FORMALIZED MATHEMATICS
Volume 4, Number 1, 1993
Université Catholique de Louvain

Binary Arithmetics

Takaya Nishiyama
Shinshu University
Information Engineering Dept.
Nagano

Yasuho Mizuhara
Shinshu University
Information Engineering Dept.
Nagano

Summary. Formalizes the basic concepts of binary arithmetic and its related operations. We present the definitions for the following logical operators: 'or' and 'xor' (exclusive or) and include in this article some theorems concerning these operators. We also introduce the concept of an n-bit register. Such registers are used in the definition of binary unsigned arithmetic presented in this article. Theorems on the relationships of such concepts to the operations of natural numbers are also given.

MML Identifier: BINARITH.

The notation and terminology used in this paper are introduced in the following papers: [12], [1], [13], [15], [7], [8], [4], [2], [9], [11], [10], [5], [3], [6], and [14].

Let us observe that there exists a natural number which is non empty.

One can prove the following proposition

(1) For all natural numbers i, j holds $+_{\mathbb{N}}(i, j) = i + j$.

Let n be a natural number and let X be a non empty set. A tuple of n and X is an element of X^n.

One can prove the following propositions:

(2) Let i, n be natural numbers, and let D be a non empty set, and let d be an element of D, and let z be a tuple of n and D. If $i \in \mathrm{Seg}\, n$, then $\pi_i(z \frown \langle d \rangle) = \pi_i z$.

(3) Let n be a natural number, and let D be a non empty set, and let d be an element of D, and let z be a tuple of n and D. Then $\pi_{n+1}(z \frown \langle d \rangle) = d$.

(4) For every non empty natural number n holds $n \geq 1$.

(5) For all natural numbers i, n such that $i \in \mathrm{Seg}\, n$ holds i is non empty.

Let x, y be elements of *Boolean*. The functor $x \vee y$ yields an element of *Boolean* and is defined by:

(Def.1) $x \vee y = \neg(\neg x \wedge \neg y)$.

© 1993 Fondation Philippe le Hodey
ISSN 0777-4028

Let x, y be elements of *Boolean*. The functor $x \oplus y$ yielding an element of *Boolean* is defined by:

(Def.2) $x \oplus y = \neg x \wedge y \vee x \wedge \neg y$.

In the sequel x, y, z will denote elements of *Boolean*.

The following propositions are true:

(6) $x \vee y = y \vee x$.

(7) $x \vee \mathit{false} = x$ and $\mathit{false} \vee x = x$.

(8) $x \vee y = \neg(\neg x \wedge \neg y)$.

(9) $\neg(x \wedge y) = \neg x \vee \neg y$.

(10) $\neg(x \vee y) = \neg x \wedge \neg y$.

(11) $x \oplus y = y \oplus x$.

(12) $x \wedge y = \neg(\neg x \vee \neg y)$.

(13) $\mathit{true} \oplus x = \neg x$ and $x \oplus \mathit{true} = \neg x$.

(14) $\mathit{false} \oplus x = x$ and $x \oplus \mathit{false} = x$.

(15) $x \oplus x = \mathit{false}$.

(16) $x \wedge x = x$.

(17) $x \oplus \neg x = \mathit{true}$ and $\neg x \oplus x = \mathit{true}$.

(18) $x \vee \neg x = \mathit{true}$ and $\neg x \vee x = \mathit{true}$.

(19) $x \vee \mathit{true} = \mathit{true}$ and $\mathit{true} \vee x = \mathit{true}$.

(20) $(x \vee y) \vee z = x \vee (y \vee z)$.

(21) $x \vee x = x$.

(22) $x \wedge (y \vee z) = x \wedge y \vee x \wedge z$.

(23) $x \vee y \wedge z = (x \vee y) \wedge (x \vee z)$.

(24) $x \vee x \wedge y = x$.

(25) $x \wedge (x \vee y) = x$.

(26) $x \vee \neg x \wedge y = x \vee y$.

(27) $x \wedge (\neg x \vee y) = x \wedge y$.

(28) $x \wedge \neg x = \mathit{false}$ and $\neg x \wedge x = \mathit{false}$.

(29) $\mathit{false} \wedge x = \mathit{false}$ and $x \wedge \mathit{false} = \mathit{false}$.

(30) $z \wedge x \wedge y = x \wedge y \wedge z$.

(31) $z \wedge y \wedge x = x \wedge y \wedge z$.

(32) $x \wedge z \wedge y = x \wedge y \wedge z$.

(33) $\mathit{true} \oplus \mathit{false} = \mathit{true}$ and $\mathit{false} \oplus \mathit{true} = \mathit{true}$.

(34) $x \oplus y \oplus z = x \oplus y \oplus z$.

(35) $x \oplus \neg x \wedge y = x \vee y$.

(36) $x \vee x \oplus y = x \vee y$.

(37) $x \vee \neg x \oplus y = x \vee \neg y$.

(38) $x \wedge y \oplus z = x \wedge y \oplus x \wedge z$.

In the sequel i, j, k will be natural numbers.

Let us consider i, j. The functor $i -' j$ yields a natural number and is defined as follows:

(Def.3) (i) $i -' j = i - j$ if $i - j \geq 0$,
(ii) $i -' j = 0$, otherwise.

Next we state the proposition

(39) $(i + j) -' j = i$.

We adopt the following convention: n will denote a non empty natural number and x, y, z, z_1, z_2 will denote tuples of n and *Boolean*.

Let us consider n, x. The functor $\neg x$ yields a tuple of n and *Boolean* and is defined as follows:

(Def.4) For every i such that $i \in \mathrm{Seg}\, n$ holds $\pi_i \neg x = \neg \pi_i x$.

Let us consider y. The functor $\mathrm{carry}(x, y)$ yielding a tuple of n and *Boolean* is defined as follows:

(Def.5) $\pi_1 \,\mathrm{carry}(x, y) = \mathit{false}$ and for every i such that $1 \leq i$ and $i < n$ holds $\pi_{i+1} \,\mathrm{carry}(x, y) = \pi_i x \wedge \pi_i y \vee \pi_i x \wedge \pi_i \,\mathrm{carry}(x, y) \vee \pi_i y \wedge \pi_i \,\mathrm{carry}(x, y)$.

Let us consider n, x. The functor $\mathrm{Binary}(x)$ yielding a tuple of n and $\mathbb{N}$ is defined by:

(Def.6) For every i such that $i \in \mathrm{Seg}\, n$ holds $\pi_i \,\mathrm{Binary}(x) \doteq (\pi_i x = \mathit{false} \to 0, \text{the } i -' 1\text{-th power of } 2)$.

Let us consider n, x. The functor $\mathrm{Absval}(x)$ yielding a natural number is defined by:

(Def.7) $\mathrm{Absval}(x) = +_{\mathbb{N}} \circledast \mathrm{Binary}(x)$.

Let us consider n, x, y. The functor $x + y$ yielding a tuple of n and *Boolean* is defined by:

(Def.8) For every i such that $i \in \mathrm{Seg}\, n$ holds $\pi_i(x+y) = \pi_i x \oplus \pi_i y \oplus \pi_i \,\mathrm{carry}(x, y)$.

Let us consider n, z_1, z_2. The functor $\mathrm{add\_ovfl}(z_1, z_2)$ yielding an element of *Boolean* is defined by:

(Def.9) $\mathrm{add\_ovfl}(z_1, z_2) = \pi_n z_1 \wedge \pi_n z_2 \vee \pi_n z_1 \wedge \pi_n \,\mathrm{carry}(z_1, z_2) \vee \pi_n z_2 \wedge \pi_n \,\mathrm{carry}(z_1, z_2)$.

Let us consider n, z_1, z_2. We say that z_1 and z_2 are summable if and only if:

(Def.10) $\mathrm{add\_ovfl}(z_1, z_2) = \mathit{false}$.

Let us consider n, k. Then $n + k$ is a non empty natural number.

One can prove the following proposition

(40) For every tuple z_1 of 1 and *Boolean* holds $z_1 = \langle \mathit{false} \rangle$ or $z_1 = \langle \mathit{true} \rangle$.

Let n_1 be a non empty natural number, let n_2 be a natural number, let D be a non empty set, let z_1 be a tuple of n_1 and D, and let z_2 be a tuple of n_2 and D. Then $z_1 \frown z_2$ is a tuple of $n_1 + n_2$ and D.

Let D be a non empty set and let d be an element of D. Then $\langle d \rangle$ is a tuple of 1 and D.

The following propositions are true:

(41) Given n, and let z_1, z_2 be tuples of n and *Boolean*, and let d_1, d_2 be elements of *Boolean*, and let i be a natural number. If $i \in \mathrm{Seg}\, n$, then $\pi_i\,\mathrm{carry}(z_1 \frown \langle d_1\rangle, z_2 \frown \langle d_2\rangle) = \pi_i\,\mathrm{carry}(z_1, z_2)$.

(42) For every n and for all tuples z_1, z_2 of n and *Boolean* and for all elements d_1, d_2 of *Boolean* holds $\mathrm{add\_ovfl}(z_1, z_2) = \pi_{n+1}\,\mathrm{carry}(z_1 \frown \langle d_1\rangle, z_2 \frown \langle d_2\rangle)$.

(43) For every n and for all tuples z_1, z_2 of n and *Boolean* and for all elements d_1, d_2 of *Boolean* holds $z_1 \frown \langle d_1\rangle + z_2 \frown \langle d_2\rangle = (z_1 + z_2) \frown \langle d_1 \oplus d_2 \oplus \mathrm{add\_ovfl}(z_1, z_2)\rangle$.

(44) For every n and for every tuple z of n and *Boolean* and for every element d of *Boolean* holds $\mathrm{Absval}(z \frown \langle d\rangle) = \mathrm{Absval}(z) + (d = \mathit{false} \rightarrow 0, \text{the } n\text{-th power of } 2)$.

(45) For every n and for all tuples z_1, z_2 of n and *Boolean* holds $\mathrm{Absval}(z_1 + z_2) + (\mathrm{add\_ovfl}(z_1, z_2) = \mathit{false} \rightarrow 0, \text{the } n\text{-th power of } 2) = \mathrm{Absval}(z_1) + \mathrm{Absval}(z_2)$.

(46) For every n and for all tuples z_1, z_2 of n and *Boolean* such that z_1 and z_2 are summable holds $\mathrm{Absval}(z_1 + z_2) = \mathrm{Absval}(z_1) + \mathrm{Absval}(z_2)$.

Acknowledgments

Many thanks to Professor Andrzej Trybulec for making this article a success. We really enjoyed working with you...ARIGATOU GOZAIMASHITA.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[2] Grzegorz Bancerek. Monoids. *Formalized Mathematics*, 3(**2**):213–225, 1992.
[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[5] Czesław Byliński. A classical first order language. *Formalized Mathematics*, 1(**4**):669–676, 1990.
[6] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[9] Czesław Byliński. Semigroup operations on finite subsets. *Formalized Mathematics*, 1(**4**):651–656, 1990.
[10] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[11] Konrad Raczkowski and Andrzej Nędzusiak. Serieses. *Formalized Mathematics*, 2(**4**):449–452, 1991.
[12] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[13] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[14] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[15] Edmund Woronowicz. Many–argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.

Received October 8, 1993