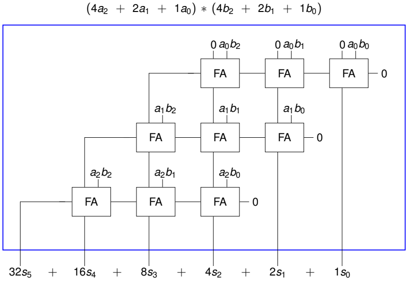
Complexity of Circuit Ideal Membership Testing

Daniela Ritirc, Armin Biere, Manuel Kauers
Johannes Kepler University
Linz, Austria

SC-Square Workshop 2017
University of Kaiserslautern, Germany
29. July 2017

Given: a (gate level) multiplier circuit C for fixed-size bitwidth n



Question: For all $a_i, b_i \in \mathbb{B}$:
$\sum_{i=0}^{2n-1} 2^i s_i - \left(\sum_{i=0}^{n-1} 2^i a_i\right)\left(\sum_{i=0}^{n-1} 2^i b_i\right)$?

Motivation

- verify circuits to avoid issuses like Pentium FDIV bug

Solving Techniques

- SAT using CNF encoding
- Binary Moment Diagrams (BMD)
- Algebraic reasoning

SAT

- verifying even small multipliers (16 Bit) is challenging (empirically)
- conjecture [Biere'16]: even simple ring-properties, e.g., $x \cdot y = y \cdot x$, require exponential sized resolution proofs (for gate-level CNF encoding)
- recent theoretical result [BeameLiew'17]:
  polynomial sized resolution proofs for simple ring-properties exist
- no theoretical nor practical results on general multiplier verification

Motivation & Solving Techniques

SAT

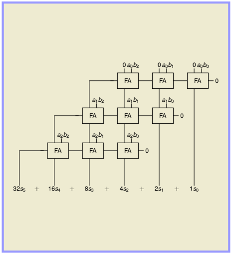
- verifying even small multipliers (16 Bit) is challenging (empirically)
- conjecture [Biere'16]: even simple ring-properties, e.g., $x \cdot y = y \cdot x$, require exponential sized resolution proofs (for gate-level CNF encoding)
- recent theoretical result [BeameLiew'17]:
  polynomial sized resolution proofs for simple ring-properties exist
- no theoretical nor practical results on general multiplier verification

BMD

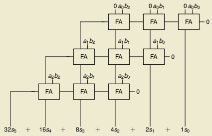
- approach not robust
- requires structural knowledge
- only works for simple (clean) multipliers

JOHANNES KEPLER UNIVERSITY LINZ

Multiplier


0 a0b2
0 a0b1
0 a0b0
FA
FA
FA
0
a1b2
a1b1
a1b0
FA
FA
FA
0
a2b2
a2b1
a2b0
FA
FA
FA
0
32s5 + 16s4 + 8s3 + 4s2 + 2s1 + 1s0

Multiplier



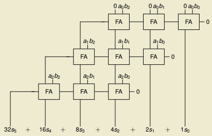
Translation

AigMulToPoly

Gröbner basis

$$B = \{\; x - a_0 * b_0,\; y - a_1 * b_1,\; s_0 - x * y,\; \}$$

Multiplier



Translation

AIGMULTOPOLY

Gröbner basis

$$B = \{\; x - a_0 * b_0,\; y - a_1 * b_1,\; s_0 - x * y,\; \}$$

Reduction

CA System

Verification

$= 0$ ✓

$\neq 0$ ✗

$$
\begin{aligned}
f &= 2x + 4y + 3 &\in \mathbb{Q}[x,y] \\
g &= y + 1 &\in \mathbb{Q}[x,y]
\end{aligned}
$$

- **Ring** $\mathbb{Q}[x,y]$
  ring of polynomials with variables x, y and coefficients in $\mathbb{Q}$

- **Polynomial** f, g
  finite sum of monomials

$$f = 2x + 4y + 3 \in \mathbb{Q}[x, y]$$
$$g = y + 1 \qquad\qquad \in \mathbb{Q}[x, y]$$

- **Monomial**
  constant multiple of a term
- **Term**
  power product $x^{e_1} y^{e_2}$ for $e_1, e_2 \in \mathbb{N}$
- **Term order**
  well-defined, $x > y > 1$
- **Leading monomial/term/coefficient**

JKU JOHANNES KEPLER UNIVERSITY LINZ

$$f = 2x + 4y + 3 \in \mathbb{Q}[x, y]$$
$$g = y + 1 \qquad \in \mathbb{Q}[x, y]$$

- **Ideal generated by $\mathbf{f}, \mathbf{g}$**
  $I = \{q_1 f + q_2 g \mid q_1, q_2 \in \mathbb{Q}[x, y]\} = \langle f, g\rangle$

$$I = \langle f, g \rangle = \langle 2x + 4y + 3, y + 1 \rangle$$

- **Ideal generated by $\mathbf{f}, \mathbf{g}$**
  $I = \{q_1 f + q_2 g \mid q_1, q_2 \in \mathbb{Q}[x, y]\} = \langle f, g \rangle$

  "I contains all elements which evaluate to 0, when f and g evaluate to 0"

$$I = \langle f, g \rangle = \langle 2x + 4y + 3, y + 1 \rangle$$

- **Ideal membership problem**
  Question: $h = 6x + y^3 + y^2 + 12y + 9 \in I$?

$$I = \langle f, g \rangle = \langle 2x + 4y + 3, y + 1 \rangle$$

- **Ideal membership problem**
  Question: $h = 6x + y^3 + y^2 + 12y + 9 \in I$?
  - for I: a priori not obvious how to check this
  - for a Gröbner basis G: “easy” reduction method really?

$$I = \langle f, g \rangle = \langle 2x + 4y + 3, y + 1 \rangle$$

- **Ideal membership problem**
  Question: $h = 6x + y^3 + y^2 + 12y + 9 \in I$?
  - for I: a priori not obvious how to check this
  - for a Gröbner basis G: "easy" reduction method really?
- **Gröbner basis**
  - every ideal of $\mathbb{Q}[X]$ has a Gröbner basis
  - construction algorithm by Buchberger

JKU JOHANNES KEPLER UNIVERSITY LINZ

$$I = \langle f, g \rangle = \langle \underline{2x} + 4y + 3, \underline{y} + 1 \rangle$$

- **Ideal membership problem**
  Question: $h = 6x + y^3 + y^2 + 12y + 9 \in I$?
  - for I: a priori not obvious how to check this
  - for a Gröbner basis G: "easy" reduction method really?
- **Gröbner basis**
  - every ideal of $\mathbb{Q}[X]$ has a Gröbner basis
  - construction algorithm by Buchberger
  - special case:
    leading terms of ideal generators have no variables in common

$$I = \langle f, g \rangle = \langle \underline{2x} + 4y + 3, \underline{y} + 1 \rangle$$
$$G = \{2x + 4y + 3, y + 1\}$$

- **Ideal membership problem**
  Question: $h = 6x + y^3 + y^2 + 12y + 9 \in I$?
  - for I: a priori not obvious how to check this
  - for a Gröbner basis G: "easy" reduction method really?

- **Gröbner basis**
  - every ideal of $\mathbb{Q}[X]$ has a Gröbner basis
  - construction algorithm by Buchberger
  - special case:
    leading terms of ideal generators have no variables in common

$G = \{f, g\}$ is a Gröbner basis for I

JKU JOHANNES KEPLER UNIVERSITY LINZ

$$I = \langle f, g \rangle = \langle 2x + 4y + 3, y + 1 \rangle$$
$$G = \{2x + 4y + 3, y + 1\}$$

- **Ideal membership problem**
  Question: $h = 6x + y^3 + y^2 + 12y + 9 \in I$?
  - for I: a priori not obvious how to check this
  - for a Gröbner basis G: "easy" reduction method really?
- **Reduction**
  multivariate version of polynomial division with remainder
  - divide h by elements of G
  - remainder r contains no term that is a multiple of any of the leading terms of G
  - Notation: r = Remainder(h, G)

$$I = \langle f, g \rangle = \langle 2x + 4y + 3, y + 1 \rangle$$
$$G = \{2x + 4y + 3, y + 1\}$$

- **Ideal membership problem**
  Question: $h = 6x + y^3 + y^2 + 12y + 9 \in I$?

$$I = \langle f, g \rangle = \langle 2x + 4y + 3, y + 1 \rangle$$
$$G = \{2x + 4y + 3, y + 1\}$$

- **Ideal membership problem**
  Question: $h = 6x + y^3 + y^2 + 12y + 9 \in I$?

  Answer: Yes
  $h = 3 * (2x + 4y + 3) + y^2 * (y + 1)$
  Remainder(h, G)=0

$$I = \langle f, g \rangle = \langle 2x + 4y + 3, y + 1 \rangle$$
$$G = \{2x + 4y + 3, y + 1\}$$

- **Ideal membership problem**
  Question: $h = 6x + y^3 + y^2 + 12y + 10 \in I$?

$$I = \langle f, g \rangle = \langle 2x + 4y + 3, y + 1 \rangle$$
$$G = \{2x + 4y + 3, y + 1\}$$

- **Ideal membership problem**
  Question: $h = 6x + y^3 + y^2 + 12y + 10 \in I$?

  Answer: No
  $h = 3 * (2x + 4y + 3) + y^2 * (y + 1) + 1$
  Remainder(h, G)=1

Polynomial Representation of Circuit Gates

Polynomial Representation of Circuit Gates

- Boolean Gate Polynomials

$$
\begin{array}{lll}
u = \neg v & \text{implies} & 0 = -u + 1 - v \\
u = v \wedge w & \text{implies} & 0 = -u + vw \\
u = v \vee w & \text{implies} & 0 = -u + v + w - vw \\
u = v \oplus w & \text{implies} & 0 = -u + v + w - 2vw
\end{array}
$$

Polynomial Representation of Circuit Gates

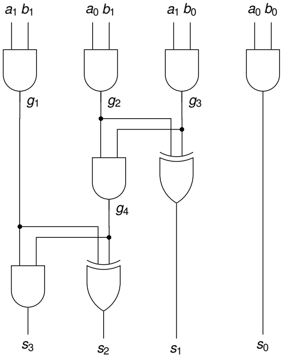
- Boolean Gate Polynomials

$$
\begin{aligned}
u = \neg v &\quad \text{implies} \quad 0 = -u + 1 - v \\
u = v \wedge w &\quad \text{implies} \quad 0 = -u + vw \\
u = v \vee w &\quad \text{implies} \quad 0 = -u + v + w - vw \\
u = v \oplus w &\quad \text{implies} \quad 0 = -u + v + w - 2vw
\end{aligned}
$$

- Field Polynomials

$$
\text{“ } u \in \mathbb{B} \text{ ”} \quad \text{implies} \quad 0 = u(u-1) \qquad 0 = u^2 - u
$$

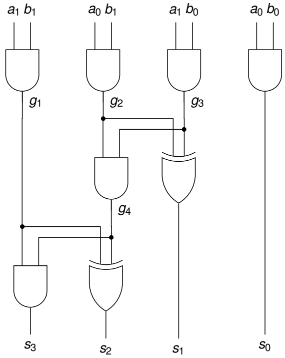
n-Bit Multipliers



- $n * n = 2n$
- $2n$ inputs: $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1}$
- $2n$ outputs: $s_0, \ldots, s_{2n-1}$
- one variable to each internal gate output: $g_0, \ldots, g_k$

JKU JOHANNES KEPLER UNIVERSITY LINZ

n-Bit Multipliers



- $n * n = 2n$
- $2n$ inputs: $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1}$
- $2n$ outputs: $s_0, \ldots, s_{2n-1}$
- one variable to each internal gate output: $g_0, \ldots, g_k$

Values of $g_0, \ldots, g_k$ and $s_0, \ldots, s_{2n-1}$ are uniquely determined as soon as $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1}$ are fixed.

Polynomial Circuit Constraints

- A polynomial p is called a *polynomial circuit constraint (PCC)* for a circuit C if for every choice of

$$(a_0, \dots, a_{n-1}, b_0, \dots, b_{n-1}) \in \{0,1\}^{2n}$$

and resulting values $g_1, \dots, g_k, s_0, \dots, s_{2n-1}$ implied by the gates of C the substitution of these values into p gives zero.

JKU JOHANNES KEPLER UNIVERSITY LINZ

Polynomial Circuit Constraints

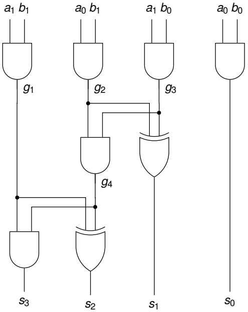
- A polynomial p is called a *polynomial circuit constraint (PCC)* for a circuit C if for every choice of

$$(a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1}) \in \{0, 1\}^{2n}$$

  and resulting values $g_1, \ldots, g_k, s_0, \ldots, s_{2n-1}$ implied by the gates of C the substitution of these values into p gives zero.
- The set of all PCCs for C is denoted by $I(C)$.
- $I(C)$ is an ideal.

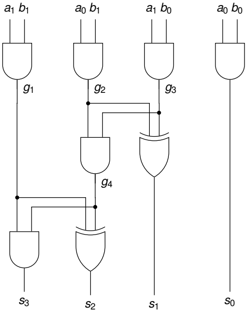
JOHANNES KEPLER UNIVERSITY LINZ

Ideals associated to Circuits



Examples for PCCs:

- $p_0 = s_0 - a_0 b_0$ — and gate
- $p_1 = a_1^2 - a_1$ — a_1 boolean
- $p_2 = g_2^2 - g_2$ — g_2 boolean
- $p_3 = s_1 g_4$ — xor-and constraint
- ...



Examples for PCCs:

- $p_0 = s_0 - a_0 b_0$ — and gate
- $p_1 = a_1^2 - a_1$ — a_1 boolean
- $p_2 = g_2^2 - g_2$ — g_2 boolean
- $p_3 = s_1 g_4$ — xor-and constraint
- ...

A circuit C is called a *multiplier* if

$$\sum_{i=0}^{2n-1} 2^i s_i - \left(\sum_{i=0}^{n-1} 2^i a_i\right)\left(\sum_{i=0}^{n-1} 2^i b_i\right) \in I(C).$$

Problem: Definition of $I(C)$ does not provide a basis

Problem: Definition of $I(C)$ does not provide a basis

We can deduce at least some elements of $I(C)$:

- $G = \{\text{Gate Polynomials}\} \cup \{\text{Field Polynomials for inputs}\}$
- The ideal generated by G is denoted by $J(C)$.

JKU JOHANNES KEPLER UNIVERSITY LINZ

Problem: Definition of $I(C)$ does not provide a basis

We can deduce at least some elements of $I(C)$:

- $G = \{\text{Gate Polynomials}\} \cup \{\text{Field Polynomials for inputs}\}$
- The ideal generated by G is denoted by $J(C)$.

- Reverse topological order:
  output variable of a gate is greater than input variables
  $\rightarrow$Then G is a Gröbner basis for $J(C)$.

Theorem

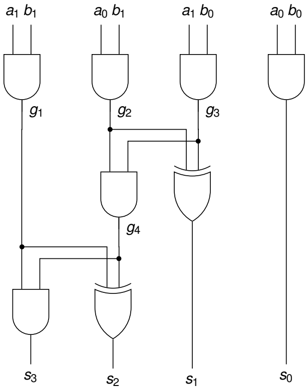
For all acyclic circuits C, we have $J(C) = I(C)$.

JKU
JOHANNES KEPLER
UNIVERSITY LINZ

Theorem

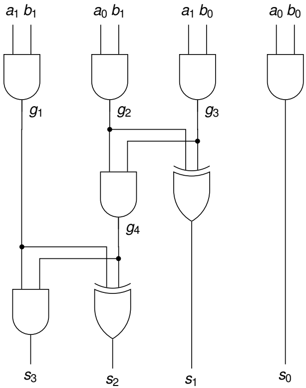
For all acyclic circuits C, we have $J(C) = I(C)$.

- $J(C) \subseteq I(C)$: corresponds to soundness
- $I(C) \subseteq J(C)$: corresponds to completeness

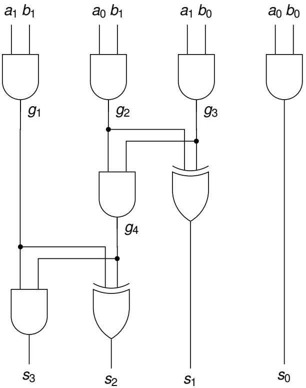


$J(C) = \langle$

Ideals associated to Circuits



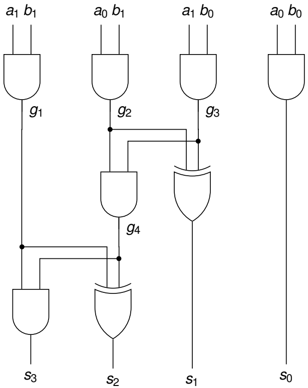
$$J(C) = \langle$$
$$-s_3 + g_1 g_4,$$
$$-s_2 + g_1 + g_4 - 2g_1 g_4,$$



$$J(C) = \langle$$
$$-s_3 + g_1 g_4,$$
$$-s_2 + g_1 + g_4 - 2g_1 g_4,$$
$$-g_4 + g_2 g_3,$$
$$-s_1 + g_2 + g_3 - 2g_2 g_3,$$

JOHANNES KEPLER UNIVERSITY LINZ

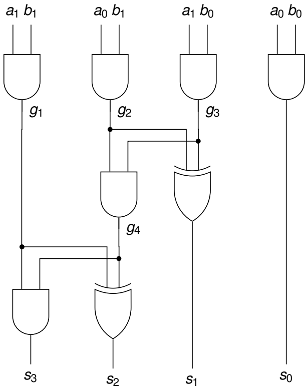
Ideals associated to Circuits



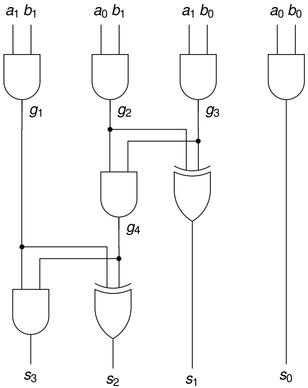
$$J(C) = \langle$$

$$-s_3 + g_1 g_4,$$
$$-s_2 + g_1 + g_4 - 2g_1 g_4,$$
$$-g_4 + g_2 g_3,$$
$$-s_1 + g_2 + g_3 - 2g_2 g_3,$$
$$-g_1 + a_1 b_1,$$
$$-g_2 + a_0 b_1,$$
$$-g_3 + a_1 b_0,$$
$$-s_0 + a_0 b_0,$$

Ideals associated to Circuits



$$
\begin{aligned}
J(C) = \langle \\
& -s_3 + g_1 g_4, \\
& -s_2 + g_1 + g_4 - 2 g_1 g_4, \\
& -g_4 + g_2 g_3, \\
& -s_1 + g_2 + g_3 - 2 g_2 g_3, \\
& -g_1 + a_1 b_1, \\
& -g_2 + a_0 b_1, \\
& -g_3 + a_1 b_0, \\
& -s_0 + a_0 b_0, \\
& -a_1^2 + a_1, -a_0^2 + a_0, \\
& -b_1^2 + b_1, -b_0^2 + b_0 \rangle
\end{aligned}
$$

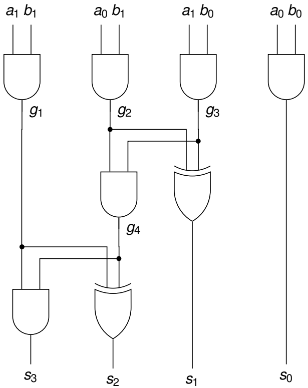


$$
\begin{aligned}
J(C) = \langle\ & \\
& -s_3 + g_1 g_4, \\
& -s_2 + g_1 + g_4 - 2 g_1 g_4, \\
& -g_4 + g_2 g_3, \\
& -s_1 + g_2 + g_3 - 2 g_2 g_3, \\
& -g_1 + a_1 b_1, \\
& -g_2 + a_0 b_1, \\
& -g_3 + a_1 b_0, \\
& -s_0 + a_0 b_0, \\
& -a_1^2 + a_1, -a_0^2 + a_0, \\
& -b_1^2 + b_1, -b_0^2 + b_0 \rangle
\end{aligned}
$$

Order: $s_3 > s_2 > g_4 > s_1 > g_1 > g_2 > g_3 > s_0 > a_1 > a_0 > b_1 > b_0$

$\Rightarrow$ Generators of J(C) form a Gröbner basis

JOHANNES KEPLER UNIVERSITY LINZ



$$
\begin{aligned}
J(C) = \langle\ & \\
& -s_3 + g_1 g_4, \\
& -s_2 + g_1 + g_4 - 2g_1 g_4, \\
& -g_4 + g_2 g_3, \\
& -s_1 + g_2 + g_3 - 2g_2 g_3, \\
& -g_1 + a_1 b_1, \\
& -g_2 + a_0 b_1, \\
& -g_3 + a_1 b_0, \\
& -s_0 + a_0 b_0, \\
& -a_1^2 + a_1, -a_0^2 + a_0, \\
& -b_1^2 + b_1, -b_0^2 + b_0 \rangle
\end{aligned}
$$

Order: $s_3 > s_2 > g_4 > s_1 > g_1 > g_2 > g_3 > s_0 > a_1 > a_0 > b_1 > b_0$

$\Rightarrow$ Generators of J(C) form a Gröbner basis

Question: $8s_3 + 4s_2 + 2s_1 + s_0 - (2a_1 + a_0)(2b_1 + b_0) \in J(C)$?

JKU JOHANNES KEPLER UNIVERSITY LINZ

Corollary

Checking non-ideal membership over $\mathbb{Q}[x_1, \ldots, x_n]$ even in terms of a given Gröbner basis is NP-hard.

COROLLARY

Checking non-ideal membership over $\mathbb{Q}[x_1, \ldots, x_n]$ even in terms of a given Gröbner basis is NP-hard.

Connection between circuit SAT and ideal membership testing

known	(circuit) SAT	circuit	ideal membership	claim

JKU
JOHANNES KEPLER UNIVERSITY LINZ

COROLLARY

Checking non-ideal membership over $\mathbb{Q}[x_1, \ldots, x_n]$ even in terms of a given Gröbner basis is NP-hard.

Connection between circuit SAT and ideal membership testing

known	(circuit) SAT	circuit	ideal membership	claim
NP-complete	SAT	not constant		

JOHANNES KEPLER UNIVERSITY LINZ

COROLLARY

Checking non-ideal membership over $\mathbb{Q}[x_1, \dots, x_n]$ even in terms of a given Gröbner basis is NP-hard.

Connection between circuit SAT and ideal membership testing

known	(circuit) SAT	circuit	ideal membership	claim
NP-complete	SAT	not constant	$\rightarrow x, x \neq 0$	NP-hard

COROLLARY

Checking non-ideal membership over $\mathbb{Q}[x_1, \ldots, x_n]$ even in terms of a given Gröbner basis is NP-hard.

Connection between circuit SAT and ideal membership testing

known	(circuit) SAT	circuit	ideal membership	claim
NP-complete	SAT	not constant	$\rightarrow x, x \neq 0$	NP-hard
Co-NP-complete	UNSAT	constant 0		

JOHANNES KEPLER UNIVERSITY LINZ

COROLLARY

Checking non-ideal membership over $\mathbb{Q}[x_1, \ldots, x_n]$ even in terms of a given Gröbner basis is NP-hard.

Connection between circuit SAT and ideal membership testing

known	(circuit) SAT	circuit	ideal membership	claim
NP-complete	SAT	not constant	$\rightarrow x, x \neq 0$	NP-hard
Co-NP-complete	UNSAT	constant 0	$\rightarrow 0$	Co-NP hard

JKU JOHANNES KEPLER UNIVERSITY LINZ

NP-hard

- transform circuit SAT problem into ideal non-membership testing
- preserves NP-hardness

NP-hard

- transform circuit SAT problem into ideal non-membership testing
- preserves NP-hardness

NP

- open question: non-membership in NP (probably not)
- h in ideal $\Leftrightarrow$ $h = \sum p_i * g_i$ for some p_i (membership)
- h not in ideal $\Leftrightarrow$ $h \neq \sum p_i * g_i$ for all p_i (non-membership)
- sufficient condition for membership being in NP:
  - or equivalently non-membership in Co-NP
  - p_i can be restricted to have polynomial size (in our situation)
  - but then NP = Co-NP

Conclusion & Future Work

Conclusion

- simple and precise mathematical formulation
- complexity result: circuit verification using computer algebra is hard
- results part of an upcoming FMCAD'17 paper
  - with further experimental results and
  - a novel column-wise incremental verification approach

Future Work

- modular multiplication ($32 \times 32 \rightarrow 32$ multiplier)
- algebraic specification of other arithmetic operators
- algebraically verifying ring-properties
- upper bounds

JKU JOHANNES KEPLER UNIVERSITY LINZ

Complexity of Circuit Ideal Membership Testing

Daniela Ritirc, Armin Biere, Manuel Kauers
Johannes Kepler University
Linz, Austria

SC-Square Workshop 2017
University of Kaiserslautern, Germany
29. July 2017

Der Wissenschaftsfonds.

Rigorous Systems Engineering

JOHANNES KEPLER UNIVERSITY LINZ