JOURNAL OF FORMALIZED MATHEMATICS
Volume 5, Released 1993, Published 2003
Inst. of Computer Science, Univ. of Białystok

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`.

WWW: `http://mizar.org/JFM/Vol5/binarith.html`

The articles [14], [9], [17], [2], [3], [15], [1], [19], [18], [7], [8], [6], [4], [13], [12], [10], [5], [11], and [16] provide the notation and terminology for this paper.

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

Next we state four propositions:

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

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

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

(5)[1] For all natural numbers i, n such that $i \in \mathrm{Seg}\, n$ holds i is non empty.

Let x, y be boolean sets. The functor $x \vee y$ is defined as follows:

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

Let us note that the functor $x \vee y$ is commutative.

Let x, y be boolean sets. The functor $x \oplus y$ is defined by:

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

Let us note that the functor $x \oplus y$ is commutative.

Let x, y be boolean sets. One can check that $x \vee y$ is boolean.

Let x, y be boolean sets. One can verify that $x \oplus y$ is boolean.

Let x, y be elements of *Boolean*. Then $x \vee y$ is an element of *Boolean*. Then $x \oplus y$ is an element of *Boolean*.

In the sequel x, y, z are boolean sets.

Next we state a number of propositions:

[1] The proposition (4) has been removed.

(7)[2] $x \vee false = x$.

(9)[3] $\neg(x \wedge y) = \neg x \vee \neg y$.

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

(12)[4] $x \wedge y = \neg(\neg x \vee \neg y)$.

(13) $true \oplus x = \neg x$.

(14) $false \oplus x = x$.

(15) $x \oplus x = false$.

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

(17) $x \oplus \neg x = true$.

(18) $x \vee \neg x = true$.

(19) $x \vee true = true$.

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

(33)[5] $true \oplus false = true$.

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

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

(Def. 3) $$i -' j = \begin{cases} i - j, & \text{if } i - j \geq 0, \\ 0, & \text{otherwise.} \end{cases}$$

The following proposition is true

(39) For all natural numbers i, j holds $(i + j) -' j = i$.

We adopt the following convention: i is a natural number, n is a non empty natural number, and x, y, z_1, z_2 are n-tuples of *Boolean*.

Let n be a natural number and let x be a n-tuple of *Boolean*. The functor $\neg x$ yields a n-tuple of *Boolean* and is defined as follows:

[2] The proposition (6) has been removed.
[3] The proposition (8) has been removed.
[4] The proposition (11) has been removed.
[5] The propositions (28)–(32) have been removed.

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

Let n be a non empty natural number and let x, y be n-tuples of *Boolean*. The functor $\mathrm{carry}(x,y)$ yielding a n-tuple of *Boolean* is defined as follows:

(Def. 5) $(\mathrm{carry}(x,y))_1 = \mathit{false}$ and for every i such that $1 \leq i$ and $i < n$ holds $(\mathrm{carry}(x,y))_{i+1} = x_i \wedge y_i \vee x_i \wedge (\mathrm{carry}(x,y))_i \vee y_i \wedge (\mathrm{carry}(x,y))_i$.

Let n be a natural number and let x be a n-tuple of *Boolean*. The functor $\mathrm{Binary}(x)$ yields a n-tuple of $\mathbb{N}$ and is defined as follows:

(Def. 6) For every i such that $i \in \mathrm{Seg}\, n$ holds $(\mathrm{Binary}(x))_i = (x_i = \mathit{false} \rightarrow 0, 2^{i-'1})$.

Let n be a natural number and let x be a n-tuple of *Boolean*. The functor $\mathrm{Absval}(x)$ yields a natural number and is defined as follows:

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

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

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

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

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

The scheme *Ind from 1* concerns a unary predicate $\mathcal{P}$, and states that:

For every non empty natural number k holds $\mathcal{P}[k]$

provided the parameters meet the following requirements:

- $\mathcal{P}[1]$, and
- For every non empty natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$.

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

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

We now state three propositions:

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

(41) For every 1-tuple z_1 of *Boolean* such that $z_1 = \langle \mathit{false} \rangle$ holds $\mathrm{Absval}(z_1) = 0$.

(42) For every 1-tuple z_1 of *Boolean* such that $z_1 = \langle \mathit{true} \rangle$ holds $\mathrm{Absval}(z_1) = 1$.

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 n_1-tuple of D, and let z_2 be a n_2-tuple of D. Then $z_1 \frown z_2$ is a $n_1 + n_2$-tuple of D.

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

We now state several propositions:

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

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

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

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

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

(48) For all n-tuples z_1, z_2 of *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. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/nat_1.html.

[2] Grzegorz Bancerek. The ordinal numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/ordinal1.html.

[3] Grzegorz Bancerek. Sequences of ordinal numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/ordinal2.html.

[4] Grzegorz Bancerek. Monoids. *Journal of Formalized Mathematics*, 4, 1992. http://mizar.org/JFM/Vol4/monoid_0.html.

[5] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/finseq_1.html.

[6] Czesław Byliński. Binary operations. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/binop_1.html.

[7] Czesław Byliński. Functions and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_1.html.

[8] Czesław Byliński. Functions from a set to a set. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_2.html.

[9] Czesław Byliński. Some basic properties of sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/zfmisc_1.html.

[10] Czesław Byliński. A classical first order language. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/cqc_lang.html.

[11] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/finseq_2.html.

[12] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/vectsp_1.html.

[13] Konrad Raczkowski and Andrzej Nędzusiak. Series. *Journal of Formalized Mathematics*, 3, 1991. http://mizar.org/JFM/Vol3/series_1.html.

[14] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. http://mizar.org/JFM/Axiomatics/tarski.html.

[15] Andrzej Trybulec. Subsets of real numbers. *Journal of Formalized Mathematics*, Addenda, 2003. http://mizar.org/JFM/Addenda/numbers.html.

[16] Wojciech A. Trybulec. Pigeon hole principle. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/finseq_4.html.

[17] Zinaida Trybulec. Properties of subsets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/subset_1.html.

[18] Edmund Woronowicz. Relations and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/relat_1.html.

[19] Edmund Woronowicz. Many-argument relations. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/margrel1.html.

Received October 8, 1993

Published January 2, 2004