FORMALIZED MATHEMATICS
Volume 9, Number 3, 2001
University of Białystok

The Correctness of the High Speed Array Multiplier Circuits

Hiroshi Yamazaki
Shinshu University
Nagano

Katsumi Wasaki
Shinshu University
Nagano

Summary. This article introduces the verification of the correctness for the operations and the specification of the high speed array multiplier. We formalize the concepts of 2-by-2 and 3-by-3 bit Plain array multiplier, 3-by-3 Wallace tree multiplier circuit, and show that outputs of the array multiplier are equivalent to outputs of normal (sequencial) multiplier.

MML Identifier: GATE_5.

The articles [3], [1], and [2] provide the terminology and notation for this paper.

1. Preliminaries

Let x_0, x_1, y_0, y_1 be sets. The functor $\mathrm{MULT}_{210}(x_1, y_1, x_0, y_0)$ yields a set and is defined as follows:

(Def. 1) $\mathrm{MULT}_{210}(x_1, y_1, x_0, y_0) = \mathrm{AND2}(x_0, y_0)$.

The functor $\mathrm{MULT}_{211}(x_1, y_1, x_0, y_0)$ yields a set and is defined by:

(Def. 2) $\mathrm{MULT}_{211}(x_1, y_1, x_0, y_0) = \mathrm{ADD1}(\mathrm{AND2}(x_1, y_0), \mathrm{AND2}(x_0, y_1), \emptyset)$.

The functor $\mathrm{MULT}_{212}(x_1, y_1, x_0, y_0)$ yielding a set is defined as follows:

(Def. 3) $\mathrm{MULT}_{212}(x_1, y_1, x_0, y_0) = \mathrm{ADD2}(\emptyset, \mathrm{AND2}(x_1, y_1), \mathrm{AND2}(x_1, y_0), \mathrm{AND2}(x_0, y_1), \emptyset)$.

The functor $\mathrm{MULT}_{213}(x_1, y_1, x_0, y_0)$ yields a set and is defined as follows:

(Def. 4) $\mathrm{MULT}_{213}(x_1, y_1, x_0, y_0) = \mathrm{CARR2}(\emptyset, \mathrm{AND2}(x_1, y_1), \mathrm{AND2}(x_1, y_0), \mathrm{AND2}(x_0, y_1), \emptyset)$.

ISSN 1426–2630

We now state the proposition

(1) Let x_0, x_1, y_0, y_1, z_0, z_1, z_2, z_3, q_0, q_1, c_1, q_{11}, c_{11} be sets such that NE q_0 iff NE AND2(x_0, y_0) and NE q_1 iff NE XOR3(AND2(x_1, y_0), AND2(x_0, y_1), $\emptyset$) and NE c_1 iff NE MAJ3(AND2(x_1, y_0), AND2(x_0, y_1), $\emptyset$) and NE q_{11} iff NE XOR3(AND2(x_1, y_1), $\emptyset$, c_1) and NE c_{11} iff NE MAJ3(AND2(x_1, y_1), $\emptyset$, c_1) and NE z_0 iff NE q_0 and NE z_1 iff NE q_1 and NE z_2 iff NE q_{11} and NE z_3 iff NE c_{11}. Then

(i) NE z_0 iff NE MULT$_{210}(x_1, y_1, x_0, y_0)$,

(ii) NE z_1 iff NE MULT$_{211}(x_1, y_1, x_0, y_0)$,

(iii) NE z_2 iff NE MULT$_{212}(x_1, y_1, x_0, y_0)$, and

(iv) NE z_3 iff NE MULT$_{213}(x_1, y_1, x_0, y_0)$.

Let x_0, x_1, x_2, y_0, y_1 be sets. The functor MULT$_{310}(x_2, x_1, y_1, x_0, y_0)$ yields a set and is defined by:

(Def. 5) MULT$_{310}(x_2, x_1, y_1, x_0, y_0)$ = AND2(x_0, y_0).

The functor MULT$_{311}(x_2, x_1, y_1, x_0, y_0)$ yields a set and is defined as follows:

(Def. 6) MULT$_{311}(x_2, x_1, y_1, x_0, y_0)$ = ADD1(AND2(x_1, y_0), AND2(x_0, y_1), $\emptyset$).

The functor MULT$_{312}(x_2, x_1, y_1, x_0, y_0)$ yields a set and is defined as follows:

(Def. 7) MULT$_{312}(x_2, x_1, y_1, x_0, y_0)$ = ADD2(AND2(x_2, y_0), AND2(x_1, y_1), AND2(x_1, y_0), AND2(x_0, y_1), $\emptyset$).

The functor MULT$_{313}(x_2, x_1, y_1, x_0, y_0)$ yields a set and is defined as follows:

(Def. 8) MULT$_{313}(x_2, x_1, y_1, x_0, y_0)$ = ADD3($\emptyset$, AND2(x_2, y_1), AND2(x_2, y_0), AND2(x_1, y_1), AND2(x_1, y_0), AND2(x_0, y_1), $\emptyset$).

The functor MULT$_{314}(x_2, x_1, y_1, x_0, y_0)$ yielding a set is defined by:

(Def. 9) MULT$_{314}(x_2, x_1, y_1, x_0, y_0)$ = CARR3($\emptyset$, AND2(x_2, y_1), AND2(x_2, y_0), AND2(x_1, y_1), AND2(x_1, y_0), AND2(x_0, y_1), $\emptyset$).

Let x_0, x_1, x_2, y_0, y_1, y_2 be sets. The functor MULT$_{321}(x_2, y_2, x_1, y_1, x_0, y_0)$ yields a set and is defined by:

(Def. 10) MULT$_{321}(x_2, y_2, x_1, y_1, x_0, y_0)$ = ADD1(MULT$_{312}(x_2, x_1, y_1, x_0, y_0)$, AND2$(x_0, y_2)$, $\emptyset$).

The functor MULT$_{322}(x_2, y_2, x_1, y_1, x_0, y_0)$ yields a set and is defined by:

(Def. 11) MULT$_{322}(x_2, y_2, x_1, y_1, x_0, y_0)$ = ADD2(MULT$_{313}(x_2, x_1, y_1, x_0, y_0)$, AND2$(x_1, y_2)$, MULT$_{312}(x_2, x_1, y_1, x_0, y_0)$, AND2$(x_0, y_2)$, $\emptyset$).

The functor MULT$_{323}(x_2, y_2, x_1, y_1, x_0, y_0)$ yields a set and is defined as follows:

(Def. 12) MULT$_{323}(x_2, y_2, x_1, y_1, x_0, y_0)$ = ADD3(MULT$_{314}(x_2, x_1, y_1, x_0, y_0)$, AND2$(x_2, y_2)$, MULT$_{313}(x_2, x_1, y_1, x_0, y_0)$, AND2$(x_1, y_2)$, MULT$_{312}(x_2, x_1, y_1, x_0, y_0)$, AND2$(x_0, y_2)$, $\emptyset$).

The functor MULT$_{324}(x_2, y_2, x_1, y_1, x_0, y_0)$ yielding a set is defined as follows:

(Def. 13) MULT$_{324}(x_2, y_2, x_1, y_1, x_0, y_0)$ = CARR3(MULT$_{314}(x_2, x_1, y_1, x_0, y_0)$, AND2$(x_2, y_2)$, MULT$_{313}(x_2, x_1, y_1, x_0, y_0)$, AND2$(x_1, y_2)$, MULT$_{312}(x_2, x_1,$

$y_1, x_0, y_0), \mathrm{AND2}(x_0, y_2), \emptyset)$.

Next we state the proposition

(2) Let x_0, x_1, x_2, y_0, y_1, y_2, z_0, z_1, z_2, z_3, z_4, z_5, q_0, q_1, q_2, c_1, c_2, q_{11}, q_{12}, c_{11}, c_{12}, q_{21}, q_{22}, c_{21}, c_{22} be sets such that NE q_0 iff NE $\mathrm{AND2}(x_0, y_0)$ and NE q_1 iff NE $\mathrm{XOR3}(\mathrm{AND2}(x_1, y_0), \mathrm{AND2}(x_0, y_1), \emptyset)$ and NE c_1 iff NE $\mathrm{MAJ3}(\mathrm{AND2}(x_1, y_0), \mathrm{AND2}(x_0, y_1), \emptyset)$ and NE q_2 iff NE $\mathrm{XOR3}(\mathrm{AND2}(x_2, y_0), \mathrm{AND2}(x_1, y_1), \emptyset)$ and NE c_2 iff NE $\mathrm{MAJ3}(\mathrm{AND2}(x_2, y_0), \mathrm{AND2}(x_1, y_1), \emptyset)$ and NE q_{11} iff NE $\mathrm{XOR3}(q_2, \mathrm{AND2}(x_0, y_2), c_1)$ and NE c_{11} iff NE $\mathrm{MAJ3}(q_2, \mathrm{AND2}(x_0, y_2), c_1)$ and NE q_{12} iff NE $\mathrm{XOR3}(\mathrm{AND2}(x_2, y_1), \mathrm{AND2}(x_1, y_2), c_2)$ and NE c_{12} iff NE $\mathrm{MAJ3}(\mathrm{AND2}(x_2, y_1), \mathrm{AND2}(x_1, y_2), c_2)$ and NE q_{21} iff NE $\mathrm{XOR3}(q_{12}, \emptyset, c_{11})$ and NE c_{21} iff NE $\mathrm{MAJ3}(q_{12}, \emptyset, c_{11})$ and NE q_{22} iff NE $\mathrm{XOR3}(\mathrm{AND2}(x_2, y_2), c_{21}, c_{12})$ and NE c_{22} iff NE $\mathrm{MAJ3}(\mathrm{AND2}(x_2, y_2), c_{21}, c_{12})$ and NE z_0 iff NE q_0 and NE z_1 iff NE q_1 and NE z_2 iff NE q_{11} and NE z_3 iff NE q_{21} and NE z_4 iff NE q_{22} and NE z_5 iff NE c_{22}. Then

(i) NE z_0 iff NE $\mathrm{MULT}_{310}(x_2, x_1, y_1, x_0, y_0)$,

(ii) NE z_1 iff NE $\mathrm{MULT}_{311}(x_2, x_1, y_1, x_0, y_0)$,

(iii) NE z_2 iff NE $\mathrm{MULT}_{321}(x_2, y_2, x_1, y_1, x_0, y_0)$,

(iv) NE z_3 iff NE $\mathrm{MULT}_{322}(x_2, y_2, x_1, y_1, x_0, y_0)$,

(v) NE z_4 iff NE $\mathrm{MULT}_{323}(x_2, y_2, x_1, y_1, x_0, y_0)$, and

(vi) NE z_5 iff NE $\mathrm{MULT}_{324}(x_2, y_2, x_1, y_1, x_0, y_0)$.

2. Logical Equivalence of Wallace Tree Multiplier

One can prove the following proposition

(3) Let x_0, x_1, x_2, y_0, y_1, y_2, z_0, z_1, z_2, z_3, z_4, z_5, q_0, q_1, q_2, q_3, c_1, c_2, c_3, q_{11}, q_{12}, q_{13}, c_{11}, c_{12}, c_{13} be sets such that NE q_0 iff NE $\mathrm{AND2}(x_0, y_0)$ and NE q_1 iff NE $\mathrm{XOR3}(\mathrm{AND2}(x_1, y_0), \mathrm{AND2}(x_0, y_1), \emptyset)$ and NE c_1 iff NE $\mathrm{MAJ3}(\mathrm{AND2}(x_1, y_0), \mathrm{AND2}(x_0, y_1), \emptyset)$ and NE q_2 iff NE $\mathrm{XOR3}(\mathrm{AND2}(x_2, y_0), \mathrm{AND2}(x_1, y_1), \mathrm{AND2}(x_0, y_2))$ and NE c_2 iff NE $\mathrm{MAJ3}(\mathrm{AND2}(x_2, y_0), \mathrm{AND2}(x_1, y_1), \mathrm{AND2}(x_0, y_2))$ and NE q_3 iff NE $\mathrm{XOR3}(\mathrm{AND2}(x_2, y_1), \mathrm{AND2}(x_1, y_2), \emptyset)$ and NE c_3 iff NE $\mathrm{MAJ3}(\mathrm{AND2}(x_2, y_1), \mathrm{AND2}(x_1, y_2), \emptyset)$ and NE q_{11} iff NE $\mathrm{XOR3}(q_2, c_1, \emptyset)$ and NE c_{11} iff NE $\mathrm{MAJ3}(q_2, c_1, \emptyset)$ and NE q_{12} iff NE $\mathrm{XOR3}(q_3, c_2, c_{11})$ and NE c_{12} iff NE $\mathrm{MAJ3}(q_3, c_2, c_{11})$ and NE q_{13} iff NE $\mathrm{XOR3}(\mathrm{AND2}(x_2, y_2), c_3, c_{12})$ and NE c_{13} iff NE $\mathrm{MAJ3}(\mathrm{AND2}(x_2, y_2), c_3, c_{12})$ and NE z_0 iff NE q_0 and NE z_1 iff NE q_1 and NE z_2 iff NE q_{11} and NE z_3 iff NE q_{12} and NE z_4 iff NE q_{13} and NE z_5 iff NE c_{13}. Then

(i) NE z_0 iff NE $\mathrm{MULT}_{310}(x_2, x_1, y_1, x_0, y_0)$,

(ii) NE z_1 iff NE $\mathrm{MULT}_{311}(x_2, x_1, y_1, x_0, y_0)$,

(iii) NE z_2 iff NE $\mathrm{MULT}_{321}(x_2, y_2, x_1, y_1, x_0, y_0)$,
(iv) NE z_3 iff NE $\mathrm{MULT}_{322}(x_2, y_2, x_1, y_1, x_0, y_0)$,
(v) NE z_4 iff NE $\mathrm{MULT}_{323}(x_2, y_2, x_1, y_1, x_0, y_0)$, and
(vi) NE z_5 iff NE $\mathrm{MULT}_{324}(x_2, y_2, x_1, y_1, x_0, y_0)$.

Let a_1, b_1, c be sets. We introduce $\mathrm{CLAADD1}(a_1, b_1, c)$ as a synonym of $\mathrm{XOR3}(a_1, b_1, c)$. We introduce $\mathrm{CLACARR1}(a_1, b_1, c)$ as a synonym of $\mathrm{MAJ3}(a_1, b_1, c)$.

Let a_1, b_1, a_2, b_2, c be sets. The functor $\mathrm{CLAADD2}(a_2, b_2, a_1, b_1, c)$ yields a set and is defined by:

(Def. 16)[1] $\mathrm{CLAADD2}(a_2, b_2, a_1, b_1, c) = \mathrm{XOR3}(a_2, b_2, \mathrm{MAJ3}(a_1, b_1, c))$.

The functor $\mathrm{CLACARR2}(a_2, b_2, a_1, b_1, c)$ yields a set and is defined by:

(Def. 17) $\mathrm{CLACARR2}(a_2, b_2, a_1, b_1, c) = \mathrm{OR2}(\mathrm{AND2}(a_2, b_2), \mathrm{AND2}(\mathrm{OR2}(a_2, b_2), \mathrm{MAJ3}(a_1, b_1, c)))$.

Let a_1, b_1, a_2, b_2, a_3, b_3, c be sets. The functor $\mathrm{CLAADD3}(a_3, b_3, a_2, b_2, a_1, b_1, c)$ yielding a set is defined as follows:

(Def. 18) $\mathrm{CLAADD3}(a_3, b_3, a_2, b_2, a_1, b_1, c) = \mathrm{XOR3}(a_3, b_3, \mathrm{CLACARR2}(a_2, b_2, a_1, b_1, c))$.

The functor $\mathrm{CLACARR3}(a_3, b_3, a_2, b_2, a_1, b_1, c)$ yields a set and is defined by:

(Def. 19) $\mathrm{CLACARR3}(a_3, b_3, a_2, b_2, a_1, b_1, c) = \mathrm{OR3}(\mathrm{AND2}(a_3, b_3), \mathrm{AND2}(\mathrm{OR2}(a_3, b_3), \mathrm{AND2}(a_2, b_2)), \mathrm{AND3}(\mathrm{OR2}(a_3, b_3), \mathrm{OR2}(a_2, b_2), \mathrm{MAJ3}(a_1, b_1, c)))$.

Let a_1, b_1, a_2, b_2, a_3, b_3, a_4, b_4, c be sets. The functor $\mathrm{CLAADD4}(a_4, b_4, a_3, b_3, a_2, b_2, a_1, b_1, c)$ yielding a set is defined by:

(Def. 20) $\mathrm{CLAADD4}(a_4, b_4, a_3, b_3, a_2, b_2, a_1, b_1, c) = \mathrm{XOR3}(a_4, b_4, \mathrm{CLACARR3}(a_3, b_3, a_2, b_2, a_1, b_1, c))$.

The functor $\mathrm{CLACARR4}(a_4, b_4, a_3, b_3, a_2, b_2, a_1, b_1, c)$ yielding a set is defined as follows:

(Def. 21) $\mathrm{CLACARR4}(a_4, b_4, a_3, b_3, a_2, b_2, a_1, b_1, c) = \mathrm{OR4}(\mathrm{AND2}(a_4, b_4), \mathrm{AND2}(\mathrm{OR2}(a_4, b_4), \mathrm{AND2}(a_3, b_3)), \mathrm{AND3}(\mathrm{OR2}(a_4, b_4), \mathrm{OR2}(a_3, b_3), \mathrm{AND2}(a_2, b_2)), \mathrm{AND4}(\mathrm{OR2}(a_4, b_4), \mathrm{OR2}(a_3, b_3), \mathrm{OR2}(a_2, b_2), \mathrm{MAJ3}(a_1, b_1, c)))$.

One can prove the following proposition

(4) Let x_0, x_1, x_2, y_0, y_1, y_2, z_0, z_1, z_2, z_3, z_4, z_5, q_0, q_1, q_2, q_3, c_1, c_2, c_3 be sets such that NE q_0 iff NE $\mathrm{AND2}(x_0, y_0)$ and NE q_1 iff NE $\mathrm{XOR3}(\mathrm{AND2}(x_1, y_0), \mathrm{AND2}(x_0, y_1), \emptyset)$ and NE c_1 iff NE $\mathrm{MAJ3}(\mathrm{AND2}(x_1, y_0), \mathrm{AND2}(x_0, y_1), \emptyset)$ and NE q_2 iff NE $\mathrm{XOR3}(\mathrm{AND2}(x_2, y_0), \mathrm{AND2}(x_1, y_1), \mathrm{AND2}(x_0, y_2))$ and NE c_2 iff NE $\mathrm{MAJ3}(\mathrm{AND2}(x_2, y_0), \mathrm{AND2}(x_1, y_1), \mathrm{AND2}(x_0, y_2))$ and NE q_3 iff NE $\mathrm{XOR3}(\mathrm{AND2}(x_2, y_1), \mathrm{AND2}(x_1, y_2), \emptyset)$ and NE c_3 iff NE MAJ3(AND2(x_2,

[1] The definitions (Def. 14) and (Def. 15) have been removed.

$y_1), \mathrm{AND2}(x_1, y_2), \emptyset)$ and NE z_0 iff NE q_0 and NE z_1 iff NE q_1 and NE z_2 iff NE CLAADD1$(q_2, c_1, \emptyset)$ and NE z_3 iff NE CLAADD2$(q_3, c_2, q_2, c_1, \emptyset)$ and NE z_4 iff NE CLAADD3(AND2$(x_2, y_2), c_3, q_3, c_2, q_2, c_1, \emptyset)$ and NE z_5 iff NE CLACARR3(AND2$(x_2, y_2), c_3, q_3, c_2, q_2, c_1, \emptyset)$. Then

(i) NE z_0 iff NE $\mathrm{MULT}_{310}(x_2, x_1, y_1, x_0, y_0)$,

(ii) NE z_1 iff NE $\mathrm{MULT}_{311}(x_2, x_1, y_1, x_0, y_0)$,

(iii) NE z_2 iff NE $\mathrm{MULT}_{321}(x_2, y_2, x_1, y_1, x_0, y_0)$,

(iv) NE z_3 iff NE $\mathrm{MULT}_{322}(x_2, y_2, x_1, y_1, x_0, y_0)$,

(v) NE z_4 iff NE $\mathrm{MULT}_{323}(x_2, y_2, x_1, y_1, x_0, y_0)$, and

(vi) NE z_5 iff NE $\mathrm{MULT}_{324}(x_2, y_2, x_1, y_1, x_0, y_0)$.

References

[1] Yatsuka Nakamura. Logic gates and logical equivalence of adders. *Formalized Mathematics*, 8(**1**):35–45, 1999.

[2] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[3] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.

Received August 28, 2000