Verification of logic circuits using Mizar and its application to an adder circuit on a radix-2^k SD number.

Hidetaka SHIMIZU
Yatsuka NAKAMURA
Yoshinori FUJISAWA
Yasushi FUWA

1. Introduction

To answer the request of higher performance from electric equipment, logic circuit is becoming more complicated and more large-scaled. This makes it more difficult to verify correctness of a designed circuit.

Heretofore, to verify a logical circuit, output for every possible state and input should be confirmed by simulation. However, when the scale of a circuit increases, states of circuit increases exponentially, accordingly (Example, when a circuit has 100 return wires, it has 2^{100} states.). So it is impossible or very difficult to complete such a simulation for large-scaled circuits.

As a new way to verify correctness of logical circuit, we express logical circuit with mathematical description (called mathematical model). The correctness of the circuits is assured when correctness of the
A proof checker system has been used to verify correctness of proof in mathematics. It can be applied to verifying correctness of a designed circuit with the method we suggest.

In this paper, after introducing the proof checker system Mizar which is used to verify correctness of proof (Section 2), we give some definitions as a preparation for mathematics descriptions of a logical circuit (Section 3). Then, we explain how a logical circuit is described by these definitions, and how its correctness is verified by the system (Section 4). At last, as an example, we apply the method in designing the adder circuit on a radix-2 \(k\)SD number.

2. Proof checker system Mizar

As an attempt to reconstruct mathematical vernacular, the Mizar project started in 1973. \(^{[1]}\)

And, it has become the most important activity in the project to develop the database of mathematics since 1989. Now, more than 2,000 definitions and 20,000 theorems are included in the increasing database.

As a characteristic of Mizar, useful verified proof is accepted by Mizar's library. Using Mizar, besides mathematical proof, a mathematical model can be verified too.

Just as a large-scale circuit can be designed as a combination of
smaller circuits which function has been verified, the correctness of a model can be showed when the model is a combination of smaller models which has been accepted by the library.

3. Preparation for mathematical description of a logical circuit

We give a relation between basic concepts of logical circuits and mathematics as follows:

(1) We think input and output signals as sets. The logic of a signal line has 2 states, 0 and 1. 0 is defined as the empty set $\phi$, and 1 is defined as a non-empty set.

It is described as follows at Mizar:

```plaintext
definition let a be set;
redefine attr a is empty;
anomaly $a$;
end;
```

(2) We consider the expression of every possible states formed by input and output signals. It is described like this:

```plaintext
$\forall$0 iff $\land$ (NOT $q_2$, NOT $q_1$)
```

(3) We define a circuit as a Boolean function of sets defined above.

For example, NOT circuit writes follows:

```plaintext
func NOT1 a $\Rightarrow$ set equals
 $\phi$ if $a$
otherwise {$\phi$ : not contradiction};
end;
```
4. A new method of logic circuit's verification using Mizar system

Here, we introduce how the new method works with a simple example.

Consider a 3bit up counter circuit. The correctness of the circuit can be guaranteed with Mizar at the following steps.

(1) Describing the input and output as sets.

(2) Defining every possible state of input and output as following with the set of step 1. (Fig.1)

\[
\begin{align*}
&s_0 = \text{AND3}(\text{NOT}1\ q_3, \text{NOT}1\ q_2, \text{NOT}1\ q_1); \\
&s_1 = \text{AND3}(\text{NOT}1\ q_3, \text{NOT}1\ q_2, q_1); \\
&s_2, s_3, s_4, s_5, s_6, s_7 \text{ is similar to } s_0, s_1.
\end{align*}
\]

(3) Expressing the behavior of 3bit up counter circuit with Boolean expressions as follows: (Fig.2)

\[
\begin{align*}
&s_n q_1 = \text{AND2}(\text{NOT}1\ q_1, R) \\
&s_n q_2 = \text{AND2}(\text{XOR2}(q_1, q_2), R) \\
&s_n q_3 = \text{AND2}(\text{OR2}(\text{AND2}(q_3, \text{NOT}1\ q_1), \text{AND2}(q_1, \text{XOR2}(q_2, q_3))), R)
\end{align*}
\]

Here, $q_1, q_2, q_3, R$ are circuit inputs and $s_n q_1, s_n q_2, s_n q_3$ are outputs.

(4) Verifying the correctness of circuit by confirming its Boolean expressions' tautology using Mizar system.

\[
\begin{align*}
&(s_n s_1 \text{ iff } \text{AND2}(s_0, R)) \& (s_n s_2 \text{ iff } \text{AND2}(s_1, R)) \& (s_n s_3 \text{ iff } \text{AND2}(s_2, R)) \& (s_n s_4 \text{ iff } \text{AND2}(s_3, R)) \& (s_n s_5 \text{ iff } \text{AND2}(s_4, R)) \& (s_n s_6 \text{ iff } \text{AND2}(s_5, R)) \& (s_n s_7 \text{ iff } \text{AND2}(s_6, R)) \& (s_n s_0 \text{ iff } \text{SOR2}(s_7, \text{NOT}1\ R));
\end{align*}
\]

Here, $s_0, \ldots, s_7$ means current states and $s_n s_0, \ldots, s_n s_7$ means next states of current states.
($ns1$ iff $\text{AND2}(s0, R)$) means the next state will be $ns1$, if and only if the current state is $s0$ and $R$ is "1".

Behavior of a 3bit up counter circuit

Have 4 inputs($R, q3, q2, q1$) and 3 outputs($nq3, nq2, nq1$)
States change as follows:
000$\rightarrow$001$\rightarrow$010$\rightarrow$011$\rightarrow$100$\rightarrow$101$\rightarrow$110$\rightarrow$111$\rightarrow$000$\rightarrow$
return to the initial state(000) by the reset input

Signal definitions

Fig. 1 Definitions of 3bit up counter.

Definitions and proof to correctness of a 3bit up counter

Fig. 2 Definitions (cont.) and proof of correctness of 3bit up counter.
5. An application to a radix-2^kSD number coded adder circuit

Here, we apply the new method to designing an adder circuit on a radix-2^kSD number.

In a radix-2^kSD (signed-digit) coded adder circuit, calculations can be finished in a constant time no matter whether there is a ripple carry.

Here, we will verify the correctness of such a circuit of case k=2.

A designed radix-4SD number circuit and signal layouts

Fig. 3 Signal layout of radix-4SD number coded adder circuit
The correctness of a 4-SD number adder circuit is verified with the 4 steps described in former section.

First, input and output status can be defined as follows:

**INPUT STATE:**

($x_{m3}$ iff $\text{SAND3}(x_2, \text{NOT1} x_1, x_0))$

($x_{m2}$ iff $\text{SAND3}(x_2, x_1, \text{NOT1} x_0))$

($x_{m1}$ iff $\text{SAND3}(x_2, x_1, x_0))$

($x_{z}$ iff $\text{SAND3}(\text{NOT1} x_2, \text{NOT1} x_1, \text{NOT1} x_0))$

($x_{p1}$ iff $\text{SAND3}(\text{NOT1} x_2, \text{NOT1} x_1, x_0))$

($x_{p2}$ iff $\text{SAND3}(\text{NOT1} x_2, x_1, \text{NOT1} x_0))$

($x_{p3}$ iff $\text{SAND3}(\text{NOT1} x_2, x_1, x_0))$

Here, $x_0, x_1, x_2$ express the three inputs of PART1 (Fig.3), $x_{m3}, x_{m2}, x_{m1}, x_{z}, x_{p1}, x_{p2}, x_{p3}$ are all possible input states. The expression $x_{m3}$ iff $\text{SAND3}(x_2, \text{NOT1} x_1, x_0)$ means that an input state is called $x_{m3}$ if and only if inputs $x_2 = "1", x_1 = "0", x_0 = "1"$. 
$\text{Sym3, Sym2, Sym1, Syz, Syp1, Syp2, Syp3} \text{ can be defined similarly.}$

**OUTPUT STATE:**

Output states can be defined in same way as follows.

($\text{Snz} \iff \text{SAND5(NOT1 nc1, NOT1 nc0, NOT1 nw2, NOT1 nw1, NOT1 nw0)} \land \text{SAND5(NOT1 nc1, NOT1 nc0, NOT1 nw2, NOT1 nw1, NOT1 nw0)} \land \text{SAND5(NOT1 nc0, NOT1 nw2, NOT1 nw1, NOT1 nw0)} \land \text{SAND5(NOT1 nc1, nc0, nw2, nw1, nw0)} \land \text{SAND5(NOT1 nc1, nc0, NOT1 nw2, NOT1 nw1, NOT1 nw0)} \land \text{SAND5(NOT1 nc1, nc0, NOT1 nw2, NOT1 nw1, NOT1 nw0)} \land \text{SAND5(NOT1 nc1, nc0, NOT1 nw2, NOT1 nw1, NOT1 nw0)}$)

Next, the behavior of PART1 can be described as a Boolean function as follows.

($\text{Sn0} \iff \text{SOR8(AND4(NOT1 x2, x1, NOT1 y2, y1)},$

\begin{align*}
&\text{AND3(NOT1 x2, NOT1 y2, OR2(AND2(x1, x0), AND2(y1, y0)))}, \\
&\text{AND3(NOT1 x2, NOT1 y2, OR2(AND2(x1, y0), AND2(x0, y1)))}, \\
&\text{AND3(NOT1 x1, NOT1 y1, OR2(AND4(x2, x0, NOT1 y2, NOT1 y0), AND4(NOT1 x2, NOT1 x0, y2, y0)))}, \\
&\text{AND5(x2, x1, y2, NAND2(x0, y0)), AND5(x2, x1, y2, NOT1 y1, y0)}, \\
&\text{AND5(x2, NOT1 x1, x0, y2, y1), AND6(x2, NOT1 x1, x0, y2, NOT1 y1, y0))}
\end{align*}$

$\text{Sn1, Snw2, Snw1, Snw0} \text{ can be described in same way.}$

Then, the relation between input status and output status is built.

The following expression is showed tautology by Mizar system. So the correctness of PART1 circuit is verified. (Fig.5)

($\text{Snm6} \iff \text{SAND2(xm3, ym3)}) \land \text{SAND2(xm2, ym2)}) \land \text{SAND2(xm1, ym3))} \land \text{SAND2(xm3, yz)}, \text{AND2(xm2, ym1)}, \text{AND2(xm1, ym2),}

\begin{align*}
&\text{AND2(xz, ym3))} \land \\
&\text{SAND5(AND2(xm3, yp1)), AND2(xm2, yz), AND2(xm1, ym1),} \\
&\text{AND2(xz, ym2), AND2(xp1, ym3))} \land \\
&\text{SAND6(AND2(xm3, yp2), AND2(xm2, yp1), AND2(xm1, yz),}
\end{align*}$

\begin{align*}
&\text{AND2(xz, ym1), AND2(xp1, ym2), AND2(xp2, ym3))}
\end{align*}$
Here, for example, the expression \((\text{Sn}_5 \iff \text{SOR}_2(\text{AND}_2(\text{x}_3,\text{y}_2), \text{AND}_2(\text{x}_1,\text{y}_1), \text{AND}_2(\text{z},\text{y}_z), \text{AND}_2(\text{y}_1,\text{y}_m), \text{AND}_2(\text{y}_2,\text{y}_m))) \& \text{AND}_2(\text{z},\text{y}_z), \text{AND}_2(\text{y}_1,\text{y}_m)))\) means a state is called \(\text{Sn}_5(-5)\) if and only if the input state \((\text{Sn}_3(\text{x}_3=-3) \text{ and } \text{Sn}_2(\text{y}_2=-2)) \text{ or } (\text{Sn}_2(\text{x}_2=-2) \text{ and } \text{Sn}_3(\text{y}_3=-3))\).

Other expressions are similar.

The correctness of PART2 can be verified in same way. (Fig.6)

Thus, the behavior of the whole circuit can be expressed by the following expressions.

\[
\begin{align*}
(\text{Sn}_2 & \iff \text{SAND}_3(\text{x}_2, \text{x}_1, \text{NOT}_1 \text{x}_0)) \& \\
(\text{Sn}_1 & \iff \text{SAND}_3(\text{x}_2, \text{x}_1, \text{x}_0)) \& \\
(\text{Sx}_2 & \iff \text{SAND}_3(\text{NOT}_1 \text{x}_2, \text{NOT}_1 \text{x}_1, \text{NOT}_1 \text{x}_0)) \& \\
(\text{Sp}_1 & \iff \text{SAND}_3(\text{NOT}_1 \text{x}_2, \text{NOT}_1 \text{x}_1, \text{x}_0)) \& \\
(\text{Sp}_2 & \iff \text{SAND}_3(\text{NOT}_1 \text{x}_2, \text{x}_1, \text{NOT}_1 \text{x}_0)) \& \\
(\text{Sc}_1 & \iff \text{SAND}_2(\text{c}_1, \text{c}_0)) \& \\
(\text{Sc}_2 & \iff \text{SAND}_2(\text{NOT}_1 \text{c}_1, \text{NOT}_1 \text{c}_0)) \& \\
(\text{Sp}_3 & \iff \text{SAND}_2(\text{NOT}_1 \text{c}_1, \text{c}_0)) \& \\
(\text{SN}_3 & \iff \text{SAND}_3(\text{ns}_2, \text{NOT}_1 \text{ns}_1, \text{ns}_0)) \& \\
(\text{SN}_2 & \iff \text{SAND}_3(\text{ns}_2, \text{ns}_1, \text{NOT}_1 \text{ns}_0)) \& \\
(\text{SN}_1 & \iff \text{SAND}_3(\text{ns}_2, \text{ns}_1, \text{ns}_0)) \& \\
(\text{Sn}_2 & \iff \text{SAND}_3(\text{NOT}_1 \text{ns}_2, \text{NOT}_1 \text{ns}_1, \text{NOT}_1 \text{ns}_0)) \& \\
(\text{Sp}_1 & \iff \text{SAND}_3(\text{NOT}_1 \text{ns}_2, \text{NOT}_1 \text{ns}_1, \text{ns}_0)) \& \\
\end{align*}
\]
\[\text{np2 iff } \text{AND3(NOTI ns2, ns1, NOT1 ns0)} \] & \\
\[\text{np3 iff } \text{AND3(NOTI ns2, ns1, ns0)} \] & \\
\[\text{ns0 iff } \text{SOR4(AND4(NOT1 x2, NOT1 x1, NOT1 x0, c0), AND3(x1, NOT1 x0, c0), AND5(NOT1 x2, NOT1 x1, x0, NOT1 c1, NOT1 c0), AND5(x2, x1, x0, NOT1 c1, NOT1 c0))} \] & \\
\[\text{ns1 iff } \text{SOR5(AND5(NOT1 x2, NOT1 x1, NOT1 x0, c1, c0), AND5(NOT1 x2, NOT1 x1, x0, NOT1 c1, NOT1 c0), AND3(x1, NOT1 x0, NOT1 c1), AND5(x2, x1, x0, NOT1 c1, NOT1 c0), AND5(x2, x1, x0, c1, c0))} \] & \\
\[\text{ns2 iff } \text{SOR7(AND2(c1, NOT1 c0), AND4(NOT1 x2, NOT1 x1, NOT1 x0, c1), AND3(NOT1 x2, x1, x0), AND3(x2, x1, NOT1 x0), AND2(x2, NOT1 x1), AND3(x2, NOT1 c1, NOT1 c0), AND2(x2, c1))} \] & \\
\[\text{nm3 iff } \text{AND2(xm2, cm)} \] & \\
\[\text{nm2 iff } \text{SOR2(AND2(xm2, cz), AND2(xm1, cm))} \] & \\
\[\text{nm1 iff } \text{SOR3(AND2(xm2, cp), AND2(xm1, cz), AND2(xz, cm))} \] & \\
\[\text{nz iff } \text{SOR3(AND2(xm1, cp), AND2(xz, cz), AND2(xp1, cm))} \] & \\
\[\text{np1 iff } \text{SOR3(AND2(xz, cp), AND2(xp1, cz), AND2(xp2, cm))} \] & \\
\[\text{np2 iff } \text{SOR2(AND2(xp1, cp), AND2(xp2, cz))} \] & \\
\[\text{np3 iff } \text{AND2(xp2, cp)} \] & \\

The tautology can be showed because part 1 and part 2 have been verified. So the correctness of radix-4SD adder circuit is verified.
\[\begin{align*}
\text{nc1} &= x_2 \cdot -x_1 \cdot -x_0 + y_2 \cdot -y_1 \cdot -y_0 \\
&\quad + -x_2 \cdot -x_1 \cdot -x_0 \cdot y_2 \cdot -y_1 + x_2 \cdot -x_1 \cdot -y_2 \cdot -y_1 \cdot -y_0 \\
&\quad + x_2 \cdot y_2 \cdot (-x_1 + -y_1) + x_2 \cdot y_2 \cdot (x_1 \cdot -x_0 + y_1 \cdot -y_0) \\
\text{nc0} &= -x_2 \cdot -y_2 \cdot (x_1 \cdot x_0 + y_1 \cdot y_0) \\
&\quad + -x_2 \cdot -y_2 \cdot (x_1 \cdot y_0 + x_0 \cdot y_1) + -x_2 \cdot x_1 \cdot -y_2 \cdot y_1 \\
&\quad + -x_1 \cdot -y_1 \cdot (x_2 \cdot x_0 \cdot -y_2 \cdot -y_0 + -x_2 \cdot -x_0 \cdot y_2 \cdot y_0) \\
\text{w2} &= x_2 \cdot x_1 \cdot y_2 \cdot y_1 \cdot (x_0 \text{ NAND} y_0) \\
&\quad + x_2 \cdot x_1 \cdot -y_2 \cdot -y_1 \cdot (x_0 \text{ NAND} y_0) \\
\text{sl} &= -w_2 \cdot w_1 \cdot -w_0 \cdot -c_1 \cdot -c_0 + -x_2 \cdot x_1 \\
\text{w0} &= x_1 \text{ XOR} y_1 \cdot (x_0 \text{ XOR} y_0) \\
\text{w1} &= (x_1 \text{ XOR} y_1) \cdot (x_0 \cdot y_0) + (x_1 \text{ XOR} y_1) \cdot (x_0 \text{ NAND} y_0) \\
\text{w0} &= x_0 \text{ XOR} y_0
\end{align*}\]

Fig. 5 The circuit verified of correctness by Mizar system (PART1)

\[\begin{align*}
\text{w2} &= -x_2 \cdot -y_2 \cdot (x_1 \text{ XOR} y_1) \cdot (x_0 \text{ XOR} y_0) \\
&\quad + x_2 \cdot x_1 \cdot -y_2 \cdot -y_1 \cdot (x_0 \text{ NAND} y_0) \\
&\quad + -x_2 \cdot -x_1 \cdot y_2 \cdot y_1 \cdot (x_0 \text{ NAND} y_0) \\
&\quad + x_2 \cdot -x_1 \cdot y_1 \cdot -y_0 + x_1 \cdot -x_0 \cdot y_2 \cdot -y_1 \\
&\quad + -x_1 \cdot x_0 \cdot -y_1 \cdot y_0 \cdot (x_2 \text{ XOR} y_2) \\
&\quad + x_2 \cdot x_0 \cdot y_2 \cdot y_0 \cdot (x_1 \text{ XOR} y_1) \\
\text{sl} &= -w_2 \cdot -w_1 \cdot -w_0 \cdot -c_1 \cdot -c_0 + -x_2 \cdot x_1 \\
\text{w0} &= x_1 \text{ XOR} y_1 \cdot (x_0 \cdot y_0) + (x_1 \text{ XOR} y_1) \cdot (x_0 \text{ NAND} y_0) \\
\text{w0} &= x_0 \text{ XOR} y_0
\end{align*}\]

Fig. 6 The circuit verified of correctness by Mizar system (PART2)
6. Conclusion

We showed it is possible to verify correctness of logical circuit’s mathematical model using proof checker Mizar.

This can be considered as a new approach to verifying correctness of logical circuit.

The circuit we proved has been accepted by the library of Mizar, and it can be used to prove larger circuits.

When the library is substantially in future, verification of logical circuits in practice can be expected. Verification of cryptogram circuit can be realized in the same way.

References