MULTI-LEVEL SYNTHESIS FOR SAFE REPLACEABILITY

by

Carl Pixley, Vigyan Singhal, Adnan Aziz, and Robert K. Brayton

Memorandum No. UCB/ERL M94/31

26 April 1994

COVER PAGE

MULTI-LEVEL SYNTHESIS FOR SAFE REPLACEABILITY

by

Carl Pixley, Vigyan Singhal, Adnan Aziz, and
Robert K. Brayton

Memorandum No. UCB/ERL M94/31

26 April 1994

ELECTRONICS RESEARCH LABORATORY

College of Engineering
University of California, Berkeley
94720

MULTI-LEVEL SYNTHESIS FOR SAFE REPLACEABILITY

by

Carl Pixley, Vigyan Singhal, Adnan Aziz, and
Robert K. Brayton

Memorandum No. UCB/ERL M94/31

26 April 1994

ELECTRONICS RESEARCH LABORATORY

College of Engineering
University of California, Berkeley
94720

Multi-level Synthesis for Safe Replaceability

Carl Pixley **Vigyan Singhal**[*] **Adnan Aziz**[†] **Robert K. Brayton**

Motorola Inc., MD OE321
6501 Wm Cannon Drive West
Austin, TX 78735

Department of Electrical Engg. and Computer Sc.
University of California at Berkeley
Berkeley, CA 94720

Abstract

We describe the condition that a sequential digital design is a safe replacement for an existing design without making any assumptions about a known initial state of the design or about its environment. We formulate a safe replacement condition which guarantees that if an original design is replaced by a new design, the interacting environment cannot detect the change by observing the input-output behavior of the new design; conversely, if a replacement design does not satisfy our condition an environment can potentially detect the replacement (in this sense the replacement is potentially unsafe). Our condition allows simplification of the state transition diagram of an original design. We use the safe replacement condition to derive a sequential resynthesis method for area reduction of gate-level designs. We have implemented our resynthesis algorithm and we report experimental results.

1 Introduction

We are concerned with the problem of sequential resynthesis for gate-level synchronous, sequential designs. We start with a given design and replace it with a modified design so that an environment around the original design cannot detect the replacement by observing the input-output behavior of the design. We want to make no assumptions about the environment. The state of a sequential

[*]Research supported by NSF/DARPA Grant MIP-8719546 and a summer internship from Motorola, Inc.
[†]Research supported by SRC Grant 94-DC-324

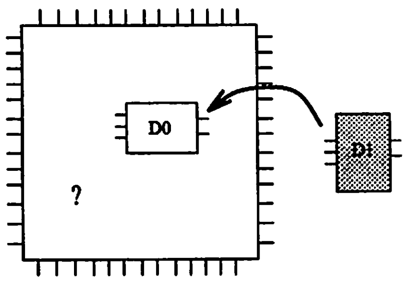

Figure 1: Replacement of a sequential design

design is captured the values of the latches in the design. We will not make any assumption about a known initial state of the sequential circuit. It is here that we differ from most previous research in sequential synthesis of circuits. In many industrial-level designs many latches do not have a reset line. While it is well accepted that this statement is true in the data part of the designs, it is our experience that even in the control part many latches do not have a reset line. Avoiding routing reset lines yields significant gain in area, and is an important reason why latches may not have reset lines. Also, latches without reset lines cost less (in number of transistors required) that those with reset lines.

Figure 1 illustrates the problem. We would like to replace the design with another without making any assumptions about the interacting environment and the state the design can power up in.

Many researchers have been able to obtain and exploit sequential flexibility in gate-level designs by using the knowledge of the designated start state. Some of these include using don't care resulting from unreachable states [LTN90], redundant latch removal [BCM90, LN91], sequential redundancy removal [CHS91] and equivalence net detection [BT93]. All these methods rely on the flexibility introduced because many states in the design are not reachable from the start state, and hence we are free to modify the behavior of any unreachable state arbitrarily. However, if latches do not have reset lines, *all* states are reachable, and methods which rely on unreachable states cannot provide any more flexibility than the regular combinational flexibility afforded by the network. In this paper, we use our replaceability notion to obtain area reductions without assuming a designated start state.

We describe our condition for safe replacement and synthesis techniques which does not assume reset lines. We describe how our condition differs from other notions used to describe sequential equivalence [Pix92, Che93]. We also discuss how other sequential resynthesis methods, like retiming/resynthesis [MSBS91] and synchronous relation minimization [DD92, SWB93], which do not directly use the knowledge of a designated start state indirectly rely on the existence of an initial state. It is surprising even though the design may power up in any state that we are able to obtain some area reductions beyond combinational resynthesis. Furthermore, it is not necessary to preserve the underlying state transition graph of the design (as in the state re-encoding problem).

In Section 2, we provide the basic definitions and terminology for this paper. Section 3 presents the previous work on sequential equivalence and motivates why we need a stronger equivalence condition. Section 4 presents "safe replaceability" and how we use this for multi-level sequential resynthesis. Finally, we conclude with some initial experimental experience.

2 Terminology and Background

We now make precise the notion of a finite state machine and our model for sequential hardware. We also define classical notions of equivalence for states in a machine, and for machines.

Definition 1 A *deterministic Finite State Machine (DFSM) M* is a quintuple, $(Q, I, O, \lambda, \delta)$, where Q is the set of states, I is the set of input values, O is the set of output values, λ is the output function, and δ is the next state function. The output function λ is a completely-specified function with domain $(Q \times I)$ and range O. The next state function is a completely-specified function with domain $(Q \times I)$ and range Q.

A hardware *design D* consists of a set of interconnected latches and gates, as illustrated in Figure 2. For the purposes of this paper, a design with n input wires, m output wires and t latches is characterized by an associated DFSM with state space $Q_D = \{0,1\}^t$, input space $I = \{0,1\}^n$, and output space $O = \{0,1\}^m$; the next state and output functions are defined by the corresponding logic. We will routinely refer to the states in Q_D as the states of the design. I^* refers to the set of all finite input sequences.

We also use λ and δ to denote the output and next state functions on sequences of inputs. So, if $\pi = a_1 \cdot a_2 \cdot a_3 \cdots a_p \in I^p$ is a sequence of p inputs, these functions are recursively defined as

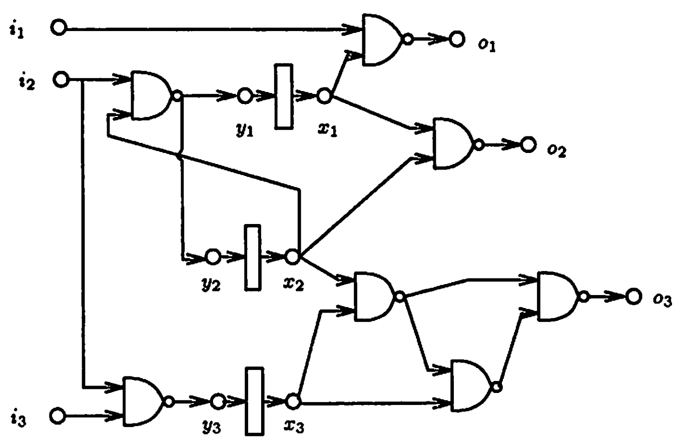

Figure 2: Gates + Latches = Sequential Network

$\lambda(s,\pi) = \lambda(s,a_1) \cdot \lambda(\delta(s,a_1),\pi')$ and $\delta(s,\pi) = \delta(\delta(s,a_1),\pi')$, where $\pi' = a_2 \cdot a_3 \cdots a_p$. Thus, the range-domain relationships are $\lambda : Q \times I^p \rightarrow O^p$ and $\delta : Q \times I^p \rightarrow Q$.

Two designs are said to be *compatible* if they have the same number of input and output wires. All notions of equivalence and replaceability developed in this paper are meaningful only for pairs of compatible designs. Henceforth, when talking about two different designs compatibility is assumed.

Definition 2 Given a design D_0, and states $s_0 \in Q_{D_0}$ and $s_1 \in Q_{D_1}$, state s_0 is *equivalent* to state s_1 ($s_0 \sim s_1$) if for any sequence of inputs $\pi \in I^*$, $\lambda_{D_0}(s_0,\pi) = \lambda_{D_1}(s_1,\pi)$. It can be easily shown that if $s_0 \sim s_1$, then for any input sequence $\pi \in I^*$, $\delta_{D_0}(s_0,\pi) \sim \delta_{D_1}(s_1,\pi)$.

The classical notion of equivalence between two DFSM's [HS66, page 23] is the following:

Definition 3 Two DFSM's M_1 and M_2 are *equivalent* ($M_1 \equiv M_2$) if for each state s in M_1 there is a state t in M_2 such that $s \sim t$, and for each state t in M_2 there is a state s in M_1 such that $s \sim t$.

3 Previous Work

In this section we describe the few known notions of sequential equivalence for circuits which do not have reset lines, and argue why these might cause unsafe replacements in some cases.

3.1 Sequential Hardware Equivalence (SHE)

Here we will briefly review the work presented in [Pix92] regarding equivalence between two gate-level hardware designs. When the design powers up, the state it powers up in cannot be predicted, and the desired input/output behavior is achieved from the design by driving a fixed synchronizing sequence of input vectors through the design after power-up.

Definition 4 Given a design D_0, a sequence of inputs $\pi \in I^*$ is called an *essential reset sequence* (or a *synchronizing sequence*) for the design if for any pair of states $s_0, s_1 \in Q_{D_0}$, $\delta_{D_0}(s_0, \pi) \sim \delta_{D_0}(s_1, \pi)$. A state $s \in Q_{D_0}$ is called an *essential reset state* if there exists a state $s_0 \in Q_{D_0}$ and a synchronizing sequence π such that $\delta(s_0, \pi) \sim s$. A design which has an essential reset state is called *essentially resettable.*

Definition 5 Given two designs D_0 and D_1, a state pair $(s_0, s_1) \in Q_{D_0} \times Q_{D_1}$ is *alignable* if there is a sequence of inputs $\pi \in I^*$ such that $\delta_{D_0}(\pi, s_0) \sim \delta_{D_1}(\pi, s_1)$. The sequence π is called an *aligning sequence.*

The following definition defines the notion of sequential hardware equivalence.

Definition 6 Designs D_0 and D_1 are *equivalent* ($D_0 \approx D_1$) if all state pairs are alignable.

Theorem 3.1 $D_0 \approx D_1$ if and only if there is a single (but not necessarily unique) aligning sequence that aligns all state pairs in $Q_{D_0} \times Q_{D_1}$.

Now we argue why the notion of SHE does not work for safe replacement of sequential designs.

From Theorem 3.1, two designs are considered equivalent if there exists a universal aligning sequence. This sequence is a synchronizing sequence for either design. However, in the design process, often the designers do not know the synchronizing sequence for their designs. Even if they can determine such a sequence π for a design, it may not be possible for the environment to generate π. So, for a safe replacement we need to preserve all initializing sequences, and not just one. In that case the one used being used by the environment will be preserved.

The notion of SHE does not place any constraints on the outputs of the designs during the synchronization phase. However, we claim that this condition is too weak for a safe replacement.

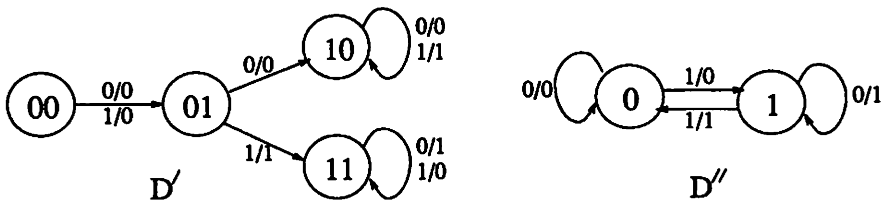

Figure 3: Examples of two designs which do not have any synchronizing sequences

A priori, we cannot assume that the external environment is not sensitive to the outputs during the synchronization phase. This is especially important because there may be another interacting design whose synchronizing sequence may be driven by an output of design D_0. Thus affecting the outputs of D_0 during synchronization may destroy that synchronizing sequence.

Finally, the notion of SHE does not work for designs which are not essentially resettable (such a design is not even equivalent to itself because it does not have an aligning sequence with itself). For example, the design D' in Figure[1] 3 is not equivalent to itself because the state pair $(10, 11)$ is not alignable. However, we can imagine at least two classes of real designs which are not essentially resettable. First, if the environment has some flexibility for the input/output behavior it can accept from the design, the design may have multiple steady-state behaviors (for example, design D' in Figure 3). In this example, the environment has a don't care condition so that the design is acceptable as long as it always toggles the input (state 11) or always outputs the input (state 10), after the synchronization phase. For the second class, consider the design D'' in Figure 3. It can be seen that there is no synchronizing sequence for this design, and hence this design is not essentially resettable. However, once the design powers up, its state can be determined from its outputs, and based on the outputs the design can be driven to state 0. Thus, the behavior of this design can be controlled.

[1]We frequently represent designs by state transition graphs (STG's). A t-bit binary-valued label on a state denotes that, in the design, the state is implemented by that assignment of the t latches. Notice that because a combinational function can be implemented in many different ways, the design-to-STG transformation is a many-to-one mapping.

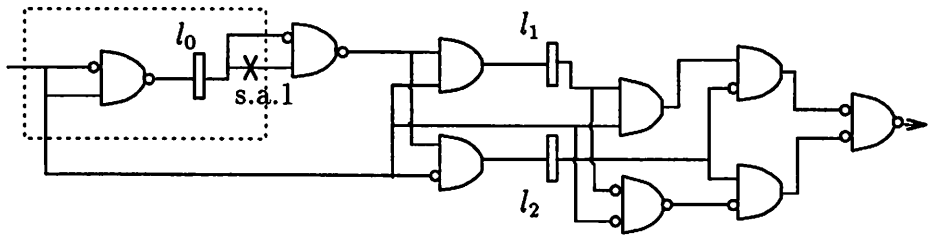

Figure 4: An irredundant stuck-at-fault for a circuit is redundant for a sub-circuit

3.2 Redundancy Removal for Circuits with no Reset Lines

Here we briefly describe the sequential equivalence condition used by Cheng [Che93] for resynthesis of circuits by removing redundant lines from the circuits. The basic idea is to check if the input/output "behavior" of the circuit is acceptable even after an internal line has been set to 0 or 1. If so, then the line can be replaced by a constant, and the circuit simplified.

Definition 7 A fault is *sequentially redundant* if for any input sequence, any output line and any state of the faulty circuit D_1, the circuit D_1 produces 1 (0) whenever the original circuit D_0 produces 1 (0) from all states of D_0. If D_0 produces an unknown output U on some input sequence (i.e. 1 from at least one power-up state and 0 from at least another) then D_1 is allowed to produce either 0, 1 or U on that input sequence.

If a fault is sequentially redundant, the circuit may be replaced by the faulty circuit, thereby simplifying the design. While the condition in Definition 7 makes sense for resynthesis of a single machine in isolation (because the new design is restricted to produce the same output as the original design if the output is deterministic), in hierarchical resynthesis, the condition can cause unacceptable (unsafe) replacements.

Consider the gate-level design shown in Figure 4. This circuit produces a 1 if and only if the inputs over the last two clock cycles are identical (the output on the first cycle is arbitrary). Suppose we select a window in the design (shown by the circuit inside the dotted rectangle) and resynthesize this sub-circuit. It is easily seen that the stuck-at-1 fault is sequentially redundant for this sub-circuit. However, for the faulty circuit, if the design of Figure 4 powers up in state ($l_0 = 0, l_1 = 0, l_2 = 0$) and input sequence $1 \cdot 1$ is provided, it produces a 0 at the second clock

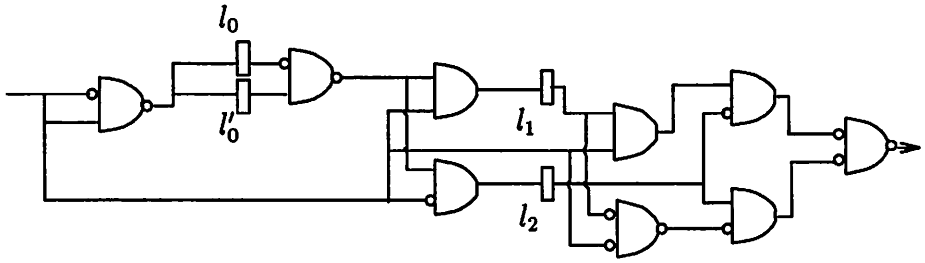

Figure 5: Retiming a latch across a fanout

cycle (the initial design outputs a 1). This motivates the need for a safe replacement condition— a condition so that the environment does not see any new input/output behavior after the replacement.

In this paper, we consider the more general problem of modifying the internal nodes of a circuit arbitrarily so that the "behavior' of the modified circuit is acceptable according to our safe replacement criterion. In Section 4.7, we show that setting the internal node input lines to constants and verifying the validity of the modified design is a special case.

3.3 Retiming and Resynthesis

Retiming and resynthesis [MSBS91] can be used to perform sequential optimization by alternating steps of moving of latches across combinational logic (retiming) and performing combinational resynthesis.

Retiming seems to be able to work if latches do not have reset lines. However, consider once again the circuit in Figure 4. If we retime this circuit to the circuit in Figure 5, we observe that a power-up state ($l_0 = 0, l_0' = 1, l_1 = 0, l_2 = 0$) produces a 0 on input sequence $1 \cdot 1$, whereas no power-up state in the original design exhibits this behavior. So the reason given in Section 3.2, for searching for a new safe replacement condition, applies here as well.

3.4 Synchronous Relations

Damiani and De Micheli [DD92] proposed using synchronous recurrence equations (or synchronous relations) to capture don't care information in sequential circuits. Since exact synchronous relation minimization is a hard problem, a heuristic algorithm is provided in [SWB93].

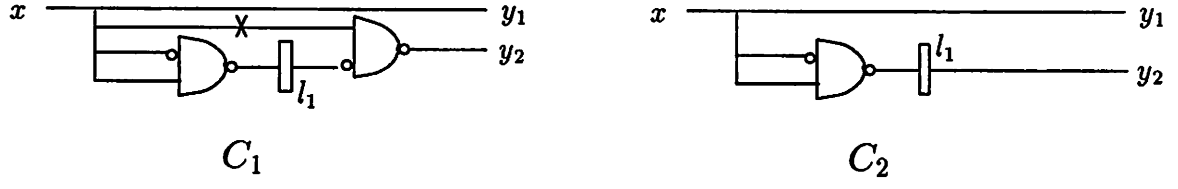

Figure 6: Logic optimization using synchronous relations

$(\mathbf{x}^1, \mathbf{x}^2)$	$(\mathbf{y}^1)$
(0,0)	{(01)}
(0,1)	{(11)}
(1,0)	{(01)}
(1,1)	{(11)}

Figure 7: Synchronous relation expressing flexibility for sequential design

A synchronous relation expresses the flexibility for a sub-circuit in a sequential gate-level design as a Boolean relation on finite sequences of inputs and outputs. Although the synchronous relation does not depend on a designated start state, the start state has to be taken into account as a post-processing step.

For a design without reset lines, we can construct an example where two designs satisfy the same synchronous relation but a state of one design may exhibit some behavior exhibited by no state of the other design. Construct the original design C_1 shown in Figure 6. The synchronous relation that expresses all the flexibility for this circuit is shown in Figure 7. Notice that, in the figure, $\mathbf{x} = x$ represents the input line; $\mathbf{x}^1$ represents input at the current clock cycle and $\mathbf{x}^2$ represents the value of the input at the previous clock cycle. Similarly, $\mathbf{y} = y_1 y_2$ represents the output wires, and $\mathbf{y}^1$ represents the value of the outputs at the current clock cycle. Also, notice that since we are expressing the flexibility of a design in isolation (the environment is null), there is exactly one output sequence allowed for each possible input sequence; when synchronous relations are used to express the flexibility for a sub-design which lies in a larger design, there are often multiple choices for each input sequence (see [SWB93] for an example). For the synchronous relation shown in Figure 7, another design which satisfies the relation is design C_2 shown in Figure 6. However, consider the

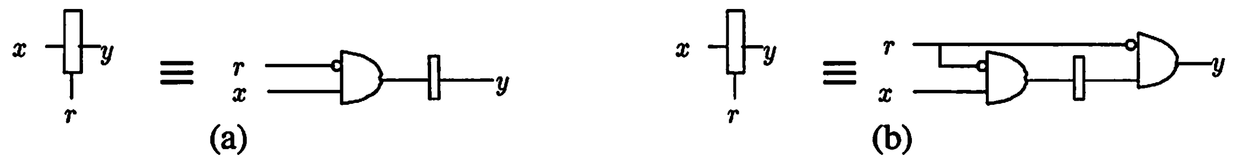

Figure 8: Replacing reset-latches with no-reset-latches (a) synchronous reset latch, (b) asynchronous reset latch

input sequence 0. For this input sequence, the original design C_1 outputs 01 (from both power-up states of l_1). However, design C_2 outputs 00 for the same input sequence if the latch powers up in state 0. So, using synchronous relations for minimization for designs without reset lines might change the input/output behavior of a design. In fact, even Cheng's redundancy removal condition from Section 3.2 would not allow this replacement— circuit C_2 can be obtained from circuit C_1 if the marked fault is a stuck-at-0 fault; however, this fault is not sequentially redundant from Definition 7 because on input 0, design C_1 produces 01 whereas design C_2 produces $0D$.

4 Safe Replaceability

4.1 Reset Line as Another Input

First, we digress and show that if some latches in a design have a reset line, they can be modeled by a latch without a reset line if we treat the reset line as another primary input. This modeling is well-known and we describe it here for the sake of completion.

There are two kinds of reset latches: synchronous, where the latch output is reset in the clock cycle after the reset line is activated; asynchronous, where the latch output is immediately reset. We will consider the case when pulling the reset line high (1) sets the output of the latch to be 0. The other three combinations of setting/resetting the latch by pulling the reset line high/low can be modelled similarly. Figure 8 illustrates the transformation for the case of synchronous and asynchronous reset latches.

Henceforth, in the sequel, we will assume that no latch in a design has a reset line.

4.2 Safe Replacement Condition

We want a condition for safe replacement which guarantees that if we replace an old design with a new one, it is impossible for any environment to detect that the replacement has been made. Conversely, we would like all replacements that cannot be detected by any environment to satisfy our condition. Since it cannot be predicted which state the design powers up in, we can safely assume that no matter which state the original design powers up in, the subsequent input/output behavior of the design is acceptable to the environment. Based on this observation, we give the following condition (the *safe replacement condition*):

Definition 8 Design D_1 is a *safe replacement* for design D_0 ($D_1 \preceq D_0$) if given any state $s_1 \in Q_{D_1}$ and any finite input sequence $\pi \in I^*$, there exists some state $s_0 \in Q_{D_0}$ such that the output behavior $\lambda_{D_1}(s_1, \pi) = \lambda_{D_0}(s_0, \pi)$.

We argue that the above condition provides maximum flexibility while guaranteeing that the replacement cannot be detected by the environment. First, if we make the above condition any weaker, then there exists an input sequence π and a state in the new design D_1 so that if the D_1 powers up in this state and sees the sequence π, it will produce a behavior which could not have been seen from any state in D_0. This violates our requirement that no environment should be able to detect the replacement. Secondly, since we have assumed that the power-up state of a design cannot be predicted, if $D_1 \preceq D_0$, then for every input sequence any power-up state of D_1 behaves like some power-up state of D_0. This implies that any behavior from any state of D_1 is acceptable. Thus our condition guarantees that replacing D_0 by D_1 cannot be detected by any environment.

Any design which has the same state transition graph as the original design trivially satisfies the above condition. As a non-trivial example consider designs D_0 and D_1 in Figure 9, where $D_1 \preceq D_0$. States 00, 11 and 01 in D_1 behave like states 000, 011 and 101, respectively, in D_0 for all input sequences. The remaining state 10 in D_1 behaves like state 010 for all input sequences starting with 0, and like state 101 for all input sequences starting with 1. Notice that state 10 in D_1 is not equivalent to any state in D_0; conversely, no state in D_1 is equivalent to state 001 in D_0. Definition 8 guarantees that there is no input/output behavior in D_1 which is not present in D_0. However, state 001 in D_0 outputs sequence $1 \cdot 1 \cdot 0$ on the input sequence $1 \cdot 1 \cdot 1$ whereas no state of D_1 can exhibit

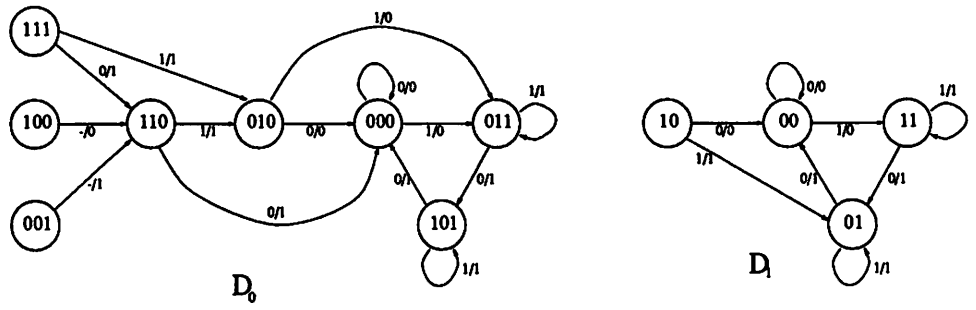

Figure 9: Example of a safe replacement

this behavior. This apparent paradox can be explained by the observation that since it is not true that every power-up state of D_0 exhibits this behavior, the environment of D_0 could not possibly depend on this behavior, and hence it cannot always expect the output sequence for $1 \cdot 1 \cdot 0$ for the input use $1 \cdot 1 \cdot 1$ each time the design powers up.

Definition 9 Given a design D, a set of states $S \subseteq Q_D$ is a *closed set* if for any input $a \in I$, any state $s \in S$: $\delta_D(s, a) \in S$.

Definition 10 A *terminal strongly connected component (tSCC)* of a design D is a closed set of states $S \subseteq Q_D$ such that for every pair of states $s_0, s_1 \in S$: there exists an input sequence $\pi \in I^*$ such that $\delta_D(s_0, \pi) = s_1$,

We have shown other properties of safe replacement in [SP94]:

- The relation $\preceq$ is transitive and reflexive, but not symmetric.
- A replacement design can have fewer or more latches than the original design (in Figure 9, D_0 has 3 latches whereas D_1 has 2).
- Unlike sequential hardware equivalence [Pix92], safe replaceability also applies to a design which does not have any synchronizing sequence.
- If $D_1 \preceq D_0$, every synchronizing sequence for D_0 is a synchronizing sequence for D_1 as well.
- If $D_1 \preceq D_0$, then every tSCC in D_1 must be equivalent (by Definition 3) to a tSCC in D_0.

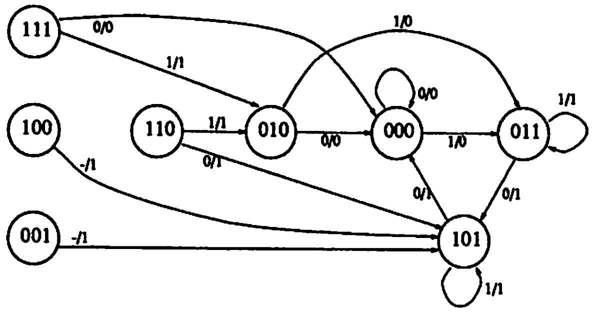

Figure 10: Design D_2 (a safe replacement for D_0)

4.3 Flexibility for Sequential Synthesis

We want to exploit the flexibility provided by the safe replacement condition in Definition 8 to optimize synchronous sequential circuits. Unfortunately, Definition 8 does not directly provide a closed form expression to express all the flexibility for safe replacement.

A sequential gate-level design can be viewed as a connection between a purely combinational part and a set of latches (Figure 2). The inputs to the combinational part are the real primary outputs of the design $\vec{i}$ plus the wires from the latches, or the present state vector, denoted by $\vec{x}$. The outputs of the combinational part are the real primary outputs of the design $\vec{o}$ plus the wires to the latches, or the next state vector, denoted by $\vec{y}$. We want to optimize this combinational part while maintaining the safe replacement condition. If we can express the flexibility in Definition 8 by a Boolean relation in $(\vec{i}, \vec{x}, \vec{o}, \vec{y})$, we can use known techniques [SB91] for minimizing multi-level networks given a Boolean relation, in terms of the inputs and outputs of the network.

Unfortunately, the flexibility allowed by the safe replacement condition cannot be represented by a Boolean relation between the domain space $(\vec{i}, \vec{x})$ and the range space $(\vec{o}, \vec{y})$. Consider the design D_2 in Figure 10 which is a safe replacement of the design D_0 of Figure 9. The two designs differ on their mappings of the following 6 points in $(\vec{i}, \vec{x})$: $(0,111), (0,100), (1,100,1), (0,001), (1,001), (0,110)$. One property of Boolean relations is that the flexibility for each point in the domain space is independent of other points [SSB93]. So, if the flexibility for safe replacement could be expressed by a Boolean relation, then every design corresponding to a flexibility choice for each of these 6 domain points would be a valid replacement (there are 2^6 such designs). In particular, design D_3

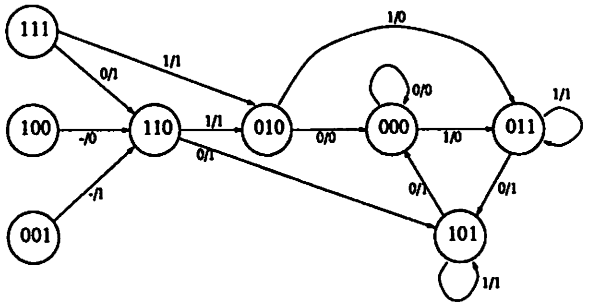

Figure 11: Design D_3 (an unsafe replacement for D_0)

in Figure 11, which behaves like D_2 on point $(0, 110)$ and like D_0 on the other points, would be a safe replacement. However, this is not so because if design D_3 powers up in state 111 and is given the input sequence $0 \cdot 0 \cdot 0$ it produces the output sequence $1 \cdot 1 \cdot 1$, whereas there is no state in D_0 which exhibits this behavior. Thus the flexibility for safe replaceable designs with the same number of latches cannot be expressed as a Boolean relation in $(\vec{i}, \vec{x}) \times (\vec{o}, \vec{y})$. One way to represent such flexibility would be through Multiple Boolean Relations [SSB93], which are arbitrary sets of Boolean relations.

4.4 Sufficient Condition for a Safe Replacement

As we argued in the last section, the complete flexibility for safe replacement can be expressed by a multiple Boolean relation. However, because of the intractably large solution space of multiple Boolean relations, there are no known general techniques to use multiple Boolean relations for logic synthesis. We now provide a sufficient (but not necessary) condition for safe replacement, from which we will obtain a Boolean relation in $(\vec{i}, \vec{x}, \vec{o}, \vec{y})$ to express partial flexibility for safe replacement.

Proposition 4.1 Given designs D_0 and D_1 such that for every state $s_1 \in Q_{D_1}$ and input $a \in I$, there exists a state $s_0 \in Q_{D_0}$ such that $\lambda_{D_1}(s_1, a) = \lambda_{D_0}(s_0, a)$ and $\delta_{D_1}(s_1, a) \sim \delta_{D_0}(s_0, a)$. Then $D_1 \preceq D_0$.

Proof: Choose any state $s_1 \in Q_{D_1}$, and any input sequence $\pi = a_0 \cdot a_1 \cdots a_p \in I^*$. Now, there exists a state $s_0 \in Q_{D_0}$ such that $\lambda_{D_1}(s_1, a_0) = \lambda_{D_0}(s_0, a_0)$ and $\delta_{D_1}(s_1, a_0) \sim \delta_{D_0}(s_0, a_0)$. Thus $\lambda_{D_1}(s_1, \pi) = \lambda_{D_0}(s_0, \pi)$, and hence $D_1 \preceq D_0$. ∎

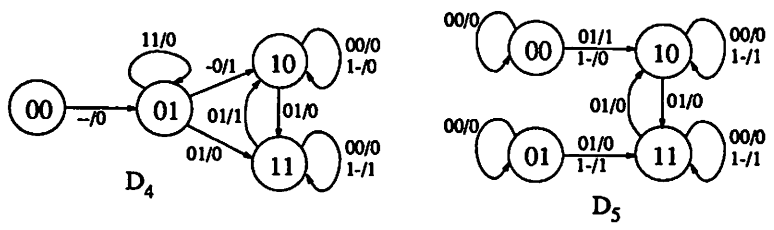

Figure 12: Example of a safe replacement

The above result is not a necessary condition for safe replacement. For example, consider the designs D_4 and D_5 in Figure 12. It can be seen that $D_5 \preceq D_4$. However, in design D_5 state 01 goes to state 01 on input 01, and no state in design D_4 is state equivalent to state 01 on design D_5. On the other hand, designs D_0 and D_1 of Figure 9 which satisfy the sufficient condition of Proposition 4.1, and thus $D_1 \preceq D_0$.

4.5 Synthesis for Safe Replaceability

We will use the sufficient condition in Proposition 4.1 to derive a method to extract and use flexibility for sequential resynthesis.

First, note that a necessary condition for safe replacement is that every tSCC in the new design must be equivalent to a tSCC in the old design. A tSCC can be thought of as defining a steady state behavior of the design. So at the state-transition level we cannot alter the behavior of the states in some tSCC of the original design. For our synthesis method we will choose a set of states which is closed under all inputs, called the *core*:

Definition 11 Given a design D, a set of states $S \subseteq Q_D$ is called a *core* of the design if it is a closed set under all inputs, i.e. for any input a and any state $s \in S$: $\delta_D(s, a) \in S$.

We will preserve the behavior of the core during resynthesis, and in order to make resynthesis tractable, we will preserve the encodings of the states in the core. Note that since the core is closed under all inputs it contains a tSCC of the original design and thus satisfies the necessary condition discussed above.

Proposition 4.1 indicates that each state reachable from some state in D_1 is equivalent to some state in D_0. The set of these states will serve as the core of the old design, which we will reproduce in the new design. We require that each of the remaining states in the new design satisfy the following Boolean relation $\mathcal{P}(\vec{i},\vec{o},\vec{y})$. In the following, $core(\vec{x}) = 1$ if and only if state $\vec{x}$ lies in the chosen core.

$$\mathcal{P}(\vec{i},\vec{o},\vec{y}) \quad = \quad core(\vec{y}) \wedge \exists \vec{x}_0[(\lambda_{D_0}(\vec{x}_0,\vec{i}) = \vec{o}) \wedge (\delta_{D_0}(\vec{x}_0,\vec{i}) = \vec{y})] \tag{1}$$

It is easy to see that if the core of the old design is preserved and the above condition holds for the remaining states of the new design, the sufficiency condition of Proposition 4.1 is satisfied

Using the relation $\mathcal{P}$ we can form a Boolean relation $\mathcal{R}(\vec{i},\vec{x},\vec{o},\vec{y})$ which expresses the flexibility for the entire network including states inside the core:

$$\mathcal{R}(\vec{i},\vec{x},\vec{o},\vec{y}) = [\ core(\vec{x}) \wedge (\vec{y} = \delta_{D_0}(\vec{x},\vec{1})) \wedge (\vec{o} = \lambda(\vec{x},\vec{i}))] \ \vee \ [\neg(core(\vec{x})) \wedge \mathcal{P}(\vec{i},\vec{o},\vec{y})] \tag{2}$$

We recall from Section 4.3 that the total flexibility for the network cannot be expressed by a Boolean relation; we are able to get a relation here because our condition in Proposition 4.1 is only a sufficient condition.

4.6 Choice of Core

For a given design there may be many choices for the core which satisfy Definition 11. Some natural choices are:

- The set of all states Q_{D_0}.
- Any onion ring [Pix90] of the design. Onion rings $A_1, A_2, \ldots$ are defined recursively:

$$\begin{aligned} A_1 &= Q_{D_0}, \\ A_{k+1} &= \{y \mid \exists i \in I, x \in A_k : \delta_{D_0}(x,i) = y\} \end{aligned} \tag{3}$$

For design D_4 in Figure 12, $A_1 = \{00,01,10,11\}, A_2 = A_3 = \cdots = A_\infty = \{01,10,11\}$. A_∞ is also called the outer envelope of a design. The outer envelope is computable by a fixed-point computation starting from Q_{D_0}.

- Any tSCC of the design. Design D_4 has only one tSCC: $\{10, 11\}$.

Any of the above choices satisfies Definition 11 and can be used in equation (2). The ideal choice is a small core to give us a large number of states outside the core because we have flexibility only in modifying the behavior of states outside the core. The smallest tSCC is the smallest set which qualifies as a core.

However, we are restricted by the requirement that the starting design must itself satisfy the Boolean relation $\mathcal{R}$. The only known method for minimizing multi-level networks under flexibility expressed by a Boolean relation [SB91] requires this restriction, as we shall see later in Section 4.7.

For example, if we choose the tSCC of design D_0 in Figure 9 (states 000, 011 and 101) as the core, the design D_0 does not satisfy relation $\mathcal{R}$ in expression (2) because the state 111 (a non-core state) does not jump to a state inside the core on input 1 and hence does not satisfy $\mathcal{P}$. Choices of core that guarantee that the given design satisfies $\mathcal{R}$ are Q_{D_0} (the set of all states) and the second onion ring A_2 (the set of states reachable in one step from Q_{D_0}). The former does not give any flexibility because all states are in the new design; so we make the latter choice. While it might seem that we lose much flexibility by having to choose a much larger core than the smallest possible, our experiments in Section 5 indicate that choosing A_2 gives us most of the flexibility for most of the examples.

4.7 Multi-level Synthesis

Previous sections referred to a *multi-level* combinational logic network that computes the next states and outputs of a sequential design. More precisely, the *Boolean network* $\mathcal{N}$ associated with a sequential circuit is a directed acyclic graph such that for each node in $\mathcal{N}$, there is a Boolean variable u_i and an associated Boolean function f_i such that $u_i = f_i$. The *support* of f_i is the set of variables corresponding to the immediate fanins of the node. The primary input variables $\{i_1, i_2, \ldots, i_n, x_1, x_2, \ldots, x_t\}$ correspond to the inputs and present states of the sequential circuit; the primary output variables $\{o_1, o_2, \ldots, o_m, y_1, y_2, \ldots, y_t\}$ correspond to the outputs and next states. *Intermediate nodes* are those which do not correspond to inputs or outputs. The network computes a function from the input space B^{n+t} to the output space B^{m+t} derived by composing the functions at the intermediate nodes.

Since hardware designs typically arise by composing small modules, it is very natural for circuits to have a multi-level structure. The nodes of the corresponding Boolean network represent the logical functionality of the modules. It has been observed that the area of the hardware implementation of a design is strongly correlated to the total number of literals in the *factored form* [BBH+88] representation of the functions at the logic nodes. Thus minimizing the function (with respect to the literal count) at the node constitutes a powerful synthesis technique.

At any intermediate node of a network there is a local function $f_i : B^r \rightarrow B$, where r is the cardinality of the support. *Node simplification* is the process of optimizing a Boolean network by using don't cares in conjunction with a two level minimizer [BHMS84] to optimize the functions at the nodes. These don't cares arise in several ways:

- Because of the structure of the network, only a certain subset of B^r may be generated by assignments to the inputs. This gives rise to *satisfiability don't care* (SDC) points for f_i [BBH+88].

- For certain input assignments, the values taken by the primary outputs of $\mathcal{N}$ may be independent of the function computed by a node; these are *observability don't care* points (ODC) for that node [SBT91].

- For certain input assignments the functionality of the node can be changed without destroying safe replaceability; this flexibility leads to the *replaceability don't cares* points (RDC).

The ODC at a node u can be computed by considering the output α_u of the node to be another input; thus the primary outputs of $\mathcal{N}$ are expressed in terms of the primary inputs and α_u. The ODC is the set of points in B^r where no primary output of $\mathcal{N}$ depends on α_u.

Let $\mathcal{R}(\vec{i}, \vec{x}, \vec{o}, \vec{y})$ be a Boolean relation expressing all the flexibility in the choice of combinational logic for a sequential circuit. Cerny and Marin [CM77] demonstrate a close relationship between optimizing a Boolean network with respect to a given Boolean relation, and computing observability don't care sets. The starting network $\mathcal{N}$ must satisfy the relation $\mathcal{R}$. The relation can be viewed as a single node with inputs $\vec{i}, \vec{x}, \vec{o}, \vec{y}$; this node is referred to as the *observability node*. Composing

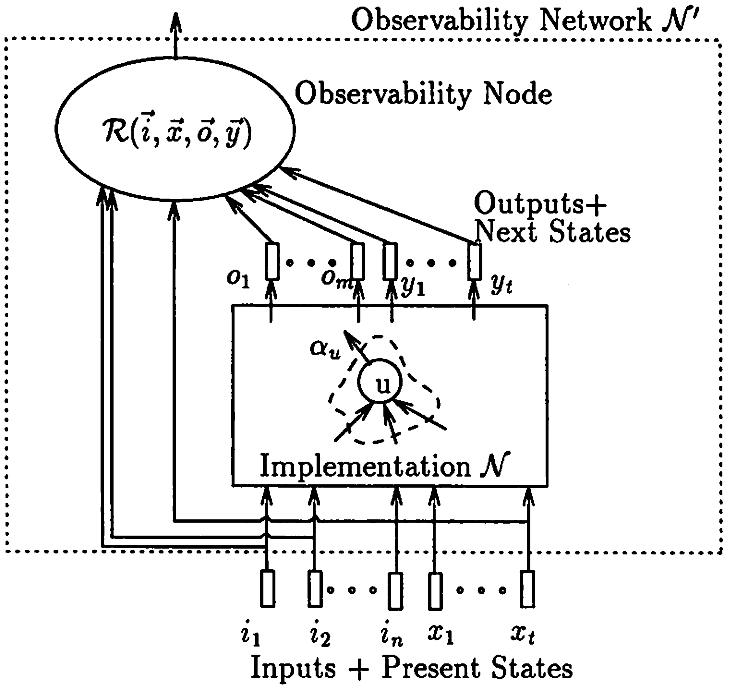

Figure 13: ODC's from the Observability Network yield flexibility under Observability Relation for nodes in Implementation Network.

this node with the network as shown in Figure 13 yields an *observability network* $\mathcal{N}'$. It is shown in [CM77, SB91] that all the don't cares that can be used to optimize the nodes in $\mathcal{N}$ are derivable from the ODC of the node in the network $\mathcal{N}'$.

In our scenario, the relation $\mathcal{R}(\vec{i},\vec{x},\vec{o},\vec{y})$ is given by equation (2) on page 16, with $core(\vec{x})$ being the set A_2 as defined in equation (3) on page 16. As discussed in section 4.6, for this choice of *core*, the combinational logic network associated with the initial design is an implementation for $\mathcal{R}(\vec{i},\vec{x},\vec{o},\vec{y})$. Using $\mathcal{R}$ as the observability node guarantees that, for any other internal node, the ODC derived from the observability network contains the RDC for the original network.

We use Binary Decision Diagrams (BDD's) to represent the design, flexibility relation, and core. There is a variable associated with each primary input and each primary output; for each latch there is a present state and next state variable. Let u be a node in the design for which the ODC is to computed. We add a new BDD variable α_u corresponding to the output of u, and generate

BDD's for the next state and output functions in terms of the primary inputs, latch outputs, and α_u. These are composed with the flexibility relation to obtain the BDD for the function computed by the observability network. Let $f(\vec{i}, \vec{x}, \alpha_u)$ be the output of the observability network; then the ODC for node u is given by $f(\vec{i}, \vec{x}, \alpha_u = 1)f(\vec{i}, \vec{x}, \alpha_u = 0) + \bar{f}(\vec{i}, \vec{x}, \alpha_u = 1)\bar{f}(\vec{i}, \vec{x}, \alpha_u = 0)$. This is in terms of primary inputs; we then project this set into the space comprised of the fanins of the node [SBT91]. These are used in conjunction with a subset of the satisfiability don't care set to optimize the function at u.

We are computing all inputs under which the outputs are independent of the function computed at the node. Thus we will detect cases where an internal line (which is an input to a node) can be set to a constant while maintaining compatibility with relation $\mathcal{R}$. This means that we automatically remove redundant faults (which satisfy $\mathcal{R}$) from the circuit. Note that we are able to detect these redundancies because we are computing the flexibility of each node just before minimizing it; if we had obtained compatible flexibility (as in [SB91]) for all nodes before minimizing them simultaneously we would not be able to claim this. The price we pay is in time: we need to simplify nodes on an individual basis, and if the node is simplified, potentially all the BDDs for functions that the node fans out to must be recomputed.

5 Experiments

We have implemented the above method for sequential resynthesis presented in this paper in the SIS sequential synthesis system [SSM+92]. We used BDD's to represent all sets and functions and to perform all the set manipulations implicitly. We have performed experiments on the ISCAS89 benchmark suite (from **s344** to **s1494**). Since some ISCAS benchmarks are very minor variations of each other and give almost identical results, we chose the largest example (for example, **s1288** represents **s1288** and **s1196**; **s444** represents **s444**, **s400** and **s382**, etc.) for each class.

We report our experiments in Table 1. First observe that, for many examples, the size of the core (the second onion ring A_2) is close to the size of the tSCC (each of the examples has exactly one tSCC) when compared to the total number of states (2^L, where L is the number of latches).

Since we are minimizing the network one node at a time, very small nodes are unlikely to yield much optimizations. The node sizes of the benchmark circuits were very small; we executed the SIS commands `sweep; eliminate 10` to partially collapse the network. For some benchmarks, a totally collapsed network had a smaller literal count than a partially collapsed one; for these circuits, we started with the totally collapsed network (using command `sweep; collapse`).

The table reports the reduction in the total number of literals of the network. We have partitioned the literal reduction into reductions due to satisfiability don't cares (SDC), observability don't cares (ODC) and replaceability don't cares (RDC) separately. We minimized each internal nodes three times: using SDC, using (SDC + ODC), using (SDC + ODC + RDC). The literal reductions under the ODC column are reductions in addition to those under the SDC column; those under the RDC column are reductions in to those under the SDC + ODC columns. Note that the literal savings under the RDC column, for example, does not indicate the savings due to the safe replaceability don't cares; it is actually the difference in the savings using (SDC + ODC + RDC) and (SDC + ODC). We have observed that a lot of the literal saving is common to all three methods: SDC, ODC and RDC. So a 0 in the RDC column might indicate that most of the flexibility due to RDC is already captured by SDC and ODC. However, the CPU times reported in the table under the three columns represent the total time taken for each method separately.

It is interesting to compare the RDC statistics to the ODC statistics because while ODC provides observability don't cares for an internal node in terms of the primary inputs, RDC provides safe replaceability don't cares in addition to the observability don't care points. Then we project these don't cares to the immediate fan-ins of the node using the same techniques used for projecting ODC points [SBT91]. We observe that for some examples, ODC gives no literal reductions beyond SDC alone but RDC is able to obtain additional, though modest, reductions. These reductions are of the order of 5% on these circuits. On other circuits RDC gives no additional improvements over SDC and ODC. For these examples, most replaceability don't care points may be overlapping with satisfiability and observability don't care points. Except for 2 examples, the CPU time taken by RDC flexibility is of the same order as the time taken to utilize the SDC and ODC flexibility.

ISCAS89 benchmarks may not constitute a good source of examples to judge the potential of our approach. This is because for many of the circuits, collapsing the logic to two levels before applying our minimization yields a smaller circuit, thus negating the whole basis of doing multi-level logic

Ckt.	I/O/L	#states		#literals		Savings (in #literals)			Time (in seconds)		
		tSCC	core	start	end	SDC	ODC	RDC	SDC	ODC	RDC
s349	9/11/15	1487	23232	173	157	9	7	0	0.57	1.40	123.89
s386	7/7/6	13	13	205	138	53	0	14	0.83	1.03	1.83
s444	3/6/21	8864	23740	236	171	50	15	0	0.76	1.56	4.71
s510	19/7/6	47	61	307	255	52	0	0	1.97	2.35	3.17
s526	3/6/21	8868	401460	323	233	79	0	11	6.32	6.61	10.80
s713	35/23/19	1544	6663	285	timeout after 10000 sec						
s832	18/19/5	25	25	470	351	110	0	9	3.04	4.18	12.60
s953	16/23/29	504	504	700	597	78	20	5	3.85	17.14	37.56
s1238	14/14/18	2615	2652	882	636	98	148	0	14.74	176.26	1075.49
s1494	8/19/6	48	48	896	542	353	0	1	26.81	34.97	58.17

Table 1: Experimental results. I/O/L denotes the number of inputs, outputs and latches. The savings reported used ODC are in addition to those under SDC; those reported under RDC are in addition to those reported under (SDC+ODC). The sum of these three columns is the difference between the starting and ending literal count.

minimizations. Furthermore, the average node size is too small to hope for any significant reduction over that given by the SDC. Hence the merit of our approach may be better judged on the basis of real multi-level designs. We are in the process of arranging to test our implementation on industrial gate-level designs.

Memory explosion is a common problem with BDD's. in the problem size. For our experiments we noted that the ability to finish the examples (and the time taken) was most influenced by the number of input wires to the design. The number of latches and the number of output wires are also a factor, though to a lesser degree. Since large designs routinely arise as set of interacting components, it is natural to decompose the design into smaller components and synthesize them independently. Intuitively, the components being smaller, will be less complex, and hence easier to synthesize. We expect that our methods will be most useful in resynthesizing an arbitrary portion of a design without worrying about any interaction with its environment.

6 Conclusions and Future Work

We have provided a notion of safe replaceability ($\preceq$) that is independent of initial states of a design and the intended environment of a design. We have used this notion to provide a method for sequential resynthesis towards an area reduction of gate-level designs; our notion does not require us to preserve the state transition behavior of the design. We have implemented our algorithm using BDD's, and we expect to be able to test our algorithm on industrial-level designs.

The synthesis method presented in this paper is just one way of exploiting the flexibility allowed by the safe replacement condition. We are looking at other methods for sequential synthesis for this notion of sequential equivalence.

We would also like to be able to handle arbitrarily large netlists for our resynthesis methods. For this we are working on partitioning algorithms which decompose a network into modules so that the number of wires running across the modules is minimized. Fewer interconnection wires gives us two advantages: we can handle larger number of latches before we run into a BDD explosion problem, and we can expect fewer states in the core (and hence more flexibility) if we have fewer controlling input lines running to the modules. Furthermore, reducing the number of output lines restricts the observable output sequences which leads to larger observable don't cares.

References

[BBH+88] K. A. Bartlett, R. K. Brayton, G. D. Hachtel, R. M. Jacoby, C. R. Morrison, R. L. Rudell, A. L. Sangiovanni-Vincentelli, and A. R. Wang. Multilevel Logic Minimization Using Implicit Don't Cares. *IEEE Transactions on Computer-Aided Design of Integrated Circuits*, 7(6):723–740, June 1988.

[BCM90] C. Berthet, O. Coudert, and J. C. Madre. New Ideas on Symbolic Manipulation of Finite State Machines. In *Proc. Intl. Conf. on Computer Design*, October 1990.

[BHMS84] R. K. Brayton, G. D. Hachtel, C. T. McMullen, and A. L. Sangiovanni-Vincentelli. *Logic Minimization Algorithms for VLSI Synthesis.* Kluwer Academic Publishers, 1984.

[BT93] G. Berry and H. J. Touati. Optimized Controller Synthesis Using Esterel. In *Workshop Notes of Intl. Workshop on Logic Synthesis*, Tahoe City, CA, May 1993.

[Che93] K.-T. Cheng. Redundancy Removal for Sequential Circuits Without Reset States. *IEEE Transactions on Computer-Aided Design of Integrated Circuits*, 12(1):13–24, January 1993.

[CHS91] H. Cho, G. D. Hachtel, and F. Somenzi. Redundancy Identification and Removal Based on Implicit State Enumeration. In *Proc. Intl. Conf. on Computer Design*, pages 77–80, October 1991.

[CM77] E. Cerny and M. A. Marin. An Approach to Unified Methodology of Combinational Switching Circuits. *IEEE Transactions on Computers*, 27(8), 1977.

[DD92] M. Damiani and G. De Micheli. Synthesis and Optimization of Synchronous Logic Circuits from Recurrence Equations. In *Proc. European Conf. on Design Automation*, pages 226–231, March 1992.

[HS66] J. Hartmanis and R. E. Stearns. *Algebraic Structure Theory of Sequential Machines.* Intl. Series in Applied Mathematics. Prentice-Hall, Englewood Cliffs, N.J., 1966.

[LN91] B. Lin and A. R. Newton. Exact Redundant State Registers Removal Based on Binary Decision Diagrams. In *Proc. of the MCNC Intl. Workshop on Logic Synthesis*, volume 1, May 1991.

[LTN90] B. Lin, H. J. Touati, and A. R. Newton. Don't Care Minimization of Multi-level Sequential Logic Networks. In *Proc. Intl. Conf. on Computer-Aided Design*, pages 414–417, November 1990.

[MSBS91] S. Malik, E. M. Sentovich, R. K. Brayton, and A. L. Sangiovanni-Vincentelli. Retiming and Resynthesis: Optimization of Sequential Networks with Combinational Techniques. *IEEE Transactions on Computer-Aided Design of Integrated Circuits*, 10(1):74–84, January 1991.

[Pix90] C. Pixley. A Computational Theory and Implementation of Sequential Hardware Equivalence. In E. M. Clarke and R. P. Kurshan, editors, *Proc. of the Workshop on Computer-Aided Verification*, volume 3 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 293–320. American Mathematical Society, June 1990.

[Pix92] C. Pixley. A Theory and Implementation of Sequential Hardware Equivalence. *IEEE Transactions on Computer-Aided Design of Integrated Circuits*, 11(12):1469–1494, December 1992.

[SB91] H. Savoj and R. K. Brayton. Observability Relations and Observability Don't Cares. In *Proc. Intl. Conf. on Computer-Aided Design*, pages 518–521, November 1991.

[SBT91] H. Savoj, R. K. Brayton, and H. Touati. Extracting Local Don't Cares for Network Optimization. In *Proc. Intl. Conf. on Computer-Aided Design*, pages 514–517, November 1991.

[SP94] V. Singhal and C. Pixley. The Verification Problem for Safe Replaceability. In D. Dill, editor, *Proc. of the Conf. on Computer-Aided Verification*, Lecture Notes in Computer Science. Springer-Verlag, June 1994.

[SSB93] E. M. Sentovich, V. Singhal, and R. K. Brayton. Multiple Boolean Relations. In *Workshop Notes of the Intl. Workshop on Logic Synthesis*, Tahoe City, CA, May 1993.

[SSM+92] E. M. Sentovich, K. J. Singh, C. Moon, H. Savoj, R. K. Brayton, and A. L. Sangiovanni-Vincentelli. Sequential Circuit Design Using Synthesis and Optimization. In *Proc. Intl. Conf. on Computer Design*, pages 328–333, October 1992.

[SWB93] V. Singhal, Y. Watanabe, and R. K. Brayton. Heuristic Minimization of Synchronous Relations. In *Workshop Notes of Intl. Workshop on Logic Synthesis*, Tahoe City, CA, May 1993.