JOURNAL OF FORMALIZED MATHEMATICS
Volume 15, Released 2003, Published 2003
Inst. of Computer Science, Univ. of Białystok

Full Subtracter Circuit. Part II

Shin'nosuke Yamaguchi
Shinshu University
Nagano

Grzegorz Bancerek
Białystok Technical University

Katsumi Wasaki
Shinshu University
Nagano

Summary. In this article we continue investigations from [22] of verification of a design of subtracter circuit. We define it as a combination of multi cell circuit using schemes from [6]. As the main result we prove the stability of the circuit.

MML Identifier: `FSCIRC_2`.

WWW: `http://mizar.org/JFM/Vol15/fscirc_2.html`

The articles [16], [15], [21], [20], [2], [17], [24], [1], [8], [9], [4], [10], [3], [18], [25], [14], [19], [12], [13], [11], [23], [5], [7], and [22] provide the notation and terminology for this paper.

Let n be a natural number and let x, y be finite sequences. The functor n-BitSubtracterStr(x,y) yields an unsplit non void strict non empty many sorted signature with arity held in gates and Boolean denotation held in gates and is defined by the condition (Def. 1).

(Def. 1) There exist many sorted sets f, g indexed by $\mathbb{N}$ such that

- (i) n-BitSubtracterStr$(x,y) = f(n)$,
- (ii) $f(0) = 1\mathrm{GateCircStr}(\varepsilon, \mathit{Boolean}^0 \longmapsto \mathit{true})$,
- (iii) $g(0) = \langle \varepsilon, \mathit{Boolean}^0 \longmapsto \mathit{true} \rangle$, and
- (iv) for every natural number n and for every non empty many sorted signature S and for every set z such that $S = f(n)$ and $z = g(n)$ holds $f(n+1) = S +\cdot \mathrm{BitSubtracterWithBorrowStr}(x(n+1), y(n+1), z)$ and $g(n+1) = \mathrm{BorrowOutput}(x(n+1), y(n+1), z)$.

Let n be a natural number and let x, y be finite sequences. The functor n-BitSubtracterCirc(x,y) yielding a Boolean strict circuit of n-BitSubtracterStr(x,y) with denotation held in gates is defined by the condition (Def. 2).

(Def. 2) There exist many sorted sets f, g, h indexed by $\mathbb{N}$ such that

- (i) n-BitSubtracterStr$(x,y) = f(n)$,
- (ii) n-BitSubtracterCirc$(x,y) = g(n)$,
- (iii) $f(0) = 1\mathrm{GateCircStr}(\varepsilon, \mathit{Boolean}^0 \longmapsto \mathit{true})$,
- (iv) $g(0) = 1\mathrm{GateCircuit}(\varepsilon, \mathit{Boolean}^0 \longmapsto \mathit{true})$,
- (v) $h(0) = \langle \varepsilon, \mathit{Boolean}^0 \longmapsto \mathit{true} \rangle$, and
- (vi) for every natural number n and for every non empty many sorted signature S and for every non-empty algebra A over S and for every set z such that $S = f(n)$ and $A = g(n)$ and $z =$

$h(n)$ holds $f(n+1) = S +\cdot$ BitSubtracterWithBorrowStr$(x(n+1), y(n+1), z)$ and $g(n+1) = A +\cdot$ BitSubtracterWithBorrowCirc$(x(n+1), y(n+1), z)$ and $h(n+1) =$ BorrowOutput$(x(n+1), y(n+1), z)$.

Let n be a natural number and let x, y be finite sequences. The functor n-BitBorrowOutput(x,y) yields an element of InnerVertices(n-BitSubtracterStr(x,y)) and is defined by the condition (Def. 3).

(Def. 3) There exists a many sorted set h indexed by $\mathbb{N}$ such that n-BitBorrowOutput$(x,y) = h(n)$ and $h(0) = \langle\varepsilon, \mathit{Boolean}^0 \longmapsto \mathit{true}\rangle$ and for every natural number n holds $h(n+1) =$ BorrowOutput$(x(n+1), y(n+1), h(n))$.

We now state several propositions:

(1) Let x, y be finite sequences and f, g, h be many sorted sets indexed by $\mathbb{N}$. Suppose that

(i) $f(0) =$ 1GateCircStr$(\varepsilon, \mathit{Boolean}^0 \longmapsto \mathit{true})$,

(ii) $g(0) =$ 1GateCircuit$(\varepsilon, \mathit{Boolean}^0 \longmapsto \mathit{true})$,

(iii) $h(0) = \langle\varepsilon, \mathit{Boolean}^0 \longmapsto \mathit{true}\rangle$, and

(iv) for every natural number n and for every non empty many sorted signature S and for every non-empty algebra A over S and for every set z such that $S = f(n)$ and $A = g(n)$ and $z = h(n)$ holds $f(n+1) = S +\cdot$ BitSubtracterWithBorrowStr$(x(n+1), y(n+1), z)$ and $g(n+1) = A +\cdot$ BitSubtracterWithBorrowCirc$(x(n+1), y(n+1), z)$ and $h(n+1) =$ BorrowOutput$(x(n+1), y(n+1), z)$.

Let n be a natural number. Then n-BitSubtracterStr$(x,y) = f(n)$ and n-BitSubtracterCirc$(x,y) = g(n)$ and n-BitBorrowOutput$(x,y) = h(n)$.

(2) For all finite sequences a, b holds 0-BitSubtracterStr$(a,b) =$ 1GateCircStr$(\varepsilon, \mathit{Boolean}^0 \longmapsto \mathit{true})$ and 0-BitSubtracterCirc$(a,b) =$ 1GateCircuit$(\varepsilon, \mathit{Boolean}^0 \longmapsto \mathit{true})$ and 0-BitBorrowOutput$(a,b) = \langle\varepsilon, \mathit{Boolean}^0 \longmapsto \mathit{true}\rangle$.

(3) Let a, b be finite sequences and c be a set. Suppose $c = \langle\varepsilon, \mathit{Boolean}^0 \longmapsto \mathit{true}\rangle$. Then 1-BitSubtracterStr$(a,b) =$ 1GateCircStr$(\varepsilon, \mathit{Boolean}^0 \longmapsto \mathit{true}) +\cdot$ BitSubtracterWithBorrowStr$(a(1), b(1), c)$ and 1-BitSubtracterCirc$(a,b) =$ 1GateCircuit$(\varepsilon, \mathit{Boolean}^0 \longmapsto \mathit{true}) +\cdot$ BitSubtracterWithBorrowCirc$(a(1), b(1), c)$ and 1-BitBorrowOutput$(a,b) =$ BorrowOutput$(a(1), b(1), c)$.

(4) For all sets a, b, c such that $c = \langle\varepsilon, \mathit{Boolean}^0 \longmapsto \mathit{true}\rangle$ holds 1-BitSubtracterStr$(\langle a\rangle, \langle b\rangle) =$ 1GateCircStr$(\varepsilon, \mathit{Boolean}^0 \longmapsto \mathit{true}) +\cdot$ BitSubtracterWithBorrowStr(a,b,c) and 1-BitSubtracterCirc$(\langle a\rangle, \langle b\rangle) =$ 1GateCircuit$(\varepsilon, \mathit{Boolean}^0 \longmapsto \mathit{true}) +\cdot$ BitSubtracterWithBorrowCirc(a,b,c) and 1-BitBorrowOutput$(\langle a\rangle, \langle b\rangle) =$ BorrowOutput(a,b,c).

(5) Let n be a natural number, p, q be finite sequences with length n, and p_1, p_2, q_1, q_2 be finite sequences. Then n-BitSubtracterStr$(p \frown p_1, q \frown q_1) = n$-BitSubtracterStr$(p \frown p_2, q \frown q_2)$ and n-BitSubtracterCirc$(p \frown p_1, q \frown q_1) = n$-BitSubtracterCirc$(p \frown p_2, q \frown q_2)$ and n-BitBorrowOutput$(p \frown p_1, q \frown q_1) = n$-BitBorrowOutput$(p \frown p_2, q \frown q_2)$.

(6) Let n be a natural number, x, y be finite sequences with length n, and a, b be sets. Then $(n+1)$-BitSubtracterStr$(x \frown \langle a\rangle, y \frown \langle b\rangle) = (n$-BitSubtracterStr$(x,y)) +\cdot$ BitSubtracterWithBorrowStr$(a, b, n$-BitBorrowOutput$(x,y))$ and $(n+1)$-BitSubtracterCirc$(x \frown \langle a\rangle, y \frown \langle b\rangle) = (n$-BitSubtracterCirc$(x,y)) +\cdot$ BitSubtracterWithBorrowCirc$(a, b, n$-BitBorrowOutput$(x,y))$ and $(n+1)$-BitBorrowOutput$(x \frown \langle a\rangle, y \frown \langle b\rangle) =$ BorrowOutput$(a, b, n$-BitBorrowOutput$(x,y))$.

(7) Let n be a natural number and x, y be finite sequences. Then $(n+1)$-BitSubtracterStr$(x,y) = (n$-BitSubtracterStr$(x,y)) +\cdot$ BitSubtracterWithBorrowStr$(x(n+1), y(n+1), n$-BitBorrowOutput$(x,y))$ and $(n+1)$-BitSubtracterCirc$(x,y) = (n$-BitSubtracterCirc$(x,y)) +\cdot$ BitSubtracterWithBorrowCirc$(x(n+1), y(n+1), n$-BitBorrowOutput$(x,y))$ and $(n+1)$-BitBorrowOutput$(x,y) =$ BorrowOutput$(x(n+1), y(n+1), n$-BitBorrowOutput$(x,y))$.

(8) For all natural numbers n, m such that $n \leq m$ and for all finite sequences x, y holds InnerVertices(n-BitSubtracterStr(x,y)) $\subseteq$ InnerVertices(m-BitSubtracterStr(x,y)).

(9) For every natural number n and for all finite sequences x, y holds InnerVertices($(n+1)$-BitSubtracterStr(x,y)) $=$ InnerVertices(n-BitSubtracterStr(x,y)) $\cup$ InnerVertices(BitSubtracterWithBorrowStr($x(n+1), y(n+1)$, n-BitBorrowOutput(x,y))).

Let k, n be natural numbers. Let us assume that $k \geq 1$ and $k \leq n$. Let x, y be finite sequences. The functor (k,n)-BitSubtracterOutput(x,y) yields an element of InnerVertices(n-BitSubtracterStr(x,y)) and is defined as follows:

(Def. 4) There exists a natural number i such that $k = i+1$ and (k,n)-BitSubtracterOutput(x,y) $=$ BitSubtracterOutput($x(k), y(k)$, i-BitBorrowOutput(x,y)).

One can prove the following propositions:

(10) For all natural numbers n, k such that $k < n$ and for all finite sequences x, y holds $(k+1,n)$-BitSubtracterOutput(x,y) $=$ BitSubtracterOutput($x(k+1), y(k+1)$, k-BitBorrowOutput(x,y)).

(11) For every natural number n and for all finite sequences x, y holds InnerVertices(n-BitSubtracterStr(x,y)) is a binary relation.

(12) For all sets x, y, c holds InnerVertices(BorrowIStr(x,y,c)) $= \{\langle\langle x,y\rangle, \mathrm{and}_{2a}\rangle, \langle\langle y,c\rangle, \mathrm{and}_{2}\rangle, \langle\langle x,c\rangle, \mathrm{and}_{2a}\rangle\}$.

(13) For all sets x, y, c such that $x \neq \langle\langle y,c\rangle, \mathrm{and}_{2}\rangle$ and $y \neq \langle\langle x,c\rangle, \mathrm{and}_{2a}\rangle$ and $c \neq \langle\langle x,y\rangle, \mathrm{and}_{2a}\rangle$ holds InputVertices(BorrowIStr(x,y,c)) $= \{x,y,c\}$.

(14) For all sets x, y, c holds InnerVertices(BorrowStr(x,y,c)) $= \{\langle\langle x,y\rangle, \mathrm{and}_{2a}\rangle, \langle\langle y,c\rangle, \mathrm{and}_{2}\rangle, \langle\langle x,c\rangle, \mathrm{and}_{2a}\rangle\} \cup \{$BorrowOutput$(x,y,c)\}$.

(15) For all sets x, y, c such that $x \neq \langle\langle y,c\rangle, \mathrm{and}_{2}\rangle$ and $y \neq \langle\langle x,c\rangle, \mathrm{and}_{2a}\rangle$ and $c \neq \langle\langle x,y\rangle, \mathrm{and}_{2a}\rangle$ holds InputVertices(BorrowStr(x,y,c)) $= \{x,y,c\}$.

(16) For all sets x, y, c such that $x \neq \langle\langle y,c\rangle, \mathrm{and}_{2}\rangle$ and $y \neq \langle\langle x,c\rangle, \mathrm{and}_{2a}\rangle$ and $c \neq \langle\langle x,y\rangle, \mathrm{and}_{2a}\rangle$ and $c \neq \langle\langle x,y\rangle, \mathrm{xor}\rangle$ holds InputVertices(BitSubtracterWithBorrowStr(x,y,c)) $= \{x,y,c\}$.

(17) For all sets x, y, c holds InnerVertices(BitSubtracterWithBorrowStr(x,y,c)) $= \{\langle\langle x,y\rangle, \mathrm{xor}\rangle$, 2GatesCircOutput$(x,y,c,\mathrm{xor})\} \cup \{\langle\langle x,y\rangle, \mathrm{and}_{2a}\rangle, \langle\langle y,c\rangle, \mathrm{and}_{2}\rangle, \langle\langle x,c\rangle, \mathrm{and}_{2a}\rangle\} \cup \{$BorrowOutput$(x,y,c)\}$.

Let n be a natural number and let x, y be finite sequences. Observe that n-BitBorrowOutput(x,y) is pair.

Next we state several propositions:

(18) Let x, y be finite sequences and n be a natural number. Then $(n\text{-BitBorrowOutput}(x,y))_{\mathbf{1}} = \varepsilon$ and $(n\text{-BitBorrowOutput}(x,y))_{\mathbf{2}} = \mathit{Boolean}^0 \longmapsto \mathit{true}$ and $\pi_1((n\text{-BitBorrowOutput}(x,y))_{\mathbf{2}}) = \mathit{Boolean}^0$ or $\overline{\overline{(n\text{-BitBorrowOutput}(x,y))_{\mathbf{1}}}} = 3$ and $(n\text{-BitBorrowOutput}(x,y))_{\mathbf{2}} = \mathrm{or}_3$ and $\pi_1((n\text{-BitBorrowOutput}(x,y))_{\mathbf{2}}) = \mathit{Boolean}^3$.

(19) Let n be a natural number, x, y be finite sequences, and p be a set. Then n-BitBorrowOutput$(x,y) \neq \langle p, \mathrm{and}_{2}\rangle$ and n-BitBorrowOutput$(x,y) \neq \langle p, \mathrm{and}_{2a}\rangle$ and n-BitBorrowOutput$(x,y) \neq \langle p, \mathrm{xor}\rangle$.

(20) Let f, g be nonpair yielding finite sequences and n be a natural number. Then InputVertices($(n+1)$-BitSubtracterStr(f,g)) $=$ InputVertices(n-BitSubtracterStr(f,g)) $\cup$ (InputVertices(BitSubtracterWithBorrowStr($f(n+1), g(n+1)$, n-BitBorrowOutput(f,g))) $\setminus$ $\{n$-BitBorrowOutput$(f,g)\}$) and InnerVertices(n-BitSubtracterStr(f,g)) is a binary relation and InputVertices(n-BitSubtracterStr(f,g)) has no pairs.

(21) For every natural number n and for all nonpair yielding finite sequences x, y with length n holds InputVertices(n-BitSubtracterStr(x,y)) $= \mathrm{rng}\, x \cup \mathrm{rng}\, y$.

(22) Let x, y, c be sets, s be a state of BorrowCirc(x,y,c), and a_1, a_2, a_3 be elements of *Boolean*. If $a_1 = s(\langle\langle x,y\rangle, \mathrm{and}_{2a}\rangle)$ and $a_2 = s(\langle\langle y,c\rangle, \mathrm{and}_2\rangle)$ and $a_3 = s(\langle\langle x,c\rangle, \mathrm{and}_{2a}\rangle)$, then $(\mathrm{Following}(s))(\mathrm{BorrowOutput}(x,y,c)) = a_1 \vee a_2 \vee a_3$.

(23) Let x, y, c be sets. Suppose $x \neq \langle\langle y,c\rangle, \mathrm{and}_2\rangle$ and $y \neq \langle\langle x,c\rangle, \mathrm{and}_{2a}\rangle$ and $c \neq \langle\langle x,y\rangle, \mathrm{and}_{2a}\rangle$ and $c \neq \langle\langle x,y\rangle, \mathrm{xor}\rangle$. Let s be a state of BorrowCirc(x,y,c). Then Following$(s,2)$ is stable.

(24) Let x, y, c be sets. Suppose $x \neq \langle\langle y,c\rangle, \mathrm{and}_2\rangle$ and $y \neq \langle\langle x,c\rangle, \mathrm{and}_{2a}\rangle$ and $c \neq \langle\langle x, y\rangle, \mathrm{and}_{2a}\rangle$ and $c \neq \langle\langle x,y\rangle, \mathrm{xor}\rangle$. Let s be a state of BitSubtracterWithBorrowCirc(x,y,c) and a_1, a_2, a_3 be elements of *Boolean*. Suppose $a_1 = s(x)$ and $a_2 = s(y)$ and $a_3 = s(c)$. Then $(\mathrm{Following}(s,2))(\mathrm{BitSubtracterOutput}(x,y,c)) = a_1 \oplus a_2 \oplus a_3$ and $(\mathrm{Following}(s,2))(\mathrm{BorrowOutput}(x,y,c)) = \neg a_1 \wedge a_2 \vee a_2 \wedge a_3 \vee \neg a_1 \wedge a_3$.

(25) Let x, y, c be sets. Suppose $x \neq \langle\langle y,c\rangle, \mathrm{and}_2\rangle$ and $y \neq \langle\langle x,c\rangle, \mathrm{and}_{2a}\rangle$ and $c \neq \langle\langle x,y\rangle, \mathrm{and}_{2a}\rangle$ and $c \neq \langle\langle x,y\rangle, \mathrm{xor}\rangle$. Let s be a state of BitSubtracterWithBorrowCirc(x,y,c). Then Following$(s,2)$ is stable.

(26) Let n be a natural number, x, y be nonpair yielding finite sequences with length n, and s be a state of n-BitSubtracterCirc(x,y). Then Following$(s, 1+2\cdot n)$ is stable.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/card_1.html.

[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/nat_1.html.

[3] Grzegorz Bancerek. Curried and uncurried functions. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/funct_5.html.

[4] 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.

[5] Grzegorz Bancerek and Yatsuka Nakamura. Full adder circuit. Part I. *Journal of Formalized Mathematics*, 7, 1995. http://mizar.org/JFM/Vol7/facirc_1.html.

[6] Grzegorz Bancerek, Shin'nosuke Yamaguchi, and Yasunari Shidama. Combining of multi cell circuits. *Journal of Formalized Mathematics*, 14, 2002. http://mizar.org/JFM/Vol14/circcmb2.html.

[7] Grzegorz Bancerek, Shin'nosuke Yamaguchi, and Katsumi Wasaki. Full adder circuit. Part II. *Journal of Formalized Mathematics*, 14, 2002. http://mizar.org/JFM/Vol14/facirc_2.html.

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

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

[10] 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.

[11] Yatsuka Nakamura and Grzegorz Bancerek. Combining of circuits. *Journal of Formalized Mathematics*, 7, 1995. http://mizar.org/JFM/Vol7/circcomb.html.

[12] Yatsuka Nakamura, Piotr Rudnicki, Andrzej Trybulec, and Pauline N. Kawamoto. Preliminaries to circuits, II. *Journal of Formalized Mathematics*, 6, 1994. http://mizar.org/JFM/Vol6/msafree2.html.

[13] Yatsuka Nakamura, Piotr Rudnicki, Andrzej Trybulec, and Pauline N. Kawamoto. Introduction to circuits, II. *Journal of Formalized Mathematics*, 7, 1995. http://mizar.org/JFM/Vol7/circuit2.html.

[14] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Journal of Formalized Mathematics*, 5, 1993. http://mizar.org/JFM/Vol5/binarith.html.

[15] Andrzej Trybulec. Enumerated sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/enumset1.html.

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

[17] Andrzej Trybulec. Tuples, projections and Cartesian products. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/mcart_1.html.

[18] Andrzej Trybulec. Many-sorted sets. *Journal of Formalized Mathematics*, 5, 1993. http://mizar.org/JFM/Vol5/pboole.html.

[19] Andrzej Trybulec. Many sorted algebras. *Journal of Formalized Mathematics*, 6, 1994. http://mizar.org/JFM/Vol6/msualg_1.html.

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

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

[22] Katsumi Wasaki and Noboru Endou. Full subtracter circuit. Part I. *Journal of Formalized Mathematics*, 11, 1999. `http://mizar.org/JFM/Vol11/fscirc_1.html`.

[23] Katsumi Wasaki and Pauline N. Kawamoto. 2's complement circuit. *Journal of Formalized Mathematics*, 8, 1996. `http://mizar.org/JFM/Vol8/twoscomp.html`.

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

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

Received February 25, 2003

Published January 2, 2004