JOURNAL OF FORMALIZED MATHEMATICS
Volume 11, Released 1999, Published 2003
Inst. of Computer Science, Univ. of Białystok

Correctness of a Cyclic Redundancy Check Code Generator

Yuguang Yang
Shinshu University
Nagano

Katsumi Wasaki
Shinshu University
Nagano

Yasushi Fuwa
Shinshu University
Nagano

Yatsuka Nakamura
Shinshu University
Nagano

Summary. We prove the correctness of the division circuit and the CRC (cyclic redundancy checks) circuit by verifying the contents of the register after one shift. Circuits with 12-bit register and 16-bit register are taken as examples. All the proofs are done formally.

MML Identifier: GATE_4.

WWW: http://mizar.org/JFM/Vol11/gate_4.html

The article [1] provides the notation and terminology for this paper.

1. Correctness of Division Circuits with 12-bit Register and 16-bit Register

The following two propositions are true:

(1) Let g_0, g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8, g_9, g_{10}, g_{11}, g_{12}, a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8, b_9, b_{10}, b_{11}, p be sets such that NE g_0 and NE g_{12} and NE b_0 iff NE XOR2$(p, \mathrm{AND2}(g_0, a_{11}))$ and NE b_1 iff NE XOR2$(a_0, \mathrm{AND2}(g_1, a_{11}))$ and NE b_2 iff NE XOR2$(a_1, \mathrm{AND2}(g_2, a_{11}))$ and NE b_3 iff NE XOR2$(a_2, \mathrm{AND2}(g_3, a_{11}))$ and NE b_4 iff NE XOR2$(a_3, \mathrm{AND2}(g_4, a_{11}))$ and NE b_5 iff NE XOR2$(a_4, \mathrm{AND2}(g_5, a_{11}))$ and NE b_6 iff NE XOR2$(a_5, \mathrm{AND2}(g_6, a_{11}))$ and NE b_7 iff NE XOR2$(a_6, \mathrm{AND2}(g_7, a_{11}))$ and NE b_8 iff NE XOR2$(a_7, \mathrm{AND2}(g_8, a_{11}))$ and NE b_9 iff NE XOR2$(a_8, \mathrm{AND2}(g_9, a_{11}))$ and NE b_{10} iff NE XOR2$(a_9, \mathrm{AND2}(g_{10}, a_{11}))$ and NE b_{11} iff NE XOR2$(a_{10}, \mathrm{AND2}(g_{11}, a_{11}))$. Then

(i) NE a_{11} iff NE AND2(g_{12}, a_{11}),

(ii) NE a_{10} iff NE XOR2$(b_{11}, \mathrm{AND2}(g_{11}, a_{11}))$,

(iii) NE a_9 iff NE XOR2$(b_{10}, \mathrm{AND2}(g_{10}, a_{11}))$,

(iv) NE a_8 iff NE XOR2$(b_9, \mathrm{AND2}(g_9, a_{11}))$,

(v) NE a_7 iff NE XOR2$(b_8, \mathrm{AND2}(g_8, a_{11}))$,

(vi) NE a_6 iff NE XOR2$(b_7, \mathrm{AND2}(g_7, a_{11}))$,

(vii) NE a_5 iff NE XOR2$(b_6, \mathrm{AND2}(g_6, a_{11}))$,

(viii) NE a_4 iff NE XOR2$(b_5, \mathrm{AND2}(g_5, a_{11}))$,

(ix) NE a_3 iff NE XOR2$(b_4, \mathrm{AND2}(g_4, a_{11}))$,

(x) NE a_2 iff NE XOR2(b_3, AND2(g_3, a_{11})),

(xi) NE a_1 iff NE XOR2(b_2, AND2(g_2, a_{11})),

(xii) NE a_0 iff NE XOR2(b_1, AND2(g_1, a_{11})), and

(xiii) NE p iff NE XOR2(b_0, AND2(g_0, a_{11})).

(2) Let g_0, g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8, g_9, g_{10}, g_{11}, g_{12}, g_{13}, g_{14}, g_{15}, g_{16}, a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8, b_9, b_{10}, b_{11}, b_{12}, b_{13}, b_{14}, b_{15}, p be sets such that NE g_0 and NE g_{16} and NE b_0 iff NE XOR2(p, AND2(g_0, a_{15})) and NE b_1 iff NE XOR2(a_0, AND2(g_1, a_{15})) and NE b_2 iff NE XOR2(a_1, AND2(g_2, a_{15})) and NE b_3 iff NE XOR2(a_2, AND2(g_3, a_{15})) and NE b_4 iff NE XOR2(a_3, AND2(g_4, a_{15})) and NE b_5 iff NE XOR2(a_4, AND2(g_5, a_{15})) and NE b_6 iff NE XOR2(a_5, AND2(g_6, a_{15})) and NE b_7 iff NE XOR2(a_6, AND2(g_7, a_{15})) and NE b_8 iff NE XOR2(a_7, AND2(g_8, a_{15})) and NE b_9 iff NE XOR2(a_8, AND2(g_9, a_{15})) and NE b_{10} iff NE XOR2(a_9, AND2(g_{10}, a_{15})) and NE b_{11} iff NE XOR2(a_{10}, AND2(g_{11}, a_{15})) and NE b_{12} iff NE XOR2(a_{11}, AND2(g_{12}, a_{15})) and NE b_{13} iff NE XOR2(a_{12}, AND2(g_{13}, a_{15})) and NE b_{14} iff NE XOR2(a_{13}, AND2(g_{14}, a_{15})) and NE b_{15} iff NE XOR2(a_{14}, AND2(g_{15}, a_{15})). Then

(i) NE a_{15} iff NE AND2(g_{16}, a_{15}),

(ii) NE a_{14} iff NE XOR2(b_{15}, AND2(g_{15}, a_{15})),

(iii) NE a_{13} iff NE XOR2(b_{14}, AND2(g_{14}, a_{15})),

(iv) NE a_{12} iff NE XOR2(b_{13}, AND2(g_{13}, a_{15})),

(v) NE a_{11} iff NE XOR2(b_{12}, AND2(g_{12}, a_{15})),

(vi) NE a_{10} iff NE XOR2(b_{11}, AND2(g_{11}, a_{15})),

(vii) NE a_9 iff NE XOR2(b_{10}, AND2(g_{10}, a_{15})),

(viii) NE a_8 iff NE XOR2(b_9, AND2(g_9, a_{15})),

(ix) NE a_7 iff NE XOR2(b_8, AND2(g_8, a_{15})),

(x) NE a_6 iff NE XOR2(b_7, AND2(g_7, a_{15})),

(xi) NE a_5 iff NE XOR2(b_6, AND2(g_6, a_{15})),

(xii) NE a_4 iff NE XOR2(b_5, AND2(g_5, a_{15})),

(xiii) NE a_3 iff NE XOR2(b_4, AND2(g_4, a_{15})),

(xiv) NE a_2 iff NE XOR2(b_3, AND2(g_3, a_{15})),

(xv) NE a_1 iff NE XOR2(b_2, AND2(g_2, a_{15})),

(xvi) NE a_0 iff NE XOR2(b_1, AND2(g_1, a_{15})), and

(xvii) NE p iff NE XOR2(b_0, AND2(g_0, a_{15})).

2. Correctness of CRC Circuits with Generator Polynomial of Degree 12 and 16

One can prove the following propositions:

(3) Let g_0, g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8, g_9, g_{10}, g_{11}, g_{12}, a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8, b_9, b_{10}, b_{11}, z, p be sets such that NE g_0 and NE g_{12} and not NE z and NE b_0 iff NE XOR2(p, a_{11}) and NE b_1 iff NE XOR2(a_0, AND2(g_1, b_0)) and NE b_2 iff NE XOR2(a_1, AND2(g_2, b_0)) and NE b_3 iff NE XOR2(a_2, AND2(g_3, b_0)) and NE b_4 iff NE XOR2(a_3, AND2(g_4, b_0)) and NE b_5 iff NE XOR2(a_4, AND2(g_5, b_0)) and NE b_6 iff NE XOR2(a_5, AND2(g_6, b_0)) and NE b_7 iff NE XOR2(a_6, AND2(g_7, b_0)) and NE b_8 iff NE XOR2(a_7, AND2(g_8, b_0)) and NE b_9 iff NE XOR2(a_8, AND2(g_9, b_0)) and NE b_{10} iff NE XOR2(a_9, AND2(g_{10}, b_0)) and NE b_{11} iff NE XOR2(a_{10}, AND2(g_{11}, b_0)). Then

(i) NE b_{11} iff NE XOR2(XOR2(a_{10}, AND2(g_{11}, a_{11})), XOR2(z, AND2(g_{11}, p))),

(ii) NE b_{10} iff NE XOR2(XOR2(a_9, AND2(g_{10}, a_{11})), XOR2(z, AND2(g_{10}, p))),

(iii) NE b_9 iff NE XOR2(XOR2(a_8, AND2(g_9, a_{11})), XOR2(z, AND2(g_9, p))),

(iv) NE b_8 iff NE XOR2(XOR2(a_7, AND2(g_8, a_{11})), XOR2(z, AND2(g_8, p))),

(v) NE b_7 iff NE XOR2(XOR2(a_6, AND2(g_7, a_{11})), XOR2(z, AND2(g_7, p))),

(vi) NE b_6 iff NE XOR2(XOR2(a_5, AND2(g_6, a_{11})), XOR2(z, AND2(g_6, p))),

(vii) NE b_5 iff NE XOR2(XOR2(a_4, AND2(g_5, a_{11})), XOR2(z, AND2(g_5, p))),

(viii) NE b_4 iff NE XOR2(XOR2(a_3, AND2(g_4, a_{11})), XOR2(z, AND2(g_4, p))),

(ix) NE b_3 iff NE XOR2(XOR2(a_2, AND2(g_3, a_{11})), XOR2(z, AND2(g_3, p))),

(x) NE b_2 iff NE XOR2(XOR2(a_1, AND2(g_2, a_{11})), XOR2(z, AND2(g_2, p))),

(xi) NE b_1 iff NE XOR2(XOR2(a_0, AND2(g_1, a_{11})), XOR2(z, AND2(g_1, p))), and

(xii) NE b_0 iff NE XOR2(XOR2(z, AND2(g_0, a_{11})), XOR2(z, AND2(g_0, p))).

(4) Let g_0, g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8, g_9, g_{10}, g_{11}, g_{12}, g_{13}, g_{14}, g_{15}, g_{16}, a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8, b_9, b_{10}, b_{11}, b_{12}, b_{13}, b_{14}, b_{15}, z, p be sets such that NE g_0 and NE g_{16} and not NE z and NE b_0 iff NE XOR2(p, a_{15}) and NE b_1 iff NE XOR2(a_0, AND2(g_1, b_0)) and NE b_2 iff NE XOR2(a_1, AND2(g_2, b_0)) and NE b_3 iff NE XOR2(a_2, AND2(g_3, b_0)) and NE b_4 iff NE XOR2(a_3, AND2(g_4, b_0)) and NE b_5 iff NE XOR2(a_4, AND2(g_5, b_0)) and NE b_6 iff NE XOR2(a_5, AND2(g_6, b_0)) and NE b_7 iff NE XOR2(a_6, AND2(g_7, b_0)) and NE b_8 iff NE XOR2(a_7, AND2(g_8, b_0)) and NE b_9 iff NE XOR2(a_8, AND2(g_9, b_0)) and NE b_{10} iff NE XOR2(a_9, AND2(g_{10}, b_0)) and NE b_{11} iff NE XOR2(a_{10}, AND2(g_{11}, b_0)) and NE b_{12} iff NE XOR2(a_{11}, AND2(g_{12}, b_0)) and NE b_{13} iff NE XOR2(a_{12}, AND2(g_{13}, b_0)) and NE b_{14} iff NE XOR2(a_{13}, AND2(g_{14}, b_0)) and NE b_{15} iff NE XOR2(a_{14}, AND2(g_{15}, b_0)). Then

(i) NE b_{15} iff NE XOR2(XOR2(a_{14}, AND2(g_{15}, a_{15})), XOR2(z, AND2(g_{15}, p))),

(ii) NE b_{14} iff NE XOR2(XOR2(a_{13}, AND2(g_{14}, a_{15})), XOR2(z, AND2(g_{14}, p))),

(iii) NE b_{13} iff NE XOR2(XOR2(a_{12}, AND2(g_{13}, a_{15})), XOR2(z, AND2(g_{13}, p))),

(iv) NE b_{12} iff NE XOR2(XOR2(a_{11}, AND2(g_{12}, a_{15})), XOR2(z, AND2(g_{12}, p))),

(v) NE b_{11} iff NE XOR2(XOR2(a_{10}, AND2(g_{11}, a_{15})), XOR2(z, AND2(g_{11}, p))),

(vi) NE b_{10} iff NE XOR2(XOR2(a_9, AND2(g_{10}, a_{15})), XOR2(z, AND2(g_{10}, p))),

(vii) NE b_9 iff NE XOR2(XOR2(a_8, AND2(g_9, a_{15})), XOR2(z, AND2(g_9, p))),

(viii) NE b_8 iff NE XOR2(XOR2(a_7, AND2(g_8, a_{15})), XOR2(z, AND2(g_8, p))),

(ix) NE b_7 iff NE XOR2(XOR2(a_6, AND2(g_7, a_{15})), XOR2(z, AND2(g_7, p))),

(x) NE b_6 iff NE XOR2(XOR2(a_5, AND2(g_6, a_{15})), XOR2(z, AND2(g_6, p))),

(xi) NE b_5 iff NE XOR2(XOR2(a_4, AND2(g_5, a_{15})), XOR2(z, AND2(g_5, p))),

(xii) NE b_4 iff NE XOR2(XOR2(a_3, AND2(g_4, a_{15})), XOR2(z, AND2(g_4, p))),

(xiii) NE b_3 iff NE XOR2(XOR2(a_2, AND2(g_3, a_{15})), XOR2(z, AND2(g_3, p))),

(xiv) NE b_2 iff NE XOR2(XOR2(a_1, AND2(g_2, a_{15})), XOR2(z, AND2(g_2, p))),

(xv) NE b_1 iff NE XOR2(XOR2(a_0, AND2(g_1, a_{15})), XOR2(z, AND2(g_1, p))), and

(xvi) NE b_0 iff NE XOR2(XOR2(z, AND2(g_0, a_{15})), XOR2(z, AND2(g_0, p))).

REFERENCES

[1] Yatsuka Nakamura. Logic gates and logical equivalence of adders. *Journal of Formalized Mathematics*, 11, 1999. http://mizar.org/JFM/Vol11/gate_1.html.

Received April 16, 1999

Published January 2, 2004