Complete Test Sets And Their Approximations

Eugene Goldberg

FMCAD,

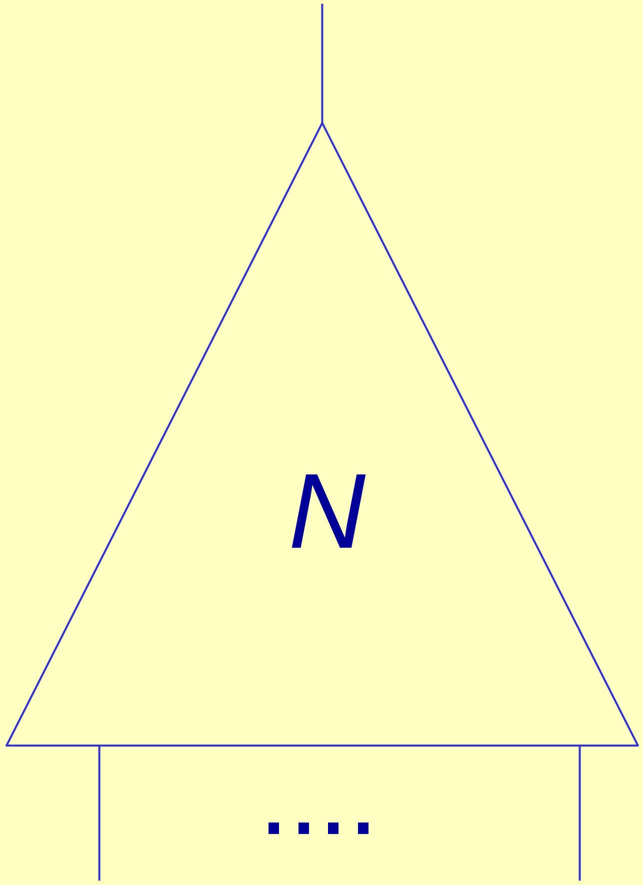
Austin, TX, USA

October 30 – November 2, 2018

Outline

- Introduction
- Complete Test Sets (CTSs)
- Experiments and conclusions

The Problem



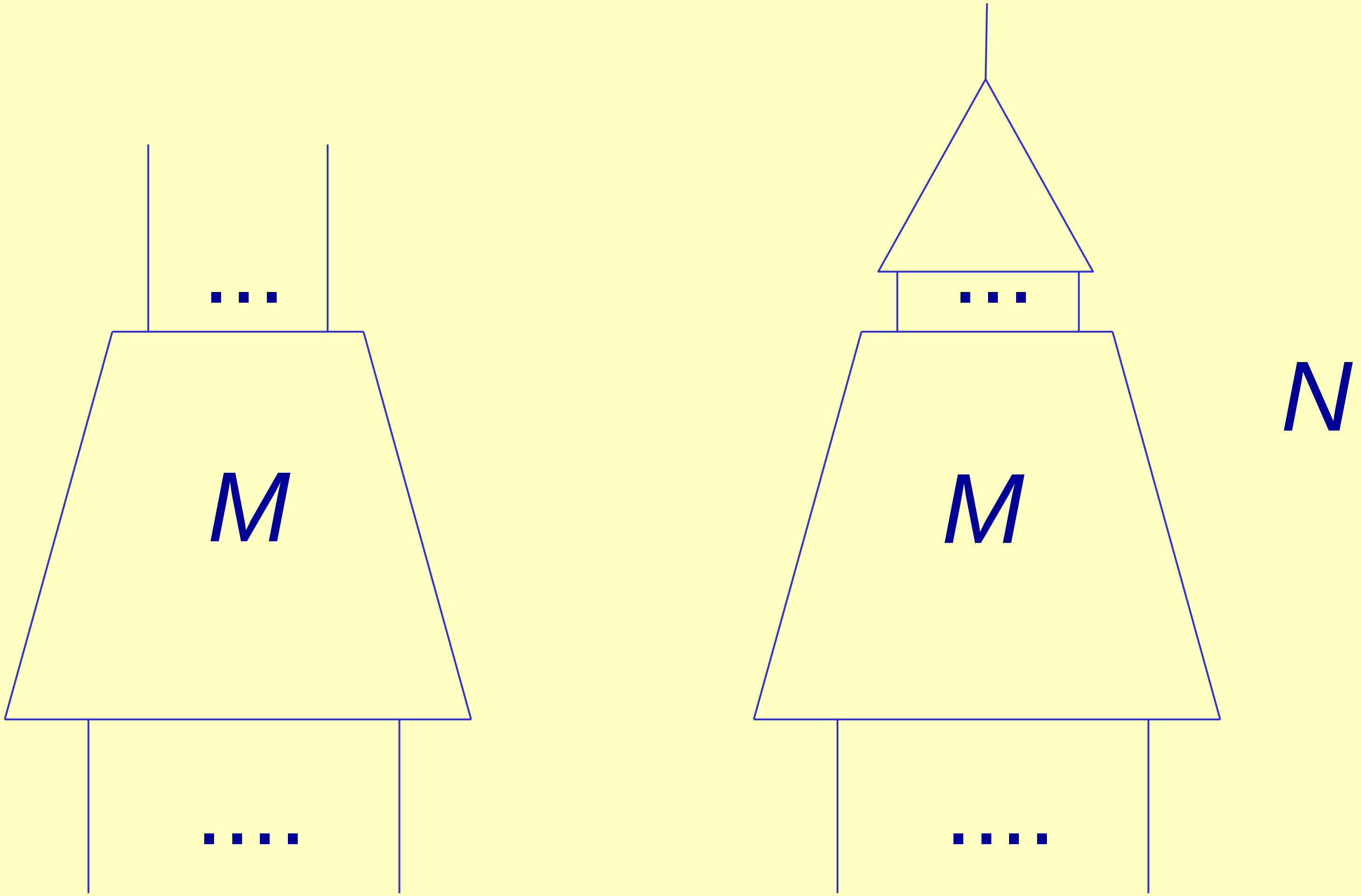
The problem we consider:

Check if $N \equiv 0$

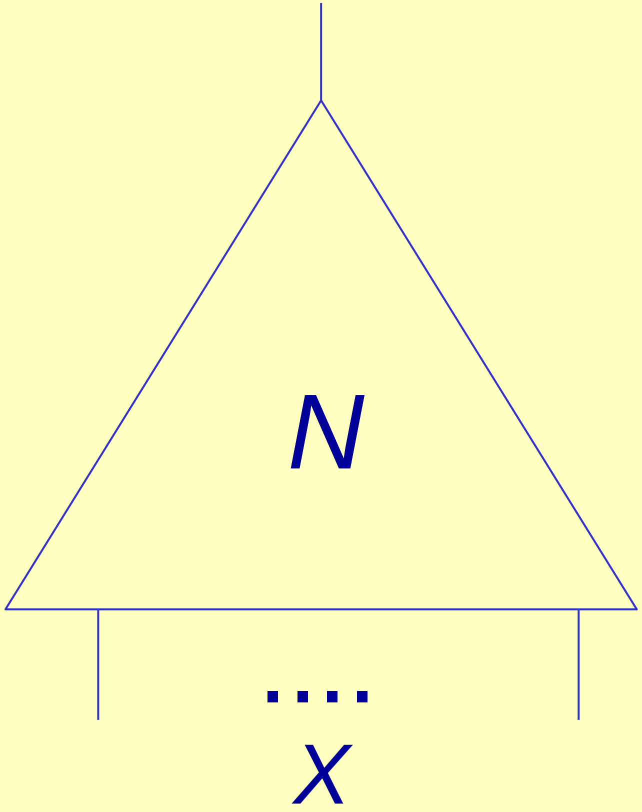
$N \equiv 0$ denotes the fact that N outputs 0 for every input

We want to prove $N \equiv 0$ by testing

The Context



Complete Test Set (CTS)



Test $\boldsymbol{x}$ is an assignment to X

Test set $T = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m\}$,

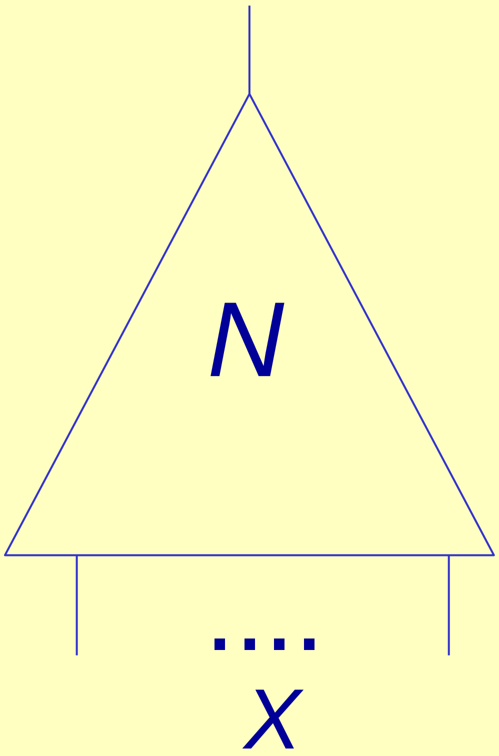
T is a CTS if

$N(T) = 0 \Rightarrow N \equiv 0$

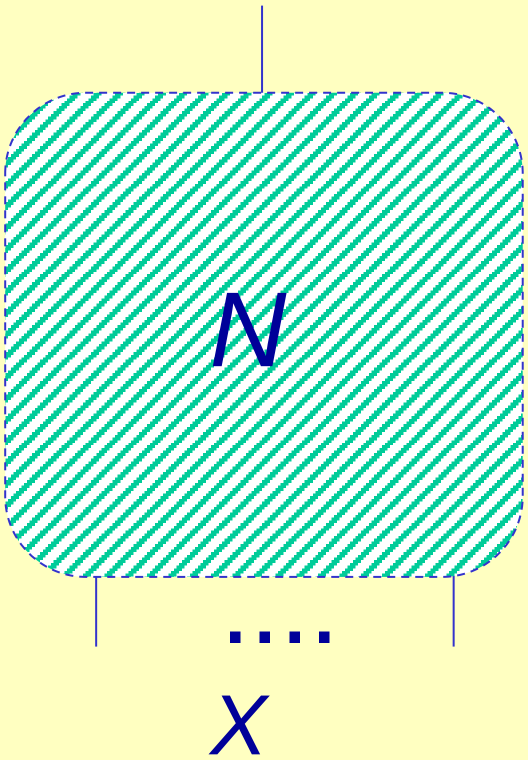
T is a trivial CTS

if $|T| = 2^{|X|}$

Black/White Box Testing



$|T_{CTS}| \leq 2^{|X|}$



$|T_{CTS}| = 2^{|X|}$

Testing as Structural Derivation

$N \equiv 0$ is a semantic property of N:

$(N \equiv 0) \wedge (N^* \equiv N)$ implies $N^* \equiv 0$

A non-trivial CTS is a structural property of N:

T is a CTS for N and $N^* \equiv N \quad \not\Rightarrow$

T is a CTS for N^*

Testing: Make a *semantic* derivation ($N \equiv 0$) by proving a *structural* property (non-trivial CTS)

Some Applications Exploiting Reusability of Tests

Let ξ be a property of *M.* Formal proof of ξ is hard to reuse.

Let $N \equiv 0 \Leftrightarrow \xi$ holds

Let *T* be generated to test *N*

Set *T* can be reused

- to check other properties of *M*
- to check input/output behavior of *M*
- to check ξ after *M* is modified

Outline

- Introduction
- Complete Test Sets (CTSs)
- Experimens and conclusions

Stable Set of Assignments (SSA)

Given CNF formula $G(W)$, $P = \{\boldsymbol{q}_1,..,\boldsymbol{q}_m\}$ is an SSA

- $\forall\, \boldsymbol{q}_i \in P, \quad G(\boldsymbol{q}_i) = 0$
- P is closed w.r.t. to a neighborhood relation

G is unsatisfiable iff it has an SSA

Trivial SSA: all $2^{|W|}$ assignments

Non-trivial SSA is a structural property:

P is an SSA for G and $G^* \equiv G \;\not\Rightarrow$

P is an SSA for G^*

Example of SSA

$G = C_1 \wedge .. \wedge C_4$,

$C_1 = w_1 \vee w_2 \vee w_3$,

$C_2 = \sim w_1$,

$C_3 = \sim w_2$,

$C_4 = \sim w_3$

$\boldsymbol{q_1}=(w_1=0,\ w_2=0,\ w_3=0)$ falsifies C_1

$Nbhd(\boldsymbol{q_1},C_1) = \{\boldsymbol{q_2},\boldsymbol{q_3},\boldsymbol{q_4}\}$

$\boldsymbol{q_2}=(w_1=1,\ w_2=0,\ w_3=0)$,

$\boldsymbol{q_3}=(w_1=0,\ w_2=1,\ w_3=0)$,

$\boldsymbol{q_4}=(w_1=0,\ w_2=0,\ w_3=1)$,

Example of SSA (continued)

$C_1 = w_1 \vee w_2 \vee w_3$, $C_2 = \sim w_1$, $C_3 = \sim w_2$, $C_4 = \sim w_3$

$P = \{\boldsymbol{q_1}, \boldsymbol{q_2}, \boldsymbol{q_3}, \boldsymbol{q_4}\}$,

$\boldsymbol{q_1} = (0\ 0\ 0)$, $\boldsymbol{q_2} = (1\ 0\ 0)$, $\boldsymbol{q_3} = (0\ 1\ 0)$, $\boldsymbol{q_4} = (0\ 0\ 1)$

$Nbhd(\boldsymbol{q_1}, C_1) = \{\boldsymbol{q_2}, \boldsymbol{q_3}, \boldsymbol{q_4}\}$

$Nbhd(\boldsymbol{q_2}, C_2) = \{\boldsymbol{q_1}\}$

$Nbhd(\boldsymbol{q_3}, C_3) = \{\boldsymbol{q_1}\}$,

$Nbhd(\boldsymbol{q_4}, C_4) = \{\boldsymbol{q_1}\}$

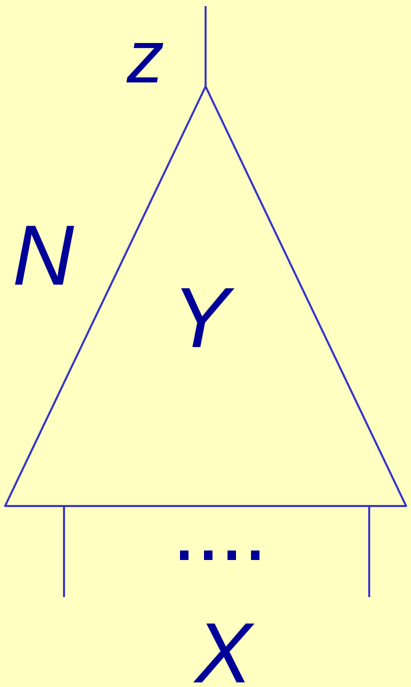
P is closed: $\forall\ \boldsymbol{q_k} \in P$, $\exists C_j \in G$
s.t. $C_j(\boldsymbol{q_k}) = 0$ and $Nbhd(\boldsymbol{q_k}, C_j) \subseteq P$

P is an SSA for $G = C_1 \wedge .. \wedge C_4$

Building Complete Test Set

Let $F_N(X,Y,z)$ be CNF specifying N

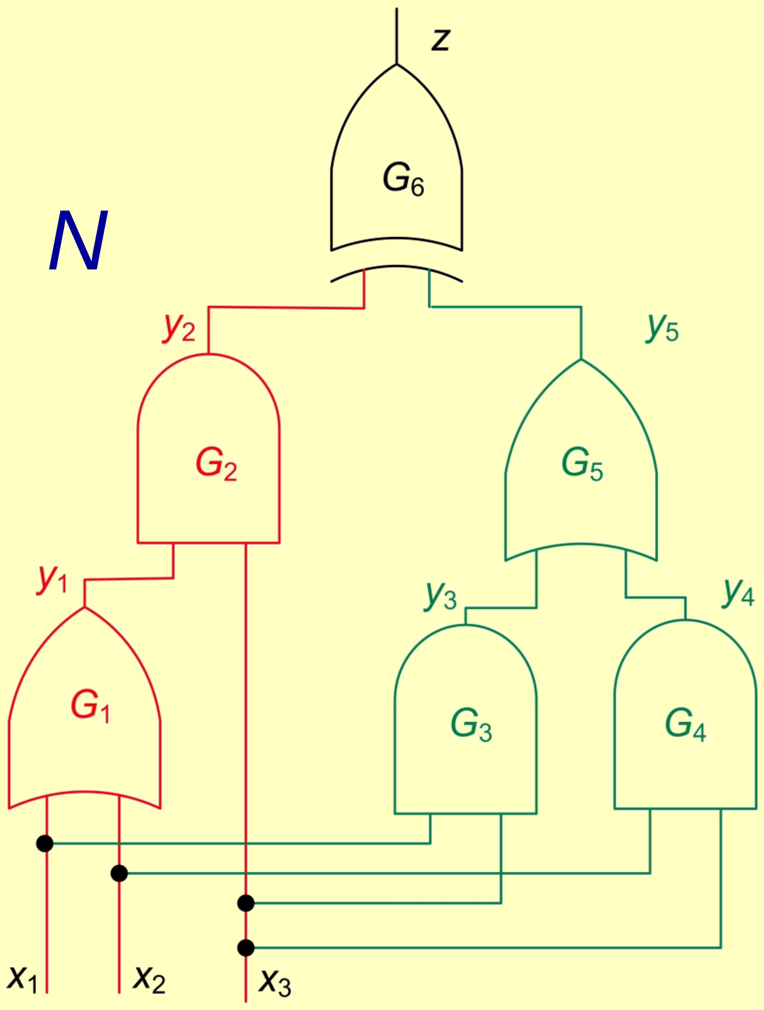
$N \equiv 0 \Leftrightarrow F_N \wedge z \equiv 0$



1. Build SSA $\{\boldsymbol{q_1},..,\boldsymbol{q_m}\}$ for $F_N \wedge z$
2. Form $T = \{\boldsymbol{x_1},..,\boldsymbol{x_m}\}$, $\boldsymbol{x}_i = proj(\boldsymbol{q}_i,X)$, $i=1,..,m$
3. Remove duplicates from T

T is a CTS for N

Example of CTS



$(x_1 \vee x_2) \wedge x_3 \equiv$

$(x_1 \wedge x_3) \vee (x_2 \wedge x_3)$

$F_N \wedge z$ has SSA P of 21 assignments to $X \cup Y \cup \{z\}$

where $X = \{x_1, x_2, x_3\}$, $Y = \{y_1, .. y_5\}$

P has 5 different assignments to $X \Rightarrow$ **CTS of 5 tests**

CTSs Are Too Large

Even non-trivial CTSs are too large $\Rightarrow$
Approximate CTS (denoted as CTS^{aprx})

Build T for a projection of N on $V \subset X \cup Y \cup \{z\}$

1. Generate $G(V)$ implied by $F_N \wedge z$
2. Build SSA P for G
3. Extract test set T from P

Proving $F_N \wedge z \equiv 0$ in two steps.

- Semantic step: $F_N \wedge z \Rightarrow G$
- Structural step: SSA P for G

Outline

- Introduction
- Complete Test Sets (CTSs)
- Experiments and conclusions

Testing Misdefined Properties

- Property ξ of sequential circuit *M* is misdefined
- ξ holds while the correct property ξ^* does not

- False positives are hard to deal with
- Propping up formal verification by testing (assuming that ξ and ξ^* are close)

1. Form N_k , where $N_k \equiv 0 \Leftrightarrow \xi$ holds for *k* transitions
2. Build CTS^{aprx} *T* for a projection of N_k.
3. Run *T* to test *M* for *k* transitions

Description of Experiment

- HWMCC-10 benchmarks are used
- The original (true) property ξ is misdefined
- The “correct” property ξ^* fails in *k* transitions

Let N_k and N^*_k specify ξ and ξ^* for *k* transitions

1. Generate a CTS^{aprx} T to prove $N_k \equiv 0$
2. Run T to break $N^*_k \equiv 0$
3. Compare *T* with random and coverage tests

Some Results

name	#time frames	#inp vars	#gates × 10^3	cov. metric		random		CTS^{aprx}	
				#tests	time (s)	#tests	time (s)	#tests	time (s)
bobco..	19	38	1.6	740	0.4	$1.0*10^7$	294	3,339	1.1
cmugig..	4	88	4.3	2,150	6.3	$1.4*10^6$	158	923	3.7
eijks256	39	117	18	8,976	70	$4.5*10^6$	5,000	183	31
kenopp1	3	129	1.7	1,202	0.5	10^8	695	1,344	0.4
nusmv-guidan..	6	504	10	7,922	27	$2.1*10^7$	5,000	378	2.3
nusmvt-casp2	7	1,029	19	11,510	82	$4.5*10^7$	5,000	3,549	53
cmupe-riodic	34	1,220	51	30,999	760	$9.5*10^6$	5,000	5,611	240
pj2002	4	4,054	137	61,113	3,868	$0.6*10^6$	5,000	161	7.9

Conclusions

- White-box testing $\Rightarrow$ non-trivial CTS
- Even a non-trivial CTS is usually impractical
- Build CTS^{aprx}, approximation of CTS
- CTS^{aprx} can be computed efficiently
- CTS^{aprx} preserves high quality of CTS
- Our approach has numerous applications