Complete Test Sets And Their Approximations

Eugene Goldberg
eu.goldberg@gmail.com

Abstract—We use testing to check if a combinational circuit $N$ always evaluates to 0 (written as $N \equiv 0$). We call a set of tests proving $N \equiv 0$ a complete test set (CTS). The conventional point of view is that to prove $N \equiv 0$ one has to generate a trivial CTS. It consists of all $2^{|X|}$ input assignments where $X$ is the set of input variables of $N$. We use the notion of a Stable Set of Assignments (SSA) to show that one can build a non-trivial CTS consisting of less than $2^{|X|}$ tests. Given an unsatisfiable CNF formula $H(W)$, an SSA of $H$ is a set of assignments to $W$ that proves unsatisfiability of $H$. A trivial SSA is the set of all $2^{|W|}$ assignments to $W$. Importantly, real-life formulas can have non-trivial SSAs that are much smaller than $2^{|W|}$. In general, construction of even non-trivial SSAs is inefficient. We describe a much more efficient approach where tests are extracted from an SSA built for a “projection” of $N$ on a subset of variables of $N$. These tests can be viewed as an approximation of a CTS for $N$. We give experimental results and describe potential applications of this approach.

I. INTRODUCTION

Testing is an important part of verification flows. For that reason, any progress in understanding testing and improving its quality is of great importance. In this paper, we consider the following problem. Given a single-output combinational circuit $N$, find a set of input assignments (tests) proving that $N$ evaluates to 0 for every test (written as $N \equiv 0$) or find a counterexample. We will call a set of input assignments proving $N \equiv 0$ a complete test set (CTS). We will call the set of all possible tests a trivial CTS. Typically, one assumes that proving $N \equiv 0$ involves derivation of the trivial CTS, which is infeasible in practice. Thus, testing is used only for finding an input assignment refuting $N \equiv 0$. We present an approach for building a non-trivial CTS consisting of a subset of possible tests. In general, finding even a non-trivial CTS for a large circuit is impractical. We describe a much more efficient approach where an approximation of a CTS is generated.

The circuit $N$ above usually describes a property $\xi$ of a multi-output combinational circuit $M$, the latter being the real object of testing. For instance, $\xi$ may state that $M$ never produces some output assignments. To differentiate CTSs and their approximations from conventional test sets verifying $M$ “as a whole”, we will refer to the former as property-checking test sets. Let $\Xi := \{\xi_1, \ldots, \xi_k\}$ be the set of properties of $M$ formulated by a designer. Assume that every property of $\Xi$ holds and $T_i$ is a test set generated to check property $\xi_i \in \Xi$. There are at least two reasons why applying $T_i$ to $M$ makes sense. First, if $\Xi$ is incomplete a test of $T_i$ can expose a bug, if any, breaking a property of $M$ that is not in $\Xi$. Second, if property $\xi_i$ is defined incorrectly, a test of $T_i$ may expose a bug breaking the correct version of $\xi_i$. On the other hand, if $M$ produces proper output assignments for all tests of $T_1 \cup \cdots \cup T_k$, one gets extra guarantee that $M$ is correct. In Section [V] we list some other applications of property-checking test sets such as verification of design changes, hitting corner cases and testing sequential circuits.

Let $N(X, Y, z)$ be a single-output combinational circuit where $X$ and $Y$ specify the sets of input and internal variables of $N$ respectively and $z$ specifies the output variable of $N$. Let $F_N(X, Y, z)$ be a formula defining the functionality of $N$ (see Section [III]). We will denote the set of variables of circuit $N$ (respectively formula $H$) as $\text{Vars}(N)$ (respectively $\text{Vars}(H)$).

Every assignment to $\text{Vars}(F_N)$ satisfying $F_N$ corresponds to a consistent assignment to $\text{Vars}(N)$ and vice versa. Then the problem of proving $N \equiv 0$ reduces to showing that formula $F_N \land z$ is unsatisfiable. From now on, we assume that all formulas mentioned in this paper are propositional. Besides, we will assume that every formula is represented in CNF i.e. as a conjunction of disjunctions of literals.

Our approach is based on the notion of a Stable Set of Assignments (SSA) introduced in [9]. Given formula $H(W)$, an SSA of $H$ is a set $P$ of assignments to variables of $W$ that have two properties. First, every assignment of $P$ falsifies $H$. Second, $P$ is a transitive closure of some neighborhood relation between assignments (see Section [II]). The fact that $H$ has an SSA means that the former is unsatisfiable. Otherwise, an assignment satisfying $H$ is generated when building its SSA. If $H$ is unsatisfiable, the set of all $2^{|W|}$ assignments is always an SSA of $H$. We will refer to it as trivial. Importantly, a real-life formula $H$ can have a lot of SSAs whose size is much less than $2^{|W|}$. We will refer to them as non-trivial. As we show in Section [III] the fact that $P$ is an SSA of $H$ is a structural property of the latter. That is this property cannot be expressed in terms of the truth table of $H$ (as opposed to a semantic property of $H$). For that reason, if $P$ is an SSA for $H$, it may not be an SSA for some other formula $H'$ that is logically equivalent to $H$. In other words, a structural property is formula-specific.

We show that a CTS for $N$ can be easily extracted from an SSA of formula $F_N \land z$. This makes a non-trivial CTS

---

1Term CTS is sometimes used to say that a test set invokes every event specified by a coverage metric. Our application of this term is quite different.

2That is $M$ can be incorrect even if all properties of $\Xi$ hold.

---

By an assignment to a set of variables $V$, we mean a full assignment where every variable of $V$ is assigned a value.

An assignment to a gate $G$ of $N$ is called consistent if the value assigned to the output variable of $G$ is implied by values assigned to its input variables.

An assignment to variables of $N$ is called consistent if it is consistent for every gate of $N$. 

---

arXiv:1808.05750v1 [cs.LO] 16 Aug 2018
a structural property of circuit $N$ that cannot be expressed in its truth table. Building an SSA for a large formula is inefficient. So, we present a procedure constructing a simpler formula $H(V)$ implied by $F_N \land z$ (where $V \subseteq \text{Vars}(F_N \land z)$) and building an SSA of $H$. The existence of such an SSA means that $H$ (and hence $F_N \land z$) is unsatisfiable. So, $N \equiv 0$ holds. A test set extracted from an SSA of $H$ can be viewed as a way to verify a “projection” of $N$ on variables of $V$. On the other hand, one can consider this set as an approximation of a CTS for $N$. We will refer to the procedure above as $\text{SemStr}$ (“Semantics and Structure”). $\text{SemStr}$ combines semantic and structural derivations, hence the name. The semantic part of $\text{SemStr}$ is used to derive $H$. Its structural part consists of constructing an SSA of $H$ thus proving that $H$ is unsatisfiable.

The contribution of this paper is fourfold. First, we introduce the notion of non-trivial CTSs (Section II). Second, we present a method for efficient construction of property-checking tests that are approximations of CTSs (Sections II and III). Third, we describe applications of such tests (Section IV). Fourth, we give experimental results showing the effectiveness of property-checking tests (Section VII).

II. STABLE SET OF ASSIGNMENTS

A. Definitions

We will refer to a disjunction of literals as a clause. Let $\vec{p}$ be an assignment to a set of variables $V$. Let $\vec{p}$ falsify a clause $C$. Denote by $\text{Nbhd}(\vec{p}, C)$ the set of assignments to $V$ satisfying $C$ that are at Hamming distance 1 from $\vec{p}$. (Here $\text{Nbhd}$ stands for “Neighborhood”). Thus, the number of assignments in $\text{Nbhd}(\vec{p}, C)$ is equal to that of literals in $C$. Let $\vec{q}$ be another assignment to $V$ (that may be equal to $\vec{p}$). Denote by $\text{Nbhd}(\vec{q}, \vec{p}, C)$ the subset of $\text{Nbhd}(\vec{p}, C)$ consisting only of assignments that are farther away from $\vec{q}$ than $\vec{p}$ (in terms of the Hamming distance).

Example 1: Let $V = \{v_1, v_2, v_3, v_4\}$ and $\vec{p} = 0110$. We assume that the values are listed in $\vec{p}$ in the order the corresponding variables are numbered i.e. $v_1 = 0$, $v_2 = 1$, $v_3 = 1$, $v_4 = 0$. Let $C = v_1 \lor \neg v_2$. (Note that $\vec{p}$ falsifies $C$.) Then $\text{Nbhd}(\vec{p}, C) = \{\vec{p}_1, \vec{p}_2\}$ where $\vec{p}_1 = 1110$ and $\vec{p}_2 = 0100$. Let $\vec{q} = 0000$. Note that $\vec{p}_2$ is actually closer to $\vec{q}$ than $\vec{p}$. So $\text{Nbhd}(\vec{q}, \vec{p}, C) = \{\vec{p}_1\}$. 

Definition 1: Let $H$ be a formula specified by a set of clauses $\{C_1, \ldots, C_k\}$. Let $P = \{\vec{p}_1, \ldots, \vec{p}_m\}$ be a set of assignments to $\text{Vars}(H)$ such that every $\vec{p}_i \in P$ falsifies $H$. Let $\Phi$ denote a mapping $P \rightarrow H$ where $\Phi(\vec{p}_i)$ is a clause $C$ of $H$ falsified by $\vec{p}_i$. We will call $\Phi$ an AC-mapping where “AC” stands for “Assignment-to-Clause”. We will denote the range of $\Phi$ as $\text{range}(P)$. (So, a clause $C$ of $H$ is in $\text{range}(P)$ iff there is an assignment $\vec{p}_i$ in $P$ such that $C = \Phi(\vec{p}_i)$.)

Definition 2: Let $H$ be a formula specified by a set of clauses $\{C_1, \ldots, C_k\}$. Let $P = \{\vec{p}_1, \ldots, \vec{p}_m\}$ be a set of assignments to $\text{Vars}(H)$. $P$ is called a Stable Set of Assignment (SSA) of $H$ with center $\vec{p}_{init} \in P$ if there is an AC-mapping $\Phi$ such that for every $\vec{p}_i \in P$, $\text{Nbhd}(\vec{p}_{init}, \vec{p}_i, C) \subseteq P$ holds where $C = \Phi(\vec{p}_i)$.

Example 2: Let $H$ consist of four clauses: $C_1 = v_1 \lor v_2 \lor v_3$, $C_2 = \neg v_1$, $C_3 = \neg v_2$, $C_4 = \neg v_3$. Let $P = \{\vec{p}_1, \vec{p}_2, \vec{p}_3, \vec{p}_4\}$ where $\vec{p}_1 = 000$, $\vec{p}_2 = 100$, $\vec{p}_3 = 010$, $\vec{p}_4 = 001$. Let $\Phi$ be an AC-mapping specified as $\Phi(\vec{p}_1) = C_1$, $i = 1, \ldots, 4$. Since $\vec{p}_i$ falsifies $C_i$, $i = 1, \ldots, 4$. $\Phi$ is a correct AC-mapping. $P$ is an SSA of $H$ with respect to $\Phi$ and center $\vec{p}_{init} = \vec{p}_1$. Indeed, $\text{Nbhd}(\vec{p}_{init}, \vec{p}_i, C_i) = \{\vec{p}_2, \vec{p}_3, \vec{p}_4\}$ where $C_1 = \Phi(\vec{p}_1)$ and $\text{Nbhd}(\vec{p}_{init}, \vec{p}_i, C_i) \subseteq P$, where $C_i = \Phi(\vec{p}_i)$, $i = 2, 3, 4$. Thus, $\text{Nbhd}(\vec{p}_{init}, \vec{p}_i, \Phi(\vec{p}_i)) \subseteq P$, $i = 1, \ldots, 4$.

B. SSAs and satisfiability of a formula

Proposition 1: Formula $H$ is unsatisfiable iff it has an SSA. The proof is given Appendix. A similar proposition is proved in [9] for “uncentered” SSAs (see Footnote 7).

The set of all assignments to $\text{Vars}(H)$ forms the trivial unsatisfactory SSA of $H$. Example 2 shows a non-trivial SSA. The fact that formula $H$ has a non-trivial SSA $P$ is its structural property. That is one cannot check whether $P$ is an SSA of $H$ if only the truth table of $H$ is known. In particular, $P$ may not be an SSA of a formula $H'$ logically.

The relation between SSAs and satisfiability can be explained as follows. Suppose that formula $H$ is satisfiable. Let $\vec{p}_{init}$ be an arbitrary assignment to $\text{Vars}(H)$ and $\vec{s}$ be a satisfying assignment that is the closest to $\vec{p}_{init}$ in terms of the Hamming distance. Let $P$ be the set of all assignments to $\text{Vars}(H)$ that falsify $H$ and $\Phi$ be an AC-mapping from $P$ to $H$. Then $\vec{s}$ can be reached from $\vec{p}_{init}$ by procedure $\text{BuildPath}$ shown in Figure 1. It generates a sequence of assignments $\vec{p}_1, \ldots, \vec{p}_i$ where $\vec{p}_1 = \vec{p}_{init}$ and $\vec{p}_i = \vec{s}$. First, $\text{BuildPath}$ checks if current assignment $\vec{p}_i$ equals $\vec{s}$. If so, then $\vec{s}$ has been reached. Otherwise, $\text{BuildPath}$ uses clause $C = \Phi(\vec{p}_i)$ to generate next assignment. Since $\vec{s}$

Footnote 7: In [9], the notion of “uncentered” SSAs was introduced. The definition of an uncentered SSA is similar to Definition 2. The only difference is that one requires that for every $\vec{p}_i \in P$, $\text{Nbhd}(\vec{p}_{init}, \vec{p}_i, C) \subseteq P$ holds instead of $\text{Nbhd}(\vec{p}_{init}, \vec{p}_i, C) \subseteq P$. 

Footnote 8: The proof of Proposition 1 presented in report is inaccurate.
for instance, respectively. Formula \( F \) of gate \( N \) is unsatisfiable due to functional equivalence of expressions \((x_1 \lor x_2) \land x_3 \) and \((x_1 \land x_3) \lor (x_2 \land x_3)\). Thus, \( N \equiv 0 \).

Let \( \bar{x} \) be a test i.e. an assignment to \( X \). The set of assignments to \( Vars(N) \) sharing the same assignment \( \bar{x} \) to \( X \) forms a cube of \( 2^{\lvert Y \rvert + 1} \) assignments. (Recall that \( Vars(N) = X \cup Y \cup \{z\} \)). Denote this set as \( Cube(\bar{x}) \). Only one assignment of \( Cube(\bar{x}) \) specifies the correct execution trace produced by \( N \) under \( \bar{x} \). All other assignments can be viewed as "erroneous" traces under test \( \bar{x} \).

Definition 3: Let \( T \) be a set of tests \( \{\bar{x}_1, \ldots, \bar{x}_k\} \) where \( k \leq 2^{|X|} \). We will say that \( T \) is a Complete Test Set (CTS) for \( N \) if \( Cube(\bar{x}_1) \cup \cdots \cup Cube(\bar{x}_k) \) contains an SSA for formula \( F_N \land z \).

If \( T \) satisfies Definition 3 set \( Cube(\bar{x}_1) \cup \cdots \cup Cube(\bar{x}_k) \) "contains" a proof that \( N \equiv 0 \) and so \( T \) can be viewed as complete. If \( k = 2^{|X|} \), \( T \) is the trivial CTS. In this case, \( Cube(\bar{x}_1) \cup \cdots \cup Cube(\bar{x}_k) \) contains the trivial SSA consisting of all assignments to \( Vars(F_N \land z) \). Given an SSA \( P \) of \( F_N \land z \), one can easily generate a CTS by extracting all different assignments to \( X \) that are present in the assignments of \( P \).

Example 4: Formula \( F_N \land z \) of Example 3 has an SSA of 21 assignments to \( Vars(F_N \land z) \). They have only 5 different assignments to \( X = \{x_1, x_2, x_3\} \). The set \( \{101,100,011,010,000\} \) of those assignments is a CTS for \( N \).

Definition 3 is meant for circuits that are not "too redundant". Highly-redundant circuits are discussed in report [11] and Appendix II.

IV. SemStr Procedure

A. Motivation

Building an SSA for a large formula is inefficient. So, constructing a CTS of \( N \) from an SSA of \( F_N \land z \) is impractical. To address this problem, we introduce a procedure called \( SemStr \) (a short for "Semantics and Structure"). Given formula \( F_N \land z \) and a set of variables \( V \subseteq Vars(F_N \land z) \), \( SemStr \) generates a simpler formula \( H(V) \) implied by \( F_N \land z \) at the same time trying to build an SSA for \( H \). If \( SemStr \) succeeds in constructing such an SSA, formula \( H \) is unsatisfiable and so is \( F_N \land z \). Then a set of tests \( T \) is extracted from this SSA. As we show in Subsection V-A, one can view \( T \) as an approximation of a CTS for \( N \) (if \( X \subseteq V \)) or an "approximation of approximation" of a CTS (if \( X \not\subseteq V \)).

Example 5: Consider the circuit \( N \) of Figure 3 where \( X = \{x_1, x_2, x_3\} \). Assume that \( V = X \). Application of \( SemStr \) to \( F_N \land z \) produces \( H(X) = (x_1 \lor x_2) \land (x_2 \lor x_3) \lor (x_1 \lor x_2) \land x_3 \). \( SemStr \) also generates an SSA of \( H \) of four assignments to \( X: \{000, 001, 011, 101\} \) with center \( p_{init} = 000 \). (We omit the AC-mapping here.) These assignments form an approximation of CTS for \( N \).
B. Description of SemStr

The pseudocode of SemStr is shown in Figure 4. SemStr accepts formula G (in our case, G := FN ∧ z) and a set of variables V ⊆ Vars(G). SemStr outputs an assignment satisfying G or formula H(V) implied by G and an SSA of H. Originally, the set of clauses H is empty. H is computed in a while loop. First, SemStr tries to build an SSA for the current formula H by calling BuildSSA (line 3). If H is unsatisfiable, BuildSSA computes an SSA P returned by SemStr (line 5). Otherwise, BuildSSA returns an assignment  a satisfying H. In this case, SemStr calls procedure GenCls to build a clause C falsified by  . Clause C is obtained by resolving clauses of G on variables of W. (Hence C is implied by ) If  can be extended to an assignment  satisfying G, SemStr terminates (lines 7-8). Otherwise, C is added to H and a new iteration begins.

Procedure GenCls is shown in Figure 5. First, GenCls generates formula G| W obtained from G by discarding clauses satisfied by  and removing literals falsified by  . Then GenCls checks if there is an assignment  satisfying G| W. If so,  is returned as an assignment satisfying G. Otherwise, a proof R of unsatisfiability of G| W is produced. Then GenCls forms a set V' ⊆ V. A variable w is in V' if a clause of G| W is used in proof R and its parent clause from G has a literal of w falsified by . Finally, clause C is generated as a disjunction of literals of V' falsified by  . By construction, clause C is implied by G and falsified by  .

V. BUILDING APPROXIMATIONS OF CTS

A. Two kinds of approximations of CTSs

GenTests(FN, X, P, Tries){
1 T := ∅
2 for each v ∈ P {
3 s := SatAssgn(FN,v)
4 if (s ̸= nil) {
5 ̅s := ExtrTest(s, X)
6 T := T ∪ ̅s
7 else
8 for (i = 0; i < Tries; i++){
9 FN := Relax(FN)
10 s := SatAssgn(FN,v)
11 if (s ̸= nil) continue
12 ̅s := ExtrTest(s, X)
13 T := T ∪ ̅s
14 return(T)
15
16 return(Gs ∪ Inps)
}Fig. 7. GenTests procedure

As before, let H(V) denote a formula implied by FN ∧ z that is generated by SemStr and P denote an SSA for H. Projections of N can be of two kinds depending on whether X ⊆ V holds. Let X ⊆ V hold and T be the test set extracted from P as described in Section III. That is T consists of all different assignments to X present in the assignments of P. On one hand, using the reasoning of Section III one can show that T is a CTS for projection of N on V. On the other hand, since H(V) is essentially an abstraction of FN ∧ z, set T is an approximation of a CTS for N. For that reason, we will refer to T as a CTS of N where superscript “a” stands for “approximation”.

Now assume that X ⊄ V holds. Generation of a test set T from P for this case is described in the next section. The set T can be viewed as an approximation of a set T' built for projection of N on set V ∪ X. Since T' is a CTS of N, we will refer to T as CTS N where “aa” stands for “approximation of approximation”.

B. Construction of CTS

Consider extraction of a test set T from SSA P of formula H(V) when X ⊄ V. Since V, in general, contains internal variables of N, translation of P to a test set T needs a special procedure GenTests shown in Figure 6. For every assignment  of P, GenTests checks if formula T| w is satisfiable under assignment  (i.e. if there exists a test under which N assigns  to V). If so, an assignment  to X is extracted from the satisfying assignment and added to T as a test. Otherwise, GenTests runs a for loop (lines 8-13) of Tries iterations. In every iteration, GenTests relaxes FN by removing the clauses specifying a small subset of gates picked randomly. If the relaxed version of FN is satisfiable, a test is extracted from the satisfying assignment and added to T.

C. Finding a set of variables to project on

GenCut(N, Size){
1 Gout := OutGate(N)
2 Gts := {Gout}
3 Dpth(Gout) := 0
4 Inps := ∅
5 while (|Gts ∪ Inps| < Size) {
6 G := Mndepth(Gts, Dpth)
7 Gts := Gts ∪ {G}
8 Seen(G) := true
9 foreach G' ∈ FanIn(G)
10 if (Seen(G')) continue
11 if (G' ∈ Inps) continue
12 Inps := Inps ∪ {G'}
13 continue
14 Dpth(G') := Dpth(G) + 1
15 Gts := Gts ∪ {G'}
16 return(Gts ∪ Inps)
}Fig. 7. GenCut procedure

Intuitively, a good choice of the set V to project on N is a (small) coherent subset of variables of N reflecting its structure and/or semantics. One obvious choice of V is the set of input variables of N. In this section, we describe generation of a set V whose variables form an internal cut of N denoted as Cut. Procedure GenCut for generation of set Cut consisting of Size gates is shown in Figure 7. Set V is formed from output variables of the cut gates.

The current cut is specified by Gts ∪ Inps. Set Gts is initialized with the output gate Gout of circuit N and Inps is originally empty. GenCut computes the depth of every gate of Gts. The depth of Gout is set to 0. Set Gts is processed in a while loop (lines 5-15). In every iteration, a gate of the smallest depth is picked from Gts. Then GenCut removes gate G from Gts and examines the fan-in gates of G (lines 9-15). Let G' be a fan-in gate of G that has not been seen yet and is not a primary input of N. Then the depth of G' is set to that of G plus 1 and G' is added to Gts. If G' is a primary input of N it is added to Inps.

VI. APPLICATIONS OF PROPERTY-CHECKING TESTS

Given a multi-output circuit M, traditional testing is used to verify M “as a whole”. In this paper, we describe generation of a test set meant for checking a particular property of M.

1 If the special case Inps ⊂ X holds, every assignment of P can be easily turned into a test by assigning values to variables of X \ V (e.g. randomly).
specified by a single-output circuit $N$. In this section, we present some applications of property-checking test sets.

A. Testing properties specified by similar circuits

Let $N$ be a single-output circuit and $T$ be a test set generated when proving $N \equiv 0$. Let $N^*$ be a circuit that is similar to $N$. (For instance, $N$ can specify a property of a circuit $M$ whereas $N^*$ specifies the same property after a modification of $M$.) Then one can use $T$ to verify if $N^* \equiv 0$. Since $T$ is generated for a similar circuit $N$, there is a good chance that it contains a counterexample to $N^* \equiv 0$, if any. (Of course, the fact that $N^*$ evaluates to 0 for all tests of $T$ does not mean that $N^* \equiv 0$ even if $T$ is a CTS for $N$). In Subsection VII-B we give experimental evidence supporting the observation above.

Assuming that $N \equiv 0$ was proved formally, checking if $N^* \equiv 0$ holds can be verified formally too. So applying tests of $T$ to $N^*$ can be viewed as a “light” verification procedure for exposing bugs. On the other hand, one can re-use test $T$ in situations where the necessity to apply a formal tool is overlooked or formal methods are not powerful enough.

Let $N$ specify a property $\xi$ of a component of a design $D$. Suppose that this component is modified under assumption that preserving $\xi$ is not necessary any more. By applying $T$ to $D$ one can invoke behaviors that break $\xi$ and expose a bug in $D$, if any, caused by ignoring $\xi$. If $D$ is a large design, finding such a bug by formal verification may not be possible.

B. Verification of corner cases

Let $K$ be a single-output subcircuit of circuit $M$ as shown in Figure 8. For the sake of simplicity we consider here the case where the set $X_K$ of input variables of $K$ is a subset of the set $X$ of input variables of $M$. (The technique below can also be applied when input variables of $K$ are internal variables of $M$.) Suppose $K$ evaluates, say, to value 0 much more frequently then to 1. Then one can view an input assignment of $M$ for which $K$ evaluates to 1 as specifying a “corner case” i.e. a rare event. Hitting such a corner case by a random test can be very hard. This issue can be addressed by using a coverage metric that requires setting the value of $K$ to both 0 and 1. (The task of finding a test for which $K$ evaluates to 1 can be solved, for instance, by a SAT-solver.) The problem however is that hitting a corner case only once may be insufficient.

One can increase the frequency of hitting the corner case above as follows. Let $N$ be a miter of circuits $K'$ and $K''$ (see Figure 9) i.e. a circuit that evaluates to 1 iff $K'$ and $K''$ are functionally inequivalent. Let $K'$ and $K''$ be two copies of circuit $K$. So $N \equiv 0$ holds. Let test set $T_K$ be extracted from an SSA built for a projection of $N$ on a set $V \subseteq \text{Vars}(N)$. Set $T_K$ can be viewed as a result of “squeezing” the truth table of $K$. Since this truth table is dominated by input assignments for which $K$ evaluates to 0, this part of the truth table is reduced the most. So, one can expect that the ratio of tests of $T_K$ for which $K$ evaluates to 1 is higher than in the truth table of $K$. In Subsection VII-C we substantiate this intuition experimentally. One can easily extend an assignment $\vec{x}_K$ of $T_K$ to an assignment $\vec{x}$ to $X$ e.g. by randomly assigning values to the variables of $X \setminus X_K$.

C. Dealing with incomplete specifications

One can use property-checking tests to mitigate the problem of incomplete specifications. By running tests generated for an incomplete set of properties of $M$, one can expose bugs overlooked due to missing some properties. An important special case of this problem is as follows. Let $\xi$ be a property of $M$ that holds. Assume that the correctness of $M$ requires proving a slightly different property $\xi'$ that is not true. By running a test set $T$ built for property $\xi$, one may expose a bug overlooked in formal verification due to proving $\xi$ instead of $\xi'$. In Subsection VII-D we illustrate the idea above experimentally.

D. Testing sequential circuits

There are a few ways to apply property-checking tests meant for combinational circuits to verification of sequential circuits. Here is one of them based on bounded model checking [3]. Let $M$ be a sequential circuit and $\xi$ be a property of $M$. Let $N(X,Y,Z)$ be a circuit such that $N \equiv 0$ holds iff $\xi$ is true for $k$ time frames. Circuit $N$ is obtained by unrolling $M$ $k$ times and adding logic specifying property $\xi$. Set $X$ consists of the subset $X'$ specifying the state variables of $M$ in the first time frame and subset $X''$ specifying the combinational input variables of $M$ in $k$ time frames.

Having constructed $N$, one can build CTSs, CTS's and CTS''s for testing property $\xi$ of $M$. The only difference here from the problem we have considered so far is as follows. Circuit $M$ starts in a state satisfying some formula $I(X')$ that specifies the initial states. So, one needs to check if $N \equiv 0$ holds only for the assignments to $X$ satisfying $I(X')$. A test here is an assignment $(\vec{x}_1', \vec{x}_{i1}', ..., \vec{x}_{ik}')$ where $\vec{x}_1'$ is an initial state and $\vec{x}_{ii}'$, $1 \leq i \leq k$ is an assignment to the combinational input variables of $i$-th time frame. Given a test, one can easily compute the corresponding sequence of states $(\vec{x}_1', ..., \vec{x}_k')$ of $M$. In Subsection VII-D we give an example of building an CTS'' for a sequential circuit.

VII. Experiments

In this section, we describe experiments with property-checking tests (PCT) generated by procedure GenPCT shown in Figure 10. GenPCT accepts a single-output circuit $N$ and outputs a set of tests $T$. (For the sake of simplicity, we assume here that $N \equiv 0$ holds.) GenPCT starts with generating
formula \( F_N \land z \) and a set of variables \( V \subseteq \text{Vars}(F_N \land z) \). Then it calls \( \text{SemStr} \) (see Fig. 5) to compute an SSA \( P \) of \( \text{formula} \ H(V) \) describing a projection of circuit \( N \) on \( V \). If \( H(V) \) does not depend on a variable \( w \) in \( V \), all assignments of \( P \) have the same value of \( w \). Procedure \( \text{Diversify} \) randomizes the value of \( w \) in the assignments of \( P \). Finally, \( \text{BldTests} \) uses \( P \) to extract a test set for circuit \( N \). If \( X \cap V \) holds (where \( X \) is the set of input variables of \( N \)), \( \text{BldTests} \) outputs all the different assignments to \( X \) present in assignments of \( P \). Otherwise, \( \text{BldTests} \) calls procedure \( \text{GenTests} \) (see Fig. 6).

If \( V = \text{Vars}(F_N \land z) \), then \( H(V) = F_N \land z \) itself and \( \text{GenPCT} \) produces a CTS of \( N \). Otherwise, according to the definition of Subsection V-A \( \text{GenPCT} \) generates a CTS (if \( X \subseteq V \)) or \( \text{CTS}^{aa} \) (if \( X \not\subseteq V \)).

In the following subsections, we describe results of four experiments. In the first three experiments we used circuits specifying next state functions of latches of HWMCC-10 benchmarks. (The motivation was to use realistic circuits.) In our implementation of \( \text{SemStr} \), as a SAT-solver, we used Minisat 2.0 [6, 17]. We also employed Minisat to run simulation. To compute the output value of \( N \) under test \( \bar{x} \), we added unit clauses specifying \( \bar{x} \) to formula \( F_N \land z \) and checked its satisfiability.

A. Comparing CTSs, CTS\(^a\)s and CTS\(^aa\)s

The objective of the first experiment was to give examples of circuits with non-trivial CTSs and compare the efficiency of computing CTSs, CTS\(^a\)s and CTS\(^aa\)s. In this experiment, \( N \) was a miter specifying equivalence checking of circuits \( M' \) and \( M'' \) (see Figure 9). \( M'' \) was obtained from \( M' \) by optimizing the latter with \( \text{ABC} \) [14].

The results of the first experiment are shown in Table I. The first two columns specify an HWMCC-10 benchmark and its latch whose next state function was used as \( M' \). The next two columns give the number of input variables and that of gates in the miter \( N \). The following pair of columns describe computing a CTS for \( N \). The first column of this pair gives the size of the SSA \( P \) found by \( \text{GenPCT} \) in thousands. The number of tests in the set \( T \) extracted from \( P \) is shown in the parentheses in thousands. The second column of this pair gives the run time of \( \text{GenPCT} \) in seconds.

The last four columns of Table I describe results of computing test sets for a projection of \( N \) on a set of variables \( V \). The first column of this group shows if CTS\(^a\) or CTS\(^aa\) was computed whereas the next column gives the size of \( V \). The third column of this group provides the size of SSA \( P \) and the test set \( T \) extracted from \( P \) (in parentheses). Both sizes are given in thousands. The last column shows the run time of \( \text{GenPCT} \). For the first five examples, we used a projection of \( N \) on \( X \), thus constructing a CTS\(^a\) of \( N \). For the last four examples we computed a projection of \( N \) on an internal cut (see Subsection V-C), thus generating a CTS\(^aa\) of \( N \). \( \text{GenPCT} \) was called with parameter \( \text{Tries} \) set to 5 (see Fig. 6 and 10).

For the first three examples, \( \text{GenPCT} \) managed to build non-trivial CTSs that are smaller than \( 2^{|X|} \). For instance, the trivial CTS for example bob3 consists of \( 2^{14} = 16,384 \) tests, whereas \( \text{GenPCT} \) found a CTS of 2,004 tests. (So, to prove \( M' \) and \( M'' \) equivalent it suffices to run 2,004 out of 16,384 tests.) For the other examples, \( \text{GenPCT} \) failed to build a non-trivial CTS due to exceeding the memory limit (1.5 Gbytes). On the other hand, \( \text{GenPCT} \) built a CTS\(^a\) or CTS\(^aa\) for all nine examples of Table I. Note, however, that CTS\(^a\)s give only a moderate improvement over CTSs. For the last four examples \( \text{GenPCT} \) failed to compute an CTS\(^a\) of \( N \) due to memory overflow whereas it had no problem computing an CTS\(^aa\) of \( N \). So CTS\(^aa\)s can be computed efficiently even for large circuits. Further, we show that CTS\(^aa\)s are also very effective.

B. Re-using property-checking tests to detect bugs

In the second experiment, we employed the idea of re-using property-checking tests (see Subsection VI-A) to verify relaxed equivalence [16]. Let circuit \( M^\pi \) be obtained from circuit \( M \) by applying a set of changes \( \pi \). Regular equivalence of \( M \) and \( M^\pi \) means that these circuits produce the same output assignment for the same input assignment. Relaxed equivalence requires only that the difference between output assignments of \( M \) and \( M^\pi \) is in a specified range. So regular equivalence implies relaxed one and hence the latter is a weaker property than the former. Intuitively, this makes relaxed equivalence harder for testing (because the space of buggy behaviors is smaller).

In this experiment, we compared two-output circuits \( M \) and \( M^\pi \). Namely we checked property \( \xi(M, M^\pi) \) that \( (y_1 = y'_{1}) \lor (y_2 = y'_{2}) \) holds where \( y_1, y_2 \) and \( y'_1, y'_2 \) specify the outputs of \( M \) and \( M^\pi \) respectively. Property \( \xi(M, M^\pi) \) states that the Hamming distance between the output assignments produced by \( M \) and \( M^\pi \) for the same input assignment is less or equal to 1. Circuit \( M \) was extracted from the transition relation of an HWMCC-10 benchmark. Circuit \( M^\pi \) was obtained from \( M \) by making changes \( \pi \) that broke property \( \xi(M, M^\pi) \).

Let \( N^\pi \) denote a circuit specifying property \( \xi(M, M^\pi) \). In the experiment, we tested \( N^\pi \) using three approaches. The first approach was to apply tests generated to detect stuck-at faults (SAF) [11] in \( M \). We used SAF tests as an example of
a test set driven by a coverage metric. The second approach was random testing of \( N^\pi \). In the third approach we did the following. First, we built a CTS for circuit \( N^\pi \) specifying property \( \xi(M, M^\pi) \) for the case where \( \pi = \emptyset \) and hence \( M^\pi \) was identical to \( M \). (Obviously, \( N^\emptyset = \emptyset \).) Then we re-used this CTS to verify circuit \( N^\pi \) for the case \( \pi \neq \emptyset \).

A representative subset of examples we tried is shown in Table II. The first column gives the name of the HWMCC-10 benchmark from which circuit \( M \) was extracted. The next two columns show the size of the circuit. The following two columns list the number of SAF tests and the total run time (i.e. time taken to generate tests and run simulation by Minisat). The next two columns show the performance of random testing. The last three columns describe testing by CTSs. The first column of the three gives the size of the SSA for formula \( H(V) \) generated by \textit{GenPCT}. The set of variables \( V, |V| = 18 \), forming an internal cut was generated by procedure \textit{GenCut} (see Fig. 7). The next column shows the size of a CTS obtained with \textit{Tries} set to 100. The last column gives the total run time.

The test sets with a counterexample breaking \( \xi(M, M^\pi) \) are marked with an asterisk. Table II shows that SAF tests failed to detect a bug, random tests found a bug for two examples and CTSs succeeded for all examples. (On the other hand, the same SAF tests and CTSs found bugs in all eight examples modified to check regular equivalence i.e. the property \( (y_1 = y_1^R) \land (y_2 = y_2^R) \). Random testing limited to 100 million tests found a bug in five examples.) So CTSs proved effective even in testing a “weak” property.

C. Testing corner cases

In the third experiment, we generated CTSs and CTSs to test corner cases (see Subsection VI-B). First, we formed a circuit \( K \) that evaluates to 0 for almost all input assignments. So, the assignments for which \( K \) evaluates to 1 are corner cases. We compared the frequency of hitting corner cases by random tests and by tests of a set \( T \) built by \textit{GenPCT} as follows. Let \( N \) be a miter of copies \( K' \) and \( K'' \) (see Figure 9). The set \( T \) was generated using a projection of \( N \) either on the set \( X \) of input variables or an internal cut of \( N \).

To build circuit \( K \), we extracted the circuit \( R \) specifying the next state function of a latch of a HWMCC-10 benchmark and composed it with an \( n \)-input AND gate as shown in Figure 11. The circuit \( K \) outputs 1 only if \( R \) evaluates to 1 and the first \( n-1 \) inputs variables of the AND gate are set to 1 too. So the input assignments for which \( K \) evaluates to 1 are “corner cases”.

The results of the experiment are given in Table III. The first two columns name the benchmark and latch whose next state function was used as circuit \( R \). The next three columns give the total number of input variables of \( K \), the value of \( n \) in the \( n \)-input AND gate fed by \( R \) and the number of gates in circuit \( K \). The following pair of columns describes the performance of random testing. The first column of this pair gives the total number of tests. The next column shows the percentage of times circuit \( K \) evaluated to 1 (and so a corner case was hit). The last five columns of Table III describe the results of \textit{GenPCT}. The first column of the five indicates whether a CTS or CTS was generated. The second column gives the size of set \( V \) on which the projection of \( N \) was computed. CTSs were generated with \( V = X \). When computing CTSs, the set \( V \) formed an internal cut of \( N \) and the value of \textit{Tries} was set to 1. The next column shows the size of the test set. The fourth column gives the percentage of times a corner case was hit. The last column shows the total run time.

The examples of Table III were generated in pairs that shared the same circuit \( R \) and were different only in the size of the AND gate fed by \( R \). For instance, in the first and second entry of Table III circuit \( K \) was obtained by composing the
same circuit $R$ extracted from benchmark pdtvisgigamax5 with 10-input and 30-input AND gates respectively. Table III shows that for circuits with a 10-input AND gate, random testing hit corner cases but the percentage of those events was much lower than for CTS's and CTS's. On the other hand, 100 millions of random tests failed to hit a single corner case for examples with a 30-input AND gate in sharp contrast to CTS's and CTS's.

### D. Testing properties defined incorrectly

| $C_a$ | Time frames | Tests | SAF tests | CTS tests |
|-------|-------------|-------|-----------|-----------|
| $C_4$ | 14          | 0.001 | 1.772     | 1.572     |
| $C_5$ | 30          | 28*   | 505       | 2.139*    |
| $C_6$ | 62          | 100   | 1.276     | 338*      |
| $C_7$ | 126         | 100   | 3.031     | 1.025*    |

Table IV shows that random testing broke $\xi'$ only for $C_4$ and $C_5$ and SAF tests succeeded only for $C_4$. Tests of CTS's broke $\xi'$ for all 4 examples.

### VIII. Background

As we mentioned earlier, traditional testing checks if a circuit $M$ is correct as a whole. This notion of correctness means satisfying a conjunction of many properties of $M$. For this reason, one tries to spray tests uniformly in the space of all input assignments. To improve the effectiveness of testing, one can try to run many tests at once as it is done in symbolic simulation [4]. To avoid generation of tests that for some reason should be or can be excluded, a set of constraints can be used [12]. Another method of making testing more reliable is to generate tests exciting a particular set of events specified by a coverage metric [15]. Our approach is different from those above in that it is aimed at testing a particular property of $M$.

The method of testing introduced in [10] is based on the idea that tests should be treated as a “proof encoding” rather than a sample of the search space. (The relation between tests and proofs have been also studied in software verification, e.g. in [17].) In this paper, we take a different point of view where testing becomes a part of a formal proof namely the part that performs structural derivations.

Reasoning about SAT in terms of random walks was pioneered in [13]. The centered SSAs we introduce in this paper bear some similarity to sets of assignments generated in derandomization of Schöning’s algorithm [5]. Typically, centered SSAs are much smaller than uncentered SSAs of [9].

The first version of SemStr procedure is presented in report [11]. It has a much tighter integration between the structural part (computation of SSAs) and semantic part (derivation of formula $H$ implied by the original formula). The advantage of the new version of SemStr described in this paper is twofold. First, it is much simpler than SemStr of [11]. In particular, any resolution based SAT-solver that generates proofs can be used to implement the new SemStr. Second, the simplicity of the new version makes it much easier to achieve the level of scalability where SemStr becomes practical.

### IX. Conclusion

We consider the problem of finding a Complete Test Set (CTS) for a combinational circuit $N$ that is a test set proving $N \equiv 0$. We use the machinery of stable sets of assignments to derive non-trivial CTSs i.e. those that do not include all possible input assignments. Computing a CTS for a large circuit $N$ is inefficient. So, we present a procedure that generates a test set for a “projection” of $N$ on a subset $V$ of variables of $N$. Depending on the choice of $V$, this procedure generates a test set CTS that is an approximation of an CTS or a test set CTS that is an approximation of CTS. We give experimental results showing that CTS's can be efficiently computed even for large circuits and are effective in solving verification problems.
that is an SSA of $H$ with respect to some center $\vec{p}_{\text{init}}$ and AC-mapping $\Phi$. QED

APPENDIX II

CTSs AND CIRCUIT REDUNDANCY

Let $N \equiv 0$ hold. Let $R$ be a cut of circuit $N$. We will denote the circuit between this cut and the output of $N$ as $N_R$ (see Figure 2). We will say that $N$ is non-redundant if $N_R \neq 0$ for any cut $R$ other than the cut specified by primary inputs of $N$. Note that if $N_R \neq 0$ for some cut $R$, then $N_R' \neq 0$ for every cut $R'$ located above $R$.

Definition 3 of a CTS may not work well if $N$ is highly redundant. Assume, for instance, that $N_R \equiv 0$ holds for a cut $R$. This means that the clauses specifying gates of $N$ below $R$ (i.e. those that are not in $N_R$) are redundant in $F_N \land z$. Then one can build an SSA $P$ for $F_N \land z$ as follows. Let $P_R$ be an SSA for $F_{N_R} \land z$. Let $\vec{v}$ be an arbitrary assignment to the variables of $\text{Vars}(N) \setminus \text{Vars}(N_R)$. Then by adding $\vec{v}$ to every assignment of $P_R$ one obtains an SSA for $F_N \land z$. This means that for any test $\vec{x}$, Cube($\vec{x}$) contains an SSA of $F_N \land z$. Therefore, according to Definition 3, circuit $N$ has a CTS consisting of just one test.

The problem above can be solved using the following observation. Let $T$ be a set of tests $\{\vec{x}_1, \ldots, \vec{x}_k\}$ for $N$ where $k \leq 2^{\lceil |X| \rceil}$. Denote by $r_i^\top$ the assignment to the variables of cut $R$ produced by $N$ under input $\vec{x}_i$. Let $T_R$ denote $\{r_1^\top, \ldots, r_k^\top\}$. Denote by $T_R^*$ the set of assignments to variables of $R$ that cannot be produced in $N$ by any input assignment. Now assume that $T$ is constructed so that $T_R^* \cup T_R^*$ is a CTS for circuit $N_R$. This does not change anything if $N_R$ is itself redundant (i.e. if $N_R' \equiv 0$ for some cut $R'$ that is closer to the output of $N$ than $R$). In this case, it is still sufficient to use $T$ of one test because $N_R$ has a CTS of one assignment (in terms of cut $R$). Assume however, that $N_R$ is non-redundant. In this case, there is no “degenerate” CTS for $N_R$ and $T$ has to contain at least $|T_R|$ tests. Assuming that $T_R^*$ alone is far from being a CTS for $N_R$, a CTS $T$ for $N$ will consist of many tests.

So, one can modify the definition of CTS for a redundant circuit $N$ as follows. A test set $T$ is a CTS for $N$ if there is a cut $R$ such that

- circuit $N_R$ is non-redundant i.e.
  - $N_R' \equiv 0$ holds
  - $N_R' \neq 0$ for every cut $R'$ above $R$
- set $T_R \cup T_R^*$ is a CTS for $N_R$.

APPENDIX I

PROOFS

**Proposition 1:** Formula $H$ is unsatisfiable iff it has an SSA.

**Proof:** If part. Assume the contrary i.e. $P$ is an SSA of $H$ with center $\vec{p}_{\text{init}}$ and AC-mapping $\Phi$ and $H$ is satisfiable. Let $\vec{s}$ be an assignment satisfying $H$ that is the closest to $\vec{p}_{\text{init}}$ in terms of the Hamming distance. Then procedure BuildPath (see Fig. [1]) can build a sequence of assignments $\vec{p}_1, \ldots, \vec{p}_i$ such that

- $i = \text{Hamming-distance}(\vec{p}_{\text{init}}, \vec{s}) + 1$
- $\vec{p}_1 = \vec{p}_{\text{init}}$ and $\vec{p}_i = \vec{s}$

By definition of BuildPath, assignment $\vec{p}_{i+1}$ is closer to $\vec{s}$ and farther away from $\vec{p}_i$ than $\vec{p}_j$ where $1 \leq j \leq i - 1$. This means that $\vec{p}_{i+1}$ is in $\text{Nbhd}(\vec{p}_{\text{init}}, \vec{p}_i, C)$ where $C = \Phi(\vec{p}_i)$. In particular, $\vec{s}$ is in $\text{Nbhd}(\vec{p}_{\text{init}}, \vec{p}_i, C)$ and so $\vec{s}$ is in $P$. However, by definition of an SSA, $P$ consists only of assignments falsifying $H$. Thus, we have a contradiction.

Only if part. Assume that formula $H$ is unsatisfiable. By applying BuildSSA (see Fig. [2]) to $H$, one generates a set $P$