Fast Formal Verification of Multiplier Circuits using Computer Algebra

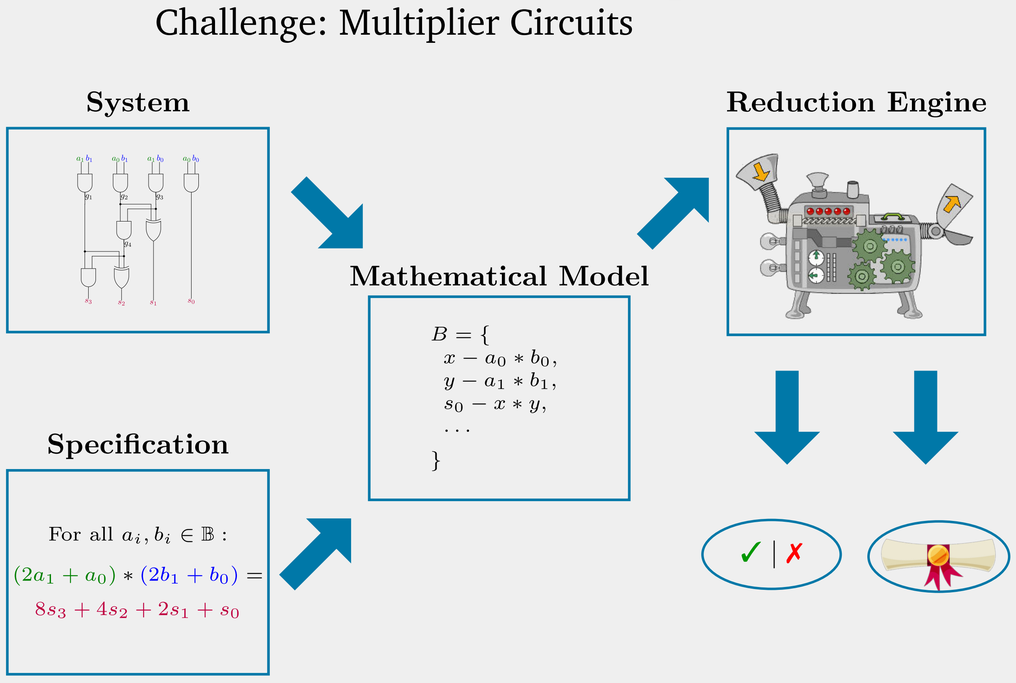
JOHANNES KEPLER UNIVERSITY LINZ

Daniela Kaufmann
fmv.jku.at/kaufmann

Formal Verification

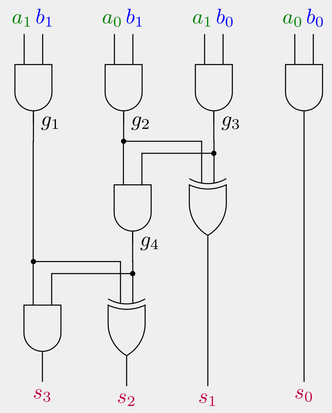
Bugs in hardware are expensive!

Challenge: Multiplier Circuits



Computer Algebra

System



Model

$s_3 = g_1 \wedge g_4$	$-s_3 + g_1 g_4,$
$s_2 = g_1 \oplus g_4$	$-s_2 - 2g_4 g_1 + g_4 + g_1,$
$g_4 = g_2 \wedge g_3$	$-g_4 + g_2 g_3,$
$s_1 = g_2 \oplus g_3$	$-s_1 - 2g_2 g_3 + g_2 + g_3,$
$g_1 = a_1 \wedge b_1$	$-g_1 + a_1 b_1,$
$g_2 = a_0 \wedge b_1$	$-g_2 + a_0 b_1,$
$g_3 = a_1 \wedge b_0$	$-g_3 + a_1 b_0,$
$s_0 = a_0 \wedge b_0$	$-s_0 + a_0 b_0,$
$a_1 \in \mathbb{B}$	$-a_1^2 + a_1,$
$a_0 \in \mathbb{B}$	$-a_0^2 + a_0,$
$b_1 \in \mathbb{B}$	$-b_1^2 + b_1,$
$b_0 \in \mathbb{B}$	$-b_0^2 + b_0$

Specification

$(2a_1 + a_0) * (2b_1 + b_0) =$
$8s_3 + 4s_2 + 2s_1 + s_0$

Reduction

$8s_3 + 4s_2 + 2s_1 + s_0 - 4a_1b_1 - 2a_1b_0 - 2a_0b_1 - a_0b_0$
$4s_2 + 8g_4g_1 + 2s_1 + s_0 - 4a_1b_1 - 2a_1b_0 - 2a_0b_1 - a_0b_0$
$4g_4 + 2s_1 + 4g_1 + s_0 - 4a_1b_1 - 2a_1b_0 - 2a_0b_1 - a_0b_0$
$\vdots$
0 ✓

Contributions

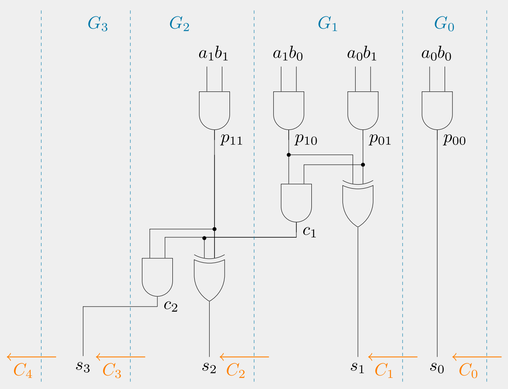
Precise Formalization [FMCAD'17]

Let $I(C) = \{p \in \mathbb{Q}[X] \mid p(X) = 0 \text{ forall } a_0, \dots, a_{n-1}, b_0, \dots, b_{n-1} \in \mathbb{B}\}$.
Let $J(C) = \langle -s_3 + g_1 g_4, -s_2 - 2g_1 g_4 + g_4 + g_1, \dots \rangle \subseteq \mathbb{Q}[X]$.

A circuit C is a *multiplier* iff $\sum_{i=0}^{2n-1} 2^i s_i - \left(\sum_{i=0}^{n-1} 2^i a_i\right)\left(\sum_{i=0}^{n-1} 2^i b_i\right) \in I(C)$.

Soundness and completeness: For acyclic circuits C, we have $J(C) = I(C)$.

Incremental Column-Based Algorithm [FMCAD'17]



Column-Wise Checking Algorithm

input: Circuit C with sliced Gröbner bases G_i
output: Determine whether C is a multiplier

$C_{2n} \leftarrow 0$
for $i \leftarrow 2n-1$ **to** 0
  $C_i \leftarrow$ Remainder $(2C_{i+1} + s_i - P_i, \quad G_i)$
return $C_0 = 0$

Proof Certificates [SC2'18]

Practical algebraic calculus:
Sequence $P = (p_1, \dots p_n)$, where each p_k is obtained by:

$+ : p_i,\ p_j,\ p_i + p_j;$ $\quad p_i, p_j$ appearing earlier in the proof

$* : p_i,\ q,\ qp_i;$ $\quad p_i$ appearing earlier in the proof, q arbitrary

Certificates are obtained as by-product of polynomial reduction.

Simplified Rewriting Techniques [DATE'18, FMCAD'19]

Full Adder

$-c_2 + g_2 + g_1 - g_2 g_1,$
$-s_2 + g_0 + c_1 - 2g_0 c_1,$
$-g_2 + g_0 c_1,$
$-g_1 + p_{20} p_{11},$
$-g_0 + p_{20} + p_{11} - 2p_{20} p_{11}$
→ $-2c_2 - s_2 + p_{20} + p_{11} + c_1$

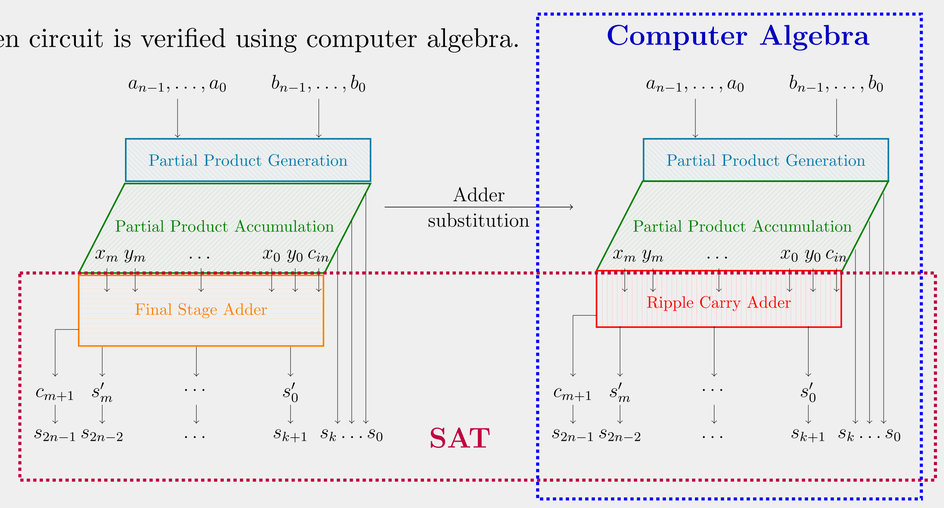
- Previously: Identify syntactic patterns.
- New: Identify single-dependency variables.
- Eliminate internal variables.
- Uses elimination theory of Gröbner bases.

Modular Reasoning [FMCAD'19]

- Use polynomial ring $\mathbb{Z}_{2^l}[X]$, with $l \in \mathbb{N}$, instead of $\mathbb{Q}[X]$.
- Eliminates certain vanishing monomials.
- Allows verification of truncated multipliers.

SAT & Computer Algebra [FMCAD'19, DATE'20]

- Substitute final stage adders by simpler adder circuits.
- Correctness of replacement is verified using SAT.
- Rewritten circuit is verified using computer algebra.



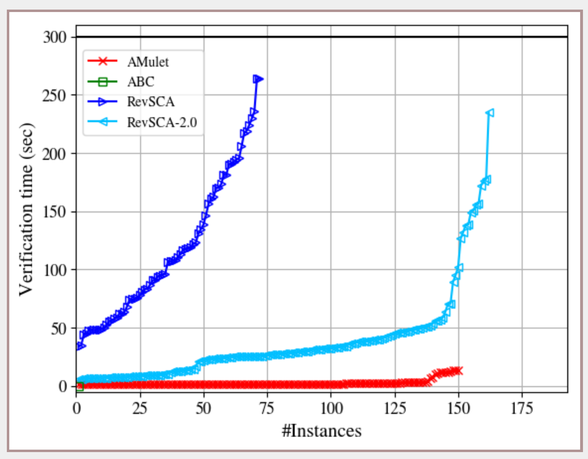
Experimental Results

Verification Tool AMulet [github.com/d-kfmnn/amulet]

- 192 multiplier architectures.
- Input bit-width $n = 64$.
- Time out: 300 sec.

Comparing to

- ABC: M. Ciesielski et al., TCAD, 2019.
- RevSCA: A. Mahzoon et al., DAC, 2019.
- RevSCA-2.0: A. Mahzoon et al., 2020.



AMulet & Proof Checker PACtrim [fmv.jku.at/pac]

- Scales up to bit-width 2048.
- None of related work produces certificates.
- Time in min.

architecture	bit-width	Verify				Verify + Certificates				Check Certificates			total
		sub	sat	c.alg	tot	sub	sat	c.alg	tot	sat	c.alg	tot	
btor	512	0	0	16	16	0	0	23	23	0	7	7	30
kjvnkv	512	0	0	13	13	0	0	15	15	0	9	9	25
sp-ar-rc	512	0	0	13	13	0	0	16	16	0	10	10	26
sp-dt-lf	512	1	0	25	26	1	0	25	26	0	11	11	37
sp-wt-bk	512	1	0	26	27	0	0	26	26	0	11	11	38
btor	1024	2	0	177	179	2	0	219	219	0	51	51	272
kjvnkv	1024	2	0	91	93	2	0	172	172	0	72	72	245
btor	2048	17	0	1 493	1 510	17	0	2 552	2 552	0	430	430	2 982
kjvnkv	2048	18	0	1 129	1 147	18	0	2 077	2 077	0	1 228	1 228	3 307

PhD Forum - Design, Automation and Test in Europe Conference (DATE) 2020