数理解析研究所講究録
975 巻 1996 年 176-184

The Concept of a Many Sorted Algebra and a Model of Digital Circuits

Shinshu University, Pauline N. Kawamoto (ポーリン・カワモト)
Warsaw University, Andrzej Trybulec (アンジェイ・トリブレッツ)

ABSTRACT. In this paper, we present the concept of a *many sorted algebra* and demonstrate its application in the modelling of digital circuits. The many sorted algebra is based on the notion of a many sorted signature which we can use to define the static structure (operators, connections, etc.) of a circuit and the algebra defines the circuit logic. By defining such concepts as circuit state, depth, stability, etc. based on this type of model, we can study various static and dynamic characteristics of circuits mathematically.

1. INTRODUCTION

By using the concept of a *many sorted algebra*, proposed earlier in [1], we can form mathematical models of digital circuits. With the growing scale and complexity of digital circuits being developed,

---

1991 *Mathematics Subject Classification.* 08A99.
Keywords and phrases. many sorted algebras, modelling of digital circuits, circuit stability.

Verification of the definitions and proofs in this work are pursued using the Mizar proof checking system developed at the Institute of Mathematics, Warsaw University, POLAND.

this type of formalization is essential in automating the verification processes of such mechanisms.

In Section 2, we present the concepts necessary in formalizing a many sorted algebra and in Section 3 we demonstrate how it is used to model a digital circuit. In Section 4, we discuss some properties of circuits based on this model and summarize our work in Section 5.

2. Preliminaries

We begin with some preliminary concepts and notations used in this work to define a many sorted algebra.

Definition 1. Let A be a set. L is a *set of finite sequences of A elements* if $L = \bigcup_{n=0}^{\infty} A^{N_n}$. Here, N_n S $= \{1, 2, \ldots, n\}$. We write $A* = L$.

Definition 2. A quadruple $S = (c, o, a, r)$ is called a *many sorted signature* when c is a non-empty set, o is a set, a is a mapping $o \rightarrow c*$, r is a mapping $o \rightarrow c$. We call c the *carrier of S*, o the *OperSymbols of S*, a the *Arity of S*, and r the *ResultSort of S* and write them as c_S, o_S, a_S, and r_S, respectively.

Definition 3. Let I be a set and F a set-valued function. F is a *many sorted set of I* if dom $F = I$.

Definition 4. Let I be a set. Let A, B be many sorted sets of I. G is called a *many sorted function of A, B* if $G(i)$ is a mapping

$A(i) \to B(i)$, for all $i \in I$.

Definition 5. Let A be a set-valued function. L is a *product of* A if $L = \{g : \text{dom } g = \text{dom } A, \forall x' \in \text{dom } A : g(x') \in A(x')\}$. We write product $A = L$.

Definition 6. Let I be a set, M a many sorted set of I, and L a set-valued function. L is a *pound of M* if $L(i) = \text{product}(M \cdot i)$, for all $i \in I$. We write $M\# = L$.

The above concepts are used to define a many sorted algebra below.

Definition 7. Let S be a many sorted signature. $A = (s, ch)$ is called a *many sorted algebra over S* when s is a non-empty many sorted set of c_S and ch is a many sorted function of $s\# \cdot a_S$, $s \cdot r_S$. We call s the *Sorts of A* and ch the *Charact of A* and write them as s_A and ch_A, respectively.

3. Application

This section describes by way of example how to use the many sorted signature and many sorted algebra concepts presented above to formalize a model of digital circuits.

A many sorted signature with the following attribute can be used to describe the structure of a circuit.

Definition 8. Let S be a many sorted signature. S is said to be *circuit-like* if $(\forall o_1, o_2 \in o_S)\ (r_S(o_1) = r_S(o_2) \Rightarrow o_1 = o_2)$.

That is, elements of the carrier can be the result sort of no more than one OperSymbol element.

For example, consider the simple circuit in Figure 1 consisting of one AND gate and one OR gate.

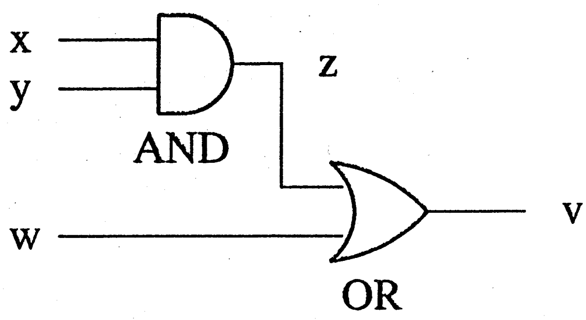

Figure 1: Example of a two-gate circuit.

We can describe this structure of this circuit as a many sorted signature $S = (c, o, a, r)$ where:

$$\begin{aligned} c &= \{x, y, z, w, v\} \\ o &= \{AND, OR\} \\ a &: AND \mapsto < *x, y* >,\ OR \mapsto < *z, w* > \\ r &: AND \mapsto z,\ OR \mapsto v \end{aligned} \quad (1)$$

S is circuit-like by Definition 8. In terms of digital circuits, this means that a circuit contains no wired OR connections.

Once the structure of a circuit is decided, its behavior is described with a many sorted algebra.

Definition 9. Let S be a many sorted signature. A is said to be a *circuit of* S if S is circuit-like and A is a many sorted algebra over S.

For the example of Figure 1, we can define a many sorted algebra $A = (s, ch)$ where:

$$\begin{aligned} s &: c \rightarrow \{\{0,1\}\} \\ ch &: AND \mapsto \cdot\, logic,\ OR \mapsto +\, logic \end{aligned}$$

Here, we use

$$\begin{aligned} \cdot\, logic &: \{(1,0),(2,0)\} \mapsto 0,\ \{(1,0),(2,1)\} \mapsto 0, \\ &\quad\ \{(1,1),(2,0)\} \mapsto 0,\ \{(1,1),(2,1)\} \mapsto 1, \\ +\, logic &: \{(1,0),(2,0)\} \mapsto 0,\ \{(1,0),(2,1)\} \mapsto 1, \\ &\quad\ \{(1,1),(2,0)\} \mapsto 1,\ \{(1,1),(2,1)\} \mapsto 1, \end{aligned} \tag{2}$$

4. Some Properties of Circuits

Based on the model of circuits described in the previous section, we can formalize some static and dynamic properties of circuits as follows.

The state of a circuit is defined below.

Definition 10. Let S be a circuit-like many sorted signature, A a circuit of S. q is called a *state of* A if $q \in \text{product}(s_A)$.

For the digital circuit example of Figure 1, the available states are:

$$\begin{aligned}
\{\, q_1 &: x \mapsto 0,\ y \mapsto 0,\ z \mapsto 0, w \mapsto 0,\ v \mapsto 0,\\
q_2 &: x \mapsto 0,\ y \mapsto 0,\ z \mapsto 0, w \mapsto 0,\ v \mapsto 1,\\
&\quad \cdots\\
q_{32} &: x \mapsto 1,\ y \mapsto 1,\ z \mapsto 1, w \mapsto 1,\ v \mapsto 1 \,\}
\end{aligned}$$

When the current state of a circuit is given, we can compute the next state of the circuit using the following concepts.

Definition 11. Let f be a function. L is called the *set of range elements of* f if $L = \{y :^{\exists} x \in \text{dom } f \text{ and } y = f(x)\}$. We write rng $f = L$.

Definition 12. Let S be a many sorted signature. L is called the *set of input vertices of* S if $L = c_S \setminus \text{rng } r_S$. We write InputVertices $S = L$.

Definition 13. Let S be a many sorted signature. L is called the *set of inner vertices of* S if $L = \text{rng } r_S$. We write InnerVertices $S = L$.

Definition 14. Let S be a circuit-like many sorted signature, v an element of InnerVertices S. L is called the *action at* v if $L = r_S(v)$.

Definition 15. Let S be a circuit-like many sorted signature, v an element of c_S, op an element of o_S, A a circuit of S, q a state of

A. L is called the *inputs of op in q* if $L = q \cdot a_S(op)$.

If we consider the many sorted signature S given in Equation 1 for the circuit example of Figure 1, InputVertices $S = \{x, y, w\}$ and InnerVertices $S = \{z, v\}$. The action at z is AND and the action at v is OR.

If we assume a state $q : x \mapsto 0,\ y \mapsto 0,\ z \mapsto 0,\ w \mapsto 1,\ v \mapsto 1$ for the circuit of S given in Equation 2, we have the inputs of AND in $q : 1 \mapsto 0, 2 \mapsto 0$ and the inputs of OR in $q : 1 \mapsto 0, 2 \mapsto 1$.

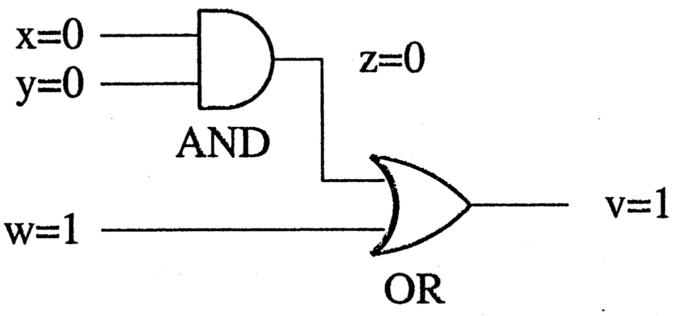

Figure 2: Example of circuit state.

Finally, to compute the next state of a circuit, we use the following definition.

Definition 16. Let S be a circuit-like many sorted signature, A a circuit of S, and q a state of A. q' is called a *following state of q* if $(^{\forall}v \in c_S)$ ($v \in$ InputVertices $S \Rightarrow q'(v) = q(v)$ and $v \in$ InnerVertices $S \Rightarrow q'(v) =$ (ch_A(action at v)) (inputs of action at v in q)). We write Following $q = q'$.

Another important property of circuits is the notion of stability.

Definition 17. Let S be a circuit-like many sorted signature, A a circuit of S, and q a state of A. q is said to be *stable* when $q = Following\ q$.

5. Conclusion

Based on the concepts presented above, we can make some formal evaluations of circuits. (Note, the proofs of the following theorems appear in the database of the Mizar proof checking system [2][3][4][5].)

For example, some rules are necessary for specifying how to construct the many sorted algebra describing the logic of a circuit.

Theorem 1. *Let S be a Circuit-like many sorted signature, A a circuit of S, q a state of A, o an element of o_S. Then, $(ch_A(o))$ $(inputs\ of\ o\ in\ q) \in s_A\ (r_S\ (o))$.*

Another important characteristic of circuits to be studied is the number of layers of gates it uses. The concept of depth here is defined in [4].

Theorem 2. *Let S be a Circuit-like many sorted signature, A a circuit of S, v, v_1 elements of c_S such that $v \in InnerVertices\ S$ and $v_1 \in rng\ a_S\ (action\ at\ v)$. Then, $depth(v_1, A) < depth\ (v, A)$.*

The formal treatment of circuits in this work can be extended to provide a mathematical background for studying other characteristics of circuits (e.g, speed, size, logical correctness, etc.) as well.

References

1. A. Trybulec, *Many Sorted Algebras*, Formalized Mathematics, 5 (1996), 37-42.
2. Y. Nakamura, P. Rudnicki, A. Trybulec, and P. N. Kawamoto, *Preliminaries to Circuits, I*, Formalized Mathematics, 5 (1996), 167-172.
3. Y. Nakamura, P. Rudnicki, A. Trybulec, and P. N. Kawamoto, *Preliminaries to Circuits, II*, Formalized Mathematics, 5 (1996), 215-220.
4. Y. Nakamura, P. Rudnicki, A. Trybulec, and P. N. Kawamoto, *Introduction to Circuits, I*, Formalized Mathematics, 5 (1996), 227-232.
5. Y. Nakamura, P. Rudnicki, A. Trybulec, and P. N. Kawamoto, *Introduction to Circuits, II*, Formalized Mathematics, 5 (1996), 273-278.

Shinshu University, Faculty of Engineering, Department of Information Engineering, Wakasato 500, Nagano 380, Japan
E-mail address: `pauline@cs.shinshu-u.ac.jp`

Warsaw University, Bialystok Branch, Institute of Mathematics, ul. Akademicka 2 15-267 Bialystok, Poland
E-mail address: `trybulec@math.uw.bialystok.pl`