentences in each arithmetic $\mathcal{A}^k(A)$. (4) We give a general classification of all Goldbach sentences in each arithmetic $\mathcal{A}^k(A)$ $(k \geq 0)$. (5) For a certain constant $\beta_2 \geq 3$, there exist Goldbach sentences in an infinite number of arithmetics $\mathcal{A}^k(A)$ $(k \geq \beta_2)$ which are independent of $\mathcal{A}^k(A)$ $(k \geq \beta_2)$ respectively. (6) We show that arithmetics $\mathcal{A}^k(A)$ $(k \geq 0)$ are simultaneous abstractions of both the multiplicative arithmetic of the prime numbers and the arithmetic of partitions (partitio numerorum). (7) We show that there exists a weakened form of the Goldbach conjecture which is false.

CONTENTS

CHAPTER 1

HILBERT-ACKERMANN NUMBER-SYSTEMS

§1.1. Hilbert-Ackermann functions

As in (4,5), the Hilbert-Ackermann functions $\xi_1(x,y) = x^y$, $\xi_2(x,y)$, ... are defined by the following equations for $k \geq 1$:

$$\xi_{k+1}(x,0) = 1,$$
$$\xi_{k+1}(x,y+1) = \xi_k(x, \xi_{k+1}(x,y)).$$

We also include $\xi_0(x,y) = x \cdot y$ to the Hilbert-Ackermann functions.

We introduce the complementary number-systems Q^k $(k \geq 0)$ as follows:

$$Q^k = \{ \xi_k(x,y) \mid x>1,\ y>1 \} \qquad (k \geq 0).$$

1.1.1. Lemma. $Q^k \supset Q^{k+1}$ $(k \geq 0)$.

The proof is by induction. Clearly, $Q^0 \supset Q^1$, since every element of Q^1 is not a prime number. Next, suppose for some k that $Q^k \supset Q^{k+1}$. In turn, assume that $z = \xi_{k+2}(x,y)$. If $y = 2$ then $z = \xi_{k+2}(x,2)$ and $z \in Q^{k+1}$, since $\xi_{k+1}(x,x) = z$. If $y = w+1$ then $z = \xi_{k+2}(x,w+1)$ and $z \in Q^{k+1}$, since $\xi_{k+1}(x, \xi_{k+2}(x,w)) = \xi_{k+2}(x,w+1)$. Therefore, $Q^{k+1} \supset Q^{k+2}$.

1.1.2. Lemma. For $k \geq 0$, we have $4 \in Q^k$.

Since 4 is not a prime number, we have $4 \in Q^0$. Also, $\xi_1(2,2) = 4$, hence $4 \in Q^1$. Suppose now that $\xi_k(2,2) = 4$. Then $\xi_{k+1}(2,2) = \xi_k(2, \xi_{k+1}(2,1)) = \xi_k(2,2) = 4$. Therefore, if $4 \in Q^k$ then $4 \in Q^{k+1}$.

1.1.3. Lemma. For $k \geq 1$ and $x \geq 2$, $\xi_k(x, y) > 0$.

For $x \geq 2$, $\xi_1(x, y) = x^y > 0$. Suppose $\xi_k(x, y) > 0$ for some k. Then $\xi_{k+1}(x, 0) = 1 > 0$ and $\xi_{k+1}(x, y+1) = \xi_k(x, \xi_{k+1}(x, y)) > 0$ by the inductive hypothesis.

1.1.4. Lemma. For $k \geq 1$ and $x \geq 2$, if $\xi_k(x, y) = \xi_k(x, 0)$ then $y = 0$.

Consider the case $k = 1$. Clearly, if $x^y = x^0$ then $y = 0$. Assume that the lemma is true for some k and assume that $\xi_{k+1}(x, y) = \xi_{k+1}(x, 0)$. If $y > 0$ then $y = z+1$. Therefore, $\xi_{k+1}(x, z+1) = \xi_{k+1}(x, 0) = \xi_k(x, 0)$, i.e., $\xi_k(x, \xi_{k+1}(x, z)) = \xi_k(x, 0)$, and by the inductive hypothesis $\xi_{k+1}(x, z) = 0$. However, this contradicts Lemma 1.1.3. Consequently, we must have $y = 0$.

1.1.5. Lemma. For $k \geq 1$ and $x \geq 2$, if $\xi_k(x, y) = \xi_k(x, z)$ then $y = z$.

First, consider the case $k = 1$. If $\xi_1(x, y) = \xi_1(x, z)$, i.e., $x^y = x^z$, then clearly $y = z$. Assume that the lemma holds for some k. In turn, let $\xi_{k+1}(x, y) = \xi_{k+1}(x, z)$. If $y = z$ then clearly the lemma is true. If $y > z$ and $z = 0$, we have $y = 0$ by Lemma 1.1.4. Consequently, there are y_1 and z_1 such that $y = y_1+1$, $z = z_1+1$ and $y_1 > z_1$. From $\xi_{k+1}(x, y_1+1) = \xi_{k+1}(x, z_1+1)$, we obtain $\xi_k(x, \xi_{k+1}(x, y_1)) = \xi_k(x, \xi_{k+1}(x, z_1))$ and by the inductive hypothesis $\xi_{k+1}(x, y_1) = \xi_{k+1}(x, z_1)$. Repeating this z-times we get $\xi_{k+1}(x, y-z) = \xi_{k+1}(x, 0)$. Then, by Lemma 1.1.4, we have $y-z = 0$, i.e., $y = z$. The case $y < z$ is carried out similarly.

1.1.6. Lemma. For $k \geq 1$, $x \geq 2$ and $y \geq 2$, we have (1) $\xi_k(x, y) > y+1$ and (2) $\xi_k(x, y) > \xi_k(x, y-1) + 1$.

We consider the case $k = 1$. We have to prove: (i) $x^y > y+1$ for $x \geq 2$ and $y \geq 2$; (ii) $x^y > x^{y-1} + 1$ for $x \geq 2$ and $y \geq 2$. Firstly, the

relation $x^2 > 3$ for $x \geq 2$ is clear. Assume that $x^n > n+1$ for $x \geq 2$ and $n \geq 2$. Then $x^{n+1} = x^n \cdot x > (n+1)x > 2(n+1) > n+2$. This proves (i). Clearly $x^2 = x \cdot x \geq x \cdot 2 = x+x > x+1$. Assume $x^n > x^{n-1} + 1$. Then $x^{n+1} = x^n \cdot x > (x^{n-1}+1)x = x^n + x > x^n + 1$. This proves (ii).

In turn, for some k, let (1) and (2) of the lemma be true. Clearly, $\xi_{k+1}(x, y) = \xi_{k+1}(x, (y-1)+1) = \xi_k(x, \xi_{k+1}(x, y-1))$. From (1), by the inductive hypothesis, we obtain $\xi_{k+1}(x, y) > \xi_{k+1}(x, y-1) + 1$. This proves (ii). On the other hand, by (2), we get

$$(3) \qquad \xi_{k+1}(x, y) > \xi_{k+1}(x, y-1) + 1 \ .$$

Since $\xi_{k+1}(x, y-1) = \xi_k(x, \xi_{k+1}(x, y-2))$ $(y \geq 2)$, we obtain $\xi_{k+1}(x, y-1) > \xi_{k+1}(x, y-1) + 1$, i.e., $\xi_{k+1}(x, y) > \xi_{k+1}(x, y-2) + 2$, by (1). For $y = 2$, this gives $\xi_{k+1}(x, 2) > \xi_{k+1}(x, 0) + 2 = 3$, i.e., $\xi_{k+1}(x, 2) > 2 + 1$. Let $\xi_{k+1}(x, n) > n+1$. By (3) we then obtain $\xi_{k+1}(x, n+1) > \xi_{k+1}(x, n) + 1 > (n+1) + 1$, i.e., $\xi_{k+1}(x, y) > y+1$.

1.1.7. Lemma. For $k \geq 1$, $x \geq 2$, $z_1 \geq 2$ and $z_2 \geq 2$, if $\xi_k(x, z_1) = \xi_{k+1}(x, z_2)$ then $z_1 > z_2$.

Since $z_2 \geq 2$, let $z_2 = z_3 + 1$. Consequently, we have $\xi_k(x, z_1) = \xi_{k+1}(x, z_3+1) = \xi_k(x, \xi_{k+1}(x, z_3))$. By Lemma 1.1.5, we obtain $z_1 = \xi_{k+1}(x, z_3)$, and by Lemma 1.1.6, we get $z_1 > z_3+1$. Therefore, $z_1 > z_2$.

1.1.8. Lemma. For $x \geq 2$ and $k \geq 1$, $\xi_k(x, y) = x$ if and only if $y = 1$.

Let $y = 1$. Then $\xi_1(x, 1) = x$. Assume that $\xi_k(x, 1) = x$. Then $\xi_{k+1}(x, 1) = \xi_k(x, \xi_{k+1}(x, 0)) = \xi_k(x, 1) = x$.

On the other hand, assume that $\xi_k(x, y) = x$. For $k = 1$, we have $x^y = x$ and since $x \geq 2$ this gives $y = 1$. Suppose that for some $k \geq 1$, if $\xi_k(x, y) = x$ then $y = 1$. Let $\xi_{k+1}(x, y) = x$. We cannot have $y = 0$, since $\xi_{k+1}(x, 0) = 1$. Therefore, let $y = y_1 + 1$. Then we have

$$\Xi^{(k)}_{1\leq r\leq 1} x_r = x_1 \ ,$$

$$\Xi^{(k)}_{1\leq r\leq \mu+1} x_r = \xi_k(x_{\mu+1}, \Xi^{(k)}_{1\leq r\leq \mu} x_r) \ ,$$

and we let

$$\Xi^{(0)}_{1\leq r\leq \mu} x_r =_{\text{Def}} \prod_{1\leq r\leq \mu} x_r \ .$$

When using elements in the Hilbert-Ackermann number-systems P^k, a convenient notation for $\Xi^{(k)}_{1\leq r\leq \mu} p^{(k)}_r$ is the following concatenative notation:

$$p^{(k)}_{i_\mu} p^{(k)}_{i_{\mu-1}} \ldots p^{(k)}_{i_2} p^{(k)}_{i_1} =_{\text{Def}} \Xi^{(k)}_{1\leq r\leq \mu} p^{(k)}_{i_r} \quad (k \geq 0) \ .$$

For example, $p^{(0)}_{i_1} p^{(0)}_{i_2} p^{(0)}_{i_3} = p_{i_1} \times p_{i_2} \times p_{i_3}$ (ordinary multiplication)

$p^{(1)}_{i_1} p^{(1)}_{i_2} p^{(1)}_{i_3} = \xi_1(p^{(1)}_{i_1}, \xi_1(p^{(1)}_{i_2}, p^{(1)}_{i_3}))$ (ordinary exponentiation), and so on.

We recall [8, 9] the author's unique resolution theorems with respect to the Hilbert-Ackermann number-systems:

1.2.4. Theorem. For any $k > 0$, every positive integer $n > 1$ can be uniquely expressed in unique order as $n = p^{(k)}_{i_1} p^{(k)}_{i_2} \ldots p^{(k)}_{i_\mu}$, where $p^{(k)}_{i_1}, p^{(k)}_{i_2}, \ldots, p^{(k)}_{i_\mu} \in P^k$.

This theorem was proved by the author using noncommutative free monoids with an infinite number of generators.

Note, we can express the familiar prime-number unique resolution theorem as follows:

1.2.5. Theorem. For $k = 0$, every positive integer $n > 1$ can be uniquely expressed in nonunique order as $n = p^{(k)}_{i_1} p^{(k)}_{i_2} \ldots p^{(k)}_{i_\mu}$, where $p^{(k)}_{i_1}, \ldots, p^{(k)}_{i_\mu} \in P^k$.

We conclude this section with a short Table of some initial elements in the Hilbert-Ackermann number-systems P^0, P^1, P^2 and P^3, in which the rows contain equal numbers:

Value	P^0	P^1	P^2	P^3
2	$p_1^{(0)}$	$p_1^{(1)}$	$p_1^{(2)}$	$p_1^{(3)}$
3	$p_2^{(0)}$	$p_2^{(1)}$	$p_2^{(2)}$	$p_2^{(3)}$
4	2×2	$\xi_1(2,2)$	$\xi_2(2,2)$	$\xi_3(2,2)$
5	$p_3^{(0)}$	$p_3^{(1)}$	$p_3^{(2)}$	$p_3^{(3)}$
6	2×3	$p_4^{(1)}$	$p_4^{(2)}$	$p_4^{(3)}$
7	$p_4^{(0)}$	$p_5^{(1)}$	$p_5^{(2)}$	$p_5^{(3)}$
8	2×2×2	$\xi_1(2,3)$	$p_6^{(2)}$	$p_6^{(3)}$
9	3×3	$\xi_1(3,2)$	$p_7^{(2)}$	$p_7^{(3)}$
10	2×5	$p_6^{(1)}$	$p_8^{(2)}$	$p_8^{(3)}$
11	$p_5^{(0)}$	$p_7^{(1)}$	$p_9^{(2)}$	$p_9^{(3)}$
12	3×2×2	$p_8^{(1)}$	$p_{10}^{(2)}$	$p_{10}^{(3)}$
13	$p_6^{(0)}$	$p_9^{(1)}$	$p_{11}^{(2)}$	$p_{11}^{(3)}$
14	2×7	$p_{10}^{(1)}$	$p_{12}^{(2)}$	$p_{12}^{(3)}$
15	3×5	$p_{11}^{(1)}$	$p_{13}^{(2)}$	$p_{13}^{(3)}$
16	2×2×2×2	$\xi_1(2, \xi_1(2,2)$	$\xi_2(2,3)$	$p_{14}^{(3)}$
17	$p_7^{(0)}$	$p_{12}^{(1)}$	$p_{14}^{(2)}$	$p_{15}^{(3)}$
18	2×3×3	$p_{13}^{(1)}$	$p_{15}^{(2)}$	$p_{16}^{(3)}$
19	$p_8^{(0)}$	$p_{14}^{(1)}$	$p_{16}^{(2)}$	$p_{17}^{(3)}$
20	2×2×5	$p_{15}^{(1)}$	$p_{17}^{(2)}$	$p_{18}^{(3)}$
21	3×7	$p_{16}^{(1)}$	$p_{18}^{(2)}$	$p_{19}^{(3)}$
22	2×11	$p_{17}^{(1)}$	$p_{19}^{(2)}$	$p_{20}^{(3)}$
23	$p_9^{(0)}$	$p_{18}^{(1)}$	$p_{20}^{(2)}$	$p_{21}^{(3)}$
24	2×2×2×3	$p_{19}^{(1)}$	$p_{21}^{(2)}$	$p_{22}^{(3)}$
25	5×5	$\xi_1(5,2)$	$p_{22}^{(2)}$	$p_{23}^{(3)}$
26	2×13	$p_{20}^{(1)}$	$p_{23}^{(2)}$	$p_{24}^{(3)}$
27	3×3×3	$\xi_1(3,3)$	$\xi_2(3,2)$	$p_{25}^{(3)}$

$\xi_{k+1}(x, y_1+1) = x$, i.e., $\xi_k(x, \xi_{k+1}(x, y_1)) = x$. By the inductive hypothesis, we get $\xi_{k+1}(x, y_1) = 1 = \xi_{k+1}(x, 0)$. By Lemma 1.1.5, we obtain $y_1 = 0$, i.e., $y = 1$.

1.1.9. Proposition. For any $k \geq 0$, Q^k is infinite and has an infinite complement.

The set Q^0 trivially satisfies the theorem. For $k \geq 1$, since $Q^k = \{\xi_k(x, y) \mid x > 1, y > 1\}$ and $\xi_k(2, 2) > 0$ by Lemma 1.1.3, we obtain the inequality $\xi_k(x, y+1) > \xi_k(x, y) + 1$ for $x \geq 2$ and $y \geq 1$, by virtue of (2) of Lemma 1.1.6. Therefore, $\xi_k(2, y)$ is a monotonically increasing sequence such that between $\xi_k(2, y)$ and $\xi_k(2, y+1)$ there is at least one positive integer. This proves that Q^k is infinite. Since $Q^0 \subset Q^k$ $(k \geq 1)$, the complement of Q^0 is contained in the complement of Q^k $(k \geq 1)$. Since the complement of Q^0 is infinite, it follows that every complement of Q^k is also infinite.

1.1.10. Lemma. For $k \geq 1$, $x \geq 2$ and $y \geq 1$, we have $\xi_k(x, y) \geq 2$.

This lemma follows from Lemma 1.1.6.

1.1.11. Lemma. For $k \geq 1$, $x \geq 2$ and $y \geq 2$, we have $\xi_k(x, y) > x$.

For $k = 1$, we have $x^y \geq x^2 > x$, since $y \geq 2$ and $x \geq 2$. Let the lemma hold for some k. Then, by Lemma 1.1.10, $\xi_{k+1}(x, (y-1) + 1) = \xi_k(x, \xi_{k+1}(x, y-1))$ and $\xi_{k+1}(x, y-1) \geq 2$. By the inductive hypothesis, $\xi_k(x, z) > x$ if $x \geq 2$ and $z \geq 2$, consequently $\xi_{k+1}(x, y) > x$.

1.1.12. Lemma. For some $k \geq 1$, $x \geq 2$, $z_1 \geq 2$, $z_2 \geq 2$ and $n \geq 1$, if $\xi_k(x, z_1) = \xi_{k+n}(x, z_2)$ then $z_1 > z_2$.

For $n = 1$, the lemma is true by virtue of Lemma 1.1.7. Assume that the lemma is true for some n, and let $\xi_k(x, z_1) = \xi_{k+n+1}(x, z_2)$. Since

$\xi_{k+n+1}(x, z_2) = \xi_{k+n}(x, \xi_{k+n+1}(x, z_2-1))$, we obtain by Lemma 1.1.10 $\xi_{k+n+1}(x, z_2-1) \geq 2$ and $z_1 > \xi_{k+n+1}(x, z_2-1)$. We have to consider the cases $z_2 > 2$ and $z_2 = 2$. If $z_2 > 2$, then by (1) of Lemma 1.1.6 we obtain $\xi_{k+n+1}(x, z_2-1) > (z_2-1) + 1 = z_2$, i.e., $z_1 > z_2$. Next, assume that $z_2 = 2$. Then $z_1 > \xi_{k+n+1}(x,1) = x$. Since $x \geq 2$, we obtain $z_1 > 2$, i.e., $z_1 > z_2$.

1.1.13. Theorem. If $n \neq 4$, then there exists a k such that $n \notin Q^k$ and $n \notin Q^h$ for all $h > k$.

Suppose that $n \in Q^k$ for all $k \geq 0$. Since $n \in Q^0$, this means that n is not a prime number. Moreover, there is a double sequence (u_i, v_i), where $u_i \geq 2$ and $v_i \geq 2$, such that $n = \xi_i(u_i, v_i)$ $(i \geq 1)$. By Lemma 1.1.6 and Lemma 1.1.10, $n > v_i+1$ and $n > u_i (i \geq 1)$. Consequently, an infinite number of the v_i must be equal and also an infinite number of the u_i must be equal. Therefore, there is an infinite number of indices $i_1 < i_2 < \ldots$ and two fixed numbers s and t such that $\xi_{i_a}(s, t) = n$ $(a \geq 1)$. From $\xi_{i_1}(s, t) = \xi_{i_2}(s, t)$ $(i_1 < i_2)$, by Lemma 1.1.12 we obtain the contradiction $t > t$.

§1.2. Hilbert-Ackermann number-systems

We introduce the Hilbert-Ackermann number-systems P^k $(k \geq 0)$ as follows:

$$P^k =_{\text{Def}} N^{(2)} \setminus Q^k \quad (k \geq 0)$$

where $N^{(2)} = \{2, 3, 4, 5, \ldots\}$. We denote the elements of P^k as:

$$P^k = \{p_1^{(k)}, p_2^{(k)}, p_3^{(k)}, \ldots\} \quad (k \geq 1) \ .$$

We include the set of all prime numbers as a Hilbert-Ackermann number-system, which we denote as:

$$P^0 = \{p_1^{(0)}, p_2^{(0)}, p_3^{(0)}, \ldots\} \ ,$$

where $p_1^{(0)} = 2$. In the case of prime numbers it is convenient to denote them also as follows:

$$P^0 = \{ p_1, p_2, p_3, \cdots \}.$$

1.2.1. Theorem. $P^k \subset P^{k+1}$ $(k \geq 0)$.

This theorem follows from Lemma 1.1.1.

1.2.1.1. Corollary. $P^0 \subset P^k$ $(k \geq 1)$.

1.2.1.2. Corollary. If $m < n$, then

$$\{ p_1^{(m)}, p_2^{(m)}, \cdots \} \subset \{ p_1^{(n)}, p_2^{(n)}, \cdots \}.$$

If $\{ p_1^{(m)}, p_2^{(m)}, \cdots \} = \{ p_{i_1}^{(n)}, p_{i_2}^{(n)}, \cdots \}$, where $p_k^{(m)} = p_{i_k}^{(n)}$, then we say that P^m is written in the numbering of P^n, and we denote this renumbering as $[P^m]^n$ and denote the elements of $[P^m]^n$ as $[p_\mu^{(m)}]^{(n)}$.

1.2.2. Theorem. For every positive integer $n \neq 1$ and $n \neq 4$, there exists a k such that $n \in P^k$ and $n \in P^h$ for all $h > k$.

This theorem follows from Theorem 1.1.13.

1.2.3. Proposition. For any $k \geq 0$, there exist an infinite number of positive integers which are not contained in P^k.

This proposition follows from Proposition 1.1.9.

We define the arithmetical chains

$$\prod_{1 \leq r \leq \mu}^{(k)} x_r \quad (k \geq 1)$$

by the following equations for $k \geq 1$:

§1.3. Brun number-system

We introduce the Brun number-system B as follows:

$$B =_{Def} \{x \mid x \neq 1,\ x = p_{i_1} p_{i_2} \cdots p_{i_\mu},\ p_{i_1}, p_{i_2}, \ldots, p_{i_\mu} \in P^0,\ 1 \leq \mu \leq 9\} .$$

We call the elements in B the Brun almost-prime numbers.

In order to prove a relation between the Brun number-system and the Hilbert-Ackermann number-systems we need the following lemmas.

1.3.1. Lemma. For any $k > 0$ and $r \geq 1$, if $n = p_{i_r}^{(k)} p_{i_{r-1}}^{(k)} \cdots p_{i_1}^{(k)}$, where $p_{i_1}^{(k)}, \ldots, p_{i_r}^{(k)}$ are not all equal, then $n \in P^{k+1}$.

Let the assumption of the theorem hold. On the strength of Theorem 1.2.4, let

$$n = p_{j_s}^{(k+1)} p_{j_{s-1}}^{(k+1)} \cdots p_{j_1}^{(k+1)} \quad (s \geq 1) .$$

We shall show that $s = 1$. For convenience, let $p_\mu^{(k+1)} = p_{j_s}^{(k+1)}$ and let $y = p_{j_{s-1}}^{(k+1)} \cdots p_{j_1}^{(k+1)}$. Consider

$$n = p_{i_r}^{(k)} p_{i_{r-1}}^{(k)} \cdots p_{i_1}^{(k)} = p_\mu^{(k+1)} y ,$$

and in turn

$$\xi_k(p_{i_r}^{(k)}, p_{i_{r-1}}^{(k)} \cdots p_{i_1}^{(k)}) = \xi_{k+1}(p_\mu^{(k+1)}, y) = \xi_k(p_\mu^{(k+1)}, \xi_{k+1}(p_\mu^{(k+1)}, y-1)) .$$

On the strength of Theorem 1.2.4, let

$$p_\mu^{(k+1)} = p_{h_t}^{(k)} p_{h_{t-1}}^{(k)} \cdots p_{h_1}^{(k)} .$$

Consequently, we have

(1) $$\xi_k(p_{i_r}^{(k)}, p_{i_{r-1}}^{(k)} \cdots p_{i_1}^{(k)}) = \xi_k(p_{h_t}^{(k)} p_{h_{t-1}}^{(k)} \cdots p_{h_1}^{(k)}, \xi_{k+1}(p_\mu^{(k+1)}, y-1)) .$$

Again, by Theorem 1.24, we must have

$$p_{i_r}^{(k)} = p_{h_t}^{(k)}, p_{i_{r-1}}^{(k)} = p_{h_{t-1}}^{(k)}, \ldots, p_{i_1}^{(k)} = p_{h_1}^{(k)} .$$

Therefore, from (1), it follows that

$$\xi_{k+1}(p_\mu^{(k+1)}, y-1) = 1 ,$$

and by the definition of Hilbert-Ackermann functions it follows that $y-1 = 0$ or $y = 1$, i.e., $s = 1$. Hence, $n = p_\mu^{(k+1)}$ and $n \in P^{k+1}$.

1.3.2. Lemma. For any $r > 1$, if $\gcd(a_1, a_2, \ldots, a_r) = 1$ and $n = p_{i_1}^{a_1} p_{i_2}^{a_2} \ldots p_{i_r}^{a_r}$, where $i_1, \ldots, i_r$ are all distinct, then $n \in P^1$.

Assume that $n \notin P^1$. Hence, $n \in Q^1$ and $n = \xi_1(x, y) = x^y$ $(x > 1, y > 1)$ by the definition of Q^1. By the ordinary unique factorization Theorem 1.2.5, we have

$$x^y = (p_{i_1}^{\beta_1} p_{i_2}^{\beta_2} \ldots p_{i_r}^{\beta_r})^y = p_{i_1}^{a_1} \ldots p_{i_r}^{a_r} ,$$

and from $y > 1$, we obtain the contradiction that $\gcd(a_1, \ldots, a_r) \neq 1$.

1.3.3. Lemma. For any $r > 1$, if $\gcd(a_1, \ldots, a_r) = 1$, $n = (p_{i_1}^{a_1} \ldots p_{i_r}^{a_r})^\beta$, where $\beta \in P^1$ and $i_1, \ldots, i_r$ are distinct, and $p_{i_1}^{a_1} \ldots p_{i_r}^{a_r} \neq \beta$, then $n \in P^2$.

By Lemma 1.3.2 and the assumption of the theorem, we obtain $p_{i_1}^{a_1} \ldots p_{i_r}^{a_r} \in P^1$. Let $p_\mu^{(1)} = p_{i_1}^{a_1} \ldots p_{i_r}^{a_r}$ and $p_\nu^{(1)} = \beta$. Consequently, we have $(p_{i_1}^{a_1} \ldots p_{i_r}^{a_r})^\beta = p_\mu^{(1)} p_\nu^{(1)}$. Since $p_\mu^{(1)} \neq p_\nu^{(1)}$ by assumption, we obtain $p_\mu^{(1)} p_\nu^{(1)} \in P^2$, i.e., $n \in P^2$, by virtue of Lemma 1.3.1.

1.3.4. Lemma. For any $r \geq 1$ and $k \geq 0$,
$$\xi_{k+1}(p_\mu^{(k)}, r) = p_\mu^{(k)} p_\mu^{(k)} \ldots p_\mu^{(k)} \quad (p_\mu^{(k)} \text{ r-times}).$$

This lemma follows directly from the definition of Hilbert-Ackermann functions.

1.3.5. Lemma. For any $p_\mu \in P^0$, we have the following properties: (1) if $n = 1, 6, 8, 9$ then $\xi_1(p_\mu, n) \in P^2$, (2) if $n = 3, 5, 7$ and $p_\mu \neq n$ then $\xi_1(p_\mu, n) \in P^2$, (3) if $p_\mu = 3, 5, 7$ then $\xi_1(p_\mu, p_\mu) \in P^3$, (4) if $p_\mu \neq 2$ then $\xi_1(p_\mu, 4) \in P^2$, (5) if $p_\mu = 2$ then $\xi_1(p_\mu, 4) \in P^3$.

For property (1), since $8 = \xi_1(2, 3)$, $9 = \xi_1(3, 2)$ and $6 \in P^1$, we have $\xi_1(p_\mu, n) \in P^2$ by Lemma 1.3.1 and Theorem 1.2.1.

For property (2), since $n \in P^0$ and $p_\mu \neq n$, we have $\xi_1(p_\mu, n) \in P^2$ by Lemma 1.3.1.

For property (3), since $\xi_1(p_\mu, p_\mu) = \xi_2(p_\mu, 2)$ by Lemma 1.3.4, we have $\xi_1(p_\mu, p_\mu) \in P^3$ by Lemma 1.3.1.

For property (4), since $\xi_1(p_\mu, 4) = \xi_1(p_\mu, \xi_1(2, 2))$, we have $\xi_1(p_\mu, 4) \in P^2$ by Lemma 1.3.1.

For property (5), we have $\xi_1(2, 4) = \xi_1(2, \xi_1(2, 2)) = \xi_2(2, 3)$ and $\xi_2(2, 3) \in P^3$ by Lemma 1.3.1.

1.3.6. Theorem. $B \subset P^3 \cup \{4\}$.

In accordance to B, we have to consider all possible products of the form
$$p_{i_1}^{a_1} p_{i_2}^{a_2} \ldots p_{i_r}^{a_r} \qquad (1 \leq r \leq 9),$$
where $r \leq a_1 + a_2 + \ldots + a_r \leq 9$ $(1 \leq r \leq 9)$. When r satisfies $2 \leq r \leq 9$, we clearly have the greatest common divisors $\gcd(a_1, a_2, \ldots, a_r) = 1, 2, 3$ or 4. There are 96 different possibilities to consider and we dispose of them as

follows.

(i) The Brun almost-primes where r satisfies $2 \leq r \leq 9$ and the greatest common divisor $\gcd(a_1, a_2, \ldots, a_r)$ is equal to 1, 2 or 3 belong to P^1 or P^2 by Lemma 1.3.2 and Lemma 1.3.3 and hence belong to P^3 by Theorem 1.2.1.

(ii) The Brun almost-primes with property $\gcd(a_1, \ldots, a_r) = 4$ turns out to be a single case, namely, $p_{i_1}^4 \cdot p_{i_2}^4 = \xi_1(p_{i_1} p_{i_2}, \xi_1(2,2))$ and by Lemma 1.3.2 and Lemma 1.3.1 it belongs to P^2, and so in P^3 by Theorem 1.2.1.

(iii) With the exception of $\xi_1(2,2) \in B$, all the Brun almost-primes with $r = 1$, i.e., $p_{i_1}^{a_1}$ $(1 \leq a_1 \leq 9)$, are exactly accounted for by Lemma 1.3.5, which means that they are either in P^2 or P^3 and therefore in P^3 by Theorem 1.2.1.

(iv) The final case $\xi_1(2,2) = 4$ certainly satisfies $4 \in P^3 \cup \{4\}$.

From the above, it follows that all elements in B are contained in $P^3 \cup \{4\}$. On the other hand, it is clear that $B \not\supset P^3 \cup \{4\}$, since P^3 contains prime-number products of length greater than 9.

§1.4. Partition number systems

Let S denote any set of positive integers. We define the partition number-systems $G(S)$ by the following three conditions: (1) For any $s_1, s_2 \in S$, if s_1+s_2 is an even number, then $s_1+s_2 \in G(S)$. (2) If $e \in G(S)$, then e is an even number and $e = s_1+s_2$ for some $s_1, s_2 \in S$. (3) $G(S)$ contains only the elements prescribed by conditions (1) and (2).

In other words, $G(S)$ consists of all even ordinary sums s_1+s_2, where s_1 and s_2 are in the set S.

Let E^n denote the set of all even numbers greater than the positive integer n.

By ordinary arithmetic, we clearly have $E^4 \supseteq G(P^0 \setminus \{2\})$. The

Goldbach conjecture claims that the following relation holds:

$$E^4 = G(P^0 \setminus \{2\}) \ .$$

We now state a corollary of a well-known theorem due to Brun [1]:

1.4.1. Theorem. There exists a positive-integer constant β_1, called the first Brun constant, for which we have the relation $E^{\beta_1} \subset G(B)$, where B is the Brun number-system.

The following is a consequence of Theorem 1.4.1, Theorem 1.3.6, Theorem 1.2.2 and Theorem 1.2.1.

1.4.2. Theorem. There exists a constant $\beta_2 \geqslant 3$, called the second Brun constant, for which we have the equality $E^4 = G(P^{\beta_2} \setminus \{2\})$.

For any $k \geq 0$, since $G(P^k \cup \{4\})$ contains only even numbers, we clearly have

$$(1) \quad E^2 \supseteq G(P^k \cup \{4\}).$$

By Theorem 1.4.1 and Theorem 1.3.6, it follows that

$$(2) \quad E^{\beta_1} \subset G(P^3 \cup \{4\}),$$

where β_1 is the first Brun constant. In turn, we let

$$(3) \quad E^{\beta_1} \cup E = E^2,$$

where E is a finite set of even numbers $4, 6, 8, \ldots, 2n \leq \beta_1$. By ordinary arithmetic, it follows that the even numbers in E can be expressed as sums of two elements taken from some finite set $I = \{n_1, n_2, \ldots, n_m\}$ of positive integers greater than 1. If the set I

is not contained in $P^3 \cup \{4\}$, then by Theorem 1.2.2 it will be contained in $P^\gamma \cup \{4\}$ for some $\gamma > 3$, in other words, $I \subset P^\gamma \cup \{4\}$ for some $\gamma \geqq 3$. Consequently,

$$E \subset G(P^\gamma \cup \{4\}). \tag{4}$$

By Theorem 1.2.1 and (2), we have

$$E^{\beta_1} \subset G(P^\gamma \cup \{4\}). \tag{5}$$

From (3), (4) and (5), it follows that

$$E^2 \subset G(P^\gamma \cup \{4\}). \tag{6}$$

In turn, from (1) and (6), it follows that

$$E^2 = G(P^\gamma \cup \{4\}). \tag{7}$$

Next, we consider the set of all sums of the form $p_\mu^{(\gamma)} + 4$ in $G(P^\gamma \cup \{4\})$. Since $p_\mu^{(\gamma)} + 4 = (p_\mu^{(\gamma)} + 2) + 2$ for all $p_\mu^{(\gamma)} > 2$, if $p_\mu^{(\gamma)} + 2 \notin P^\gamma$, then clearly $(p_\mu^{(\gamma)} + 2) \in P^\sigma$, $(p_\mu^{(\gamma)} + 2) + 2 \in G(P^\sigma)$ for some constant $\sigma > \gamma$, by virtue of Theorem 1.2.1 and 1.2.2. Combining the above, since $p_\mu^{(\sigma)} + 4 \in G(P^\sigma)$ for $\sigma \geqq 3$, we must have

$$G(P^\gamma \cup \{4\}) = G(P^\sigma), \tag{8}$$

by Theorem 1.2.1 and (7).

Finally, consider the set of all sums of the form $p_\mu^{(\sigma)} + 2$ in $G(P^\sigma)$, where $p_\mu^{(\gamma)} \in P^\sigma \setminus \{2\}$. Clearly, we have $p_\mu^{(\sigma)} + 2 = (p_\mu^{(\sigma)} - 1) + 3$, where obviously $p_\mu^{(\sigma)} - 1$ is odd, $p_\mu^{(\sigma)} \neq 1$ and $p_\mu^{(\sigma)} \neq 2$. Again, if $(p_\mu^{(\sigma)} - 1) \notin P^\sigma \setminus \{2\}$, then certainly $(p_\mu^{(\sigma)} - 1) \in P^{\beta_2} \setminus \{2\}$, $(p_\mu^{(\sigma)} - 1) + 3 \in G(P^{\beta_2} \setminus \{2\})$ for some constant $\beta_2 > \sigma$, i.e., the second Brun constant. Consequently,

$$G(P^\sigma \setminus \{2\}) = G(P^{\beta_2} \setminus \{2\}), \tag{9}$$

by Theorem 1.2.1, (8) and $E^2 \setminus \{2\} = G(P^\sigma \setminus \{2\})$. Since $4 = 2 + 2$ and we eliminated 2, from (7), (8) and (9) we get

$$E^4 = G(P^{\beta_2} \setminus \{2\}),$$

where β_2 is the second Brun constant.

1.4.3. Theorem. For any $k > \beta_2$, where β_2 is the second Brun constant, we have the equality $E^4 = G(P^k \setminus \{2\})$.

This theorem is a simple consequence of Theorem 1.4.2 and Theorem 1.2.1.

We conclude this section with the following number-system:

$$M = \{ 2p_\mu \mid p_\mu \in P^0 \ , \mu \in P^0 \ , \mu \geq 2 \} .$$

1.4.4. Theorem. (1) $M \subset P^1$,

(2) $E^{10} \neq G(M)$.

Property (1) is a consequence of Lemma 1.3.2. For property (2), we cite the following example. We note that the positive integer 30 can be expressed only by the following representations:

$$p_4 + p_9 \ , \quad p_5 + p_8 \ , \quad p_6 + p_7 \ ,$$

i.e., $7+23$, $11+19$ and $13+17$. Clearly, no pair of indices in $p_4 + p_9$, $p_5 + p_8$ and $p_6 + p_7$ are both prime numbers. Therefore, $30 \neq p_{p_\mu} + p_{p_\nu}$ for all $p_\mu , p_\nu \in P^0$. From this, it follows that $2 \cdot 30 \neq 2(p_{p_\mu} + p_{p_\nu})$ and $60 \neq 2p_{p_\mu} + 2p_{p_\nu}$ for all $2p_\mu , 2p_\nu \in M$.

On the strength of Theorem 1.4.4, we shall write $[M]^k$ to denote the set M written in the numbering of P^k $(k \geq 1)$.

CHAPTER II

FREE MONOIDS AND FREE MONOIDULES

§2.1. Nonconcatenative commutative monoids

In abstract arithmetics $\mathfrak{A}^{K}(A)$ introduced in the following chapter, we work with a denumerably infinite set A called an alphabet consisting of abstract signs $a_1, a_2, a_3, \ldots$, where the signs in question are combined concatenatively, nonconcatenatively or in both ways by means of certain laws of composition. In this section, with respect to the above-mentioned signs, we introduce algebraic structures with laws of composition which are not concatenative.

The alphabet $A = \{ a_1, a_2, \ldots$ will be our ground alphabet throughout this paper. We assume that the signs in A are ordered by the relation $a_\mu \leqq a_\nu$ for any $a_\mu, a_\nu \in A$ defined by $a_\mu \leqq a_\nu$ if and only if $\mu \leqq \nu$. Let $\#$ denote the empty word. It is convenient to denote the empty word $\#$ alternatively as a_0, and to denote the set $\{a_0, a_1, a_2, \ldots\}$ as $A^{\#}$, where $a_0 < a_\mu$ for all $a_\mu \in A$.

A nonconcatenative additive monoid, denoted S_A, consists of the set $A^{\#}$ together with the law of composition $a_\mu \boxplus a_\nu$ $(a_\mu, a_\nu \in A^{\#})$, satisfying the associative, commutative and cancellative laws and axioms (1) $a_\mu \boxplus a_1 = a_{\mu+1}$ and (2) $a_\mu \boxplus \# = a_\mu$ $(a_\mu \in A^{\#})$.

A nonconcatenative multiplicative monoid, denoted M_A, consists of the alphabet A together with the law of composition $a_\mu \boxdot a_\nu$ $(a_\mu, a_\nu \in A)$, which satisfies the associative, commutative and cancellative laws and the equation $a_\mu \boxdot a_1 = a_\mu$ $(a_\mu \in A)$, and furthermore it is assumed that M_A has a unique factorization into prime elements in $\Pi_A = \{ \pi_1, \pi_2, \cdots \}$,

where $\overline{\pi}_\mu = a_{p_\mu}$ $(p_\mu \in P^0)$.

A nonconcatenative semiring, denoted SM_A, consists of the monoids S_A and M_A, connected by the distributive law $a_\mu \boxdot (a_\alpha \boxplus a_\beta) = (a_\mu \boxdot a_\alpha) \boxplus (a_\mu \boxdot a_\beta)$.

2.1.1. Proposition. In the semiring SM_A, we have the following:

$$(1) \quad a_\mu \boxplus a_\nu = a_{\mu+\nu} \qquad (a_\mu, a_\nu \in A^{\#}),$$

$$(2) \quad a_\mu \boxdot a_\nu = a_{\mu\cdot\nu} \qquad (a_\mu, a_\nu \in A),$$

$$(3) \quad a_\mu \boxdot \# = \# \qquad (a_\mu \in A^{\#}).$$

For property (1), we use axiom (1) of S_A, for (2) and (3) we use axiom (1) of S_A and the distributive law.

§2.2. Free monoids

In algebra (2), definitions of free monoids F are based on the property that every map from any set S into any monoid M extends to a unique homorphism $\varphi : F \to M$. In this section, however, we introduce free monoids by arithmetical means using successor functions rather than homomorphisms.

A commutative free monoid F(A) in the alphabet $A = \{a_1, a_2, \ldots\}$ with the identity $\#$, satisfying $a_\mu \neq \#$ $(a_\mu \in A)$, is defined as:

$$F(A) = \bigcup_{K=0}^{\infty} H_K,$$

where $H_0 = \{\#\}$, $H_{K+1} = \{a_\mu X \mid a_\mu \in A, \ X \in F(A)\}$, where the denumerably infinite set of successor functions $a_\mu X$ $(a_\mu \in A, X \in F(A))$ satisfy the axioms:

2.2.1. Axiom. For any $a_\mu \in A$, $a_\mu \# = a_\mu$.

2.2.2. Axiom. For any $a_\mu, a_\nu, a_\alpha, a_\beta \in A$ and $X, Y \in F(A)$,

(1) $a_\mu(a_\nu X) = a_\nu(a_\mu Y)$ iff $X = Y$, (2) $a_\mu(a_\nu X) = a_\alpha(a_\beta X)$ iff either $a_\mu = a_\alpha$ and $a_\nu = a_\beta$, or $a_\mu = a_\beta$ and $a_\nu = a_\alpha$.

2.2.3. Axiom. For any $a_\mu, a_\nu \in A$, $X \in F(A)$, if $a_\mu X = a_\nu \#$ then $a_\mu = a_\nu$ and $X = \#$.

The elements of F(A) are called words, and # is called the empty word.

2.2.4. Proposition. In F(A), we have the following properties:

(1) $\# \in F(A)$; (2) for any $X \in F(A)$, if $X \neq \#$ then $X = a_\mu Y$ for some $a_\mu \in A$ and $Y \in F(A)$; (3) for any $X \in F(A)$, $a_\mu X \neq \#$ $(a_\mu \in A)$.

Properties (1) and (3) follow from the definition of F(A) and Axioms 2.2.1 and 2.2.2. As for (2), from its assumption $X \in F(A)$ and $X \neq \#$, and the definition of H_K, we get $X \in H_K$ for some k, therefore $X = a_\mu Y$ for some $Y \in H_{k-1}$ and $a_\mu \in A$.

2.2.5. Theorem. (Induction Theorem) If S is any subset of F(A) such that

(i) $\# \in S$ and (ii) whenever $X \in S$ then $a_\mu X \in S$ $(a_\mu \in A)$, then $S = F(A)$.

Let the assumption of the theorem hold. Assume that $S \neq F(A)$, which means that there must exist a nonempty word $X \in F(A)$ containing the least number of signs such that $X \notin S$. By Proposition 2.2.4, we have $X = a_\mu Y$, and since $a_\mu Y \notin S$, by the least-sign assumption and (i) we must have $Y \in S$, but this means $a_\mu Y \notin S$ and $Y \in S$, which contradicts the assumption of the theorem.

2.2.6. Theorem. (Symbolic uniqueness theorem) Every nonempty word $X \in F(A)$ can be expressed uniquely, save for the ordering of the signs, as $X = a_{i_r} a_{i_{r-1}} \cdots a_{i_1}$ $(r \geq 1)$, where $a_{i_1}, a_{i_2}, \cdots, a_{i_r} \in A$.

Existence. For any $X \in F(A)$, if $X \neq \#$, we have $X \in H_K$ for some k. Therefore, $X = a_{i_r} Y_1$ for some $a_{i_r} \in A$ and $Y_1 \in H_{k-1}$, $\cdots$, $Y_{r-1} = a_{i_1} Y_r$ for some $a_{i_1} \in A$ and $Y_r \in H_0$, which means $X = a_{i_r} a_{i_{r-1}} \cdots a_{i_1}$.

Uniqueness. Word length is clearly unique. Assume that $a_{i_r} a_{i_{r-1}} \cdots a_{i_1} = a_{j_r} a_{j_{r-1}} \cdots a_{j_1}$ for some odd $r > 1$ and assume that there exists an a_{i_K} such that $a_{i_K} \neq a_{j_h}$ $(h = 1, 2, \cdots, r)$. Let the words $a_{i_r} \cdots a_{i_1}$ and $a_{j_r} \cdots a_{j_1}$ with a_{i_K} and some a_{j_h} deleted respectively from them be denoted as X and Y.

If $a_{i_K} \neq a_{j_h}$, then on the strength of Axiom 2.2.2 we must have $a_{\mu_1}a_{\mu_2}\cdots a_{\mu_{r-1}}a_{i_K} \neq a_{\nu_1}a_{\nu_2}\cdots a_{\nu_{r-1}}a_{j_h}$ for all $a_{\mu_1}, \cdots, a_{\mu_{r-1}}$ and any permutation of them denoted as $a_{\nu_1}, \cdots, a_{\nu_{r-1}}$ in H_{r-1}, and clearly for some words $a_{\mu_1}a_{\mu_2}\cdots a_{\mu_{r-1}}$ and $a_{\nu_1}a_{\nu_2}\cdots a_{\nu_{r-1}}$ in H_{r-1} we must have $X = a_{\mu_1}a_{\mu_2}\cdots a_{\mu_{r-1}}$ and $Y = a_{\nu_1}a_{\nu_2}\cdots a_{\nu_{r-1}}$, which means $a_{i_r}\cdots a_{i_1} \neq a_{j_r}\cdots a_{j_1}$, a contradiction.

Similarly as above for an even $r > 1$, except assume two a_i different from all a_j. Case $r = 2$ follows from Axiom 2.2.2.

On the strength of the above theorem, we introduce a notation for the <u>symbolic equality</u>: $X =_A Y$ if and only if the words X and Y contain precisely the same signs taken from the alphabet A. However, for convenience, we shall abbreviate $X =_A Y$ simply as $X = Y$.

We introduce another notation as follows. Let

$$a_\mu^n = a_\mu a_\mu \cdots a_\mu \quad (a_\mu \text{ n-times}),$$

where $n \geq 1$ and $a_\mu \in A$, and let $a_\mu^0 = \#$ $(a_\mu \in A)$.

2.2.7. <u>Proposition.</u> Every nonempty word $a_{i_r}a_{i_{r-1}}\cdots a_{i_1}$ in F(A) can be uniquely expressed as

$$a_{i_r}a_{i_{r-1}}\cdots a_{i_1} = a_\mu^{n_\mu} a_{\mu-1}^{n_{\mu-1}} \cdots a_2^{n_2} a_1^{n_1},$$

where $n_1, n_2, \cdots, n_\mu \geq 0$ and $\mu \geq r$.

This proposition follows from Theorem 2.2.6 and Axiom 2.2.2.

A word X in F(A) put in the form given in Proposition 2.2.7 is called the normal form of X, which we can denote as X. This terminology

will be used in the following chapters.

We introduce the usual law of composition of the free monoid $F(A)$, called word addition or word sum, by the following equations:

$$X \oplus \# = X ,$$
$$X \oplus a_\mu Y = a_\mu (X \oplus Y) \quad (a_\mu \in A) .$$

2.2.8. Proposition. For any $X, Y, Z \in F(A)$,

(1) $X \oplus (Y \oplus Z) = (X \oplus Y) \oplus Z$,

(2) $X \oplus Y = Y \oplus X$.

Property (1) clearly holds for $Z = \#$. Assume (1) to be true for some Z, then by three applications of the definition of word addition we have

$$X \oplus (Y \oplus a_\mu Z) = X \oplus a_\mu (Y \oplus Z) = a_\mu (X \oplus (Y \oplus Z))$$
$$= a_\mu ((X \oplus Y) \oplus Z) = (X \oplus Y) \oplus a_\mu Z .$$

Consequently, the proposition is true for all Z by virtue of the Induction theorem.

With respect to property (2), since $\# \oplus \# = \#$ and $\# \oplus a_\mu Y = a_\mu (\# \oplus Y)$, we can see that the property holds for $Y = \#$. Let the property hold for some Y, then by (1)

$$X \oplus a_\mu Y = a_\mu (X \oplus Y) = a_\mu (Y \oplus X) = a_\mu \oplus (Y \oplus X)$$
$$= (a_\mu \oplus Y) \oplus X = a_\mu Y \oplus X.$$

Commutative free monoid $F(a_1)$ in the one-sign alphabet $\{a_1\}$ is defined as follows: Given the one-sign alphabet $\{a_1\}$, the empty word $\#$, the successor function $a_1 X = a_1 \oplus X$ satisfying the usual axiom, if $a_1 X = a_1 Y$ then $X = Y$, and finally given the equations $H_0 = \{\#\}$ and $H_{k+1} = \{a_1 X \mid X \in H_k\}$, the free monoid $F(a_1)$ is introduced by $F(a_1) =_{\text{Def}} \bigcup_{k=0}^{\infty} H_k$. It is evident that $F(a_1)$ is embedded in the free monoid $F(A)$. We assume the obvious linear ordering relation $X \preceq Y$ on $F(a_1)$.

We denote the nonempty elements in the free monoid $F(a_1)$ as a_1^{μ} $(\mu \geq 1)$, i.e., $a_1^1 = a_1$ and $a_1^{\mu+1} = a_1 \oplus a_1^{\mu}$. Words in the free monoid $F(a_1)$ are called natural words. Clearly, $a_1^{\mu} \oplus a_1^{\nu}$ is the word addition in $F(a_1)$.

2.2.9. Proposition. For any $a_1^{\mu}, a_1^{\nu}, a_1^{\sigma} \in F(a_1)$,

(1) $(a_1^{\mu} \oplus a_1^{\nu}) \oplus a_1^{\sigma} = a_1^{\mu} \oplus (a_1^{\nu} \oplus a_1^{\sigma})$,

(2) $a_1^{\mu} \oplus a_1^{\nu} = a_1^{\nu} \oplus a_1^{\mu}$,

(3) $a_1^{\mu} \oplus \# = a_1^{\mu}$,

(4) $a_1^{\mu} \oplus \sigma_1^{\nu} = a_1^{\mu+\nu}$.

This proposition is obvious.

We recall from Section 1.2 that P^0, P^1, P^2, ... denote the Hilbert-Ackermann number-systems, where P^0 denotes the set of all ordinary prime numbers. Since the nonempty words in $F(a_1)$ are of the form $a_1^1, a_1^2, a_1^3, \ldots$, we can give names to certain subsets of $F(a_1)$ as follows. For every $k \geq 0$,

(1) $$\pi_{\mu}^{(k)} =_{\text{Def}} a_1^{p_{\mu}^{(k)}} \qquad (p_{\mu}^{(k)} \in P^k,\ \mu \geq 1) ,$$

(2) $$\prod_{F(a_1)}^{(k)} =_{\text{Def}} \{\pi_{\mu}^{(k)} \mid \mu \geq 1\} .$$

For convenience, we also write the notation

$$\prod_{F(a_1)}^{(0)} = \{\pi_1^{(0)}, \pi_2^{(0)}, \ldots\}$$

more briefly as

(3) $$\prod_{F(a_1)} = \{\pi_1, \pi_2, \ldots\} .$$

2.2.10. Theorem. $\prod_{F(a_1)} \subset \prod_{F(a_1)}^{(k)}$ $(k \geq 1)$.

This theorem is a consequence of Corollary 1.2.1.1.

By virtue of the above theorem, we denote the elements of $\prod_{F(a_1)}$

written in the numbering of $\prod^{(k)}_{F(a_1)}$ $(k \geq 0)$ as $[\prod_{F(a_1)}]^{(k)}$, i.e., $[\prod_{F(a_1)}]^{(k)}$ denotes a set of elements $\pi^{(k)}_{i_1}, \pi^{(k)}_{i_2}, \ldots$ in $\prod^{(k)}_{F(a_1)}$ which are precisely the elements in $\prod_{F(a_1)}$.

By a numbered free monoid $F^k(a_1)$ we mean the free monoid $F(a_1)$ together with the names (1) and (2) given to relevant words in $F(a_1)$.

§2.3. Commutative free monoidule

By a commutative free monoidule on $F(A)$, denoted $M_A F(A)$, we mean the combination of algebraic structures consisting of the nonconcatenative multiplicative monoid M_A and the commutative free monoid $F(A)$ connected by means of the law of composition $a_\mu \odot X$ $(a_\mu \in M_A,\ X \in F(A))$, which satisfies the following axioms:

2.3.2. Axiom. $a_\mu \odot \# = \#$ $(a_\mu \in M_A)$.

2.3.3. Axiom. For any $a_\mu, a_\nu \in M_A$ and $X \in F(A)$,

$$a_\mu \odot (a_\nu \oplus X) = (a_\mu \boxdot a_\nu) \oplus (a_\mu \odot X).$$

2.3.4. Proposition. In the free monoidule $M_A F(A)$ we have the following properties:

(1) $a_1 \odot X = X$,

(2) $a_\mu \odot (X \oplus Y) = (a_\mu \odot X) \oplus (a_\mu \odot Y)$,

(3) $(a_\mu \boxdot a_\nu) \odot X = a_\mu \odot (a_\nu \odot X)$,

(4) $a_\mu \boxdot a_\nu = a_\mu \odot a_\nu$.

Property (1) is true for $X = \#$ by Axiom 2.3.2. Let it be true for some X, then by Axiom 2.3.3

$$a_1 \odot a_\mu X = a_1 \odot (a_\mu \oplus X) = (a_1 \boxdot a_\mu) \oplus (a_1 \odot X) = a_\mu \oplus X \neq a_\mu X.$$

Property (2) for $Y = \#$ is true by virtue of $X \oplus \# = X$ and Axiom 2.3.2. Let (2) be true for some Y, then, by Axiom 2.3.3,

$$
\begin{aligned}
a_\mu \odot (X \oplus a_\nu Y) &= a_\mu \odot a_\nu (X \oplus Y) = a_\mu \odot (a_\nu \oplus (X \oplus Y)) \\
&= (a_\mu \boxdot a_\nu) \oplus (a_\mu \odot (X \oplus Y)) \\
&= (a_\mu \boxdot a_\nu) \oplus ((a_\mu \odot X) \oplus (a_\mu \odot Y)) \\
&= (a_\mu \odot X) \oplus ((a_\mu \boxdot a_\nu) \oplus (a_\mu \odot Y)) \\
&= (a_\mu \odot X) \oplus (a_\mu \odot (a_\nu \oplus Y)) \\
&= (a_\mu \odot X) \oplus (a_\mu \odot a_\nu X).
\end{aligned}
$$

Hence, property (2) is true for all Y on the strength of the Induction theorem.

Property (3) holds for $X = \#$ by virtue of Axiom 2.3.2. Let (3) hold for some X, then by Axiom 2.3.3

$$
\begin{aligned}
(a_\mu \boxdot a_\nu) \odot a_\alpha X &= (a_\mu \boxdot a_\nu) \odot (a_\alpha \oplus X) \\
&= ((a_\mu \boxdot a_\nu) \boxdot a_\alpha) \oplus ((a_\mu \boxdot a_\nu) \odot X)) \\
&= (a_\mu \boxdot (a_\nu \boxdot a_\alpha) \oplus (a_\mu \odot (a_\nu \odot X)) \\
&= a_\mu \odot ((a_\nu \boxdot a_\alpha) \oplus (a_\nu \odot X)) \\
&= a_\mu \odot (a_\nu \odot (a_\alpha \oplus X)) \\
&= a_\mu \odot (a_\nu \odot a_\alpha X).
\end{aligned}
$$

Finally, property (4) is an obvious consequence of property (3).

Because properties (1), (2) and (3) of Proposition 2.3.4 resemble the axioms of a free module, one naturally asks whether it is possible to replace the nonconcatenative multiplicative monoid M_A by the nonconcatenative semiring SM_A in order to obtain something like $(a_\mu \boxplus a_\nu) \odot X = (a_\mu \odot X) \oplus (a_\nu \odot X)$, however this is false in a free monoidule and the only property resembling it is a version of Axiom 2.3.3, namely, $(a_\mu \oplus X) \odot a = (a_\mu \boxdot a_\nu) \oplus (a_\nu \odot X)$.

We conclude this section by showing that the free monoidule $M_A F(A)$ can be extended to a commutative semiring $RM_A F(A)$ by assuming the axioms of the free monoidule $M_A F(A)$ and by introducing the law of composition $X \odot Y$ $(X, Y \in F(A))$ satisfying the following axioms:

2.3.5. Axiom. $X \odot \# = \#$.

2.3.6. Axiom. $X \odot (a_\mu \oplus Y) = (a_\mu \odot X) \oplus (X \odot Y)$.

2.3.7. Proposition. In the semiring $RM_A F(A)$, we have the following properties:

(1) $a_1 \odot X = X$,

(2) $X \odot (Y \oplus Z) = (X \odot Y) \oplus (X \odot Z)$,

(3) $(Y \oplus Z) \odot X = (Y \odot X) \oplus (Z \odot X)$,

(4) $X \odot Y = Y \odot X$,

(5) $a_\mu \odot (X \odot Y) = (a_\mu \odot X) \odot Y$,

(6) $X \odot (Y \odot Z) = (X \odot Y) \odot Z$.

Property (1) follows from Proposition 2.3.4.

Property (2) for $Z = \#$ is clear. Let property (2) be true for some Z, then, by definitions $\oplus$ and $\odot$ and Proposition 2.2.8, we get

$$\begin{aligned} X \odot (Y \oplus a_\mu Z) &= X \odot a_\mu (Y \oplus Z) \\ &= (a_\mu \odot X) \oplus (X \odot (Y \oplus Z)) \\ &= (a_\mu \odot X) \oplus ((X \odot Y) \oplus (X \odot Z)) \\ &= (X \odot Y) \oplus (a_\mu \odot X) \oplus (X \oplus Z) \\ &= (X \odot Y) \oplus X \odot (a_\mu \oplus Z) \\ &= (X \odot Y) \oplus X \odot a_\mu Z . \end{aligned}$$

Property (3) is obvious for $X = \#$. Let (3) hold for some X, then, by Proposition 2.2.4 and Proposition 2.2.8

$$(Y \oplus Z) \odot a_\mu X = a_\mu \odot (Y \oplus Z) \oplus (Y \oplus Z) \odot X$$
$$= a_\mu \odot (Y \oplus Z) \oplus (Y \odot X) \oplus (Z \odot X)$$
$$= (a_\mu \odot Y \oplus Y \odot Z) \oplus (a_\mu \odot Z \oplus Z \odot X)$$
$$= (Y \odot a_\mu X) \oplus (Z \odot a_\mu X).$$

Property (4) is clear for $Y = \#$. Assume the inductive hypothesis, then by property (3) we have

$$X \odot a_\mu Y = (a_\mu \odot X) \oplus (X \odot Y)$$
$$= (a_\mu \odot X) \oplus (Y \odot X)$$
$$= (a_\mu \oplus Y) \odot X = a_\mu Y \odot X.$$

Property (5) for $Y = \#$ is clear. Let it be true for some Y, then by Proposition 2.2.4 and commutativity in M_A, we get

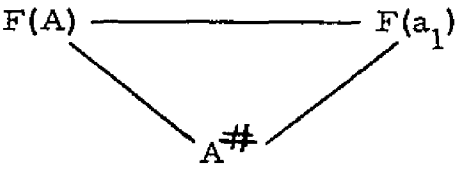
$$a_\mu \odot (X \odot a_\nu Y) = a_\mu \odot (a_\nu \odot X \oplus X \odot Y)$$
$$= a_\mu \odot (a_\nu \odot X) \oplus a_\mu \odot (X \odot Y)$$
$$= a_\mu \odot (a_\nu \odot X) \oplus (a_\mu \odot X) \odot Y$$
$$= (a_\mu \boxdot a_\nu) \odot X \oplus (a_\mu \odot X) \odot Y$$
$$= a_\nu \odot (a_\mu \odot X) \oplus (a_\mu \odot X) \odot Y$$
$$= (a_\mu \odot X) \odot (a_\nu \oplus Y)$$
$$= (a_\mu \odot X) \odot a_\nu Y .$$

Since property (6) is clear for $Z = \#$, assume the inductive hypothesis, then by properties (2), (4) and (5) we get

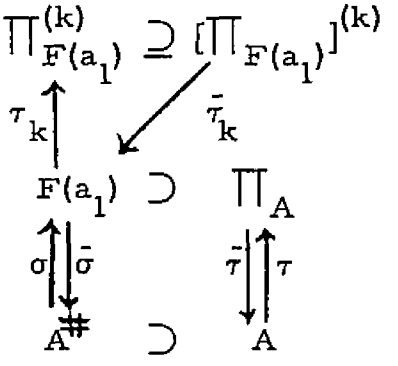
$$X \odot (Y \odot a_\mu Z) = X \odot (a_\mu \odot Y \oplus Y \odot Z)$$
$$= X \odot (a_\mu \odot Y) \oplus X \odot (Y \odot Z)$$
$$= a_\mu \odot (X \odot Y) \oplus (X \odot Y) \odot Z$$
$$= (X \odot Y) \odot (a_\mu \oplus Z)$$
$$= (X \odot Y) \odot a_\mu Z .$$

§2.4. Arithmetical maps

The arithmetics in the following sections depend on certain mappings of words contained in the three objects in the following mapping diagram:



In particular, we need to define the following set of mappings for $k \geq 0$:



We define the above mappings as follows:

The additive maps σ and $\bar{\sigma}$, mapping S_A and $F(a_1)$, are defined by the following equations:

(1) $\sigma(\#) = \#$, $\sigma(a_\mu \boxplus a_1) = \sigma(a_\mu) \oplus a_1$ $(a_\mu \in S_A)$,

(2) $\bar{\sigma}(\#) = \#$, $\bar{\sigma}(a_1^\mu \oplus a_1) = \bar{\sigma}(a_1^\mu) \boxplus a_1$ $(a_1^\mu \in F(a_1))$.

2.4.1. Proposition. For any $a_\mu, a_\nu \in S_A$ and $a_1^\mu, a_1^\nu \in F(a_1)$,

(1) $\sigma(a_\mu) = a_1^\mu$, $\bar{\sigma}(a_1^\mu) = a_\mu$,

(2) $\sigma(a_\mu \boxplus a_\nu) = \sigma(a_\mu) \oplus \sigma(a_\nu)$,

(3) $\bar{\sigma}(a_1^\mu \oplus a_1^\nu) = \bar{\sigma}(a_1^\mu) \boxplus \bar{\sigma}(a_1^\nu)$.

Property (1) is trivial for $a_\mu = a_1^\mu = a_1$. Assume that (1) holds for some a_μ, then by the above definitions we get $\sigma(a_{\mu+1}) = \sigma(a_\mu \boxplus a_1) = \sigma(a_\mu) \oplus a_1 = a_1^\mu \oplus a_1 = a_1^{\mu+1}$, and in turn $\bar{\sigma}(a_1^{\mu+1}) = \bar{\sigma}(a_1^\mu \oplus a_1) = \bar{\sigma}(a_1^\mu) \boxplus a_1 = a_\mu \boxplus a_1 = a_{\mu+1}$.

Property (2) for $a_\nu = a_1$ follows from definition, and using above

definitions, property (1) and induction, we obtain $\sigma(a_\mu \boxplus a_{\nu+1}) = \sigma((a_\mu \boxplus a_\nu) \boxplus a_1) = \sigma(a_\mu) \oplus \sigma(a_\nu) \oplus \sigma(a_1) = \sigma(a_\mu) \oplus a_1^{\nu+1} = \sigma(a_\mu) \oplus \sigma(a_{\nu+1})$.

Property (3) is clear for $a_\nu = a_1$ and for $a_{\nu+1}$, like (2), we have $\bar{\sigma}(a_1^\mu \oplus a_1^{\nu+1}) = \bar{\sigma}((\sigma_1^\mu \oplus a_1^\nu) \oplus a_1) = \bar{\sigma}(a_1^\mu) \boxplus \bar{\sigma}(a_1^\nu) \boxplus \bar{\sigma}(a_1) = \bar{\sigma}(a_1^\mu) \boxplus a_{\nu+1} = \bar{\sigma}(a_1^\nu) \boxplus \bar{\sigma}(a_1^{\nu+1})$.

The multiplicative maps τ_k and $\bar{\tau}_k$ $(k \geq 0)$, mapping $F(a_1)$ and $\prod^{(k)}_{F(a_1)}$ $(k \geq 0)$, are defined by the following equations for $k \geq 0$:

(1) For any $a_1^\mu \in F(a_1)$, $\tau_k(a_1^\mu) = \pi_\mu^{(k)}$ $(\pi_\mu^{(k)} \in \prod^{(k)}_{F(a_1)}, \ \mu \geq 1)$,

(2) $\bar{\tau}_k(\pi_\mu^{(k)}) = a_1^\mu$ if $\pi_\mu^{(k)} \in [\prod_{F(a_1)}]^{(k)}$,

$= \#$ if $\pi_\mu^{(k)} \notin [\prod_{F(a_1)}]^{(k)}$.

Note, $\bar{\tau}_k$ is the inverse of τ_k only if $k = 0$, and of course $\bar{\sigma}$ is the inverse of the map σ.

The alphabetical multiplicative maps τ and $\bar{\tau}$, mapping A and $\prod_A$, are defined by the following equations:

(1) For any $a_\mu \in A$, $\tau(a_\mu) = \bar{\pi}_\mu$ $\quad (\bar{\pi}_\mu \in \prod_A)$.

(2) For any $\pi_\mu \in \prod_A$, $\bar{\tau}(\bar{\pi}_\mu) = a_\mu$ $\quad (a_\mu \in A)$.

We state the following consequence of the above definitions:

2.4.2. Proposition. For any $\mu \geq 1$ and $k \geq 0$,

(1) $a_\mu \xrightarrow{\tau_k \sigma} \pi_\mu^{(k)}$,

(2) $\pi_\mu^{(k)} \xrightarrow{\bar{\sigma}\bar{\tau}_k} a_\mu$ if $\pi_\mu^{(k)} \in [\prod_{F(a_1)}]^{(k)}$.

Next, we have the length map, a mapping between $F(A)$ and $F(a_1)$, usually called a length function, denoted as $\lambda(X)$, defined by the following equations:

$$\lambda(\#) = \#,$$

$$\lambda(a_\mu X) = a_1 \oplus \lambda(X) \quad (a_\mu \in A,\ X \in F(A)).$$

2.4.3. Proposition. For any $X, Y \in F(A)$,

(1) $\lambda(X \oplus Y) = \lambda(X) \oplus \lambda(Y)$,

(2) in the free monoidule $M_A F(A)$, $\lambda(a_\mu \odot X) = \lambda(X)$,

(3) $\lambda(X \odot Y) = \lambda(X) \odot \lambda(Y)$.

Property (1) for $Y = \#$ is clear. Let (1) hold for some Y, then

$$\begin{aligned}\lambda(X \oplus a_\mu Y) &= \lambda(a_\mu(X \oplus Y)) = a_1 \oplus \lambda(X \oplus Y)\\ &= a_1 \oplus \lambda(X) \oplus \lambda(Y) = \lambda(X) \oplus (a_1 \oplus \lambda(Y))\\ &= \lambda(X) \oplus \lambda(a_\mu X).\end{aligned}$$

With respect to (2), the equality clearly holds for $X = \#$. Let it hold for some X, then by Proposition 2.3.4 and property (1)

$$\begin{aligned}\lambda(a_\mu \odot a_\nu X) &= \lambda((a_\mu \odot a_\nu) \oplus (a_\mu \odot X)) = \lambda(a_\mu \odot a_\nu) \oplus \lambda(a_\mu \odot X)\\ &= \lambda(a_\mu \odot a_\nu) \oplus \lambda(X) = \lambda(a_\mu \boxdot a_\nu) \oplus \lambda(X)\\ &= a_1 \oplus \lambda(X) = \lambda(a_\mu X).\end{aligned}$$

Property (3) is clear for $Y = \#$. Let it hold for some Y, then by properties (1) and (2)

$$\begin{aligned}\lambda(X \odot a_\mu Y) &= \lambda((a_\mu \odot X) \oplus (X \odot Y)) = \lambda(a_\mu \odot X) \oplus \lambda(X \odot Y)\\ &= \lambda(X) \oplus (\lambda(X) \odot \lambda(Y)) = \lambda(X) \odot (a_1 \oplus \lambda(Y))\\ &= \lambda(X) \odot \lambda(a_\mu Y).\end{aligned}$$

The auxiliary additive map $\sigma^*(X)$, mapping $F(A)$ and S_A, is defined by the following equations:

$$\sigma^*(\#) = \#,$$

$$\sigma^*(a_\mu X) = a_\mu \boxplus \sigma^*(X) \quad (a_\mu \in A,\ X \in F(A)).$$

2.4.4. Proposition. For any $X, Y \in F(A)$,

$$\sigma^*(X \oplus Y) = \sigma^*(X) \boxplus \sigma^*(Y).$$

For $Y = \#$, the theorem is clear. Assume that the equality holds for some Y. Then

$$\sigma^*(X \oplus a_\mu Y) = \sigma^*(a_\mu(X \oplus Y)) = a_\mu \boxplus \sigma^*(X \oplus Y)$$
$$= a_\mu \boxplus \sigma^*(X) \boxplus \sigma^*(Y)$$
$$= \sigma^*(X) \boxplus (a_\mu \boxplus \sigma^*(Y))$$
$$= \sigma^*(X) \boxplus \sigma^*(a_\mu Y).$$

With the help of $\sigma^*(X)$ we define the map $\kappa(X)$, between $F(A)$ and $A^{\#}$, by the following equations:

$$\kappa(\#) = \#,$$
$$\kappa(X \odot a_\mu Y) = (a_\mu \odot \sigma^*(X)) \boxplus \kappa(X \odot Y).$$

2.4.4. Proposition. For any $X, Y \in F(A)$,

(1) $\kappa(X) = \sigma^*(X)$,
(2) $\kappa(a_\mu X) = a_\mu \boxplus \kappa(X)$,
(3) $\kappa(X \oplus Y) = \kappa(X) \boxplus \kappa(Y)$,
(4) $\kappa(X \odot Y) = \kappa(X) \odot \kappa(Y)$,
(5) if $X \neq \#$ then $\lambda(\kappa(X)) = a_1$,
(6) $\kappa(X) \boxdot \kappa(Y) = \kappa(X) \odot \kappa(Y)$.

Since we only need the above properties incidentally, we omit the long proof.

We conclude this section with the map $\partial(X)$, mapping $F(A)$ and M_A, defined as follows:

$$\partial(\#) = a_1$$
$$\partial(a_\mu X) = \tau(a_\mu) \boxdot \partial(X) \quad (a_\mu \in A,\ X \in F(A)).$$

2.4.5. Proposition. For any $X, Y \in F(A)$,

(1) $\partial(X \oplus Y) = \partial(X) \boxdot \partial(Y)$,
(2) $\partial(X) = \partial(Y)$ if and only if $X = Y$.

Property (1) for $Y = \#$ is trivial. Let it hold for some Y, then

$$\partial(X \oplus a_\mu Y) = \partial(a_\mu(X \oplus Y)) = \tau(a_\mu) \boxdot \partial(X \oplus Y)$$
$$= \tau(a_\mu) \boxdot \partial(X) \boxdot \partial(Y)$$
$$= \partial(X) \boxdot \partial(a_\mu Y).$$

Property (2) follows from the symbolic uniqueness theorem and the unique factorization in M_A.

§2.5. Noncommutative free monoids in finite alphabets

In this section, we simply introduce a terminology for later use.

Let $A_n^{\#} = \{a_0, a_1, a_2, \ldots, a_{n-1}\}$ $(n > 1)$.

The additive monoid S_n $(n > 1)$ consists of the set $A_n^{\#}$ together with the law of composition $a_\mu \boxplus_n a_\nu = a_{\mu+\nu}$ modulo n which of course satisfies the associative and commutative laws and the equation $a_\mu \boxplus_n a_0 = a_\mu$ $(a_\mu \in A_n^{\#})$.

The additive groupoid S_n^* $(n > 1)$ in the nonconcatenative additive monoid S_A consists of the law of composition $a_\mu \boxplus_n^* a_\nu$ defined on $A_n^{\#}$, with the help of the monoid S_A, by the following equations:

$$\begin{aligned} a_\mu \boxplus_n^* a_\nu &= a_0 \quad \text{if} \quad a_\mu \boxplus a_\nu < a_n, \\ &= a_1 \quad \text{if} \quad a_\mu \boxplus a_\nu \geq a_n. \end{aligned}$$

The multiplicative monoid M_{10} consists of the set $A_{10}^{\#}$ together with the law of composition $a_\mu \boxdot_{10} a_\nu = a_{\mu\cdot\nu}$ modulo 10 which of course satisfies the associative and commutative laws and the equation $a_\mu \boxdot_{10} a_1 = a_\mu$ $(a_\mu \in A_{10}^{\#})$.

The multiplicative groupoid M_{10}^* in the nonconcatenative multiplicative monoid M_A consists of the law of composition $a_\mu \boxdot_{10}^* a_\nu$ defined on $A_{10}^{\#}$ with the help of the monoid M_A by the following equations:

$$\begin{aligned} a_\mu \boxdot_{10}^* a_\nu &= a_0 \quad \text{if} \quad a_0 \leq a_\mu \boxdot a_\nu \leq a_9, \\ &= a_1 \quad \text{if} \quad a_{10} \leq a_\mu \boxdot a_\nu \leq a_{18}, \\ &= a_2 \quad \text{if} \quad a_{19} \leq a_\mu \boxdot a_\nu \leq a_{28}, \\ &= a_3 \quad \text{if} \quad a_{29} \leq a_\mu \boxdot a_\nu \leq a_{36}, \\ &= a_4 \quad \text{if} \quad a_{37} \leq a_\mu \boxdot a_\nu \leq a_{49}, \\ &= a_5 \quad \text{if} \quad a_{50} \leq a_\mu \boxdot a_\nu \leq a_{56}, \\ &= a_6 \quad \text{if} \quad a_{57} \leq a_\mu \boxdot a_\nu \leq a_{64}, \\ &= a_7 \quad \text{if} \quad a_{65} \leq a_\mu \boxdot a_\nu \leq a_{72}, \\ &= a_8 \quad \text{if} \quad a_{73} \leq a_\mu \boxdot a_\nu \leq a_{81}. \end{aligned}$$

The free monoid $G(A_n^{\#})$ $(n>1)$ in the finite alphabet $A_n^{\#}$ with the empty word $\#$ is defined as follows:

$$G(A_n^{\#}) = \bigcup_{K=0}^{\infty} H_K ,$$

where $H_0 = \{\#\}$, $H_{K+1} = \{ a_\mu X \mid a_\mu \in A_n^{\#} , X \in H_K \}$,

where the seccessor functions a_0X, a_1X, ... , $a_{n-1}X$ with a_0, a_1, ..., a_{n-1} in A and $X \in G(A_n^{\#})$ satisfy the following axioms:

2.5.1. Axiom. $a_0 a_\mu = a_\mu$ $(a_\mu \in A_n^{\#})$ and $a_0 = \#$.

2.5.2. Axiom. For any $a_\mu \in A_n^{\#}$ and $X,Y \in G(A_n^{\#})$,

if $a_\mu X = a_\mu Y$ then $X = Y$.

The equality relation of $G(A_n^{\#})$ is $=_{A_n^{\#}}$, which we abbreviate as $=$.

With respect to $G(A_n^{\#})$, for $n = 10$, it is customary to denote the signs in the alphabet $A_{10}^{\#}$ as 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Note that the words in $G(A_{10}^{\#})$ are read from left to right, i.e., e.g., the digits in the number 1230 are reversed and written in $G(A_{10}^{\#})$ as 0321.

As in the case of the free monoid $F(A)$, we immediately have the following:

2.5.3. Theorem. For the free monoid $G(A_n^{\#})$ $(n > 1)$, we have the following:

(1) $\# \in G(A_n^{\#})$,

(2) for any $X \in G(A_n^{\#})$, if $X \neq \#$ then $X = a_\mu Y$ for some $a_\mu \in A_n^{\#}$ and $Y \in G(A_n^{\#})$,

(3) for any $a_\mu \neq a_0$ and $X \in G(A_n^{\#})$, $a_\mu X \neq \#$,

(4) if S is a subset of $G(A_n^{\#})$ such that

(i) $\# \in S$ and (ii) if $X \in G(A_n^{\#})$ then $a_\mu X \in S$,

then $S = G(A_n^{\#})$.

The word addition $X \oplus_n Y$ of $G(A_n^{\#})$ is introduced by the equations:

$$X \oplus_n \# = X, \quad X \oplus_n a_\mu Y = a_\mu \oplus_n (X \oplus_n Y).$$

By an additive free monoidule on $G(A_n^{\#})$ $(n > 1)$, denoted $S_n G(A_n^{\#})$, we mean the combination of structures consisting of S_n, S_n^* and $G(A_n^{\#})$, connected by means of the law of composition $a_\mu \otimes_n X$ $(a_\mu \in S_n,\ X \in G(A_n^{\#}))$, satisfying the following axioms:

2.5.4. Axiom. $a_\mu \otimes_n \# = a_\mu, \quad \# \otimes_n X = X.$

2.5.5. Axiom. $a_\mu \otimes_n (a_\nu \oplus_n X) = (a_\mu \boxplus_n a_\nu) \oplus_n ((a_\mu \boxplus_n^* a_\nu) \otimes_n X).$

By a multiplicative free monoidule on $G(A_{10}^{\#})$, denoted $M_{10} G(A_{10}^{\#})$, we mean the combination of structures consisting of M_{10}, M_{10}^*, S_{10} and $G(A_{10}^{\#})$, connected by the law of composition $a_\mu \odot_{10} X$ $(a_\mu \in M_{10},\ X \in G(A_{10}^{\#}))$, satisfying the following axioms:

2.5.6. Axiom. $a_\mu \odot_{10} \# = \#, \quad \# \odot_{10} X = \#.$

2.5.7. Axiom. $a_\mu \odot_{10} (a_\nu \oplus_{10} X) = (a_\mu \boxdot_{10} a_\nu) \oplus_{10} [(a_\mu \boxdot_{10}^* a_\nu) \boxplus_{10} (a_\mu \odot_{10} X)].$

CHAPTER III

ABSTRACT ARITHMETICS $\mathcal{A}^k(A)$

§3.1. Commutative frames and definition structures

For any $k \geq 0$, by a commutative k-frame we mean the collection of algebraic structures consisting of the nonconcatenative structures S_A, M_A and SM_A, the free monoids $F(a_1)$, $F^k(a_1)$ and $F(A)$, the free monoidule $M_A F(A)$, and the arithmetical maps σ, $\bar{\sigma}$, τ, $\bar{\tau}$, τ_k, $\bar{\tau}_k$, κ and ∂. We denote a commutative k-frame as $\mathfrak{A}^k$. (Actually, ∂ is redundant, since it can be introduced by τ.)

For any $k \geq 0$, by a k-definition structure, denoted $\mathfrak{D}^k$, we mean the collection consisting of the frame $\mathfrak{A}^k$, a class of starting functions enumerated below, certain schemes enumerated below for generating new functions, the inequality relations $\leq$, $\preceq$ on $A^{\#}$, $F(a_1)$ respectively, and the symbolic equality relation $=_A$ of $F(A)$ which we abbreviate as $=$.

The starting functions of $\mathfrak{D}^k$ are the laws of composition and arithmetical maps included in the frame $\mathfrak{A}^k$, together with the empty-word functions $Z_n(X_1, X_2, \ldots, X_n) = \#$ $(n \geq 1)$ and the projection functions $P^i_n(X_1, \ldots, X_i, \ldots, X_n) = X_i$ $(n \geq 1,\ 1 \leq i \leq n)$. We point out that the successor functions $a_\mu X$ are already included in $F(A)$.

Let $\mathfrak{X}^n_\mu$ denote the set of variables $X_1, X_2, \ldots, X_n$ $(n \geq 1)$. We enumerate the schemes of $\mathfrak{D}^k$ $(k \geq 0)$ as follows.

(1) The composition scheme of $\mathfrak{D}^k$ is given by the equation:

$$F(\mathfrak{X}^n) = H(G_1(\mathfrak{X}^n), \ldots, G_m(\mathfrak{X}^n)),$$

where the functions $H, G_1, G_2, \ldots, G_m$ are either defined functions or starting functions of $\mathfrak{D}^k$.

(2) The single arithmetical schemes of $\mathfrak{D}^k$ are given by the following equations:

$$F(\mathfrak{X}^n, \#) = G(\mathfrak{X}^n),$$

$$F(\mathfrak{X}^n, a_\mu Y) = H(\mathfrak{X}^n, Y, G_1(a_\mu, X_1), \ldots, G_n(a_\mu, X_n), F(\mathfrak{X}^n, Y)),$$

$$F(\mathfrak{X}^n, a_\mu a_\nu Y) = F(\mathfrak{X}^n, a_\nu a_\mu Y),$$

where $H, G_1, G_2, \ldots, G_n$ are defined or starting functions of $\mathcal{D}^k$;

$$F(\mathfrak{X}^n, \#) = G(\mathfrak{X}^n),$$
$$F(\mathfrak{X}^n, a_\mu^\alpha \overline{Y}) = H(\mathfrak{X}^n, \overline{Y}, G_1(a_\mu^\alpha, \overline{X}_1), \ldots, G_n(a_\mu^\alpha, \overline{X}_n), F(\mathfrak{X}^n, \overline{Y})),$$

where the variables are in normal form (see section 2.2) and the functions $H_1, G_1, \ldots, G_n$ are either defined or starting functions of $\mathcal{D}^k$.

(3) The double arithmetical schemes of $\mathcal{D}^k$ are given by the following equations:

$$F(\mathfrak{X}^n, X, \#) = A(\mathfrak{X}^n, X),$$
$$F(\mathfrak{X}^n, \#, a_\mu Y) = B(\mathfrak{X}^n, Y, A_i(a_\mu, X_i)),$$
$$F(\mathfrak{X}^n, a_\nu X, a_\mu Y) = C(\mathfrak{X}^n, X, Y, B_i(a_\nu, X_i), C_i(a_\mu, X_i), F(\mathfrak{X}^n, X, Y))$$
$$F(\mathfrak{X}^n, a_\nu a_\rho X, a_\kappa a_\beta Y) = F(\mathfrak{X}^n, a_\rho a_\nu X, a_\beta a_\kappa Y), \qquad (1 \leq i \leq n),$$

where A, B, C, A_i, B_i, C_i $(1 \leq i \leq n)$ are defined or starting functions of $\mathcal{D}^k$;

$$F(\overline{\mathfrak{X}}^n, \overline{X}, \#) = A(\overline{\mathfrak{X}}^n, \overline{X}),$$
$$F(\overline{\mathfrak{X}}^n, \#, a_\mu^\alpha \overline{Y}) = B(\overline{\mathfrak{X}}^n, \overline{Y}, A_i(a_\mu^\alpha, \overline{X}_i)),$$
$$F(\overline{\mathfrak{X}}^n, a_\nu^\beta \overline{X}, a_\mu^\alpha \overline{Y}) = C(\overline{\mathfrak{X}}^n, \overline{X}, \overline{Y}, B_i(a_\nu^\beta, \overline{X}_i), C_i(a_\mu^\alpha, \overline{X}_i), F(\overline{\mathfrak{X}}^n, \overline{X}, \overline{Y})) \ (1 \leq i \leq n),$$

where the variables are in normal form and the functions A, B, C, A_i, B_i, C_i $(1 \leq i \leq n)$ are defined or starting functions $\mathcal{D}^k$.

With respect to the definition structure $\mathcal{D}^k$ $(k \geq 0)$, we note that we do not assume that the maps $\tau, \bar{\tau}, \tau_k$ and $\bar{\tau}_k$, taken as starting functions in $\mathcal{D}^k$, are recursive in the usual sense, i.e., recursive with respect to $F(a_1)$ or $A^\#$.

§3.2. Foundations of abstract arithmetics $\mathcal{A}^k(A)$

For any $k \geq 0$, the abstract arithmetic $\mathcal{A}^k(A)$ consists of the following objects and rules:

(I) Commutative k-frame $\mathcal{K}^k$.

(II) The k-definition structure $\mathcal{D}^k$.

(III) Propositional calculus with the logical constants: $\wedge$ (conjunction), $\vee$ (disjunction), $\Longrightarrow$ (implication), $\Longleftrightarrow$ (equivalence), ^{non} or / (negation),

$\bigwedge \partial(X) \leq \partial(Y)$ (restricted universal quantifier), $\bigvee \partial(X) \leq \partial(Y)$ (restricted existential quantifier), and $\mu\partial(X) \leq \partial(Y)$ (restricted minimalization).

(IV) The rules of proof in arithmetic $\mathcal{A}^k(A)$ are restricted to those in the propositional calculus and the following induction rules:

(1) Suppose that for each word X in F(A) we are given a sentence $\mathfrak{F}(X)$, and that we can prove the following. (i) The sentence $\mathfrak{F}(\#)$ is true. (ii) For each word X, if $\mathfrak{F}(Y)$ is true then $\mathfrak{F}(a_\mu Y)$ is true. Then sentence $\mathfrak{F}(X)$ is true for all X. This is the Induction Theorem 2.2.5.

(2) Suppose that for each word X in F(A) we are given a sentence $\mathfrak{H}(X)$, and that we can prove the following. (i) The sentence $\mathfrak{H}(\#)$ is true. (ii) For each word X, if $\mathfrak{H}(Y)$ is true for any Y with one of the following properties

(a) $\# \trianglelefteq \lambda(Y) \trianglelefteq \lambda(X)$,

(b) $\# \leq \partial(Y) \leq \partial(X)$,

(c) $\# \leq \mathfrak{k}(Y) \leq \mathfrak{k}(X)$,

then $\mathfrak{H}(a_\mu X)$ is true. Then the sentence $\mathfrak{H}(X)$ is true for all X.

As Skolem [10, 11] pointed out, the main purpose of the above type of restrictions is to insure us against inconsistency occurring in arithmetics.

In the following chapters, for convenience of reading, we shall not in general fully adhere to the usual complete symbolic statements of definitions and theorems in $\mathcal{A}^k(A)$ $(k \geq 0)$.

§3.3. Inequality and word subtraction

Recalling chapter II, in arithmetic $\mathcal{A}^k(A)$ $(k \geq 0)$, the word addition is $X \oplus Y$ and word multiplication is $X \odot Y$, which we reintroduce as follows:

(1)
$$X \oplus \# = X,$$
$$X \oplus a_\mu Y = a_\mu(X \oplus Y),$$

(2)
$$X \odot \# = \#,$$
$$X \odot a_\mu Y = (a_\mu \odot X) \oplus (X \odot Y).$$

See Proposition 2.3.7 for the properties of word multiplication.

In turn, the inequality relation $X \lesssim Y$ with respect to $X \oplus Y$ is defined in arithmetic $\mathcal{Q}^k(A)$ $(k \geq 0)$ as follows:

(3) $$X \lesssim Y \iff \bigvee \partial(Z) \leq \partial(Y) \{Y = X \oplus Z\}.$$

3.3.1. Proposition. In arithmetic $\mathcal{Q}^k(A)$ $(k \geq 0)$, we have the following:

(1) $X \lesssim X$,

(2) if $X \lesssim Y$ and $Y \lesssim X$ then $X = Y$,

(3) if $X \lesssim Y$ and $Y \lesssim Z$ then $X \lesssim Z$.

Property (1) is obvious. As for property (2), from its assumption we have $Y = X \oplus I_1$, $X = Y \oplus I_2$ for some words I_1, I_2 in $F(A)$. Substituting and using the associative law, we obtain $X = (X \oplus I_1) \oplus I_2 = X \oplus (I_1 \oplus I_2)$. By the symbolic uniqueness Theorem 2.2.6, both I_1 and I_2 must be empty words, consequently, $X = Y$.

For Property (3), from its assumption, we have $Y = X \oplus I_1$ and $Z = Y \oplus I_2$, and by substituting and using the associative law, $Z = Y \oplus I_2 = (X \oplus I_1) \oplus I_2 = X \oplus (I_1 \oplus I_2)$, consequently $X \lesssim Z$.

In order to define word subtraction in $\mathcal{Q}^k(A)$ $(k \geq 0)$, it is convenient to introduce the word predecessor function $\mathrm{pred}_\nu(X)$ by the following equations:

$$\mathrm{pred}_\nu(\#) = \#,$$
$$\mathrm{pred}_\nu(a_\mu X) = X \text{ if } \nu = \mu,$$
$$= a_\mu \oplus \mathrm{pred}_\nu(X) \text{ if } \nu \neq \mu.$$

With the help of $\mathrm{pred}_\nu(X)$, we define word subtraction $X [\dot{-}] Y$ in $\mathcal{Q}^k(A)$ as follows:

$$X [\dot{-}] \# = X,$$
$$X [\dot{-}] a_\mu Y = \mathrm{pred}_\mu(X [\dot{-}] Y).$$

We note that in $\mathcal{Q}^k(A)$ $(k \geq 0)$ there are various other forms of word subtractions, which we shall not study in this paper. In turn, we note that the length function $\lambda(X)$ is introduced in arithmetic $\mathcal{Q}^k(A)$ as shown in section 2.4.

3.3.2. Proposition. In arithmetic $\mathcal{A}^k(A)$ $(k \geq 0)$,

(1) $a_\mu X \,[\dot{-}]\, a_\mu Y = X \,[\dot{-}]\, Y$,

(2) $X \,[\dot{-}]\, X = \#$;

(3) $\# \,[\dot{-}]\, X = \#$;

(4) $(X \oplus Y) \,[\dot{-}]\, Y = X$,

(5) if $Y \prec X$ then $(X[\dot{-}]Y) \oplus Y = X$,

(6) if $X \,[\dot{-}]\, Y = \#$ then either $X = \#$, $X \prec Y$ or $X = Y$,

(7) if $X \preceq Y$ then $\lambda(Y \,[\dot{-}]\, X) = \lambda(Y) \,[\dot{-}]\, \lambda(X)$.

Property (1) is trivial for $Y = \#$. Let it hold for some Y, then

$$a_\mu X \,[\dot{-}]\, a_\mu(a_a Y) = \mathrm{pred}_a(a_\mu X \,[\dot{-}]\, a_\mu Y)$$
$$= \mathrm{pred}_a(X \,[\dot{-}]\, Y) = X \,[\dot{-}]\, a_a Y.$$

Consequently, this property holds for all Y.

Property (2) is also trivial for $X = \#$. Suppose it is true for some X. Then by property (1), using the inductive hypothesis, we have $a_\mu X \,[\dot{-}]\, a_\mu X = X \,[\dot{-}]\, X = \#$.

Property (3) is obvious for $X = \#$. Let it hold for some X, then

$$\# \,[\dot{-}]\, a_\mu X = \mathrm{pred}_\mu(\# \,[\dot{-}]\, X) = \mathrm{pred}_\mu(\#) = \#.$$

Property (4) is clear for $Y = \#$, and supposing the inductive hypothesis, by property (1) we get

$$(X \oplus a_\mu Y) \,[\dot{-}]\, a_\mu Y = a_\mu(X \oplus Y) \,[\dot{-}]\, a_\mu Y = (X \oplus Y)[\dot{-}]\, Y = X .$$

For property (5), let $Y \prec X$, then $X = Y \oplus I$ for some I in $F(A)$, and in turn by property (4) we obtain

$$(X \,[\dot{-}]\, Y) \oplus Y = ((Y \oplus I) \dot{-} Y) \oplus Y = I \oplus Y = X.$$

Property (6) follows from properties (2) and and definitions.

For property (7), let $X \preceq Y$ and $Y = X \oplus I$ for some $I \in F(A)$. Then by (4), $\lambda(Y \,[\dot{-}]\, X) = \lambda((X \oplus I) \,[\dot{-}]\, X) = \lambda(I)$. On the other hand, since $\lambda(X \oplus I) = \lambda(X) \oplus \lambda(I)$ by Proposition 2.4.3, we obtain by property (4), $\lambda(X \oplus I) \,[\dot{-}]\, \lambda(X) = (\lambda(X) \oplus \lambda(I)) \,[\dot{-}]\, \lambda(X) = \lambda(I)$. Consequently, property (7) is true.

In order to give our next result, we recall from section 2.2 that the words in $F(A)$ can be put in normal form as $a_\mu^m \overline{X}$ $(\mu \geq 1,\ m \geq 0)$. In turn, note the following definition

$$a_\nu^n \,[\dot{-}]\, a_\mu^m = \# \qquad \text{if } n \leq m \text{ and } \mu \leq \nu,$$
$$\text{or } n \leq m \text{ and } \mu > \nu,$$
$$\text{or } n > m \text{ and } \mu \leq \nu,$$
$$= a_{\mu-\nu}^{n-m} \quad \text{if } n > m \text{ and } \mu > \nu.$$

3.3.3. Lemma. For normal-form words in $F(A)$, we have

$$a_\nu^n \overline{X} \,[\dot{-}]\, a_\mu^m \overline{Y} = (a_\nu^n \,[\dot{-}]\, a_\mu^m) \oplus (\overline{X} \,[\dot{-}]\, \overline{Y}).$$

When $\overline{X} = \#$, then it is clear from the definitions of $a_\nu^n \,[\dot{-}]\, a_\mu^m$ and $\overline{X} \,[\dot{-}]\, \overline{Y}$. Let the theorem hold for some normal-form word $\overline{Y}$. Let

$$\mathrm{pred}_\sigma^s(X) = \mathrm{pred}_\sigma(\mathrm{pred}_\sigma(\ldots \mathrm{pred}_\sigma(\mathrm{pred}_\sigma(X))\ldots))(\mathrm{pred}_\sigma \text{ s-times}).$$

Then, using the definitions in this section, we have

$$\begin{aligned}
(a_\nu^n \,[\dot{-}]\, a_\mu^m) \oplus (\overline{X} \,[\dot{-}]\, a_\sigma^s \overline{Y}) &= (a_\nu^n \,[\dot{-}]\, a_\mu^m) \oplus \mathrm{pred}_\sigma^s(\overline{X} \,[\dot{-}]\, \overline{Y}) \\
&= \mathrm{pred}_\sigma^s((a_\nu^n \,[\dot{-}]\, a_\mu^m) \oplus (\overline{X} \,[\dot{-}]\, \overline{Y})) \\
&= \mathrm{pred}_\sigma^s(a_\nu^n \overline{X} \,[\dot{-}]\, a_\mu^m \overline{Y}) \\
&= a_\nu^n \overline{X} \,[\dot{-}]\, a_\sigma^s(a_\mu^m \overline{Y}) \\
&= a_\nu^n \overline{X} \,[\dot{-}]\, a_\mu^m(a_\sigma^s \overline{Y}).
\end{aligned}$$

3.3.4. Theorem. For all X, Y and Z in $F(A)$,

$$Z \odot (X \,[\dot{-}]\, Y) = (Z \odot Y) \,[\dot{-}]\, (Z \odot Y).$$

In this proof we assume all variables to be in normal form. Firstly, let $Z = a_\sigma^s$, $X = a_\nu^n$ and $Y = a_\mu^m$. If $a_\nu^n = a_\mu^m$ then clearly $a_\sigma^s \odot a_\nu^n = a_\sigma^s \odot a_\mu^m$ and $a_\sigma^s \odot a_\nu^n \,[\dot{-}]\, a_\sigma^s \odot a_\mu^m = a_\sigma^s \odot (a_\nu^n \,[\dot{-}]\, a_\mu^m)$. On the other hand, if $a_\nu^n \neq a_\mu^m$ then clearly $a_\sigma^s \odot a_\nu^n \neq a_\sigma^s \odot a_\mu^m$ and

$$a_\sigma^s \odot a_\nu^n \,[\dot{-}]\, a_\sigma^s \odot a_\mu^m = a_\sigma^s \odot a_\nu^n,\ a_\sigma^s \odot (a_\nu^n \,[\dot{-}]\, a_\mu^m) = a_\sigma^s \odot a_\nu^n.$$

Secondly, consider the case $Z = a_\sigma^s$ and X and Y arbitrary. If $X = Y$, then $a_\sigma^s \odot X = a_\sigma^s \odot Y$ and clearly

$$a_\sigma^s \odot X \,[\dot{-}]\, a_\sigma^s Y = a_\sigma^s \odot (X \,[\dot{-}]\, Y).$$

In turn, consider the case $X \neq Y$. Putting X and Y in normal form, assume that the theorem holds for some $\overline{X}$ and $\overline{Y}$, then by using Lemma 3.3.3 and the above we get

$$\begin{aligned}
a_\sigma^s \odot X \,[\dot{-}]\, a_\sigma^s \odot Y &= (a_\sigma^s \odot a_\nu^n \overline{X}) \,[\dot{-}]\, (a_\sigma^s \odot a_\mu^m \overline{Y}) = \\
&= [(a_\sigma^s \odot a_\nu^n) \oplus (a_\sigma^s \odot \overline{X})] \,[\dot{-}]\, [(a_\sigma^s \odot a_\mu^m) \oplus (a_\sigma^s \odot \overline{Y})] \\
&= [(a_\sigma^s \odot a_\nu^n) \,[\dot{-}]\, (a_\sigma^s \odot a_\nu^m)] \oplus (a_\sigma^s \odot \overline{X} \,[\dot{-}]\, a_\sigma^s \odot \overline{Y}) \\
&= a_\sigma^s \odot (a_\nu^n \,[\dot{-}]\, a_\mu^m) \oplus a_\sigma^s \odot (\overline{X} \,[\dot{-}]\, \overline{Y}) \\
&= a_\sigma^s \odot [(a_\sigma^n \,[\dot{-}]\, a_\mu^m) \oplus (\overline{X} \,[\dot{-}]\, \overline{Y})] \\
&= a_\sigma^s \odot (a_\nu^n \overline{X} \,[\dot{-}]\, a_\mu^m \overline{Y}) \\
&= a_\sigma^s \odot (X \,[\dot{-}]\, Y).
\end{aligned}$$

Finally, for arbitrary Z, X and Y, the case $X = Y$ is obvious, and for the case $X \neq Y$, let $Z = a_\sigma^{s_\sigma} a_{\sigma-1}^{s_{\sigma-1}} \ldots a_1^{s_1}$, $X = a_\mu^m \overline{X}$ and $Y = a_\nu^n \overline{Y}$. Using the definition of word multiplication, definitions of word subtractions above, the distributive law, Lemma 3.3.3, carrying out the following procedure term-by-term, we have:

$$\begin{aligned}
Z \odot X \,[\dot{-}]\, Z \odot Y &= a_\sigma^{s_\sigma} \ldots a_1^{s_1} \odot X \,[\dot{-}]\, a_\sigma^{s_\sigma} \ldots a_1^{s_1} \odot Y = \\
&= (a_\sigma^{s_\sigma} \odot X \oplus \ldots \oplus a_1^{s_1} \odot X) \,[\dot{-}]\, (a_\sigma^{s_\sigma} \odot Y \oplus \ldots \oplus a_1^{s_1} \odot Y) \\
&= ((a_\sigma^{s_\sigma} \odot a_\mu^m \oplus a_\sigma^{s_\sigma} \odot \overline{X}) \oplus \ldots \oplus a_1^{s_1} \odot X) \,[\dot{-}]\, ((a_\sigma^{s_\sigma} \odot a_\nu^n \oplus a_\sigma^{s_\sigma} \odot \overline{Y}) \oplus \ldots \oplus a_1^{s_1} \odot Y)) \\
&= (a_\sigma^{s_\sigma} \odot a_\mu^m \,[\dot{-}]\, a_\sigma^{s_\sigma} \odot a_\nu^n) \oplus [(a_\sigma^{s_\sigma} \odot \overline{X} \oplus \ldots \oplus a_1^{s_1} \odot X) \,[\dot{-}]\, (a_\sigma^{s_\sigma} \odot \overline{Y} \oplus \ldots \oplus a_1^{s_1} \odot Y)] \\
&= a_\sigma^{s_\sigma} \odot (a_\mu^m \,[\dot{-}]\, a_\nu^n) \oplus [(a_\sigma^{s_\sigma} \odot \overline{X} \oplus \ldots \oplus a_1^{s_1} \odot X) \,[\dot{-}]\, (a_\sigma^{s_\sigma} \odot \overline{Y} \oplus \ldots \oplus a_1^{s_1} \odot Y)] \\
&= [a_\sigma^{s_\sigma} \odot (a_\mu^m \,[\dot{-}]\, a_\nu^n) \oplus \ldots \oplus a_1^{s_1} \odot (a_\mu^m \,[\dot{-}]\, a_1^n)] \oplus [a_\sigma^{s_\sigma} \odot (\overline{X} \,[\dot{-}]\, \overline{Y}) \oplus \ldots \oplus a_1^{s_1} \odot (\overline{X} \,[\dot{-}]\, \overline{Y})]
\end{aligned}$$

$$= [a_\sigma^{s_\sigma} \ldots a_1^{s_1} \odot (a_\mu^m [\dot{-}] a_\nu^n)] \oplus [a_\sigma^{s_\sigma} \ldots a_1^{s_1} \odot (\overline{X} [\dot{-}] \overline{Y})]$$

$$= a_\sigma^{s_\sigma} \ldots a_1^{s_1} \odot [(a_\mu^m [\dot{-}] a_\nu^n) \oplus (\overline{X} [\dot{-}] \overline{Y})]$$

$$= Z \odot (a_\mu^{m\overline{X}} [\dot{-}] a_\nu^{n\overline{Y}})$$

$$= Z \odot (X [\dot{-}] Y).$$

§3.4. Divisibility theory

In $\mathcal{A}^k(A)$ $(k \geq 0)$, we introduce the divisibility relation $X \| Y$ as follows:

$$X \| Y \Longleftrightarrow \vee \partial(Z) \leq \partial(X)\{X = Y \odot Z \wedge Z \neq \#\} .$$

3.4.1. Proposition. In $\mathcal{A}^k(A)$ $(k \geq 0)$, we have the following:

(1) if $X \| Y$ and $Y \| Z$ then $X \| Z$,

(2) if $X \| Y$ and $Y \| X$ then $X = Y$,

(3) if $X \| Y$ then $C \odot X \| C \odot Y$ $(C \neq \#)$,

(4) if $X \| Y$ and $X \| Z$ then $X \| (Y \oplus Z)$,

(5) if $Z \| (X \oplus Y)$ and $Z \| Y$ then $Z \| X$,

(6) if $Z \| (X [\dot{-}] Y)$ and $Z \| Y$ then $Z \| X$.

For property (1), let $X \| Y$ and $Y \| Z$, then $Y = X \odot I_1$ and $Z = Y \odot I_2$ for some I_1 and I_2 in $F(A)$. By substitution, we get $Z = Y \odot I_2 = (X \odot I_1) \odot I_2 = X \odot (I_1 \odot I_2)$, which means that $X \| Z$.

For property (2), let $Y = X \odot I_1$ and $X = Y \odot I_2$, then $Y = X \odot I_1 = (Y \odot I_2) \odot I_1 = Y \odot (I_2 \odot I_1)$, which means that I_1 and I_2 must be equal to a_1, hence $Y = X$.

For property (3), let $X \| Y$, then $Y = X \odot I$, for some I. Multiplying on both sides of this equation by C, where $C \neq \#$, we obtain $C \odot Y = C \odot (X \odot I) = (C \odot X) \odot I$, which means that $C \odot X \| C \odot Y$.

For property (4), from the assumption of this property, we get $Y = X \odot I_1$ and $Z = X \odot I_2$ for some I_1 and I_2. By the distributive law we obtain $Y \oplus Z = (X \odot I_1) \oplus (X \odot I_2) = X \odot (I_1 \oplus I_2)$, which means that $X \| (Y \oplus Z)$.

For property (5), let $Z \| (X \oplus Y)$ and $Z \| Y$, then $X \oplus Y = Z \odot I_1$ and $Y = Z \odot I_2$, for some I_1 and I_2. Hence, $X \oplus Y = X \oplus Z \odot I_2 = Z \odot I_1$, and by the distributive law there must exist a I_3 such that $X = Z \odot I_3$, i.e., $X \oplus (Z \odot I_2) = Z \odot I_3 \oplus Z \odot I_2 = Z \odot I_1$, where $I_1 = I_3 \oplus I_2$, which means that $Z \| X$.

For property (6), let $Z \| (X [\dot{-}] Y)$ and $Z \| Y$. Then $X [\dot{-}] Y = Z \odot I_1$ and $Y = Z \odot I_2$. Substituting, we obtain $X [\dot{-}] Y = X [\dot{-}] (Z \odot I_2) = Z \odot I_1$, and by Theorem 3.3.4, we must have $X = Z \odot I_3$, complying with $X [\dot{-}] Z \odot I_2 = Z \odot I_3 [\dot{-}] Z \odot I_2 = Z \odot (I_3 [\dot{-}] I_2)$.

Before introducing the prime words of the divisibility theory of arithmetic $\mathcal{Q}^k(A)$ $(k \geq 0)$, we note that word exponentiation in $\mathcal{Q}^k(A)$ is defined as follows:

$$X \Delta \# = a_1,$$
$$X \Delta a_\mu Y = (a_\mu \odot X) \odot (X \Delta Y).$$

3.4.2. Proposition. In $\mathcal{Q}^k(A)$ $(k \geq 0)$, for any X, Y in F(A) and nonempty B,

(1) $X \Delta a_1 = X$,

(2) $(B \Delta X) \odot (B \Delta Y) = B \Delta (X \oplus Y)$.

For property (1), given $X = \#$, we have $\# \Delta a_1 = (a_1 \odot \#) \odot (\# \Delta \#) = \# \odot a_1 = \#$. Assume the inductive hypothesis, then

$$a_\mu X \Delta a_1 = (a_1 \odot a_\mu X) \odot (a_\mu X \Delta \#) = a_\mu X \odot a_1 = a_\mu X.$$

With respect to property (2), for $Y = \#$, we have

$$(B \Delta X) \odot (B \Delta \#) = (B \Delta X) \odot a_1 = B \Delta X,$$

$$B \Delta (X \oplus \#) = B \Delta X.$$

Assume the inductive hypothesis, then

$$\begin{aligned}(B \Delta X) \odot (B \Delta a_\mu Y) &= (B \Delta X) \odot (a_\mu \odot B) \odot (B \Delta Y) \\ &= (a_\mu \odot B) \odot (B \Delta (X \oplus Y)) \\ &= B \Delta a_\mu (X \oplus Y) = B \Delta (X \oplus a_\mu Y).\end{aligned}$$

In $\mathfrak{A}^k(A)$ $(k \geqq 0)$, the prime-word relation pw(X) is defined by:

$$\mathrm{pw}(X) \iff \bigwedge \partial(Z) \leqq \partial(X)\{Z \| X \implies Z = X \vee Z = a_1\}.$$

In turn, we define the prime words $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \ldots$ in arithmetic $\mathfrak{A}^k(A)$ $(k \geqq 0)$ as follows:

$$\mathfrak{p}_1 = a_2$$
$$\mathfrak{p}_{n+1} = \mu\, \partial(Z) \leqq \partial(a_1^2 \Delta (a_1^2 \Delta a_1^{n+1}))\{\partial(\mathfrak{p}_n) < \partial(Z) \wedge \mathrm{pw}(Z)\},$$

obtaining $\mathfrak{p}_1 = a_2$, $\mathfrak{p}_2 = a_1 a_1$, $\mathfrak{p}_3 = a_3, \ldots$. We denote the set of all prime words in $\mathfrak{A}^k(A)$ by $\mathfrak{P}$.

3.4.3. Lemma. If $X \neq \#$ and $X \neq a_1$, then either pw(X) or $X = Y_1 \odot Y_2$ for some Y_1 and Y_2 in F(A).

This lemma follows directly from the above definition of the relation pw(X).

A word in F(A) is called a composite word if it is not a prime word, of course, except # and a_1.

We define the greatest common word divisor of X and Y, denoted gcd(X, Y), as follows:

$$Z = \gcd(X, Y) \iff Z \| X \wedge Z \| Y \wedge \bigwedge \partial(W) \leqq \partial(X) \wedge \partial(W) \leqq \partial(Y)\{W \| X \wedge W \| Y \implies W \| Z\}.$$

3.4.4. Lemma. In arithmetic $\mathfrak{A}^k(A)$ $(k \geqq 0)$,

(1) $\gcd(X, Y) \| X$ and $\gcd(X, Y) \| Y$,

(2) $\gcd(X, a_1) = a_1$.

Both of the above properties are consequences of the definitions of gcd and the divisibility relation.

In the following lemmas we shall assume that they pertain to any arithmetic $\mathfrak{A}^k(A)$ $(k \geqq 0)$, thereby avoiding needless repetition.

3.4.5. Lemma. If A, B and C are nonempty words in F(A), then

$$\gcd(C \odot A,\ C \odot B) = C \odot \gcd(A, B).$$

To prove this lemma we need to consider the following cases: (I) $A = B$; (II) $B \prec A$ or $B \succ A$; (III) $B \neq A$, $B \not\prec A$ and $B \not\succ A$.

(I) Let $A = B$. We dispose of this case by observing that $\gcd(A, B) = A = B$, thus $\gcd(C \odot A, C \odot B) = C \odot A = C \odot B = C \odot \gcd(A, B)$.

(II) Let A, B and C be nonempty words and let $B \prec A$. If $B = a_1$ and A is any word satisfying $B \prec A$, then by Lemma 3.4.4 (2), we have $\gcd(A, B) = a_1$, and consequently $\gcd(C \odot A, C \odot B) = C \odot a_1 = C \odot \gcd(A, B)$.

Assume that case (II) holds for every A and B such that $\lambda(A) \oplus \lambda(B) \prec \lambda(N)$ for some N in F(A).

Since $B \prec A$, by Proposition 3.3.2(5) we have $(A [\dot{-}] B) \oplus B = A$. By Lemma 3.4.4(2), we have $\gcd(A [\dot{-}] B, B) \| B$ and $\gcd(A [\dot{-}] B, B) \| (A [\dot{-}] B)$. By Proposition 3.4.1(4), we have $\gcd(A [\dot{-}] B, B) \| A$. Consequently, from the definition of gcd it follows that

$$(1)\quad \gcd(A [\dot{-}] B, B) \| \gcd(A, B).$$

On the other hand, by Lemma 3.4.4(1) we also have $\gcd(A, B) \| A$ and $\gcd(A, B) \| B$, and $\gcd(A, B) \| (A [\dot{-}] B) \oplus B$ since $(A [\dot{-}] B) \oplus B = A$. By Proposition 3.4.1(5) we obtain $\gcd(A, B) \| (A [\dot{-}] B)$.

Finally, since $\gcd(A, B) \| (A [\dot{-}] B)$ and $\gcd(A, B) \| B$, by the definition of gcd we get

$$(2)\quad \gcd(A, B) \| \gcd(A [\dot{-}] B, B).$$

By Proposition 3.4.1(2), combining (1) and (2) above, we obtain

$$(3)\quad \gcd(A, B) = \gcd(A [\dot{-}] B, B).$$

Since $B \prec A$ and $A \neq \#$, by Proposition 3.3.2(6) we have $A [\dot{-}] B \neq \#$ and by Theorem 3.3.4 we get

$$C \odot (A [\dot{-}] B) = C \odot A [\dot{-}] C \odot B,$$

consequently $C \odot A [\dot{-}] C \odot B \neq \#$, and so from (3) it follows that

$$(4)\quad \gcd(C \odot A, C \odot B) = \gcd(C \odot A [\dot{-}] C \odot B, B).$$

At this point we observe that

$$\lambda(A\ [\dot{-}]\ B) \oplus \lambda(B) \prec \lambda(N)$$

because $\lambda(A\ [\dot{-}]\ B) \oplus \lambda(B) = \lambda((A\ [\dot{-}]\ B) \oplus B)$ by Proposition 2.4.3(1), and by Proposition 3.3.2(5) we have $(A\ [\dot{-}]\ B) \oplus B = A$, which means that $\lambda(A\ [\dot{-}]\ B) \oplus \lambda(B) \prec \lambda(A) \oplus \lambda(B)$, since $B \neq \#$. Therefore, by the inductive hypothesis we obtain

$$(5)\quad \gcd(C \odot (A\ [\dot{-}]\ B),\ C \odot B) = C \odot \gcd(A\ [\dot{-}]\ B,\ B).$$

Since by Theorem 3.3.4 we have

$$C \odot (A\ [\dot{-}]\ B) = C \odot A\ [\dot{-}]\ C \odot B,$$

it follows from (4) that

$$\gcd(C \odot A,\ C \odot B) = \gcd(C \odot (A\ [\dot{-}]\ B),\ C \odot B),$$

and from (5) and (3) that

$$\begin{aligned}\gcd(C \odot A,\ C \odot B) &= C \odot \gcd(A\ [\dot{-}]\ B,\ B)\\ &= C \odot \gcd(A, B).\end{aligned}$$

(III) The final case we leave, since it requires introducing other forms of word subtractions relating to functions $k(X)$ and $\partial(X)$ given in section 2.4, which take us too far afield from the main purpose of this paper.

3.4.6. Lemma. If $C \| A$ and $C \| B$, then $C \| \gcd(A, B)$.

If $C \| A$ and $C \| B$, then $A = C \odot I_1$, $B = C \odot I_2$ and

$$(1)\quad \gcd(A, B) = \gcd(C \odot I_1,\ C \odot I_2),$$

for some I_1 and I_2. By Lemma 3.4.5 and (1) we get

$$\gcd(A, B) = C \odot \gcd(I_1, I_2),$$

which means that $C \| \gcd(A, B)$.

3.4.7. Lemma. If $B \| C \odot A$ and $\gcd(A, B) = a_1$, then $B \| C$.

From $B \| C \odot A$, $B \| C \odot B$ and Lemma 3.4.6, it follows that

$$B \| \gcd(C \odot A,\ C \odot B).$$

In turn, from the assumption $\gcd(A, B) = a_1$ and Lemma 3.4.5 we get

$$\gcd(C \odot A,\ C \odot B) = C \odot \gcd(A, B) = C,$$

and consequently $B \| C$.

3.4.8. Lemma. If $X \| \mathfrak{p}_\mu$ then $X = \mathfrak{p}_\mu$ or $X = a_1$.

If $X \| \mathfrak{p}_\mu$, then clearly by definition of a prime word it follows that $\mathfrak{p}_\mu = X$ or $\mathfrak{p}_\mu = a_1$.

3.4.9. Lemma. If $\mathfrak{p}_\mu \nparallel X$, then $\gcd(\mathfrak{p}_\mu, X) = a_1$.

From Lemma 3.4.4(1) we obtain $\gcd(\mathfrak{p}_\mu, X) \| \mathfrak{p}_\mu$, and by Lemma 3.4.8 it follows that either (1) $\gcd(\mathfrak{p}_\mu, X) = a_1$ or (2) $\gcd(\mathfrak{p}_\mu, X) = \mathfrak{p}_\mu$. Considering the case $\gcd(\mathfrak{p}_\mu, X) = \mathfrak{p}_\mu$, we see this by Lemma 3.4.4(1) leads to the contradiction $\mathfrak{p}_\mu \| X$. Therefore, case (1) must be true.

3.4.10. Lemma. If $\mathfrak{p}_\mu \| X \odot Y$, then $\mathfrak{p}_\mu \| X$ or $\mathfrak{p}_\mu \| Y$.

According to Lemma 3.4.9, either $\mathfrak{p}_\mu \| X$ or $\gcd(\mathfrak{p}_\mu, X) = a_1$, and from the assumption $\mathfrak{p}_\mu \| X \odot Y$ it follows that either (1) $\mathfrak{p}_\mu \| X$ or (2) $\mathfrak{p}_\mu \| X \odot Y$ and $\gcd(\mathfrak{p}_\mu, X) = a_1$. In turn, by 3.4.7, if $\mathfrak{p}_\mu \| X \odot Y$ and $\gcd(\mathfrak{p}_\mu, X) = a_1$ then $\mathfrak{p}_\mu \| Y$.

3.4.11. Lemma. If $\mathfrak{p}_\mu \| X_1 \odot X_2 \odot \dots \odot X_n$, then $\mathfrak{p}_\mu \| X_k$ for some k $(1 \leq k \leq n)$.

The lemma is trivial for $n = 1$. Assume the lemma to be true for some n. Then, by Lemma 3.4.10, we obtain $\mathfrak{p}_\mu \| X_{n+1}$ or $\mathfrak{p}_\mu \| X_1 \odot \dots \odot X_n$, and in turn by the inductive hypothesis we get $\mathfrak{p}_\mu \| X_k$ for some k $(1 \leq k \leq n)$. Therefore, from $\mathfrak{p}_\mu \| X_k$ for some k $(1 \leq k \leq n)$ and $\mathfrak{p}_\mu \| X_{n+1}$, it follows that $\mathfrak{p}_\mu \| X_k$ for some k $(1 \leq k \leq n)$.

3.4.12. Lemma. If $\mathfrak{p}_\mu \| \mathfrak{p}_{i_n} \odot \mathfrak{p}_{i_{n-1}} \odot \dots \odot \mathfrak{p}_{i_1}$, then $\mathfrak{p}_\mu = \mathfrak{p}_{i_k}$ for some k $(1 \leq k \leq n)$.

According to Lemma 3.4.11, if $\mathfrak{p}_\mu \| \mathfrak{p}_{i_r} \odot \cdots \odot \mathfrak{p}_{i_1}$ then $\mathfrak{p}_\mu \| \mathfrak{p}_{i_k}$ for some k $(1 \leq k \leq n)$. From $\mathfrak{p}_\mu \| \mathfrak{p}_{i_k}$ for some k $(1 \leq k \leq n)$ and Lemma 3.4.8 it follows that $\mathfrak{p}_\mu = \mathfrak{p}_{i_k}$ for some k $(1 \leq k \leq n)$ or $\mathfrak{p}_\mu = a_1$. Since $\mathfrak{p}_\mu \neq a_1$, we must have $\mathfrak{p}_\mu = \mathfrak{p}_{i_k}$ for some k $(1 \leq k \leq n)$.

3.4.13. Theorem. (Prime-word unique factorization theorem)

Except for # and a_1, every word X in F(A) can be uniquely expressed in nonunique order as $X = \mathfrak{p}_{i_r} \odot \mathfrak{p}_{i_{r-1}} \odot \cdots \odot \mathfrak{p}_{i_1}$, where $\mathfrak{p}_{i_1}, \mathfrak{p}_{i_2}, \ldots, \mathfrak{p}_{i_r} \in \mathfrak{P}$.

Existence. Assume that there exist words which cannot be expressed as word-products of prime words. By Lemma 3.4.3, since such words cannot be prime words, we must have $X = Y_1 \odot Y_2$ for some Y_1 and Y_2. From the set of such words X select the word X_0 with the least value $\partial(X_0)$. Clearly, $X_0 = X_1 \odot X_2$ for some X_1, X_2, and $X_0 \neq X_1$ and $X_0 \neq X_2$. By Proposition 2.4.5(2) it follows that $\partial(X_0) \neq \partial(X_1)$ and $\partial(X_0) \neq \partial(X_2)$. On the other hand, since $X_0 = X_1 \odot X_2$, if $X_1 = a_{i_r} a_{i_{r-1}} \ldots a_{i_1}$, then $X_0 = a_{i_r} \odot X_2 \oplus a_{i_{r-1}} \odot X_2 \oplus \ldots \oplus a_{i_1} \odot X_2$ and by Proposition 2.4.5(1) we have $\partial(X_0) = \partial(a_{i_r} \odot X_2) \boxplus \ldots \boxplus \partial(a_{i_1} \odot X_2)$, consequently we must have $\partial(X_0) > \partial(X_2)$ and also by the same way $\partial(X_0) > \partial(X_1)$. Therefore, by our assumption, the words X_1 and X_2 are expressible as word-products of prime words, hence the word X_0 must also be expressible as a word-product of prime words, which is a contradition.

Uniqueness. To prove uniqueness of prime-word factorizations, consider

$$\mathfrak{p}_{i_r} \odot \mathfrak{p}_{i_{r-1}} \odot \cdots \odot \mathfrak{p}_{i_1} = \mathfrak{p}_{j_s} \odot \mathfrak{p}_{j_{s-1}} \odot \cdots \odot \mathfrak{p}_{j_1}.$$

For the case r = 1, if $\mathfrak{p}_{i_1} = \mathfrak{p}_{j_s} \odot \cdots \odot \mathfrak{p}_{j_1}$, then by Lemma 3.4.12 we must have $\mathfrak{p}_{i_1} = \mathfrak{p}_{i_k}$ for some k $(1 \leq k \leq s)$. Hence the theorem is true for r = 1.

Assume that the theorem is true for some r. Then, from

$$\mathfrak{p}_{i_{r+1}} \odot \mathfrak{p}_{i_r} \odot \cdots \odot \mathfrak{p}_{i_1} = \mathfrak{p}_{j_s} \odot \mathfrak{p}_{j_{s-1}} \odot \cdots \odot \mathfrak{p}_{j_1},$$

we obtain

$$\mathfrak{p}_{i_{r+1}} \parallel \mathfrak{p}_{j_s} \odot \cdots \odot \mathfrak{p}_{j_1},$$

and by Lemma 3.4.12 in turn we get $\mathfrak{p}_{i_{r+1}} = \mathfrak{p}_{j_k}$ for some k $(1 \leqq k \leqq s)$. For convenience, let k = s. Then by the inductive hypothesis it follows that

$$\mathfrak{p}_{i_r} \odot \cdots \odot \mathfrak{p}_{i_1} = \mathfrak{p}_{j_{s-1}} \odot \cdots \odot \mathfrak{p}_{j_1},$$

where each $\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_r}$ equals some $\mathfrak{p}_{j_1}, \ldots, \mathfrak{p}_{j_{s-1}}$ and each $\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{j_{s-1}}$ equals some $\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_r}$. Therefore, the prime-word factorizations are unique for all r.

3.4.14. Corollary. (1) Theorem 3.4.13 implies unique factorization in the nonconcatenative multiplicative monoid M_A. (2) Theorem 3.4.13 implies unique factorization of natural words a_1^{μ} in the free monoid $F(a_1)$ or a numbered free monoid $F^k(a_1)$ $(k \geqq 0)$ in terms of prime words in $\prod_{F(a_1)}$.

§3.5. Various even and odd words

In order to introduce a certain type of even words in $\mathcal{Q}^k(A)$ $(k \geqq 0)$, we need the additive conjugation function or briefly conjugation function $\Sigma(X)$, in fact a map between the free monoids $F(A)$ and $F(a_1)$, defined by the following equations:

$$\Sigma(\#) = \#,$$
$$\Sigma(a_\mu X) = \sigma(a_\mu) \oplus \Sigma(X),$$

where σ is defined in section 2.4.

Without further mention in this section, we assume relevance to arithmetics $\mathcal{Q}^k(A)$ $(k \geqq 0)$.

3.5.1. Proposition. For any words in $F(A)$, we have the following properties:

(1) $\sigma(a_\mu \boxdot a_\nu) = \sigma(a_\mu) \odot \sigma(a_\nu)$,

(2) $\Sigma(X \oplus Y) = \Sigma(X) \oplus \Sigma(Y)$,

(3) $\Sigma(a_\mu \odot X) = \sigma(a_\mu) \odot \Sigma(X)$,

(4) $\Sigma(X \odot Y) = \Sigma(X) \odot \Sigma(Y)$.

With respect to property (1), recalling the nonconcatenative semiring SM_A, we have $\sigma(a_\mu \boxplus a_1) = \sigma(a_\mu)$ and $\sigma(a_\mu) \odot \sigma(a_1) = \sigma(a_\mu) \odot a_1 = \sigma(a_\mu)$. Let property hold for some a_ν, then by properties of SM_A and word multiplication we obtain

$$\begin{aligned}\sigma(a_\mu \boxdot (a_\nu \boxplus a_1)) &= \sigma((a_\mu \boxdot a_\nu) \boxplus (a_\mu \boxdot a_1)) = \sigma(a_\mu \boxdot a_\nu) \oplus \sigma(a_\mu) \\ &= (\sigma(a_\mu) \odot \sigma(a_\nu)) \oplus \sigma(a_\mu) \\ &= \sigma(a_\mu) \odot (\sigma(a_\nu) \oplus a_1) \\ &= \sigma(a_\mu) \odot \sigma(a_\nu \boxplus a_1).\end{aligned}$$

Property (2) is clear for $Y = \#$. Assume that this property is true for some Y. Then

$$\begin{aligned}\Sigma(X \oplus a_\mu Y) &= \Sigma(a_\mu (X \oplus Y)) = \sigma(a_\mu) \oplus \Sigma(X \oplus Y) \\ &= \sigma(a_\mu) \oplus \Sigma(X) \oplus \Sigma(Y) \\ &= \Sigma(X) \oplus \sigma(a_\mu) \oplus \Sigma(Y) \\ &= \Sigma(X) \oplus \Sigma(a_\mu Y).\end{aligned}$$

Property (3) is obvious for $X = \#$. Let it hold for some X. Then by properties (1) and (2) we get

$$\begin{aligned}\Sigma(a_\mu \odot a_\nu X) &= \Sigma(a_\mu \odot (a_\nu \oplus X)) = \Sigma((a_\mu \odot a_\nu) \oplus (a_\mu \odot X)) \\ &= \Sigma(a_\mu \odot a_\nu) \oplus \Sigma(a_\mu \odot X) \\ &= \Sigma(a_\mu \odot a_\nu) \oplus \sigma(a_\mu) \odot \Sigma(X) \\ &= \sigma(a_\mu \boxdot a_\nu) \oplus \sigma(a_\mu) \odot \Sigma(X) \\ &= (\sigma(a_\mu) \odot \sigma(a_\nu)) \oplus (\sigma(a_\mu) \odot \Sigma(X)) \\ &= \sigma(a_\mu) \odot (\sigma(a_\nu) \oplus \Sigma(X)) = \sigma(a_\mu) \odot \Sigma(a_\nu X).\end{aligned}$$

Property (4) is also obvious for $Y = \#$. Assume this property for some Y. Then by properties (2) and (3),

$$\begin{aligned}\Sigma(X \odot a_\mu Y) &= \Sigma(a_\mu \odot X \oplus X \odot Y)\\ &= \Sigma(a_\mu \odot X) \oplus \Sigma(X \odot Y)\\ &= \Sigma(a_\mu \odot X) \oplus \Sigma(X) \odot \Sigma(Y)\\ &= (\sigma(a_\mu) \odot \Sigma(X)) \oplus (\Sigma(X) \odot \Sigma(Y))\\ &= \Sigma(X) \odot (\sigma(a_\mu) \oplus \Sigma(Y))\\ &= \Sigma(X) \odot \Sigma(a_\mu Y).\end{aligned}$$

Recalling that the prime word p_2 denotes the word a_1a_1 and that a_1^μ denotes a natural word in $F(a_1)$, we define various even and odd words in $\mathcal{A}^k(A)$ $(k \geq 0)$ as follows:

(1) A word X is an a_1-<u>even word</u>, denoted as $\text{even}_{a_1}(X)$, if and only if $a_1 \preceq X$.

(2) A word X is an a_1-<u>odd word</u>, denoted $\text{odd}_{a_1}(X)$, if and only if $X \neq \#$ and $a_1 \not\preceq X$.

(3) A word X is a p_2-<u>even word</u>, denoted as $\text{even}_{p_2}(X)$, if and only if $p_2 \| X$.

(4) A word X is a p_2-<u>odd word</u>, denoted as $\text{odd}_{p_2}(X)$, if and only if $X \neq \#$ and $p_2 \nparallel X$.

(5) A word X is a σ-<u>even word</u>, denoted as $\text{even}_\sigma(X)$, if and only if X is a solution of the equation

$$\Sigma(X) = a_1^\mu,$$

where a_1^μ is a p_2-even word.

(6) A word X is a σ-<u>odd word</u>, denoted as $\text{odd}_\sigma(X)$ if and only if X is a solution of the equation

$$\Sigma(X) = a_1^\mu,$$

where a_1^μ is a p_2-odd word.

3.5.1. Proposition. (1) If X and Y are a_1-even words, then $\text{even}_{a_1}(X \oplus Y)$.

(2) If X and Y are a_1-odd words, then $\text{odd}_{a_1}(X \oplus Y)$.

(3) If $\text{even}_{a_1}(X)$ and $\text{odd}_{a_1}(Y)$, then $\text{even}_{a_1}(X \oplus Y)$.

For property (1), by definition, if X and Y are a_1-even words, then $a_1 \precsim X$ and $a_1 \precsim Y$, so clearly $a_1 \precsim X \oplus Y$.

With respect to property (2), if $a_1 \not\precsim X$ and $a_1 \not\precsim Y$, where X and Y are nonempty words, then obviously $a_1 \not\precsim X \oplus Y$.

For property (3), if $a_1 \precsim X$ and $a_1 \not\precsim Y$, then clearly $a_1 \precsim X \oplus Y$.

3.5.2. Proposition. If X and Y are both p_2-even words, then $\text{even}_{p_2}(X \oplus Y)$.

By definition, if X and Y are p_2-even words, then $p_2 \| X$ and $p_2 \| Y$. By Proposition 3.4.1(4), it follows that $p_2 \| (X \oplus Y)$, i.e., $X \oplus Y$ must be a p_2-even word.

In general, p_2-even and p_2-odd words do not behave with respect to word addition in the classical positive-integer sense. For example, words $a_1a_2a_5$ and $a_1a_3a_5$ are p_2-odd words, however their word sum $a_1a_2a_5 \oplus a_1a_3a_5$ is obviously not a p_2-even word. However, we do have the following special cases:

3.5.3. Proposition. (1) If $X = Y$ or if $X \prec Y$ and $Y [\dot{-}] X$ is a p_2-even word, where X and Y are nonempty words, then if $\text{odd}_{p_2}(X)$ and $\text{odd}_{p_2}(Y)$, then $\text{even}_{p_2}(X \oplus Y)$.

(2) The p_2-even and p_2-odd words behave in the classical manner when they are words in the free monoid $F(a_1)$.

(1) For the assumption $X = Y$, the conclusion follows by virtue of the definition of p_2-even words. If $X \prec Y$ and $Y [\dot{-}] X$ is p_2-even, then by Proposition 3.3.2(5) we get

$$X \oplus Y = X \oplus ((Y\ [\dot{-}]\ X) \oplus X)$$
$$= (X \oplus X) \oplus (Y\ [\dot{-}]\ X)$$
$$= \mathfrak{p}_2 \odot X \oplus (Y\ [\dot{-}]\ X).$$

Since by assumption $Y\ [\dot{-}]\ X$ is $\mathfrak{p}_2$-even, it follows from Proposition 3.5.2 that $\text{even}_{\mathfrak{p}_2}(X \oplus Y)$. (2) This part of the proposition is obvious.

With respect to σ-even and σ-odd words, the following shows that they behave in the classical manner.

3.5.4. Proposition. (1) If X and Y are both σ-even words, then $\text{even}_\sigma(X \oplus Y)$.

(2) If X and Y are both σ-odd words, then $\text{even}_\sigma(X \oplus Y)$.

(3) If $\text{even}_\sigma(X)$ and $\text{odd}_\sigma(Y)$, then $\text{odd}_\sigma(X \oplus Y)$.

With respect to property (1), if X and Y are σ-even, then by definition they are solutions of the equations $\Sigma(X) = a_1^\mu$ and $\Sigma(Y) = a_1^\nu$, where a_1^μ and a_1^ν are $\mathfrak{p}_2$-even words, which means that a_1^μ and a_1^ν are divisible by $\mathfrak{p}_2$. From this by Proposition 3.4.1(4) it follows that $a_1^\mu \oplus a_1^\nu$ is also divisible by $\mathfrak{p}_2$. By the definition of the conjugation function, we have $\Sigma(X) \oplus \Sigma(Y) = \Sigma(X \oplus Y)$, and therefore $\Sigma(X \oplus Y) = a_1^\mu \oplus a_1^\nu$, where $a_1^\mu \oplus a_1^\nu$ is $\mathfrak{p}_2$-even, which means $\text{even}_\sigma(X \oplus Y)$.

For property (2), if both X and Y are σ-odd words, then X and Y are solutions of the equations $\Sigma(X) = a_1^\mu$ and $\Sigma(Y) = a_1^\nu$, where a_1^μ and a_1^ν are some $\mathfrak{p}_2$-odd words, and of course $\Sigma(X) \oplus \Sigma(Y) = a_1^\mu \oplus a_1^\nu$, which means $\Sigma(X \oplus Y) = a_1^\mu \oplus a_1^\nu$. To expedite matters, note by Proposition 2.2.9 $a_1^\mu \oplus a_1^\nu = a_1^{\mu+\nu}$, and if a_1^μ and a_1^ν are both $\mathfrak{p}_2$-odd then $a_1^\mu = a_1^{2\alpha+1}$ and $a_1^\nu = a_1^{2\beta+1}$ for some α and β, and clearly $a_1^{2\alpha+1} = (a_1^2 \odot a_1^\alpha) \oplus a_1 = (\mathfrak{p}_2 \odot a_1^\alpha) \oplus a_1$ and $a_1^{2\beta+1} = (a_1^2 \odot a_1^\beta) \oplus a_1 = (\mathfrak{p}_2 \odot a_1^\beta) \oplus a_1$. Consequently, by the distributive law $a_1^\mu \oplus a_1^\nu = (\mathfrak{p}_2 \odot a_1^\alpha) \oplus a_1 \oplus (\mathfrak{p}_2 \odot a_1^\beta) + a_1 = \mathfrak{p}_2 \odot a_1^\alpha \oplus \mathfrak{p}_2 \odot a_1^\beta \oplus \mathfrak{p}_2 = \mathfrak{p}_2 \odot (a_1^\alpha \oplus a_1^\beta \oplus a_1)$, which means that $a_1^\mu \oplus a_1^\nu$ is an $\mathfrak{p}_2$-even word. Therefore, since $\Sigma(X \oplus Y) = a_1^\mu \oplus a_1^\nu$, where $a_1^\mu \oplus a_1^\nu$

is $\flat_2$-even, it follows that $\text{even}_\sigma(X \oplus Y)$.

For property (3), let $\text{even}_\sigma(X)$ and $\text{odd}_\sigma(Y)$, i.e., $\Sigma(X) = a_1^\mu$ and $\Sigma(Y) = a_1^\nu$, where $\text{even}_{\flat_2}(a_1^\mu)$ and $\text{odd}_{\flat_2}(a_1^\nu)$. In the same way as in the proof of property (2), using Proposition 2.2.9, we arrive at $a_1^\mu \oplus a_1^\nu = a_1^{2\alpha} \oplus a_1^{2\beta+1} = a_1^{2\alpha+2\beta+1} = a_1^{2(\alpha+\beta)+1} = \flat_2 \circ (a_1^\alpha \oplus a_1^\beta) \oplus a_1$, which means that $a_1^\mu \oplus a_1^\nu$ is $\flat_2$-odd. Combining the above equations we obtain $\Sigma(X \oplus Y) = a_1^\mu \oplus a_1^\nu$, where $a_1^\mu \oplus a_1^\nu$ is $\flat_2$-odd, therefore $\text{odd}_\sigma(X \oplus Y)$.

At this point, we sketch the relation between sets of a_1-even, $\flat_2$-even and σ-even words, in terms of the following example. All solutions X of the equation $\Sigma(X) = a_1^6$ are clearly σ-even words, which can be enumerated according to length as follows:

(1) a_6,

(2) a_1a_5, a_3a_3, a_2a_4,

(3) $a_1a_2a_3$, $a_1a_1a_4$, $a_2a_2a_2$,

(4) $a_1a_1a_1a_3$, $a_1a_1a_2a_2$,

(5) $a_1a_1a_1a_1a_2$,

(6) $a_1a_1a_1a_1a_1a_1$.

Clearly, a_1a_5, $a_1a_2a_3$, $a_1a_1a_4$, $a_1a_1a_1a_3$, $a_1a_1a_2a_2$, $a_1a_1a_1a_1a_2$ and $a_1a_1a_1a_1a_1a_1$ are a_1-even words, and a_3a_3, $a_1a_1a_2a_2$ and $a_1a_1a_1a_1a_1a_1$ are $\flat_2$-even words. From this example, we can see that the set of a_1-even words, the set of $\flat_2$-even words and the set of σ-even words have a common intersection, however, the set of a_1-even words does not subsume the set of σ-even words, and conversely, since, e.g., $a_1^{p_\mu}$ ($p_\mu \in P^0$, $\mu > 1$) are a_1-even words and certainly not σ-even words. Also, the set of a_1-even words does not subsume the set of $\flat_2$-even words, and conversely, since $a_1^{p_\mu}$ are not $\flat_2$-even words. However, we do have the following relation between the set of $\flat_2$-even words and the set of σ-even words:

3.5.5. Proposition. If X is a $\flat_2$-even word, then X is also a σ-even word.

Let X be a $\natural_2$-even word, then $X = \natural_2 \odot Y$ for some Y. By Proposition 3.5.4 since $\natural_2 \odot Y = Y \oplus Y$, whether Y is σ-even or σ-odd, it follows that X is an σ-even word.

3.5.6. Corollary. If X is a σ-odd word, then X is also a $\natural_2$-odd word.

3.5.7. Lemma. If λ(X) is a $\natural_2$-even word, then $\lambda(X)\ [\dot{-}]\ a_1$ is $\natural_2$-odd.

Clearly, if λ(X) is $\natural_2$-even, then $\lambda(X)\ [\dot{-}]\ a_1 = a_1^{2\mu}\ [\dot{-}]\ a_1$, for some $a_1^{2\mu}$, which means that $\lambda(X)\ [\dot{-}]\ a_1$ must be $\natural_2$-odd.

3.5.8. Lemma. If X is $\natural_2$-even, then λ(X) is $\natural_2$-even.

If X is $\natural_2$-even, then $X = \natural_2 \odot Y$ for some Y. In turn, since clearly $\lambda(X) = \lambda(\natural_2 \odot Y)$ and $\lambda(\natural_2) = \natural_2$, we have by Proposition 2.4.3(3) $\lambda(X) = \lambda(\natural_2) \odot \lambda(Y) = \natural_2 \odot \lambda(Y)$, which means that λ(X) is $\natural_2$-even.

3.5.9. Corollary. If λ(X) is $\natural_2$-odd, then X is $\natural_2$-odd

3.5.10. Lemma. Any a_μ in the alphabet A is a $\natural_2$-odd word.

This proposition follows from the definition of $\natural_2$-odd words.

3.5.11. Lemma. If X is $\natural_2$-even, then $X \oplus a_\mu$ is $\natural_2$-odd for any $a_\mu \in A$.

Let X be $\natural_2$-even and assume that $X \oplus a_\mu$ is $\natural_2$-even for some a_μ. Letting $Y = X \oplus a_\mu$, we clearly have $a_\mu \prec Y$ and $X = Y\ [\dot{-}]\ a_\mu$. Next, since $a_\mu \prec Y$, by Proposition 3.3.2(7) we have

$$\lambda(Y\ [\dot{-}]\ a_\mu) = \lambda(Y)\ [\dot{-}]\ \lambda(a_\mu) = \lambda(Y)\ [\dot{-}]\ a_1 .$$

Since Y is $\natural_2$-even by assumption, we have λ(Y) is $\natural_2$-even by Lemma 3.5.8. In turn, by Lemma 3.5.7 $\lambda(Y)\ [\dot{-}]\ a_1$ is $\natural_2$-odd, and since $X = Y\ [\dot{-}]\ a_\mu$, it follows that λ(X) must be $\natural_2$-odd. However, by Corollary 3.5.9, from λ(X) being $\natural_2$-odd we get the contradiction that X is a $\natural_2$-odd word.

3.5.12. Theorem. Every $\natural_2$-even word can be expressed as a word sum of two $\natural_2$-odd words.

Let X be a $\mathfrak{p}_2$-even word, then $X = \mathfrak{p}_2 \odot Y$ for some Y. We proceed by induction. By virtue of Lemma 3.5.10, the theorem is true for $Y = a_\mu$. Next, assume that the theorem is true for some Y such that $Y \odot \mathfrak{p}_2 = Y_1 \oplus Y_2$, where Y_1, Y_2 are some $\mathfrak{p}_2$-odd words. Then

$$a_\mu Y \odot \mathfrak{p}_2 = (a_\mu \oplus Y) \odot \mathfrak{p}_2 = (a_\mu \odot \mathfrak{p}_2) \oplus (Y \odot \mathfrak{p}_2)$$
$$= a_\mu \odot \mathfrak{p}_2 \oplus (Y_1 \oplus Y_2) = a_\mu \oplus (a_\mu \oplus (Y_1 \oplus Y_2)).$$

Since $Y_1 \oplus Y_2$ is $\mathfrak{p}_2$-even, it follows from Lemma 3.5.11 and Lemma 3.5.10 that $a_\mu \oplus (Y_1 \oplus Y_2)$ is $\mathfrak{p}_2$-odd. Consequently, the theorem is true for all Y.

3.5.13. Proposition. Every prime word is $\mathfrak{p}_2$-odd, except for $\mathfrak{p}_2$ which is a $\mathfrak{p}_2$-even word.

This proposition follows from the definitions of $\mathfrak{p}_2$-even words and prime words.

§3.6. Conjugations of words

For any natural word $a_1^\mu \in F(a_1)$, where $\mu \geq 2$, the set of all solutions X of the equation

$$\Sigma(X) = a_1^\mu$$

is called an additive conjugation of a_1^μ or more briefly conjugation of a_1^μ. We denote a conjugation of a_1^μ $(\mu \geq 2)$ as $C(a_1^\mu)$. We call a subset of a conjugation a subconjugation.

Conjugations of a_1^μ are like partitions (partitio numerorum) of positive integers μ, except for the following property (1):

3.6.1. Proposition. (1) The words in each conjugation $C(a_1^\mu)$ are distinct.
(2) Each conjugation $C(a_1^\mu)$ is nonempty and contains a finite number of words.
(3) No two conjugations contain a common word.

For property (1), the words in each conjugation must be distinct by

virtue of the symbolic equality relation $=_A$ in $F(A)$.

Property (2). The conjugate function $\Sigma(X)$, defined in section 3.5., maps words $a_{i_r} a_{i_{r-1}} \ldots a_{i_1}$ in $F(A)$ onto natural words $a_1^{i_r} \oplus a_1^{i_{r-1}} \oplus \ldots \oplus a_1^{i_1}$ in the free monoid $F(a_1)$. By associative law and the symbolic uniqueness theorem of $F(a_1)$, it is not difficult to see that any natural word a_1^{μ} can be represented only by means of a finite number of proper pairs of parentheses, i.e., as a finite "partition" of the natural word a_1^{μ}. Considering the definition of a conjugation of a_1^{μ}, the above means that the equation $\Sigma(X) = a_1^{\mu}$ can have only a finite number of solutions, or that $C(a_1^{\mu})$ contains only a finite number of words. It is clear that conjugations are nonempty.

Property (3). If two different conjugations $C(a_1^{\mu})$ and $C(a_1^{\nu})$ contain a common word X, then $\Sigma(X) = a_1^{\mu}$, $\Sigma(X) = a_1^{\nu}$ and $a_1^{\mu} = a_1^{\nu}$, which immediately contradicts the assumption that the conjugations in question are different.

We call a conjugation of the form $C(a_1^{2\mu})$ $(\mu \geq 1)$ a σ-<u>even conjugation</u> and a conjugation of the form $C(a_1^{2\mu+1})$ $(\mu \geq 1)$ an σ-<u>odd conjugation</u>.

Given any conjugation $C(a_1^{\mu})$ $(\mu \geq 1)$, the set of all words of length n $(1 \leq n \leq \mu)$ is called the <u>subconjugation of</u> $C(a_1^{\mu})$ <u>of length</u> n, which we denote by $C_n(a_1^{\mu})$ if $1 \leq n \leq \mu$.

For example, the words in the conjugation $C(a_1^8)$ can be enumerated according to length as follows:

$$C_1(a_1^8) = \{a_8\},$$

$$C_2(a_1^8) = \{a_1a_1,\ a_2a_6,\ a_5a_3,\ a_4a_4\},$$

$$C_3(a_1^8) = \{a_1a_1a_6,\ a_1a_2a_5,\ a_1a_3a_4,\ a_2a_3a_3,\ a_2a_2a_4\},$$

$$C_4(a_1^8) = \{a_1a_1a_1a_5,\ a_1a_1a_2a_4,\ a_1a_2a_2a_3,\ a_2a_2a_2a_2,\ a_1a_3a_1a_3\},$$

$$C_5(a_1^8) = \{a_1a_1a_1a_1a_4,\ a_1a_1a_1a_1a_2a_2,\ a_1a_1a_2a_2a_2\},$$

$$C_6(a_1^8) = \{a_1a_1a_1a_1a_1a_3,\ a_1a_1a_1a_1a_2a_2\},$$

$$C_7(a_1^8) = \{a_1a_1a_1a_1a_1a_1a_2\},$$

$$C_8(a_1^8) = \{a_1a_1a_1a_1a_1a_1a_1a_1\}.$$

Clearly, $C(a_1^8)$ is σ-even conjugation and each $C_n(a_1^8)$ $(1 \leq n \leq 8)$ is the subconjugation of $C(a_1^8)$ of length n.

3.6.2. Proposition. For any $\mu > 1$, if $X \in C(a_1^\mu)$, then $X \odot \beta_2 \in C(a_1^{2\mu})$.

For any $\mu > 1$, let $X \in C(a_1^\mu)$, which means that X is a solution of the equation $\Sigma(X) = a_1^\mu$. Assume that $X \odot \beta_2 \notin C(a_1^{2\mu})$, which means that $\Sigma(X \odot \beta_2) \neq a_1^{2\mu}$. By Proposition 3.5.1(4), $\Sigma(X \odot \beta_2) = \Sigma(X) \odot \Sigma(\beta_2)$, and of course $\Sigma(\beta_2) = a_1^2$. Consequently, from the assumption $\Sigma(X \odot \beta_2) \neq a_1^{2\mu}$, we obtain $\Sigma(X) \odot a_1^2 \neq a_1^\mu \odot a_1^2$, which leads to the contradiction $\Sigma(X) \neq a_1^\mu$, i.e., $X \notin C(a_1^\mu)$.

Let $p(a_1^\mu)$ denote the number of words in the conjugation $C(a_1^\mu)$. For example, the number of words in the conjugation $C(a_1^{200})$ is $p(a_1^{200}) = 3,972,999,029,388$.

3.6.3. Proposition. For any natural β_2-even word $a_1^{2\mu}$ $(\mu \geq 1)$, the number of β_2-even words in the conjugation $C(a_1^{2\mu})$ is $p(a_1^\mu)$.

This is a consequence of Proposition 3.6.2.

Given any σ-even words in $C(a_1^{2\mu})$ $(\mu \geq 1)$ we call the set of all β_2-even words in $C(a_1^{2\mu})$ a β_2-even subconjugation of $a_1^{2\mu}$. For example, the β_2-even subconjugation of $C(a_1^8)$, enumerated above, is the set $\{a_4a_4, a_2a_2a_2a_2, a_1a_3a_1a_3, a_1a_1a_1a_1a_2a_2, a_1^8\}$.

3.6.4. Proposition. Every σ-even conjugation contains a β_2-even subconjugation.

This is also a consequence of Proposition 3.6.2.

3.6.5. Proposition. (1) Every conjugation $C(a_1^\mu)$ $(\mu \geq 1)$ contains μ subconjugations, namely, $C(a_1^\mu) = C_1(a_1^\mu) \cup C_2(a_1^\mu) \cup \ldots \cup C_{\mu-1}(a_1^\mu) \cup C_\mu(a_1^\mu)$. (2) For $\mu > 2$, the subconjugations $C_1(a_1^\mu)$, $C_{\mu-1}(a_1^\mu)$ and $C_\mu(a_1^\mu)$ in $C(a_1^\mu)$ are the only subconjugations containing a single word.

The above properties are obvious.

For use in the following section, we introduce a terminology for certain sets of conjugations.

(1) We call the union $\bigcup_{\mu=1}^{\infty} C(a_1^{\mu})$ of all conjugations a range, which we denote by $\mathcal{R}$.

(2) Any set of subconjugations in $\mathcal{R}$ is called a subrange. We call the subrange $\bigcup_{\mu=1}^{\infty} C_1(a_1^{\mu})$ the trivial subrange of $\mathcal{R}$, the subrange $\bigcup_{\mu=1}^{\infty} C_{\mu}(a_1^{\mu})$ the natural subrange of $\mathcal{R}$. We call the union $\bigcup_{\mu=1}^{\infty} C(a_1^{2\mu})$ the σ-even subrange of $\mathcal{R}$. The nontrivial subrange

$$\bigcup_{\mu=3}^{\infty} C(a_1^{2\mu}) \setminus \bigcup_{\mu=3}^{\infty} C_1(a_1^{2\mu})$$

(i.e., the σ-even subrange of $\mathcal{R}$ with the conjugations $C(a_1^2)$, $C(a_1^4)$, and the subconjugations $C_1(a_1^{2\mu})$ $(\mu \geq 3)$ removed) is called the ordinary σ-even subrange of $\mathcal{R}$, which we denote by $\mathcal{R}^*$.

(3) For any $r \geq 2$, let the union of all subconjugations in $\mathcal{R}^*$ of length r (i.e., the set of all words in $\mathcal{R}^*$ with length r) be denoted as $\mathcal{L}_r$. In terms of $\mathcal{L}_r$, we define the Euler r-subrange of $\mathcal{R}^*$, denoted as $\mathcal{E}_r$, as follows:

(i) If $2 \leq r \leq 6$, then $\mathcal{E}_r =_{\text{Def}} \mathcal{L}_r$.

(ii) If $r = 2n$ $(n \geq 4)$, then

$$\mathcal{E}_{2n} =_{\text{Def}} \bigcup_{k=3}^{n-3} C_{2k}(a_1^{2k}) \cup \mathcal{L}_{2n}.$$

(iii) If $r = 2n+1$ $(n \geq 4)$, then

$$\mathcal{E}_{2n+1} =_{\text{Def}} \bigcup_{k=3}^{n} C_{2k}(a_1^{2k}) \cup \mathcal{L}_{2n+1}.$$

In the following table we point out several examples of Euler subranges in the ordinary subrange $\mathcal{R}^*$.

$C(a_1^6)$	$C(a_1^8)$	$C(a_1^{10})$	...
$C_2(a_1^6)$	$C_2(a_1^8)$	$C_2(a_1^{10})$	...
$C_3(a_1^6)$	$C_3(a_1^8)$	$C_3(a_1^{10})$	...
$C_4(a_1^6)$	$C_4(a_1^8)$	$C_4(a_1^{10})$	...
...	...	...	...
$C_6(a_1^6)$	$C_6(a_1^8)$	$C_6(a_1^{10})$	...
	$C_7(a_1^8)$	$C_7(a_1^{10})$	...
	$C_8(a_1^8)$	$C_8(a_1^{10})$	...
		$C_9(a_1^{10})$	...
		$C_{10}(a_1^{10})$	...

In the above ordinary subrange $\mathscr{R}^*$, we have the following:

$$\mathscr{L}_6 = \{C_6(a_1^6),\ C_6(a_1^8),\ C_6(a_1^{10}), \ldots\}$$
$$\mathscr{L}_7 = \{C_7(a_1^8),\ C_7(a_1^{10}),\ C_7(a_1^{12}), \ldots\},$$
$$\mathscr{L}_9 = \{C_9(a_1^{10}),\ C_9(a_1^{12}),\ C_9(a_1^{14}), \ldots\},$$
$$\mathscr{E}_7 = \{C_6(a_1^6)\} \cup \mathscr{L}_7,$$
$$\mathscr{E}_8 = \{C_6(a_1^6)\} \cup \mathscr{L}_8,$$
$$\mathscr{E}_9 = \{C_6(a_1^6),\ C_8(a_1^8)\} \cup \mathscr{L}_9.$$

We call words of the form

$$a_1^{\mu} a_{\nu}^{\alpha} \qquad (\nu > 1,\ \mu \geq 1,\ \alpha \geq 1)$$

ramified words.

3.6.6. Proposition. Words in the subconjugation $C_{\mu-1}(a_1^{\mu})$ $(\mu > 2)$ and in the subrange $\bigcup_{\mu=1}^{\infty} C_{2\mu-1}(a_1^{2\mu})$ are ramified words.

This follows directly from the above definitions.

We conclude this section with the following.

The multiplicative conjugation function $\prod\!\!\prod^k(X)$, for any $k \geq 0$, is defined as follows:

$$\prod\!\!\prod^k(\#) = a_1,$$
$$\prod\!\!\prod^k(a_\mu X) = \tau_k\sigma(a_\mu) \odot \prod\!\!\prod^k(X).$$

We recall that, by Proposition 2.4.2, the composition $\tau_k\sigma$ of mappings σ and τ_k $(k \geq 0)$ maps signs in A onto the set $\prod\!\!\prod^{(k)}_{F(a_1)}$ $(k \geq 0)$, a subset of $F^k(a_1)$.

3.6.7. Proposition. For any $k \geq 0$,

$$\prod\!\!\prod^k(X \oplus Y) = \prod\!\!\prod^k(X) \odot \prod\!\!\prod^k(Y).$$

This proposition is clear for $Y = \#$. Assume that it holds for some Y, then we have

$$\begin{aligned}\prod\!\!\prod^k(X \oplus Y) &= \prod\!\!\prod^k(a_\mu(X \oplus Y)) = \tau_k\sigma(a_\mu) \odot \prod\!\!\prod^k(X \oplus Y)\\ &= \tau_k\sigma(a_\mu) \odot \prod\!\!\prod^k(X) \odot \prod\!\!\prod^k(Y)\\ &= \prod\!\!\prod^k(X) \odot \prod\!\!\prod^k(a_\mu Y).\end{aligned}$$

For any $k \geq 0$ and any natural word $a_1^\mu \in F(a_1)$, where $\mu \geq 2$, the set of all solutions X of the equation

$$\prod\!\!\prod^k(X) = a_1^\mu$$

is called the multiplicative k-conjugation of a_1^μ. We denote a multiplicative conjugation of a_1^μ as $D^k(a_1^\mu)$.

For example, $D^2(a_1^{16}) = \{a_1a_6, a_1a_1a_1a_1\}$ and $D^1(a_1^{30}) = \{a_{23}, a_1a_{11}, a_4a_3, a_2a_6, a_1a_2a_3\}$. With respect to $D^1(a_1^{30})$, note that $D^1(a_1^{30})$ is related to the ways in which the product $\pi_1^{(1)} \odot \pi_2^{(1)} \odot \pi_3^{(1)} = a_1^{30}$ $(\pi_1^{(1)}, \pi_2^{(1)}, \pi_3^{(1)} \in [\prod\!\!\prod_{F(a_1)}]^{(1)})$ can be associated by pairs of parentheses governed by the associative law, i.e., $\pi_{23}^{(1)} = (\pi_1^{(1)} \odot \pi_2^{(1)} \odot \pi_3^{(1)})$, $\pi_1^{(1)} \odot \pi_{11}^{(1)} = \pi_1^{(1)} \odot (\pi_2^{(1)} \odot \pi_3^{(1)})$, $\pi_4^{(1)} \odot \pi_3^{(1)} = (\pi_1^{(1)} \odot \pi_2^{(1)}) \odot \pi_3^{(1)}$ and so on. In particular, note if a pair of parentheses encloses

a factor which is not an element of $\prod^{(k)}_{F(a_1)}$ then the relevant word X cannot be a solution of $\prod^{k}(X) = a_1^{\mu}$.

3.6.8. Proposition. For any $k \geq 0$, we have the following properties.

(1) The words in any multiplicative conjugation $D^k(a_1^{\mu})$ are distinct.

(2) Each multiplicative conjugation $D^k(a_1^{\mu})$ is nonempty and contains a finite number of words.

(3) No two multiplicative conjugations contain a common word.

Property (1) follows from the symbolic equality relation of $F(A)$.

Property (2). For any $k \geq 0$, the multiplicative conjugate function $\prod^{k}(X)$ maps words $a_{i_r} a_{i_{r-1}} \ldots a_{i_1}$ in $F(A)$ to natural words $\pi^{(k)}_{i_r} \odot \pi^{(k)}_{i_{r-1}} \odot \ldots \odot \pi^{(k)}_{i_1}$ in $F^k(a_1)$, i.e., to words of the form $a_1^{p^{(k)}_{i_r} \times p^{(k)}_{i_{r-1}} \times \cdots \times p^{(k)}_{i_1}}$ $(p^{(k)}_{i_1}, \ldots, p^{(k)}_{i_r} \in P^k)$. By the associative law of word multiplication and the unique-factorization Corollary 3.4.14, a word can be represented only by a finite number of proper pairs of parentheses involving factors taken from $\prod^{(k)}_{F(a_1)}$ whose product equals a_1^{μ}. By Corollary 3.4.14, multiplicative conjugations are nonempty.

Property (3). For a given $k \geq 0$, if two different multiplicative conjugations $D^k(a_1^{\mu})$ and $D^k(a_1^{\nu})$ contain a common word X, then $\prod^{k}(X) = \pi^{(k)}_{i_r} \odot \ldots \odot \pi^{(k)}_{i_1} = a_1^{\mu}$ and $\prod^{k}(X) = \pi^{(k)}_{i_r} \odot \ldots \odot \pi^{(k)}_{i_1} = a_1^{\nu}$, and of course $a_1^{\mu} = a_1^{\nu}$, which contradicts the assumption that the conjugations in question are different.

§3.7. Subprime words and p_2-subeven words

By definitions in section 2.2 and Corollary 3.4.14, the set $\prod_{F(a_1)} = \{\pi_1, \pi_2, \pi_3, \ldots\}$ denotes the set of all prime words in the free monoid $F(a_1)$.

We call a word $X \in F(A)$ a subprime word if X is a solution of the equation

$$\Sigma(X) = \pi_{\mu} ,$$

where π_{μ} is some prime word in $\prod_{F(a_1)}$.

3.7.1. Theorem. If X is a subprime word, then X is a prime word in $\mathcal{P}$. The converse is not true.

Let X be any subprime word, and assume that X is not a prime word. Let $X_1 = X_1 \circledcirc X_2$, for some $X_1, X_2 \in F(A)$. By Proposition 3.5.1(4) we obtain $\Sigma(X) = \Sigma(X_1) \circledcirc \Sigma(X_2)$, which means that $\Sigma(X_1) \| \Sigma(X)$ and $\Sigma(X_2) \| \Sigma(X)$, however, this implies the contradiction that X is not a subprime word by the definition of subprimes. With respect to the second part of the theorem, since there are prime words which are not subprimes, e.g., a_3a_5 is a prime word and certainly not a subprime, the converse cannot be true.

On the basis of Theorem 3.7.1, let $\mathcal{P}^*$ denote the set of all subprime words in $\mathcal{P}$.

We note that unlike the ordinary prime numbers there are many $\mathfrak{p}_2$-odd prime words which can be expressed as word sums of two $\mathfrak{p}_2$-odd words, e.g., the $\mathfrak{p}_2$-odd prime word $a_1a_3a_5a_7$ is expressible as $a_1a_3 \oplus a_5a_7$, where a_1a_3 and a_5a_7 are obviously $\mathfrak{p}_2$-odd prime words. However, the subprime words do not behave in this manner:

3.7.2. Proposition. If $\mathfrak{p}_{\mu}$ is a $\mathfrak{p}_2$-odd subprime word, then $\mathfrak{p}_{\mu}$ cannot be expressed as a word sum of two $\mathfrak{p}_2$-odd subprime words.

Let $\mathfrak{p}_{\mu}$ be a $\mathfrak{p}_2$-odd subprime word. Assume that $\mathfrak{p}_{\mu} = \mathfrak{p}_{\alpha} \oplus \mathfrak{p}_{\beta}$ for some $\mathfrak{p}_2$-odd subprime words $\mathfrak{p}_{\alpha}$ and $\mathfrak{p}_{\beta}$. By Proposition 3.5.1(2) we have $\Sigma(\mathfrak{p}_{\alpha} \oplus \mathfrak{p}_{\beta}) = \Sigma(\mathfrak{p}_{\alpha}) \oplus \Sigma(\mathfrak{p}_{\beta})$, and since $\mathfrak{p}_{\alpha}$ and $\mathfrak{p}_{\beta}$ are assumed to be $\mathfrak{p}_2$-odd subprime words, we also have $\Sigma(\mathfrak{p}_{\mu}) = \Sigma(\mathfrak{p}_{\alpha}) \oplus \Sigma(\mathfrak{p}_{\beta}) = \pi_{\sigma} \oplus \pi_{\tau}$ for some natural $\mathfrak{p}_2$-odd words π_{σ}, $\pi_{\tau} \in \prod_{F(a_1)}$, other than π_1, which by Proposition 3.5.3(2) contradicts the assumption that $\mathfrak{p}_{\mu}$ is a $\mathfrak{p}_2$-odd subprime word.

3.7.3. Lemma. If $a_\mu > a_1$ and $a_\mu \| (X \oplus Y)$ $(X, Y \in F(A))$, then $a_\mu \| X$ and $a_\mu \| Y$.

Let $a_\mu > a_1$ and $a_\mu \| (X \oplus Y)$. Let $X \oplus Y = a_\mu \odot Z$ for some $Z \in F(A)$. It follows from the symbolic uniqueness Theorem 2.2.6 that for every $a_\alpha \in A$ such that $a_\alpha \prec a_\mu \odot Z$ there must exist a sign $a_\beta \in A$ such that $a_\beta \prec X \oplus Y$ and $a_\beta = a_\alpha$. Consequently, for every a_α such that $a_\alpha \prec a_\mu \odot Z$, we must have $a_\mu \| a_\alpha$. Also, similarly as in the above, we get $a_\mu \| a_\beta$ for every a_β such that $a_\beta = a_\alpha$. This means that $a_\mu \| X$ and $a_\mu \| Y$.

3.7.4. Lemma. $a_\nu^\mu = a_\nu \odot a_1^\mu$ $(\mu \geq 1,\ \nu \geq 1,\ a_\nu \in A,\ a_1^\mu \in F(a_1))$.

This follows from the definitions of a_ν^μ and word multiplication.

3.7.5. Theorem. For any $\mu \geq 1$ and $\nu > 1$, if X satisfies $a_\nu^\mu \| X$, then X cannot be expressed as a word sum of two prime words.

Let $a_\nu^\mu \| X$ for some $\mu \geq 1$ and $\nu > 1$. Suppose $X = \mathfrak{p}_\alpha \oplus \mathfrak{p}_\beta$ for some prime words $\mathfrak{p}_\alpha, \mathfrak{p}_\beta \in \mathfrak{P}$. By assumption of the theorem, Lemma 3.4.8 and Lemma 3.7.4 we have $a_\nu^\mu \nparallel \mathfrak{p}_\alpha$ and $a_\nu^\mu \nparallel \mathfrak{p}_\beta$. Since $\nu > 1$, on the strength of Lemma 3.7.3 it follows that $a_\nu^\mu \nparallel (\mathfrak{p}_\alpha \oplus \mathfrak{p}_\beta)$, which means that $a_\nu^\mu \nparallel X$, a contradiction.

3.7.6. Corollary. If X is a $\mathfrak{p}_2$-even word or a σ-even word such that $a_\nu^\mu \| X$ $(\mu \geq 1,\ \nu > 1)$, then X cannot be expressed as a word sum of two subprime words or a word sum of two prime words.

For later use, we further reduce the size of the set of all $\mathfrak{p}_2$-even words as follows:

If a $\mathfrak{p}_2$-even word X satisfies the condition $a_\nu^\mu \nparallel X$ $(\mu \geq 1,\ \nu > 1)$ and $a_1^\mu \nparallel X$ $(\mu > 2)$, then we call the $\mathfrak{p}_2$-even word X a $\mathfrak{p}_2$-subeven word.

3.7.7. Proposition. (1) The $\mathfrak{p}_2$-even word $a_1a_1 \in C(a_1^2)$ and a_2a_2, $a_1a_1a_1a_1 \in C(a_1^4)$ are not $\mathfrak{p}_2$-subeven words.

(2) Every natural $\mathfrak{p}_2$-even word is not a $\mathfrak{p}_2$-subeven word.

These properties are simple consequences of the definition of $\mathfrak{p}_2$-subeven words.

3.7.8. Lemma. Ramified words $a_1^{\mu}a_{\nu}$ $(\mu \geq 1,\ \nu > 1)$ are prime words.

This is clear, since $\gcd(\mu, 1) = \gcd(1, \nu) = 1$ for all $\mu \geq 1$ and $\nu > 1$.

3.7.9. Proposition. Ramified words $a_1^{\mu}a_{\nu} \circledcirc \mathfrak{p}_2$ $(\mu \geq 1,\ \nu \geq 2)$ are $\mathfrak{p}_2$-subeven words.

Clearly, $a_1^{\mu}a_{\nu} \circledcirc \mathfrak{p}_2$ $(\mu \geq 1,\ \nu \geq 2)$ are $\mathfrak{p}_2$-even words. For such words to be $\mathfrak{p}_2$-subeven words, we have to show that they are not divisible by a_{ν}^{μ} $(\mu \geq 1,\ \nu > 1)$ and a_1^{μ} $(\mu > 2)$. By Lemma 3.7.8, ramified words $a_1^{\mu}a_{\nu}$ are prime words and of course $\mathfrak{p}_2$ is a prime word. On the strength of the prime-word unique factorization Theorem 3.4.13, since words a_{ν}^{μ} $(\mu \geq 1,\ \nu > 1)$ and a_1^{μ} $(\mu > 2)$ are obviously different from the ramified words $a_1^{\mu}a_{\nu}$ and $\mathfrak{p}_2$, it follows that words of the form $a_1^{\mu}a_{\nu} \circledcirc \mathfrak{p}_2$ $(\mu \geq 1,\ \nu \geq 2)$ cannot be divisible by a_{ν}^{μ} $(\mu \geq 1,\ \nu \geq 2)$ or a_1^{μ} $(\mu \geq 2)$.

3.7.10. Proposition. $a_1^{\mu}a_2 \circledcirc \mathfrak{p}_2 \in C(a_1^{2(\mu+2)})$ $(\mu \geq 1)$.

Note, we have $a_1^{\mu}a_2 \circledcirc \mathfrak{p}_2 = a_1^{\mu}a_2 \oplus a_1^{\mu}a_2 = a_1^{2\mu} \oplus a_2^2$, and clearly $a_1^{2\mu}a_{\nu}^2$ $(\mu \geq 1)$ are solutions of the equation $\Sigma(a_1^{2\mu}a_2^2) = a_1^{2(\mu+2)}$ $(\mu \geq 1)$. Therefore, $a_1^{\mu}a_2 \circledcirc \mathfrak{p}_2 \in C(a_1^{2(\mu+2)})$ $(\mu \geq 1)$.

CHAPTER IV

ARITHMETIZATIONS OF ABSTRACT ARITHMETICS $\mathcal{A}^k(A)$

§4.1. Primitive arithmetics

Very generally speaking, certain types of elementary properties (additive, multiplicative, exponential and so on) of the natural numbers can be, on the one hand, described elegantly in different arithmetics on different free monoids ($F(a_1)$, $F(A)$, noncommutative free monoid in an infinite alphabet [9]) and then, on the other hand, to a certain degree "compressed" on any one of these arithmetics. Because of this loose character of the properties of the natural numbers, it is convenient to select a "ground" arithmetic to serve as a frame of reference for certain properties of the natural numbers. Such an arithmetic is described in this section.

We point out that whatever "completely" means, one should not indulge in the nonsense that any single arithmetic on a given free monoid, however rudely compressed, can "completely" describe all the properties of the natural numbers, which is very much like expecting a single algebraic number-field to "completely" describe all the properties of the set of all algebraic numbers. In passing, we point out that there is an interesting analogy between the natural numbers and the algebraic integers, which we plan to describe in another paper.

For convenience, in order to avoid introducing another infinite class of different arithmetics involving an infinite number of different finite-alphabetical free monoidules and arithmetical maps together with relevant algebras with infinite numbers of laws of composition in each algebra, we shall instead indulge to a degree in the usual "compressions" on certain arithmetics. Consequently, in the following constructions we do not employ any restrictions of the type introduced in sections 3.1 and 3.2.

To construct primitive arithmetics $\mathcal{P}(A_n^{\#})$ $(n > 1)$, we start by

assuming the monoids S_n, groupoids S_n^*, free monoids $G(A_n^\#)$, and the additive free monoidules $S_n G(A_n^\#)$, all introduced in section 2.5. In each primitive arithmetic $\mathcal{P}(A_n^\#)$ $(n > 1)$, we take the law of composition $X \oplus_n Y$ of $G(A_n^\#)$ to be the word addition of $\mathcal{P}(A_n^\#)$.

Secondly, we introduce the functions $d(X)$ and $D(X)$ in $\mathcal{P}(A_n^\#)$ as follows:

(1) $$d(\#) = \#\,, \quad d(a_\mu X) = a_\mu \,,$$

(2) $$D(\#) = \#\,, \quad D(a_\mu X) = X \,.$$

Thirdly, we define the function $X \oplus_n^* Y$ in $\mathcal{P}(A_n^\#)$ by the following equation:

$$X \oplus_n^* Y = d(X) \oplus_n (d(D(X)) \otimes_n Y) \,,$$

where $\otimes_n$ is the law of composition of the free monoidule $S_n G(A_n^\#)$.

With the help of the above functions, we define <u>word multiplication</u> $X (+)_n Y$ in $\mathcal{P}(A_n^\#)$, which is in fact nothing else than ordinary addition defined in $\mathcal{P}(A_n^\#)$, by the following equations:

$$X (+)_n \# = X \,,$$

$$X (+)_n a_\mu Y = (a_\mu \otimes_n d(X)) \oplus_n^* (D(X) (+)_n Y) \,.$$

We can define the word <u>divisibility relation</u> $X \|^{(n)} Y$ and the <u>prime-word relation</u> $pw^{(n)}(X)$ in $\mathcal{P}(A_n^\#)$ as follows:

(3) $$Y \|^{(n)} X \iff \bigvee Z\{X = Y (+)_n Z\} \,,$$

(4) $$pw^{(n)}(X) \iff X \neq \# \wedge X \neq a_0 \wedge$$
$$\bigwedge Y\{Y \|^{(n)} X \implies Y = X \vee Y = a_0 \vee Y = \#\} \,.$$

Note, the prime words in $\mathcal{P}(A_n^\#)$ are of the form a_μ or

$a_0a_0 \ldots a_0a_\mu$ ($\mu \geq 1$, a_0 n-times ($n \geq 1$)).

We simply state the prime-word factorization theorem in arithmetic $\mathcal{P}(A_n^{\#})$ as follows:

4.1.1. Theorem. Except for $\#$ and a_0, every word in $\mathcal{P}(A_n^{\#})$ $(n > 1)$ can be uniquely expressed as a word product

$$\mathfrak{p}_{i_r} (+)_n \mathfrak{p}_{i_{r-1}} (+)_n \ldots (+)_n \mathfrak{p}_{i_1} ,$$

where $\mathfrak{p}_{i_1}, \mathfrak{p}_{i_2}, \ldots, \mathfrak{p}_{i_r}$ are prime words of $\mathcal{P}(A_n^{\#})$ with different lengths.

The above unique factorization theorem is related to the usual n-adic unique representations of positive integers.

At this stage of the section, we select our ground arithmetic to be $\mathcal{P}(A_{10}^{\#})$. As pointed out in section 2.5, it has been customary for several milleniums to denote the signs in the alphabet $A_{10}^{\#}$ as $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. With respect to the ground arithmetic $\mathcal{P}(A_{10}^{\#})$, it is also customary to denote its word multiplication $X (+)_{10} Y$ as $X + Y$, however we shall have occasion to make use of both notations.

We now proceed to define ordinary multiplication $X \times Y$ in arithmetic $\mathcal{P}(A_{10}^{\#})$ as follows, by assuming the additional free monoidule $M_{10}G(A_{10}^{\#})$ in $\mathcal{P}(A_{10}^{\#})$:

$$X \times \# = \# ,$$

$$X \times a_\mu Y = (a_\mu \odot_{10} X) \oplus_{10}^{*} (X \times Y) .$$

In arithmetic $\mathcal{P}(A_{10}^{\#})$ we can construct the familiar set of prime numbers P^0 and its divisibility theory using the above ordinary multiplication. In turn, we can define the Hilbert-Ackermann functions $\xi_1(X, Y)$, $\xi_2(X, Y)$, ..., simply by iteration, i.e., $\xi_1(X, Y) = X \times X \times \ldots \times X$ (X Y-times), and so on. Consequently, we can obtain the Hilbert-Ackermann number systems P^0, P^1, P^2, ... in arithmetic $\mathcal{P}(A_{10}^{\#})$.

For convenience, in the following sections, in addition to the

notation $G(A_{10}^{\#})$, we shall also use the notation N to denote the free monoid $G(A_{10}^{\#})$.

§4.2. Arithmetizations of arithmetics $\mathcal{Q}^k(A)$

Recall that N also denotes the free monoid $G(A_{10}^{\#})$. In turn, note that if $\varphi(X, Y)$ is a function of arithmetic $\mathcal{P}(A_{10}^{\#})$ then we also write it as $X\varphi Y$, and we also write concatenations of the form $(\ldots((X_1\varphi X_2)\varphi X_3)\varphi\ldots\varphi X_{n-1})\varphi X_n$ or $X_1\varphi(X_2\varphi(X_3\varphi\ldots\varphi(X_{n-1}\varphi X_n)\ldots))$ as $X_1\varphi X_2\varphi\ldots\varphi X_{n-1}\varphi X_n$.

We say that $F_\varphi(q)$ is an arithmetization of the free monoid $F(a_1)$ if the following relations hold between $F(a_1)$ and the arithmetic $\mathcal{P}(A_{10}^{\#})$: (1) there exist words p and q in the free monoid N, where q is different from p, such that p corresponds to the empty word $\#$ and $\{q\}$ corresponds to the alphabet $\{a_1\}$ in $F(a_1)$; (2) there exists a function $\varphi(X, Y)$ in arithmetic $\mathcal{P}(A_{10}^{\#})$ such that $\varphi(q, X)$ corresponds to the successor function $a_1 \oplus X$ of $F(a_1)$, and every finite concatenation $q\varphi q\varphi\ldots\varphi q$ is unique, thus satisfying the axioms of the free monoid $F(a_1)$.

4.2.1. Proposition. For any $k \geq 0$, if n denotes any nonzero element in N, $p_\mu^{(k)}$ any element in the Hilbert-Ackermann number-system P^k and ξ_k is any Hilbert-Ackermann function in arithmetic $\mathcal{P}(A_{10}^{\#})$, then $F_+(n)$ and $F_{\xi_k}(p_\mu^k)$ are arithmetizations of the free monoid $F(a_1)$.

For any $n > 0$, the arithmetizations $F_+(n)$ involving the words $0, n, n+n, n+n+n, \ldots$ are obviously unique and constitute the familiar interpretations of the free monoid $F(a_1)$. On the other hand, for $k \geq 0$, the arithmetizations $F_{\xi_k}(p_\mu^{(k)})$ $(k \geq 0)$ involving the words of the form $1, p_\mu^{(k)}, p_\mu^{(k)}p_\mu^{(k)}, p_\mu^{(k)}p_\mu^{(k)}p_\mu^{(k)}, \ldots,$ defined in section 1.2, which are unique

on the strength of Theorem 1.2.4 and Theorem 1.2.5, are clearly also arithmetizations of $F(a_1)$.

We say that $F_\varphi(Q)$ is an <u>arithmetization of the free monoid</u> $F(A)$ if the following relations hold between the free monoid $F(A)$ and the ground arithmetic $\mathcal{P}(A_{10}^{\#})$: (1) there exists a word p in N and an infinite set $Q = \{q_1, q_2, \dots\}$ of words in N, all different from p, such that p corresponds to the empty word and Q corresponds to the alphabet A in the free monoid $F(A)$; (2) there exist a function $\varphi(X, Y)$ in arithmetic $\mathcal{P}(A_{10}^{\#})$ such that $\varphi(q_\mu, X)$ $(q_\mu \in Q)$ corresponds to the successor functions $a_\mu \oplus X$ $(a_\mu \in A)$ in the free monoid $F(A)$, and every finite concatenation $q_{i_r} \varphi q_{i_{r-1}} \varphi \dots \varphi q_{i_1}$ is unique under the equality relation $=_Q$ corresponding to the equality relation $=_A$ in $F(A)$, hence satisfying the axioms of the free monoid $F(A)$.

By an <u>arithmetization</u> $\mathcal{A}_\varphi^k(Q)$ of the arithmetic $\mathcal{A}^k(A)$ $(k \geq 0)$, we mean the existence of an arithmetization $F_\varphi(Q)$ of the free monoid $F(A)$ and in turn the full development of an arithmetic on $F_\varphi(Q)$ which satisfies the axioms and rules of arithmetic $\mathcal{A}^k(A)$.

4.2.2. <u>Proposition.</u> For any $k \geq 0$, if $F_\varphi(Q)$ is an arithmetization of $F(A)$, then any arithmetic $\mathcal{A}_\varphi^k(Q)$ constructed on $F_\varphi(Q)$ is an arithmetization of $\mathcal{A}^k(A)$.

This proposition is clear.

Let $N^* = G(A_{10}^{\#}) \setminus \{\#, a_0\}$, and again recall that P^k $(k \geq 0)$ denote the Hilbert-Ackermann number-systems.

4.2.3. <u>Proposition.</u> For any $k \geq 0$, $\mathcal{A}_+^k(N^*)$ and $\mathcal{A}_\times^k(P^k)$ are arithmetizations of arithmetic $\mathcal{A}^k(A)$.

By virtue of Proposition 4.2.2, it is enough to show that $F_+(N^*)$ and $F_\times(P^k)$ are arithmetizations of $F(A)$.

With respect to $F_+(N^*)$, by definition N^* corresponds to the alphabet A in F(A), the equality relation $=_{N^*}$ in $F_+(N^*)$ corresponds to $=_A$ in F(A), and $n_\mu + X\,(n_\mu \in N^*)$ corresponds to $a_\mu \oplus X\,(a_\mu \in A)$. Clearly, $0 \in N$ must correspond to # in F(A) and $1 \in N$ corresponds to a_1 in F(A). On the strength of Proposition 3.6.1, we can set-theoretically partition the words in the free monoid F(A) into additive conjugations $C(a_1^\mu)$ $(\mu \geq 2)$, where in each conjugation $C(a_1^\mu)$ the words are finite in number and distinct. On the other hand, in $F_+(N^*)$ we consider the set of partitions $P(\mu)$ (partitio numerorum) of μ $(\mu \geq 2)$. We can see that $P(\mu)$ $(\mu \geq 2)$ in $F_+(N^*)$ corresponds exactly to the additive conjugations $C(a_1^\mu)$ $(\mu \geq 2)$ in F(A) and conversely, by their definitions. Since the symbolic equality relation $=_{N^*}$ is assumed in $F_+(N^*)$, this relation renders each word in $F_+(N^*)$ unique. From this it follows that $F_+(N^*)$ is an arithmetization of F(A).

With respect to $F_\times(P^k)$ $(k \geq 0)$, by definition P^k corresponds to the alphabet A of F(A), the equality relation $=_{P^k}$ corresponds to the symbolic equality relation $=_A$ of F(A), and $p_\mu^{(k)} \times X\,(p_\mu^{(k)} \in P^k)$ corresponds to $a_\mu \oplus X\,(a_\mu \in A)$ in F(A). Clearly, $1 \in N$ corresponds to # in F(A) and $2 \in N$ corresponds to a_1 in F(A). By virtue of Proposition 3.6.8, we can set-theoretically partition the words in F(A) into multiplicative conjugations $D^k(a_1^\mu)$ $(\mu \geq 2)$ for a given $k \geq 0$. On the other hand, in $F_\times(P^k)$ we consider the set of all "multiplicative partitions" $P_\times^k(\mu)$ of μ, i.e., sets of all ordinary products $\pi_{i_r}^{(k)} \times \pi_{i_{r-1}}^{(k)} \times \ldots \times \pi_{i_1}^{(k)}$ with factors taken from the Hilbert-Ackermann number-system P^k and such that the above-mentioned products are all equal to the positive integer μ. Similarly as pointed out in section 3.6, the set $P_\times^k(\mu)$ is obtained by means of the unique factorization theorem 1.2.5 and the associativity of ordinary multiplication. It is clear that each set $P_\times^k(\mu)$ corresponds to the multiplicative conjugation $D^k(a_1^\mu)$ and conversely by

virtue of their definitions. In turn, the symbolic equality relation $=_{P^k}$ in $F_X(P^k)$ renders each element in $P_X^k(\mu)$ unique. From this it follows that $F_X(P^k)$ is an arithmetization of $F(A)$.

4.2.4. Corollary. (1) For any $h \geq 0$ and $k \geq 1$ such that $h < k$, if $[P^h]^k \subset P^k$ then $\mathcal{A}_X^k([P^h]^k)$ is an arithmetization of $\mathcal{A}^k(A)$.
(2) $\mathcal{A}_X^k([M]^k)$ $(k \geq 1)$ is an arithmetization of $\mathcal{A}^k(A)$, where $[M]^k$ is the set defined in section 1.4.

4.2.5. Proposition. In the arithmetization $\mathcal{A}_+^k(N^*)$ of $\mathcal{A}^k(A)$ $(k \geq 0)$ we have $P^0 = \mathbb{P}^*$, where P^0 denotes the set of ordinary prime numbers and $\mathbb{P}^*$ denotes the set of all subprimes in $\mathcal{A}^k(A)$.

This proposition follows from the definition of the set $\mathbb{P}^*$ of subprimes given in section 3.7 which precisely selects in the arithmetization $\mathcal{A}_+^k(N^*)$ only words which equal ordinary prime numbers.

We now turn our attention to a certain relation between arithmetizations of the free monoid $F(a_1)$ and the arithmetizations of the free monoid $F(A)$.

We say that an arithmetization $F_\varphi(q)$ of the free monoid $F(a_1)$ is extendible to an arithmetization of the free monoid $F(A)$ if there exists an arithmetization $F_\varphi(Q)$ of $F(A)$ such that $q \in Q$, the function φ of $F_\varphi(q)$ is also the "concatenative" function of $F_\varphi(Q)$, and $F_\varphi(q)$ is embedded in $F_\varphi(Q)$.

4.2.6. Proposition. (1) For any $k > 0$, $F_{\xi_k}(p_\mu^{(k)})$ $(\mu \geq 1)$ is not extendible to any arithmetization of $F(A)$.
(2) If $F_\varphi(2)$ is extendible to an arithmetization of $F(A)$, then φ is either ordinary addition or ordinary multiplication.

(3) If $F_{\varphi}(1)$ is extendible to an arithmetization of $F(A)$, then φ is ordinary addition.

Property (1) follows from Theorem 1.2.4, where it can be seen that concatenations involving Hilbert-Ackermann functions ξ_k and number-systems P^k $(k > 0)$ are all noncommutative, consequently the concatenations in question cannot possibly satisfy the axioms of the commutative free monoid $F(A)$.

Property (2). Let $F_{\varphi}(2)$ be extendible to an arithmetization of $F(A)$. Aside from Theorems 4.1.1 and 1.2.5 and Proposition 4.2.1, the only other possible unique representations are those given by Theorem 1.2.4. Consequently, if $F_{\varphi}(2)$ is extendible to an arithmetization of $F(A)$, then it must in some way involve the above-mentioned unique representations, including unique representations which are variations of the above, i.e., e.g., representations of the form

$$p_{j_s}^{(1)} p_{j_{s-1}}^{(1)} \cdots p_{j_1}^{(1)} p_{i_r}^{(0)} p_{i_{r-1}}^{(0)} \cdots p_{i_1}^{(0)}, \quad p_{k_t}^{(2)} p_{k_{t-1}}^{(2)} \cdots p_{k_1}^{(2)} p_{j_s}^{(1)} p_{j_{s-1}}^{(1)} \cdots p_{j_1}^{(1)} p_{i_r}^{(0)} p_{i_{r-1}}^{(0)} \cdots p_{i_1}^{(0)}$$

and so on as shown earlier by the author [7]. In all the above-mentioned possibilities, aside from ordinary addition and ordinary multiplication, we see that they involve concatenations which are noncommutative. It follows that φ must be either ordinary addition or ordinary multiplication.

Property (3). From what was said above, it is clear that in this case the function φ can only be ordinary addition.

§4.3. Ordinary addition in arithmetizations of $\mathfrak{a}^k(A)$

For any $k \geq 0$, with the help of the arithmetical maps σ, $\bar{\sigma}$, τ_k and $\bar{\tau}_k$, defined in section 2.4, we introduce the following functions in $\mathfrak{a}^k(A)$:

(1) $I_k(\#) = a_1$,

$I_k(a_\mu X) = \tau_k \sigma(a_\mu) \odot I_k(X)$,

note, $I_k(X)$ is an abbreviation of $\prod^k(X)$,

(2) $$\bar{I}_k(\pi^{(k)}_{i_r} \odot \pi^{(k)}_{i_{r-1}} \odot \cdots \odot \pi^{(k)}_{i_1}) =$$

$$= \bar{\bar{\sigma\tau}}_k(\pi^{(k)}_{i_r}) \oplus \bar{\bar{\sigma\tau}}_k(\pi^{(k)}_{i_{r-1}}) \oplus \cdots \oplus \bar{\bar{\sigma\tau}}_k(\pi^{(k)}_{i_1})$$

$$= a_{i_r} a_{i_{r-1}} \cdots a_{i_1}$$

if $\pi^{(k)}_{i_1}, \pi^{(k)}_{i_2}, \ldots, \pi^{(k)}_{i_r} \in [\overline{\prod}_{F(a_1)}]^{(k)}$,

and undefined otherwise.

4.3.1. Proposition. (1) For any X and Y in F(A),

$$I_k(X \oplus Y) = I_k(X) \odot I_k(Y) \ .$$

(2) For any X and Y in $F(a_1)$ satisfying the definition of $\bar{I}_k$,

$$\bar{I}_k(X \odot Y) = \bar{I}_k(X) \oplus \bar{I}_k(Y) \ .$$

(3) For any X in $F(a_1)$ satisfying the definition of $\bar{I}_k$, $I_k(\bar{I}_k(X)) = X$.

Property (1). For $Y = \#$, we have $I_k(X \oplus \#) = I_k(X)$ and $I_k(X) \odot I_k(\#) = I_k(X) \odot a_1 = I_k(X)$. In turn, suppose that property (1) holds for some Y. Then by the definition of the function I_k we have

$$I_k(X \oplus a_\mu Y) = I_k(a_\mu(X \oplus Y)) = \tau_k\sigma(a_\mu) \odot I_k(X \oplus Y)$$

$$= \tau_k\sigma(a_\mu) \odot I_k(X) \odot I_k(Y)$$

$$= I_k(X) \odot I_k(a_\mu Y) \ .$$

Property (2). By Corollary 3.4.14(2), let $X = \pi^{(k)}_{i_r} \odot \cdots \odot \pi^{(k)}_{i_1}$ and $Y = \pi^{(k)}_{j_s} \odot \cdots \odot \pi^{(k)}_{j_1}$, where all the above factors are in $[\overline{\prod}_{F(a_1)}]^{(k)}$.

Then by the definition of $\bar{I}_k$ we get

$$\bar{I}_k(X \odot Y) = \bar{I}_k((\pi^{(k)}_{i_r} \odot \cdots \odot \pi^{(k)}_{i_1}) \odot (\pi^{(k)}_{j_s} \odot \cdots \odot \pi^{(k)}_{j_1}))$$

$$= a_{i_r} a_{i_{r-1}} \cdots a_{i_1} \oplus a_{j_s} a_{j_{s-1}} \cdots a_{j_1}$$

$$= \bar{I}_k(\pi^{(k)}_{i_r} \odot \cdots \odot \pi^{(k)}_{i_1}) \oplus \bar{I}_k(\pi^{(k)}_{i_s} \odot \cdots \odot \pi^{(k)}_{j_1}) = I_k(X) \oplus I_k(Y) \ .$$

Property (3). By Corollary 3.4.14(2), let $X = \pi^{(k)}_{i_r} \odot \cdots \odot \pi^{(k)}_{i_1}$, where $\pi^{(k)}_{i_1}, \ldots, \pi^{(k)}_{i_r} \in [\overline{\prod}_{F(a_1)}]^{(k)}$. Then by the definition of I_k and $\bar{I}_k$ and Proposition 2.4.2, we obtain

$$I_k(\bar{I}_k(X)) = I_k(\bar{I}_k(\pi^{(k)}_{i_r} \odot \cdots \odot \pi^{(k)}_{i_1}))$$

$$= I_k(a_{i_r} \cdots a_{i_1}) = \tau_k\sigma(a_{i_r}) \odot \cdots \odot \tau_k\sigma(a_{i_1})$$

$$= \pi^{(k)}_{i_r} \odot \cdots \odot \pi^{(k)}_{i_1} = X \ .$$

For any $k \geq 0$, we now define the functions $X\,[+]^k\,Y$ and $X\,[\times]^k\,Y$ in $\mathfrak{A}^k(A)$ by the following:

If $I_k(X)$ and $I_k(Y)$ are expressible as $I_k(X) = \pi^{(k)}_{i_r} \odot \cdots \odot \pi^{(k)}_{i_1}$ and $I_k(Y) = \pi^{(k)}_{j_s} \odot \cdots \odot \pi^{(k)}_{j_1}$, where the factors in $[\overline{\prod}_{F(a_1)}]^{(k)}$, then

(1) $X\,[+]^k\,Y = \bar{I}_k(I_k(X) \oplus I_k(Y))$,

(2) $X\,[\times]^k\,Y = \bar{I}_k(I_k(X) \odot I_k(Y))$.

With respect to the above definition, we point out that $X\,[+]^k\,Y$ and $X\,[\times]^k\,Y$ can also be defined equivalently in terms of the laws of composition $a_\mu \boxplus a_\nu$ and $a_\mu \boxdot a_\nu$ in the nonconcatenative semiring SM_A, introduced in section 2.1, together with the suitable arithmetical maps. We chose the above definition on the grounds that this type of

definition can be easily used involving other functions in $\mathcal{A}^k(A)$, whereas the above-mentioned semiring is limited to its two laws of composition.

4.3.2. Proposition. In accordance with the conditions in the definitions of the functions $X\,[+]^k\,Y$ and $X\,[\times]^k\,Y$,

(1) $X\,[+]^k\,Y = Y\,[+]^k\,X$,

(2) $X\,[+]^k\,(Y\,[+]^k\,Z) = (X\,[+]^k\,Y)\,[+]^k\,Z$,

(3) $X\,[\times]^k\,Y = X \oplus Y$,

(4) $X \oplus (Y\,[+]^k\,Z) = (X \oplus Y)\,[+]^k\,(X \oplus Z)$.

Property (1). By the definition of $X\,[+]^k\,Y$ and the commutativity of word addition, we have

$$\begin{aligned} X\,[+]^k\,Y &= \overline{I}_k(I_k(X) \oplus I_k(Y)) \\ &= \overline{I}_k(I_k(Y) \oplus I_k(X)) = Y\,[+]^k\,Y \ . \end{aligned}$$

Property (2). By the definition of $X\,[+]^k\,Y$, Proposition 4.3.1(3) and the associativity of word addition we get

$$\begin{aligned} X\,[+]^k\,(Y\,[+]^k\,Z) &= X\,[+]^k\,\overline{I}_k(I_k(Y) \oplus I_k(Z)) \\ &= \overline{I}_k(I_k(X) \oplus I_k(\overline{I}_k(I_k(Y) \oplus I_k(Z))) \\ &= \overline{I}_k(I_k(X) \oplus (I_k(Y) \oplus I_k(Z))) \\ &= \overline{I}_k((I_k(X) \oplus I_k(Y)) \oplus I_k(Z)) \\ &= \overline{I}_k(I_k(\overline{I}_k(I_k(X) \oplus I_k(Y)) \oplus I_k(Z)) \\ &= \overline{I}_k(I_k(X) \oplus I_k(Y))\,[+]^k\,Z \\ &= (X\,[+]^k\,Y)\,[+]^k\,Z \ . \end{aligned}$$

Property (3). By Corollary 3.4.14(2), let $I_k(X) = \pi^{(k)}_{i_r} \odot \ldots \odot \pi^{(k)}_{i_1}$ and $I_k(Y) = \pi^{(k)}_{j_s} \odot \ldots \odot \pi^{(k)}_{j_1}$, where the factors are in $[\overline{\prod}_{F(a_1)}]^{(k)}$. Then

by Proposition 4.3.1(2) and definition of $\bar{I}_k$, we have

$$\begin{aligned} X\,[\times]^k\,Y &= \bar{I}_k(I_k(X) \odot I_k(Y)) \\ &= \bar{I}_k(I_k(X)) \oplus \bar{I}_k(I_k(Y)) \\ &= \bar{I}_k(\pi^{(k)}_{i_r} \odot \cdots \odot \pi^{(k)}_{i_1}) \oplus \bar{I}_k(\pi^{(k)}_{j_s} \odot \cdots \odot \pi^{(k)}_{j_1}) \\ &= X \oplus Y \ . \end{aligned}$$

Property (4) is obtained by Proposition 4.3.1(3) and the distributive law with respect to word addition and word multiplication as follows:

$$\begin{aligned} X \oplus (Y\,[+]^k\,Z) &= \bar{I}_k(I_k(X) \odot I_k(Y\,[+]^k\,Z)) \\ &= \bar{I}_k(I_k(X) \odot I_k(\bar{I}_k(I_k(Y) \oplus I_k(Z)))) \\ &= \bar{I}_k(I_k(X) \odot (I_k(Y) \oplus I_k(Z)) \\ &= \bar{I}_k(I_k(X) \odot I_k(Y) \oplus I_k(X) \odot I_k(Z)) \\ &= \bar{I}_k(I_k(\bar{I}_k(I_k(X) \odot I_k(Y))) \oplus I_k(\bar{I}_k(I_k(X) \odot I_k(Z))) \\ &= \bar{I}_k(I_k(X) \odot I_k(Y))\,[+]^k\,\bar{I}_k(I_k(X) \odot I_k(Z)) \\ &= (X \oplus Y)\,[+]^k\,(X \oplus Z) \ . \end{aligned}$$

4.3.3. Proposition. (1) For any $k \geq 0$, the function $X\,[+]^k\,Y$ corresponds to ordinary addition in the arithmetization $\mathcal{A}^k_\times(P^k)$ of $\mathcal{A}^k(A)$.

(2) For any $k \geq 0$, the function $X \oplus Y$ corresponds to ordinary addition in the arithmetization $\mathcal{A}^k_+(N^*)$.

Property (1). For any $k \geq 0$, consider the function $X\,[+]^k\,Y$ in the arithmetization $\mathcal{A}^k_\times(P^k)$ of $\mathcal{A}^k(A)$. In $\mathcal{A}^k_\times(P^k)$, let $X = p^{(k)}_{i_r} \times p^{(k)}_{i_{r-1}} \times \ldots \times p^{(k)}_{i_1}$ and $Y = p^{(k)}_{j_s} \times p^{(k)}_{j_{s-1}} \times \ldots \times p^{(k)}_{j_1}$ be any nonempty words in $F_\times(P^k)$. By the definition of I_k, Theorem 2.4.2 and

Corollary 4.2.14, we have

(1) $$I_k(p^{(k)}_{i_r} \times \ldots \times p^{(k)}_{i_1}) = \pi^{(k)}_{i_r} \odot \ldots \odot \pi^{(k)}_{i_1} ,$$

(2) $$I_k(p^{(k)}_{j_s} \times \ldots \times p^{(k)}_{j_1}) = \pi^{(k)}_{j_s} \odot \ldots \odot \pi^{(k)}_{j_1} ,$$

(3) $$I_k(X) \oplus I_k(Y) = (\pi^{(k)}_{i_r} \odot \ldots \odot \pi^{(k)}_{i_1}) \oplus (\pi^{(k)}_{j_s} \odot \ldots \odot \pi^{(k)}_{j_1}) = \pi^{(k)}_{n_t} \odot \ldots \odot \pi^{(k)}_{n_1} ,$$

where $\pi^{(k)}_{n_1}, \ldots, \pi^{(k)}_{n_t} \in [\overline{|\ |}_{F(a_1)}]^{(k)}$. In other words, (1), (2) and (3) mean the following:

$$I_k(X) = a_1^{p^{(k)}_{i_r} \times \ldots \times p^{(k)}_{i_1}} , \quad I_k(Y) = a_1^{p^{(k)}_{j_s} \times \ldots \times p^{(k)}_{j_1}} ,$$

$$I_k(X) \oplus I_k(Y) = a_1^{(p^{(k)}_{i_r} \times \ldots \times p^{(k)}_{i_1}) + (p^{(k)}_{j_s} \times \ldots \times p^{(k)}_{j_1})} = a_1^{p^{(k)}_{n_t} \times \ldots \times p^{(k)}_{n_1}} ,$$

where $p^{(k)}_{n_1}, \ldots, p^{(k)}_{n_t} \in [P^0]^k$. With respect to the functions $\overline{I}_k$, by Theorem 2.4.2, we have

$$\overline{I}_k(\pi^{(k)}_{n_t} \odot \ldots \odot \pi^{(k)}_{n_1}) = p^{(k)}_{n_t} \times p^{(k)}_{n_{t-1}} \times \ldots \times p^{(k)}_{n_1} ,$$

which obviously is precisely the value of $X + Y$ in $\mathcal{A}^k_\times(P^k)$ for X and Y.

Property (2) is trivial, since ordinary addition in $\mathcal{A}^k_+(N^*)$ is defined to correspond to word addition in $\mathcal{A}^k(A)$.

4.3.4. Lemma. If S is any subset of N^* such that $P^k \subset S \subseteq P^n$, where $k < n$, then ordinary addition in $\mathcal{A}^k_\times(S)$ of $\mathcal{A}^k(A)$ corresponds to $X\,[+]^k\,Y$, defined only for words X and Y in $F_\times(S)$ which are products with factors in P^k.

The underlying frame $\mathcal{H}^k$ of arithmetic $\mathcal{A}^k(A)$ was constructed precisely in order to define ordinary addition in $\mathcal{A}^k_\times(P^k)$ as the function

$X\,[+]^k\,Y$. Let $S = \{s_1, s_2, \ldots\}$. In $\mathcal{A}^k_X(S)$, by definition of $X\,[+]^k\,Y$, if $X = s_{i_\alpha} s_{i_{\alpha-1}} \ldots s_{i_1}$ and $Y = s_{j_\beta} s_{j_{\beta-1}} \ldots s_{j_1}$, then

$$s_{i_\alpha} \times s_{i_{\alpha-1}} \times \ldots \times s_{i_1}\,[+]^k\, s_{j_\beta} \times s_{j_{\beta-1}} \times \ldots \times s_{j_1} =$$

$$= \bar{I}_k((\pi^{(k)}_{i_\alpha} \odot \ldots \odot \pi^{(k)}_{i_1}) \oplus (\pi^{(k)}_{j_\beta} \odot \ldots \odot \pi^{(k)}_{j_1}))\ ,$$

which clearly can correspond to ordinary addition if $s_{i_1}, \ldots, s_{i_\alpha}, s_{j_1}, \ldots, s_{j_\beta}$ are elements in P^k.

4.3.5. Theorem. For any $k \geq 0$, the functions $X \oplus Y$ and $X\,[+]^k\,Y$ are the only functions in $\mathcal{A}^k(A)$ which correspond to ordinary addition in the arithmetizations of $\mathcal{A}^k(A)$.

Since $\#$ and a_0 of N cannot be in any alphabet corresponding to A, let S be some infinite subset of N^*. In turn, let $\mathcal{A}^k_\varphi(S)$ be any arithmetization of $\mathcal{A}^k(A)$. We have to consider the following two cases:

(A) $S \subseteq P^k$,

(B) $S \supset P^k$,

where P^k is a Hilbert-Ackermann number-system.

For case (A), where $S \subseteq P^k$, on the strength of the frame $\mathcal{K}^k$ and definition structure $\mathcal{O}^k$ underlying arithmetic $\mathcal{A}^k(A)$, ordinary addition in $\mathcal{A}^k_\varphi(S)$ can only correspond to $X\,[+]^k\,Y$ and of course φ must be ordinary multiplication.

For case (B), where $S \supset P^k$, we are obliged to consider the following cases:

(I) $P^k \subset S \not\subseteq P^n$ for any $n > k$,

(II) $P^k \subset S \subseteq P^n$ for some $n > k$.

If case (I) holds, then by Theorems 1.2.1 and 1.2.2 one of the following cases must hold:

(i) $S = P^k \cup \{1,4\} \cup N_1$, where P^k, $\{1,4\}$ and N_1 are disjoint and N_1 may be empty;

(ii) $S = P^k \cup \{1\} \cup N_2$, where P^k, $\{1\}$ and N_2 are disjoint and N_2 may be empty;

(iii) $S = P^k \cup \{4\} \cup N_3$, where P^k, $\{4\}$ and N_3 are disjoint and N_3 may be empty;

(iv) $S = P^k \cup N_4$, where P^k and N_4 are disjoint and $1, 4 \notin N_4$.

In cases (i) and (ii), since $1 \in S$, by Proposition 4.2.6(3) we have $F_+(1)$ which is extendible to an arithmetization of $\mathcal{A}^k(A)$, and clearly we must have $\mathcal{A}^k_+(S)$, which means that in this case ordinary addition must correspond to the function $X \oplus Y$ in $\mathcal{A}^k(A)$.

In case (iii), since $2 \in P^k$, by Proposition 4.2.6(2), we have $F_+(2)$ or $F_\times(2)$ which are extendible to arithmetizations of $\mathcal{A}^k(A)$. However, in case (iii), since $4 \in S$, we cannot have arithmetization $F_\times(2)$, since 4 is not irreducible in any unique resolution theorem, except Theorem 4.1.1 which is irrelevant here. Consequently, we have $F_+(2)$, which means that in this case ordinary addition in $\mathcal{A}^k_+(S)$ corresponds to $X \oplus Y$.

Case (iv) is the same as case (II) by virtue of Theorem 1.2.2 which we take up next.

If case (II) holds, where we have $P^k \subset S \subseteq P^n$ for some $n > k$, then we are obliged to consider the following cases:

(a) $S = P^n$ for some $n > k$,

(b) $S \subset P^n$ for some $n > k$.

For case (a), since $2 \in S$, like the above case (iii), we have $F_+(2)$ or $F_\times(2)$. Clearly, for $F_+(2)$, we are led to $\mathcal{A}^k_+(S)$ and in turn to ordinary addition corresponding to $X \oplus Y$. For $F_\times(2)$, by Lemma 4.3.4, since we are dealing with arithmetic $\mathcal{A}^k(A)$ and we have $P^k \subset P^n = S$, we obtain ordinary addition as a partial function corresponding to $X [+]^k Y$.

For case (b), where $P^k \subset S \subset P^n$ for some $n > k$, as in case (a), since we are dealing with arithmetic $\mathcal{A}^k(A)$ and $2 \in S$, by Lemma 4.3.4,

ordinary addition must correspond to the partial function $X\,[+]^k\,Y$.

4.3.6. Proposition. If S is an infinite subset of N^* such that $\mathcal{Q}^k_\varphi(S)$ is an arithmetization of $\mathcal{Q}^k(A)$ in which ordinary addition corresponds to $X\,[+]^k\,Y$ in $\mathcal{Q}^k(A)$, then $S \subseteq P^k$.

This follows from the definition of $X\,[+]^k\,Y$ and the underlying frame $\mathcal{H}^k$ of $\mathcal{Q}^k(A)$.

4.3.7. Proposition. (1) For any $k \geq 0$, the function $X\,[+]^k\,Y$ does not correspond to ordinary addition in the arithmetization $\mathcal{Q}^k_+(N^*)$ of $\mathcal{Q}^k(A)$.
(2) The functions $X\,[+]^k\,Y$ have a different range of values in the free monoid $F(A)$ for each $k \geq 0$.

Property (1). In the arithmetization $\mathcal{Q}^k_+(N^*)$ of $\mathcal{Q}^k(A)$, for any $k \geq 0$, we have

$$(n_{i_r} + \ldots + n_{i_1})\,[+]^k\,(n_{j_s} + \ldots + n_{j_1}) = \overline{I}_k(p^{(k)}_{i_r} \times \ldots \times p^{(k)}_{i_1} + p^{(k)}_{j_s} \times \ldots \times p^{(k)}_{j_1})$$

and it is clear from the above equation that $X\,[+]^k\,Y$ cannot correspond to ordinary addition in $\mathcal{Q}^k_+(N^*)$.

Property (2). On the strength of Proposition 1.2.3, for any $k \geq 0$, we can always find $p^{(k)}_\mu, p^{(k)}_\nu$ in P^k and $p^{(k+1)}_\mu, p^{(k+1)}_\nu$ in P^{k+1} such that $p^{(k+1)}_\mu < p^{(k)}_\mu$ and $p^{(k+1)}_\nu < p^{(k)}_\nu$. Clearly, if $p^{(k+1)}_\mu < p^{(k)}_\mu$ and $p^{(k+1)}_\nu < p^{(k)}_\nu$, then $p^{(k+1)}_\mu + p^{(k+1)}_\nu < p^{(k)}_\mu + p^{(k)}_\nu$, consequently $p^{(k+1)}_\mu + p^{(k+1)}_\nu \neq p^{(k)}_\mu + p^{(k)}_\nu$. Since

$$a_\mu\,[+]^k\,a_\nu = \overline{I}_k(\pi^{(k)}_\mu \oplus \pi^{(k)}_\nu) = \overline{I}_k(a_1^{\,p^{(k)}_\mu + p^{(k)}_\nu}),$$

$$a_\mu\,[+]^{k+1}\,a_\nu = \overline{I}_{k+1}(\pi^{(k+1)}_\mu \oplus \pi^{(k+1)}_\nu) = \overline{I}_{k+1}(a_1^{\,p^{(k+1)}_\mu + p^{(k+1)}_\nu}),$$

it follows that the ranges of $X\,[+]^{k}\,Y$ and $X\,[+]^{k+1}\,Y$ cannot be the same on the free monoid $F(A)$. The above argument can be easily extended to any two different Hilbert-Ackermann number-systems. Consequently, property (2) holds for any $k \geq 0$.

CHAPTER V

GOLDBACH SENTENCES IN $\mathcal{A}^k(A)$

§5.1. Goldbach sentences

A sentence in arithmetic $\mathcal{A}^k(A)$ $(k \geq 0)$ is called a Goldbach sentence if there exists an arithmetization of $\mathcal{A}^k(A)$ in which the sentence in question is the well-known Goldbach conjecture.

5.1.1. Theorem. For any $k \geq 0$, if a Goldbach sentence is a theorem of arithmetic $\mathcal{A}^k(A)$, then the Goldbach conjecture is true.

For any $k \geq 0$, let $\mathcal{G}$ be a Goldbach sentence which is a theorem in arithmetic $\mathcal{A}^k(A)$. As in model theory, from the preceding assumption it follows that sentence $\mathcal{G}$ will be true in every arithmetization of arithmetic $\mathcal{A}^k(A)$. In particular, sentence $\mathcal{G}$ will be true in the arithmetization in which $\mathcal{G}$ is the Goldbach conjecture.

5.1.2. Theorem. For any $k \geq 0$, if every Goldbach sentence in arithmetic $\mathcal{A}^k(A)$ is independent of $\mathcal{A}^k(A)$, then the Goldbach conjecture is independent of arithmetic $\mathcal{A}^k(A)$.

Assume that all Goldbach sentences in a given arithmetic $\mathcal{A}^k(A)$ $(k \geq 0)$ are independent of $\mathcal{A}^k(A)$ and suppose that the Goldbach conjecture is not independent of $\mathcal{A}^k(A)$. To say that the Goldbach conjecture is not independent of $\mathcal{A}^k(A)$ means that there exists a sentence in $\mathcal{A}^k(A)$ which in some arithmetization of $\mathcal{A}^k(A)$ corresponds to the Goldbach conjecture, a contradiction.

An alphabetical Goldbach sentence in arithmetic $\mathcal{A}^k(A)$ $(k \geq 0)$ is a Goldbach sentence in $\mathcal{A}^k(A)$ involving in its statement the function $X\,[+]^k\,Y$, where X and Y range over some set A_0 such that $A_0 \subseteq A$,

where A is the alphabet of the free monoid F(A) in arithmetic $\mathcal{A}^k(A)$.

A prime-word Goldbach sentence in arithmetic $\mathcal{A}^k(A)$ ($k \geq 0$) is a Goldbach sentence in $\mathcal{A}^k(A)$ involving in its statement word addition $X \oplus Y$ of $\mathcal{A}^k(A)$, where X and Y range over some set $\mathcal{P}_0$ such that $\mathcal{P}_0 \subseteq \mathcal{P}$, where $\mathcal{P}$ is the set of all prime words in $\mathcal{A}^k(A)$.

5.1.3. Theorem. For any $k \geq 0$, if $\mathcal{G}$ is a Goldbach sentence in arithmetic $\mathcal{A}^k(A)$, then $\mathcal{G}$ is either an alphabetical Goldbach sentence or a prime-word Goldbach sentence in $\mathcal{A}^k(A)$.

Consider any arithmetic $\mathcal{A}^k(A)$ ($k \geq 0$). If sentence $\mathcal{G}$ is a Goldbach sentence in arithmetic $\mathcal{A}^k(A)$, then there must exist an arithmetization $\mathcal{A}^k_\varphi(S)$ of $\mathcal{A}^k(A)$ in which $\mathcal{G}$ corresponds to the Goldbach conjecture. In the arithmetization $\mathcal{A}^k_\varphi(S)$, since the Goldbach conjecture must involve ordinary addition in its statement, by virtue of Theorem 4.3.5 it follows that $\mathcal{G}$ must involve in its statement either $X\,[+]^k\,Y$ or $X \oplus Y$ of $\mathcal{A}^k(A)$.

If sentence $\mathcal{G}$ involves the function $X\,[+]^k\,Y$ in its statement, then by Proposition 4.3.6 we must have $S \subseteq P^k$ in the arithmetization $\mathcal{A}^k_\varphi(S)$ of $\mathcal{A}^k(A)$. Since the Goldbach conjecture also involves the set P^0 of prime numbers and by Corollary 1.2.1.1 we have $P^0 \subseteq P^k$ ($k \geq 0$), it follows that $P^0 \subseteq P^k \subseteq S$, where S corresponds to the alphabet A of $\mathcal{A}^k(A)$. In other words, the Goldbach sentence $\mathcal{G}$ for the case involving the function $X\,[+]^k\,Y$ must be an alphabetical Goldbach sentence in $\mathcal{A}^k(A)$.

If the Goldbach sentence $\mathcal{G}$ in $\mathcal{A}^k(A)$ involves the function $X \oplus Y$ in its statement, then we consider the following. The sentence $\mathcal{G}$ being a Goldbach sentence, there must exist an arithmetization $\mathcal{A}^k_\varphi(S)$ of $\mathcal{A}^k(A)$ in which $\mathcal{G}$ corresponds to the Goldbach conjecture, where $\mathcal{G}$ in $\mathcal{A}^k_\varphi(S)$ involves ordinary addition and the set P^0 of prime numbers. Since

we are involved with the word addition $X \oplus Y$ of $\mathcal{A}^k(A)$, the concatenative function φ must be ordinary addition. We now have to show that X and Y in the domain of $X \oplus Y$ must range over prime words. Assume that some X and Y in the domain of $X \oplus Y$ with respect to the Goldbach sentence $\mathcal{G}$ are not prime words. Clearly, X and Y in the arithmetization $\mathcal{A}_+^k(S)$ must correspond to prime numbers, otherwise $\mathcal{G}$ could not be a Goldbach sentence in this case. If X and Y in the domain of $X \oplus Y$ are not prime words, then by Lemma 3.4.3 they must be of the form $X = X_1 \odot X_2$ and $Y = Y_1 \odot Y_2$ for some X_1, X_2, Y_1 and Y_2 in F(A). On the other hand, in the arithmetization $\mathcal{A}_+^k(S)$, regarding to X and Y, we must also have

$$X = X_1 \odot X_2 = (s_{i_\alpha} + s_{i_{\alpha-1}} + \ldots + s_{i_1}) \odot (s_{j_\beta} + s_{j_{\beta-1}} + \ldots + s_{j_1}) ,$$

$$Y = Y_1 \odot Y_2 = (s_{m_\sigma} + s_{m_{\sigma-1}} + \ldots + s_{m_1}) \odot (s_{n_\tau} + s_{n_{\tau-1}} + \ldots + s_{n_1}) ,$$

where the two sums on the right side of the first equation correspond to X_1 and X_2 and the two sums on the right side of the second equation correspond to Y_1 and Y_2 respectively. In turn, by the definition of word multiplication in $\mathcal{A}^k(A)$ we have in the arithmetization $\mathcal{A}_+^k(S)$ of $\mathcal{A}^k(A)$ the following:

$$X = X_1 \odot (s_{j_\beta} + \ldots + s_{j_1}) = (s_{j_\beta} \odot X_1) + (s_{j_{\beta-1}} \odot X_1) + \ldots + (s_{j_1} \odot X_1)$$

$$= (s_{j_\beta i_\alpha} + \ldots + s_{j_\beta i_1}) + \ldots + (s_{j_1 i_\alpha} + \ldots + s_{j_1 i_1}) ,$$

$$Y = Y_1 \odot (s_{n_\tau} + \ldots + s_{n_1}) = (s_{n_\tau} \odot Y_1) + (s_{n_{\tau-1}} \odot Y_1) + \ldots + (s_{n_1} \odot Y_1)$$

$$= (s_{n_\tau m_\sigma} + \ldots + s_{n_\tau m_1}) + \ldots + (s_{n_1 m_\sigma} + \ldots + s_{n_1 m_1}) .$$

It is clear from the above equations that X and Y could not possibly be

prime numbers in the arithmetization $\mathcal{A}^{k}_{+}(S)$. Therefore, sentence $\mathcal{G}$ involving X + Y must be a prime-word Goldbach sentence.

§5.2. Alphabetical Goldbach sentences

Firstly, we need the relation H(X) and functions $g_1(X)$ and $g_2(X)$ in arithmetic $\mathcal{A}^{k}(A)$ $(k \geq 0)$, which we introduce as follows:

(1) $H(X) \Longleftrightarrow \bigvee \partial(Y) \leq \partial(X) \bigvee \partial(Z) \leq \partial(X)$

$\{X = Y \oplus Z \wedge X \neq \# \Longrightarrow Y = \# \vee Z = \#\}$,

(2) $g_1(X) = \mu\partial(Z) \leq \partial(X)\{Z = H(Z) \wedge Z = odd_{a_1}(Z) \wedge$

$\bigvee \partial(Y) \leq \partial(Z)\{Y = H(Y) \wedge Y = odd_{a_1}(Y) \wedge X = Z\,[+]^{k}\,Y\}\}$,

(3) $g_2(X) = \mu\partial(Y) \leq \partial(X)\{Y = H(Y) \wedge Y = odd_{a_1}(Y) \wedge$

$\bigvee \partial(Z) \leq \partial(Y)\{Z = H(Z) \wedge Z = odd_{a_1}(Z) \wedge X = Z\,[+]^{k}\,Y\}\}$.

In turn, we introduce the sentence $\mathcal{G}^{k}(A)$ in arithmetic $\mathcal{A}^{k}(A)$ $(k \geq 0)$ as follows:

$\mathcal{G}^{k}(A)$: If X is an a_1-even word and $X \neq \mathfrak{p}_2$,

then $X = g_1(X)\,[+]^{k}\,g_2(X)$.

The above sentence is in quantifier-free form, however it can also be stated in a more readable informal form as follows:

$\mathcal{G}^{k}(A)$: If X is an a_1-even word and $X \neq \mathfrak{p}_2$,

then there exist two a_1-odd words a_μ and a_ν

in the alphabet A such $X = a_\mu\,[+]^{k}\,a_\nu$.

5.2.1. Proposition. For any $k \geq 0$, the sentence $\mathcal{G}^{k}(A)$ in arithmetic $\mathcal{A}^{k}(A)$ is an alphabetical Goldbach sentence in $\mathcal{A}^{k}(A)$.

For $k = 0$, by Proposition 4.2.3, $\mathcal{A}_{\times}^{0}(P^{0})$ is an arithmetization of $\mathcal{A}^{0}(A)$, and in turn by Proposition 4.3.3 $p_{\mu}^{(0)}\,[+]^{(0)}\,p_{\nu}^{(0)}$ corresponds to ordinary addition in $\mathcal{A}_{\times}^{0}(P^{0})$. Clearly, products of prime numbers $p_{i_r}^{(0)} \times p_{i_{r-1}}^{(0)} \times \ldots \times p_{i_1}^{(0)}$ containing the prime $p_1^{(0)} = 2$ are even numbers, otherwise they are odd numbers.

For $k > 0$, consider $[P^{0}]^{k} \subset P^{k}$. By Corollary 4.2.4, $\mathcal{A}_{\times}^{k}([P^{0}]^{k})$ are arithmetizations of $\mathcal{A}^{k}(A)$, and in turn by Proposition 4.3.3 and Lemma 4.3.4 $[p_{\mu}^{(0)}]^{(k)}\,[+]^{k}\,[p_{\nu}^{(0)}]^{(k)}$ correspond to ordinary addition in $\mathcal{A}_{\times}^{k}([P^{0}]^{k})$. The question regarding even and odd numbers is obvious.

Consequently, we have all the ingredients of the Goldbach conjecture in arithmetizations $\mathcal{A}_{\times}^{k}([P^{0}]^{k})$ of $\mathcal{A}^{k}(A)$ $(k \geq 0)$. The fact that $\mathcal{G}^{k}(A)$ is an alphabetical Goldbach sentence in $\mathcal{A}^{k}(A)$ follows from the definition of the sentence $\mathcal{G}^{k}(A)$.

5.2.2. Theorem. For any $k \geq \beta_2$, where β_2 is the second Brun constant of section 1.4, the alphabetical Goldbach sentence $\mathcal{G}^{k}(A)$ in $\mathcal{A}^{k}(A)$ is independent of arithmetic $\mathcal{A}^{k}(A)$.

Firstly, we consider the case $k = \beta_2$, where β_2 is the second Brun constant. We denote the negation of the alphabetical Goldbach sentence $\mathcal{G}^{k}(A)$ as $^{non}\mathcal{G}^{k}(A)$ in the following. By Proposition 4.2.3, $\mathcal{A}_{\times}^{\beta_2}(P^{\beta_2})$ is an arithmetization of $\mathcal{A}^{\beta_2}(A)$. In $\mathcal{A}_{\times}^{\beta_2}(P^{\beta_2})$, the sentence $\mathcal{G}^{\beta_2}(P^{\beta_2})$ is nothing more than a statement of Theorem 1.4.2 of section 1.4. On the strength of Theorem 1.4.2, we know that sentence $\mathcal{G}^{\beta_2}(P^{\beta_2})$ is true. Therefore, sentence $^{non}\mathcal{G}^{\beta_2}(A)$ cannot be proved in arithmetic $\mathcal{A}^{\beta_2}(A)$ and consequently $^{non}\mathcal{G}^{\beta_2}(A)$ cannot be a theorem of $\mathcal{A}^{\beta_2}(A)$. On the other hand, by Corollary 4.2.4(2), we know that $\mathcal{A}_{\times}^{\beta_2}([M]^{\beta_2})$ is an arithmetization of $\mathcal{A}^{\beta_2}(A)$. By Theorem 1.4.4(2), sentence

non $\mathfrak{g}^{\beta_2}([M]^{\beta_2})$ is true. Consequently, sentence $\mathfrak{g}^{\beta_2}(A)$ cannot be a theorem of arithmetic $\mathfrak{a}^{\beta_2}(A)$. Therefore, the alphabetical Goldbach sentence $\mathfrak{g}^{\beta_2}(A)$ is independent of arithmetic $\mathfrak{a}^{\beta_2}(A)$.

The second case, where $k > \beta_2$, is obtained in essentially the same way as above, using Theorem 1.4.3 instead of Theorem 1.4.2.

§5.3. Prime-word Goldbach sentences

To abbreviate matters, we shall state the Goldbach sentences in this section informally, i.e., without resorting to their quantifier-free forms as shown in section 5.2.

We recall the following from section 3.6. A conjugation $C(a_1^{\mu})$ $(\mu \geqq 2)$ consist simply of the solutions, finite in number, of the equation $\Sigma(X) = a_1^{\mu}$. If $\mu = 2\nu$ $(\nu \geqq 1)$, then $C(a_1^{2\nu})$ is called a σ-even conjugation. A $\mathfrak{p}_2$-even subconjugation of $C(a_1^{2\nu})$ is simply the set of all $\mathfrak{p}_2$-even words in $C(a_1^{2\nu})$. Generally, Euler subranges consist of the set of all subconjugations consisting of words of a given length.

With respect to a prime-word Goldbach sentence, one is obliged, on the one hand, to cut through all conjugations $C(a_1^{2\nu})$ $(\nu \geqq 1)$, and on the other hand, to consider certain subconjugations with a certain number of words in each conjugation. The general idea is to reduce the number of words in each such subconjugation to a single word. We shall do this successively in the following.

We start with the following type of sentences:

$\mathfrak{g}^k(\mathfrak{P}^*)$: In arithmetic $\mathfrak{a}^k(A)$ $(k \geqq 0)$, there is at least one $\mathfrak{p}_2$-even word in every $\mathfrak{p}_2$-even subconjugation which can be expressed as a word sum of two $\mathfrak{p}_2$-odd subprime words in $\mathfrak{P}^*$.

5.3.1. Proposition. For any $k \geqq 0$, the sentence $\mathfrak{g}^k(\mathfrak{P}^*)$ in arithmetic $\mathfrak{a}^k(A)$ is a prime-word Goldbach sentence.

On the strength of Proposition 4.2.3, for any $k \geqq 0$, consider the

arithmetization $\mathcal{A}_+^k(N^*)$ of $\mathcal{A}^k(A)$. By Proposition 4.3.3, $X \oplus Y$ corresponds to ordinary addition in $\mathcal{A}_+^k(N^*)$. By Proposition 4.2.5, the set $\mathcal{P}^*$ of subprimes corresponds to the set P^0 of prime numbers in $\mathcal{A}_+^k(N^*)$. Every $\mathcal{P}_2$-even subconjugation in $\mathcal{A}_+^k(N^*)$ consists of sums of the form $X + X$, consequently they are all even numbers. Clearly, the $\mathcal{P}_2$-odd words are odd numbers in $\mathcal{A}_+^k(N^*)$. Therefore, sentence $\mathcal{G}^k(\mathcal{P}^*)$ corresponds to the Goldbach conjecture in $\mathcal{A}_+^k(N^*)$. It is clear from the definition of $\mathcal{G}^k(\mathcal{P}^*)$ that it is a prime-word Goldbach sentence.

Abstract versions of the classical Euler sentence [12] are the following.

$\mathcal{E}_2^k(\mathcal{P}^*)$: In arithmetic $\mathcal{A}^k(A)$ $(k \geq 0)$, every subconjugation in the Euler subrange $\mathcal{E}_2$ contains at least one σ-even word which can be expressed as a word sum of two σ-odd subprime words in $\mathcal{P}^*$.

We can subsume the above sentences in the following class of Euler sentences:

$\mathcal{E}_r^k(\mathcal{P}^*)$: In arithmetic $\mathcal{A}^k(A)$ $(k \geq 0)$, for any $r \geq 2$, every subconjugation in the Euler subrange $\mathcal{E}_r$ contains at least one σ-even word which can be expressed as a word sum of two σ-odd subprime words in $\mathcal{P}^*$.

5.3.2. Proposition. For any $k \geq 0$, every Euler sentence $\mathcal{E}_r^k(\mathcal{P}^*)$ $(r \geq 2)$ in arithmetic $\mathcal{A}^k(A)$ is a prime-word Goldbach sentence.

Firstly, we note that Euler sentences $\mathcal{E}_r^k(\mathcal{P}^*)$ $(r \geq 2)$ in arithmetic $\mathcal{A}^k(A)$ involve σ-even words and word sums of σ-odd subprime words. In the arithmetization $\mathcal{A}_+^k(N^*)$ of $\mathcal{A}^k(A)$, the set of all prime numbers corresponds to the set $\mathcal{P}^*$ of subprime words by Proposition 4.2.5, the set of even numbers greater than 4 corresponds to the set of σ-even

words for any given length by the definition of σ-even words and the definition of Euler subranges in the ordinary σ-even subrange $\mathcal{R}^*$, similarly for the odd numbers and σ-odd words. By Proposition 4.3.3, ordinary addition corresponds to word addition in $\mathcal{A}^k(A)$. In $\mathcal{A}^k_+(N^*)$, for any $r \geq 2$, by the definition of Euler subranges we see that eacl. subconjugation in the Euler subrange $\mathcal{E}_r$ consists of all ways of expressing the same even number as an ordinary sum consisting of exactly r summands. In $\mathcal{A}^k_+(N^*)$, every Euler sentence $\mathcal{E}^k_r(\mathcal{P}^*)$ $(r \geq 2)$ states that each of the above-mentioned subconjugations contains at least one even number expressible as a sum of two odd prime numbers, hence the Goldbach conjecture.

5.3.3. Theorem. For any $k \geq 0$, there exist an infinite number of different Goldbach sentences in arithmetic $\mathcal{A}^k(A)$.

On the strength of Proposition 5.3.2, we need only show that the prime-word Goldbach sentences $\mathcal{E}^k_r(\mathcal{P}^*)$ $(r \geq 2)$ are different Euler sentences in $\mathcal{A}^k(A)$. For any $r \geq 2$, we immediately see that the Euler subranges $\mathcal{E}_r$ involved in $\mathcal{E}^k_r(\mathcal{P}^*)$, except for the initial words taken from the natural subrange of $\mathcal{R}$, are concerned with sets of words of a given length r. Consequently, for each $r \geq 2$, we are dealing with a different set of words in $\mathcal{A}^k(A)$, which means that each sentence $\mathcal{E}^k_r(\mathcal{P}^*)$ $(r \geq 2)$ must be a different sentence.

We consider next sentences in which the number of words in each subconjugation is reduced to a single word, thereby dispensing with subconjugations:

$\mathcal{G}^k(\mathcal{P}^*)$: For any $k \geq 0$, in arithmetic $\mathcal{A}^k(A)$, every $\mathcal{P}_2$-subeven word can be expressed as a word sum of two $\mathcal{P}_2$-odd subprime words.

5.3.4. Proposition. For any $k \geq 0$, sentence $\mathcal{G}^k(\mathcal{P}^*)$ in $\mathcal{A}^k(A)$ implies a prime-word Goldbach sentence.

Firstly, we note that sentence $\mathfrak{S}^k(\sqcap^*)$ in arithmetic $\mathfrak{A}^k(A)$ $(k \geqq 0)$ involves $\mathfrak{p}_1$-subeven words and word sums of $\mathfrak{p}_1$-odd subprime words. By Proposition 4.2.5, in the arithmetization $\mathfrak{A}^k_+(N^*)$ of $\mathfrak{A}^k(A)$, the set $\sqcap^*$ of subprime words coincides with the set P^0 of prime numbers, and the matter of $\mathfrak{p}_1$-odd subprime words is clear. By Proposition 3.7.9, we know that ramified words $a_1^\mu a_2 \odot \mathfrak{p}_1$ $(\mu \geqq 1)$ are $\mathfrak{p}_2$-subeven words. In turn, we note that every $\mathfrak{p}_2$-even word corresponds to an even number in the arithmetization $\mathfrak{A}^k_+(N^*)$ by virtue of the definition of $\mathfrak{p}_2$-even words. Since $2(\mu+2)$ $(\mu \geqq 1)$ runs throught all even numbers greater than 4, by Proposition 3.7.10, it follows that each word $a_1^\mu a_2 \odot \mathfrak{p}_1$ $(\mu \geqq 1)$ in $\mathfrak{A}^k_+(N^*)$ corresponds to some even number greater than 4 and conversely. Consequently, sentence $\mathfrak{S}^k(\sqcap^*)$ implies the Goldbach conjecture in $\mathfrak{A}^k_+(N^*)$.

Lastly, we point out there exists a certain weakened form of the Goldbach conjecture which is false. Consider the following sentences:

$\mathfrak{t}^k(\sqcap^*)$: For any $k \geqq 0$, in arithmetic $\mathfrak{A}^k(A)$, every $\mathfrak{p}_2$-even word such that $\Sigma(X) \succ a_1'$ can be expressed as a word sum of two $\mathfrak{p}_1$-odd subprime words.

5.3.5. Theorem. For any $k \geqq 0$, sentence $\mathfrak{t}^k(\sqcap^*)$ in arithmetic $\mathfrak{A}^k(A)$ is false.

This theorem follows from Corollary 3.7.6.

In the arithmetization $\mathfrak{A}^k_+(N^*)$ of $\mathfrak{A}^k(A)$ $(k \geqq 0)$, sentences $\mathfrak{t}^k(\sqcap^*)$ lead obviously to a weakened form of the Goldbach conjecture in arithmetization $\mathfrak{A}^k_+(N^*)$, which is false in every case on the strength of Theorem 5.3.5.

REFERENCES

(1) V. Brun, Le crible d'Eratosthène et le théorème de Goldbach, (Kristiania) Videnskapsselskapets Skrifter, I Mat.-Naturv. Klasse, No. 3 (1920), 1-36.

(2) C. Chevalley, Fundamental concepts of algebra, New York, 1956.

(3) G. H. Hardy, Goldbach's theorem, Matematisk Tidsskrift B (1922), 1-16.

(4) D. Hilbert, Über das Unendliche, Math. Annalen 95 (1926), 161-190.

(5) D. Hilbert, Sur l'infini, Traduit par André Weil, Acta Math. 48 (1926), 91-122.

(6) J. G. Kemeny, Undecidable problems of elementary number theory, Math. Annalen 135 (1958), 160-169.

(7) H. A. Pogorzelski, Łańcuchy wykładnicze liczb naturalnych, Prace Matematyczne 7 (1962), 19-34.

(8) H. A. Pogorzelski, Recursive arithmetic of Skolem, Math. Scand. 11 (1962), 33-36.

(9) H. A. Pogorzelski, Recursive arithmetic of Skolem II, Math. Scand. 11 (1962), 156-160.

(10) Th. Skolem, Begründung der elementaren Arithmetik, (Kristiania) Viden. Skrifter, I Mat.-Naturv. Klasse, No. 6 (1923), 1-38.

(11) Th. Skolem, Some remarks on the foundations of set theory, Proc. International Congress of Math. 1950, vol. I, 695-704.

(12) J. J. Sylvester, The collected mathematical papers, Vol. 4 (1912).