Verifying Properties of Bit-vector Multiplication Using Cutting Planes Reasoning

Liew, Vincent; Beame, Paul; Devriendt, Jo; Elffers, Jan; Nordström, Jakob

Published in:

DOI:
10.34727/2020/isbn.978-3-85448-042-6_27

Publication date:
2020

Document version
Publisher's PDF, also known as Version of record

Document license:
CC BY

Citation for published version (APA):
Abstract—Systems mixing Boolean logic and arithmetic have
been a long-standing challenge for verification tools such as SAT-
based bit-vector solvers. Though SAT solvers can be highly effi-
cient for Boolean reasoning, they scale poorly once multiplication
is involved. Algebraic methods using Gröbner basis reduction
have recently been used to efficiently verify multiplier circuits in
isolation, but generally do not perform well on problems involving
bit-level reasoning.

We propose that pseudo-Boolean solvers equipped with cutting
planes reasoning have the potential to combine the complemen-
tary strengths of the existing SAT and algebraic approaches while
avoiding their weaknesses.

Theoretically, we show that there are optimal-length cutting
planes proofs for a large class of bit-level properties of some well
known multiplier circuits. This scaling is significantly better than
the smallest proofs known for SAT and, in some instances, for
algebraic methods. We also show that cutting planes reasoning
can extract bit-level consequences of word-level equations in
exponentially fewer steps than methods based on Gröbner bases.

Experimentally, we demonstrate that pseudo-Boolean solvers
can verify the word-level equivalence of adder-based multiplier
architectures, as well as commutativity of bit-vector multipli-
cation, in times comparable to the best algebraic methods. We
then go further than previous approaches and also verify these
properties at the bit-level. Finally, we find examples of simple
nonlinear bit-vector inequalities that are intractable for current
bit-vector and SAT solvers but easy for pseudo-Boolean solvers.

Index Terms—Multiplier circuits, bit-vector arithmetic, ver-
ification, pseudo-Boolean solving, cutting planes, SAT solving,
Gröbner bases

I. INTRODUCTION

While there has been great progress in verification tools
since the 1980s, current methods still cannot efficiently deal
with problems that combine multiplication and Boolean op-
erations. These problems are encapsulated in the theory of
bit-vector arithmetic, which supports both common bit-level
operations like shifting and word-level arithmetic operations
like addition and multiplication of bit-vectors. Thus, bit-vector
formulas can express the behavior of a program or arithmetic
circuit in a natural, yet bit-precise, manner.

Though deciding bit-vector formulas is NEXPTIME-
complete in general [31], current bit-vector solvers are fairly
efficient on many problems arising in practice ([12], [18], [22],
[27], [38], [41], [47]). However, for instances that involve
multiplication these solvers must often rely on the bit-blasting
approach [32], which determines the satisfiability of a bit-
vector formula by converting it into an equisatisfiable CNF
formula to be fed into a conflict-driven clause learning (CDCL)
SAT solver ([4], [39], [42]).

While CDCL SAT solvers effectively handle bit-level op-
erations, they tend to perform poorly when multiplication is
involved, with running times scaling exponentially in the bit-
width on such problems ([8], [14], [30]). CDCL solvers are
based on resolution ([11], [46]), in the sense that a resolution
proof can be extracted from the execution trace for an unsat-
sifiable formula [5]. Thus, weaknesses of this proof system
impose hard limits on solver performance. Resolution is very
poor at tasks like counting [24] and mod-2 reasoning [52], and
though degree-2 multiplier identities were recently shown to
have polynomial-size proofs [7], these proofs are quite large.
To unlock the ability to solve even more complicated formulas
that mix bit-level reasoning with multiplication, we need to
fundamentally improve the back-end reasoning.

Two natural approaches for strengthening resolution-based
reasoning are embodied by the proof systems polynomial
calculus [16], which reasons with polynomials instead of
clauses, and cutting planes [17], which operates on 0-1 lin-
ear inequalities. Both of these proof systems can efficiently
simulate resolution, and can be exponentially stronger.

Computer algebra has recently emerged as a powerful tool
for verifying isolated gate-level multiplier circuits ([10], [15],
[36], [37], [44], [45], [50], [51], [54]). A major advantage of
Gröbner basis methods, which perform algebraic reasoning that is captured by the polynomial calculus proof system, is that they operate with polynomials instead of disjunctive clauses. This makes it possible to encode the correctness of a multiplier with input bit-vectors \( x, y \) and output bit-vector \( (xy) \) through the word-level specification equation:

\[
\left( \sum_{i=0}^{n-1} 2^i x_i \right) \left( \sum_{i=0}^{n-1} 2^i y_i \right) - \left( \sum_{i=0}^{2n-1} 2^i (xy)_i \right) = 0.
\]

Unfortunately, for the non-algebraic parts of circuits, Gröbner basis methods are typically orders of magnitude slower than SAT solvers and scale poorly on general reasoning. We provide an explanation for this by showing, drawing on [25], that Gröbner basis methods require an exponential number of steps to derive bit-level consequences of word-level properties. Hence, these methods are unlikely to supplant the role of SAT solvers for bit-vector arithmetic.

We propose instead that conflict-driven pseudo-Boolean solvers [13] that take advantage of the cutting planes method for 0-1 linear inequalities [17] have the potential to achieve the “best of both worlds”, combining the strengths of Gröbner basis methods for polynomials with the efficiency of CDCL SAT solvers for Boolean reasoning. Cutting planes reasoning can easily express word-level properties and does not suffer the same obstacles as polynomial calculus, since only a linear number of steps are needed to derive all of the individual bit-equalities from a word-level equality.

An essential aspect of this approach in improving on SAT-based methods is that one can express the correctness of 1-bit adders, basic building blocks of arithmetic circuits, directly via pairs of inequalities, instead of using sets of clauses, and one can similarly directly express word-level properties of circuit outputs. Together, these yield a higher-level fully precise form of “bit-blasting”.

The main theoretical contribution of this paper is the construction of optimal, \( O(n^2) \)-length cutting planes proofs for a large class of \( n \)-bit ring identities, including commutativity and distributivity. We emphasize that these identities can be proven not only at the word level, but also for individual bits. While \( O(n^2) \)-length polynomial calculus proofs are known for some of these properties at the word level [29], this algebraic method cannot efficiently extract the bit-equalities. As a consequence, for example, the best known polynomial calculus proof for the bit-level property “the middle bit of \( xy \) equals the middle bit of \( yx \)” is still the \( O(n^3 \log n) \)-length resolution proof given by [7], which is much larger than our \( O(n^2) \)-length cutting planes proof.

These ring identities appeared previously as testbed instances representing the gap between word-level and bit-level methods of reasoning. For example, it was observed in 2016 that proving the commutativity of a multiplier circuit is already intractable for SAT solving at 16 bits [9]. While bit-vector solvers try to overcome this shortcoming of SAT by implementing word-level preprocessing and inprocessing, the verification of larger systems containing multiplication and bit-logic (that appear for instance, in cryptography) remains a key weakness. The ability to verify these ring identities at the bit level, rather than through preprocessing, is a good test for the potential of any method for verifying these more complex systems.

Experimentally, we are able to use pseudo-Boolean solvers to verify the word-level equivalence of several different multiplier circuits of up to 256 bits in similar times to those of the best algebraic methods. We find that these solvers can be particularly efficient at extracting all of the bit-level equalities from a word-level equality, which neither CDCL solvers nor Gröbner basis reduction can do efficiently.

We also show that pseudo-Boolean solvers can be used to efficiently verify a number of bit-vector inequalities combining multiplication with bit-wise operations. In contrast, these inequalities are much harder or intractable for the top bit-solvers Boolector ([12], [43]), Z3 [18], Yices [19] and CVC4 [2]. Our examples demonstrate some of the potential of pseudo-Boolean solvers for reasoning with nonlinear, bit-precise systems that are out of reach of current methods. These bit-vector inequalities are inspired by the combinations of arithmetic and bit-wise operations that naturally arise in embedded systems or high-performance computation, where “bit hacks” can be used to implement methods such as absolute value or “reverse the bits in a byte” (see [1] and [26]) and more complicated mixtures of arithmetic and bit-wise operations are used in cryptographic and hashing computations.

II. NOTATION AND PRELIMINARIES

We write the \( i \)-th entry of a bit-vector \( x \) as a Boolean variable \( x_i \). We typically refer to circuits by the output bit-vectors that they produce — for example we use \( C \) to refer to both a circuit and its output bit-vector, depending on the context. Often we write this output bit-vector in terms of the inputs, so that a multiplier circuit denoted by \( xy \) is understood to take input bit-vectors \( x, y \) and output a bit-vector labeled \( xy \). We label the internal variables of a circuit \( C \) using the superscript \( C \), for example: \( i^C \).

**Definition** Given a set of polynomials \( \Phi \) over a set of variables \( \{x_1, x_2, \ldots, x_n\} \) and a field \( K \), a polynomial calculus refutation of \( \Phi \) is a sequence of polynomials ending with the polynomial 1 such that each line is either in \( \Phi \) or is derived from the previous lines using the inference rules of linear combination and multiplication by a monomial \( m \):

\[
p \frac{p}{\alpha p + \beta q} (\alpha, \beta \in K) , \quad \frac{p}{m \cdot p} .
\]

The polynomials \( x^2 \) are also included as axioms for each variable \( x \) so that it only takes Boolean values. The polynomial \( p \) is interpreted to mean the equation \( p = 0 \).

**Definition** Given a set of 0-1 linear inequalities \( \Phi \) over a set of variables \( \{x_1, x_2, \ldots, x_n\} \), a cutting planes refutation of \( \Phi \) is a sequence of 0-1 linear inequalities ending with the inequality \( 0 \geq 1 \) such that each line is either in \( \Phi \) or is derived from
the previous lines using the inference rules of positive linear combination
\[ \sum_i a_i x_i \geq b \quad \sum_i a'_i x_i \geq b' \]
\[ \sum_i (\alpha a_i + \beta b_i) x_i \geq \alpha b + \beta b' \]
where \( \alpha, \beta \geq 0 \), and the division rule
\[ \sum_i (c \cdot a_i) x_i \geq b \]
\[ \sum_i a_i x_i \geq \lceil \frac{b}{c} \rceil . \]
The literal axioms \(-x \geq -1\) and \( x \geq 0 \) are also included for each variable \( x \). Throughout this paper we will use \( =\) as shorthand for the two equivalent \( \leq, \geq \) inequalities.

A. A polynomial calculus lower bound for bit-extraction

The bit-extraction lower bound discussed in the introduction follows directly from the following polynomial calculus lower bound for subset-sum equations due to Impagliazzo, Pudlak and Szegedy.

Theorem II.1 ([25]). Let \( c_1, \ldots, c_n \) be nonzero real numbers such that no subset sums to the real number \( m \). Then the equation \( m - \sum_{i=1}^n c_i x_i = 0 \) has no polynomial calculus refutation of degree \( \lceil n/2 \rceil \) in the field of real numbers.

Theorem II.2 ([25]). Suppose that \( \Phi \) is a set of polynomials of degree at most \( \sqrt{n} \), where \( n \) is the number of variables appearing in \( \Phi \). Let \( d \) denote the minimum refutation degree of \( \Phi \), and \( M \) denote the minimum number of monomials in a refutation of \( \Phi \), and assume that \( M \geq 3 \). Then \( M \geq \exp \left( (d-1)^2/4n \right) \).

We combine Theorems II.1 and II.2 to demonstrate the weakness of polynomial calculus in extracting bit-level properties from word-level ones.

Corollary II.3. For a fixed integer \( k \), any polynomial calculus refutation of the system of two polynomials:

\[ f := \sum_{i=0}^{n-1} 2^i (s_i - s'_i) \]
\[ g := s_k - s'_k - 1 \]
contains at least \( e^{n/4-1} \approx 2^{0.36n} \) monomials.

Proof. Define the polynomial \( f' := \sum_{i \neq k} 2^i (s_i - s'_i) + 2k \). Observe that Theorem II.1 gives us a degree lower bound of \( n - 1 \) on refutations of the polynomial \( \{f'\} \). Theorem II.2 translates this into a monomial size lower bound of \( e^{n/4-1} \). The reduction below lifts this lower bound on \( \{f'\} \) to the polynomials \( \{f, g\} \).

We show that a length \( l \) polynomial calculus refutation of the polynomials \( \{f, g\} \) may be converted into a length \( l \) refutation of the polynomial \( \{f'\} \) without increasing the number of monomials in each line as follows: First notice that the polynomials \( f, f' \) are equivalent modulo the polynomial \( g = s_k - s'_k - 1 \). Given a PC refutation of \( \{f, g\} \), we reduce each line by \( g \) (which effectively sets \( s_k = 1 \) and \( s'_k = 0 \)), only reducing the number of monomials, to produce a refutation of \( \{f'\} \).

As a consequence of this corollary, polynomial calculus cannot derive \( s_k = s'_k \) from the first equation using fewer than \( e^{n/4-1} \) monomials. In comparison, cutting planes has small derivations that produce all of the bit-equalities.

Proposition II.4. There is an \( O(n) \)-length cutting planes derivation of all \( n \) bit-equalities \( s_i = s'_i \) from the equation \( \sum_{i=0}^{n-1} 2^i s_i - \sum_{i=0}^{n-1} 2^i s'_i = 0 \).

Proof. We extract the individual bit-equalities in the low-to-high sequence \( s_0 = s'_0, s_1 = s'_1, \ldots s_{n-1} = s'_{n-1} \). Recall that in cutting planes, the equation \( \sum_{i=0}^{n-1} 2^i s_i - \sum_{i=0}^{n-1} 2^i s'_i = 0 \) is represented by two inequalities. Take the inequality \( \sum_{i=0}^{n-1} 2^i s_i - \sum_{i=0}^{n-1} 2^i s'_i \geq 0 \) and use the literal axioms on \( s_0, s'_0 \) to get \( \sum_{i=1}^{n-1} 2^i s_i - \sum_{i=1}^{n-1} 2^i s'_i \geq -1 \). Divide this by 2 to get \( \sum_{i=1}^{n-1} 2^{i-1} s_i - \sum_{i=1}^{n-1} 2^{i-1} s'_i \geq 0 \). Finally, use linear combination to multiply this by 2 and add it to the equation \( \sum_{i=1}^{n-1} 2^i s_i - \sum_{i=1}^{n-1} 2^i s'_i \geq 0 \) to obtain the result \( s'_i - s_i \geq 0 \).

A symmetric derivation gives \( s_i - s'_i \geq 0 \).

B. Adder and multiplier circuit constructions

Definition A ring identity \( L = R \) denotes a pair of ring expressions \( L, R \) that can be transformed into each other using commutativity, distributivity and associativity.

To prove that a given ring identity \( L = R \) holds for some choice of circuit implementations for \( + \) and \( \cdot \), we use these implementations to build a circuit \( L \) representing the expression \( L \) and another circuit \( R \) for the expression \( R \). The goal of our cutting planes proofs is to show that the resulting output bit-vectors \( L, R \) are equal bit-by-bit, i.e., that \( L_i = R_i \) holds for every \( i \).

Circuits for addition and multiplication

The circuits that we will consider are built using **adders** that output, in binary, the sum of three input bits. A (1-bit) adder is encoded as follows:

Definition For an adder \( A \) with inputs \( a_0, a_1, a_2 \), the outputs \( c, d \) are determined by the equation \( a_0 + a_1 + a_2 - 2c - d = 0 \). We call \( c \) the carry-bit and \( d \) the sum-bit.

In our circuits, each variable belongs to a column, \( i \). The variables in column \( i \) have a weight of \( 2^i \). Each adder is also assigned to a column. An adder \( A \) belonging to the \( i \)-th column takes three input bits from column \( i \) and outputs a sum-bit into column \( i+1 \) and a carry-bit into column \( i+1 \). The equation associated with \( A \) ensures that the weight of its outputs is equal to the weight of its inputs.

a) Ripple-Carry Adder: Figure 1 shows the design of a ripple-carry adder \( x + y \), which takes in two bitvectors \( x, y \) and outputs their sum in binary.

b) Multiplier circuits: Figure 2 shows the design of an array multiplier and our labeling of the internal circuit variables. The first phase of an array multiplier is a common part of many multiplier designs: the circuit computes a tableau of partial products \( t_{i,j} = x_i \wedge y_j \) for each pair of input bits \( x_i \) and \( y_j \). In the second phase, \( n \) ripple-carry adders are arranged
Lemma III.1. Suppose that we have two $n$-bit array multipliers $xy$ and $yx$ implementing the two sides of the commutativity relation $xy = yx$. Further, suppose that we are given the $n^2$ equalities between the tableau variables $t^y_{i,j} = t^x_{j,i}$. Then there is a derivation in degree 1 and length $3n^2 + 1$ of the equation $\sum_{i,j=0}^{n-1} t^i(xy)_i - \sum_{i=0}^{n-1} 2^i(yx)_i = 0$ that only uses linear combinations.

Proof. We first derive two “conservation of weight” equations for the circuits $xy$ and $yx$ that state that the total weight of a multiplier’s output bits is the same as the total weight of its tableau bits. We obtain these by adding up the adder constraints, weighting them so that the internal circuit variables cancel. For an adder in column $i$ corresponding to a constraint $a_0 + a_1 + a_2 - 2c - d = 0$, this weighting simply scales the constraint up by a factor of $2^i$. Once all the $n^2$ adder equations for an array multiplier $xy$ have been summed together, we will arrive at an equation stating that the weight of tableau variables $t^y_{i,j}$ is the same as the weight of the output variables $xy$. After repeating the same steps for the multiplier $yx$, we arrive at the two equations

$$\left(\sum_{i,j=0}^{n-1} 2^{i+j}t^y_{i,j}\right) - \left(\sum_{i=0}^{n-1} 2^i(xy)_i\right) = 0$$

$$\left(\sum_{i,j=0}^{n-1} 2^{i+j}t^y_{j,i}\right) - \left(\sum_{i=0}^{n-1} 2^i(yx)_i\right) = 0$$

having used $2n^2$ linear combination steps. We then use a total of $n^2$ further derivation steps to replace $t^y_{j,i}$ by $t^y_{i,j}$ for each pair $i,j \in [0, n-1]$ in the latter equation. Finally, we subtract the two equations to finish the derivation.

Theorem III.2. There is a polynomial calculus derivation in length $4n^2 + 1$, and also a cutting planes derivation in length $14n^2 + 2$, of the equation $\sum_{j=0}^{n-1} 2^j(xy)_i - \sum_{j=0}^{n-1} 2^j(yx)_i = 0$ from the array multiplier circuits $xy$ and $yx$.

Proof. Given the previous lemma, to complete our derivation we need to obtain the tableau equalities $t^y_{i,j} = t^x_{j,i}$. In polynomial calculus, we get each equality with one subtraction step with the equations $t^y_{i,j} = x_iy_j$ and $t^x_{j,i} = y_jx_i$. So deriving these equalities takes an additional $n^2$ polynomial calculus steps.

In cutting planes, it takes 3 linear inequalities (clauses) to represent a constraint $t^y_{i,j} = x_iy_j$. From these, we can derive that $t^y_{i,j} = t^x_{j,i}$ in eight steps. Hence, deriving the tableau
equalities takes $8n^2$ cutting planes steps. Afterwards, it takes two cutting planes steps to carry out each of the $3n^2 + 1$ linear combination steps of Lemma III.1.

In cutting planes we can use proposition II.4 to prove bit-level equality from the equation $\sum_{i=0}^{n-1} 2^i(xy)i - \sum_{i=0}^{n-1} 2^i(yx)i = 0$, which gives the following corollary.

**Corollary III.3.** There is a length-$O(n^2)$ cutting planes derivation yielding all of the $2n$ equalities $(xy)i = (yx)i$, from the array multiplier circuits $xy$ and $yx$.

For other ring identities such as distributivity, we no longer have straightforward equalities between the tableau variables on either side of the identity. For distributivity, the natural generalization of these tableau variable equalities contains nonlinear terms. Before we give our cutting planes proofs, we introduce the $(k,d)$-cutting planes proof system in the next section as a convenient way to work with nonlinear terms within cutting planes.

**IV. $(k,d)$-Cutting Planes Proofs**

Our cutting planes multiplier proofs will be written in a more convenient format that allows for a limited number of nonlinear terms in each inequality. Although cutting planes proofs only allow the use of linear inequalities, we will also be able to efficiently represent a large class of nonlinear Boolean inequalities using sets of linear inequalities.

**Definition** We say that a polynomial inequality $\phi$ on the Boolean variables $X$ is $(k,d)$-nonlinear if it is written in the form

$$\ell(X) + \sum_{i=1}^{k} \ell_i m_i \geq b$$

where $\ell(X)$ is an integer linear form (i.e., $\ell(X) = \sum c_i x_i$), each $\ell \in \{\ell_1, \ldots, \ell_k\}$ is a non-negative integer linear form (i.e., $\ell = \sum c_i x_i$ and each $c_i \geq 0$), each $m_i$ is at most $d-1$ monomial with coefficient $+1$ or $-1$, containing only variables disjoint from $\ell_i$, and lastly, $b$ is an integer.

We emphasize that this proof system distinguishes between inequalities $\phi$ and $\phi'$ that are semantically equivalent, but are syntactically different due to different factorizations. For example, the inequality $(x_1 + x_2)yi \geq b$ is not considered to be the same as the inequality $x_1 yi + x_2 yi \geq b$. The first inequality is $(1,2)$-nonlinear while the second is $(2,2)$-nonlinear. In simulating $(k,d)$-nonlinear inequalities by ordinary linear ones, these two inequalities will be represented by two different (though semantically equivalent) sets of linear inequalities.

**Definition** Let $\mathbb{CP}^{+(k,d)}$ denote the $(k,d)$-cutting planes proof system. Each line is a $(k,d)$-nonlinear inequality on a set of Boolean variables $\{x_i\}$. Its rules are as follows. The **literal axioms** are the same as in $\mathbb{CP}$: for each variable $x_i$ we have $x_i \geq 0$ and $-x_i \geq -1$. The division rule and linear combination rule from $\mathbb{CP}$ generalize as one would expect. Writing $\ell(X) = \sum_i (c \cdot a_i)x_i$:

$$\sum_i (c \cdot a_i)x_i + \sum_i (c \cdot \ell_i)m_i \geq b$$

$$\sum_i \ell_i x_i + \sum_i \ell_i m_i \geq \left| \frac{b_i}{\ell} \right|$$

And for any $\alpha, \beta \in \mathbb{N}$, as long as the result is $(k,d)$-nonlinear:

$$\sum_i \ell_i m_i + \ell(X) \geq b, \quad \sum_i \ell' m'_j + \ell'(X) \geq b'$$

$$\sum_i \alpha \ell_i m_i + \alpha \ell(X) + \sum_j \beta \ell' m'_j + \beta \ell'(X) \geq \alpha b + \beta b'$$

The **factorizing rule** is that if the $(k,d)$-nonlinear inequality $\phi$ contains two terms $\ell m$ with the same monomial $m$, then we can factor these into term $(\ell + \ell')m$. Syntactically:

$$\ell(X) + \sum_i \ell_i m_i + \ell m + \ell'm \geq b$$

$$\ell(X) + \sum_i \ell_i m_i + (\ell + \ell')m \geq b .$$

The **distributing rule** is the reverse of the factorizing rule, except we can only distribute “one at a time”. For example, rewriting $(10y_1 + 8y_2)x_1 x_2 x_3 \rightarrow (10y_1 x_1 x_2 x_3 + 8y_2 x_1 x_2 x_3)$ would require 8 applications of the distributing rule below. For a non-negative linear form $\ell = \sum c_i x_i$, where each $c_i \geq 0$, define $\max(\ell) = \sum c_i$. Because of a technical detail related to the simulation size, we require that the two inequalities $\max(\ell) \geq \ell \geq 0$ have been derived from the literal axioms before making this inference:

$$\ell(X) + \sum_i \ell_i m_i + (\ell + y_r)m_p \geq b, \quad \max(\ell) \geq \ell \geq 0 .$$

The **multiplication rule** permits the multiplication of an inequality $\phi$ by a variable $z$, provided that the resulting inequality $\phi'z$ is $(k,d)$-nonlinear. Decomposing $\ell(X) = \ell(X)^{+} - \ell(X)^{-}$ into a sum of positive terms $\ell(\ell)^{+}$ and negative terms $\ell(\ell)^{-}$:

$$\ell(X)^{+} - \ell(X)^{-} + \sum_i \ell_i m_i \geq b$$

$$\ell(X)^{+} - \ell(X)^{-} + \sum_i \ell_i m_i z - b z \geq 0 .$$

**Theorem IV.1.** Fix a pair of positive integers $k \geq 1$ and $d \geq 2$. The cutting planes proof system $\mathbb{CP}$ $p$-simulates the $\mathbb{CP}^{+(k,d)}$ proof system. In particular, a $\mathbb{CP}^{+(k,d)}$ proof of $s$ lines can be simulated by a cutting planes proof of at most $(k + 4)^d s$ lines.

The idea of the proof of Theorem IV.1 is to find a tight set of at most $d$ linear upper bounds for each degree $d$ nonlinear term. To simulate an inequality with $k$ nonlinear terms of degree at most $d$, we use the set of at most $d^k$ linear inequalities obtained by plugging in every combination of upper bounds for each nonlinear term. The full details of this simulation can be found in [34].

**V. Optimal Cutting Planes Multiplier Proofs**

In the previous proof of commutativity, we were able to give cutting planes proofs without including nonlinear terms. However, when giving proofs for distributivity and other larger identities, nonlinear terms are difficult to avoid. This is where the $(k,d)$-cutting planes format is convenient for expressing $O(n^2)$ length cutting planes proofs of distributivity. We generalize these proofs for distributivity to obtain $O(n^2)$ length proofs for a large class of degree two ring identities.
In the first half of these proofs, we sum up the adder-constraints in each ripple-carry adder circuit \( x \cdot y \) to derive the “conservation of weight” equation \( \sum \sigma i 2^i (x_i + y_i) = \sum i 2^i (x + y)_i \) and also in each multiplication circuit \( x y \) to derive the “conservation of weight” equation \( \sum \sigma i, j 2^i + 1 t_{i, j}^y = \sum i 2^i (x y)_i \).

This section focuses on the second half of the proof, where the goal is to show that both sides hold equal weight in their multiplier tableau variables. The idea is to derive an equation \( \rho (i, j) \) relating the \((i, j)\)-th tableau entry of each multiplier. Fixing \( j \) and summing these equations along \( i \) gives an equation \( \rho (j) \) relating the \( j \)-th rows of each multiplier. Finally, adding together the equations \( \rho (j) \) yields the desired equation for the full multiplier tableaus.

A. Distributivity

**Theorem V.1.** There is a length \( O(n^2) \) \( CP \) proof that the circuits \((x + y) z\) and \( x z + y z\) for length \( n \) bit-vectors \( x, y, z \) have equal outputs.

**Proof.** We will give a length \( O(n^2) \) proof in \( CP^{+(5,2)} \). By Theorem IV.1, this implies that there is an equivalent cutting planes proof that is only a constant factor larger. We begin with the following lemma, which gives a small derivation that the weight of the \( j \)-th row of the multiplier \((x + y) z\) is the same as the combined weight of the \( j \)-th rows of multipliers \( x z \) and \( y z \).

**Lemma V.2.** For each \( j \in [0, n - 1] \) there is a length \( O(n) \) derivation in \( CP^{+(5,2)} \) of the equality \( \rho (j) \), defined as:

\[
\sum i=0 \sigma i 2^i + 1 t_{i, j}^z = \sum i=0 \sigma i 2^i + 1 t_{i, j}^y + t_{i, j} \cdot \rho (i, j) \cdot \rho (i, j)
\]

from the circuits \((x + y) z\) and \( x z + y z\).

**Proof.** Fix \( j \in [0, n - 1] \). We give a constant length derivation for each cell-wise constraint \( \rho (i, j) \), defined for \( i \in [1, n - 1] \) as

\[
t_{i, j}^z = t_{i, j}^z + t_{i, j}^x + c_{i, j} z_j - 2 c_{i, j} x_j y_j
\]

and defined for \( i = 0 \) and \( i = n \) the same way, absent the non-existing variables \( c_{i, j}^x, c_{i, j}^y, c_{i, j}^z \) and \( \rho (n, j) \). Adding up the constraints \( \rho (i, j) \) will yield \( \rho (j) \).

Start with the equation \( x_i + y_i + c_{i-1}^y - 2 c_{i}^x - (x + y)_i = 0 \), given by the \( i \)-th adder in the ripple-carry adder \((x + y)\). Multiplying this equation by \( z_j \), we obtain the \((5, 2)\)-nonlinear equation \( x_i z_j + y_i z_j + c_{i-1}^x z_j - 2 c_{i}^x y_j z_j - (x + y)_i z_j = 0 \).

Substituting in the tableau variables \( t_{i, j}^z, t_{i, j}^x, t_{i, j}^y \) gives us \( \rho (i, j) \).

To derive \( \rho (j) \) we add together the constraints \( \rho (i, j) \) so that the carry terms telescope: We start with \( \rho (n, j) \). Use linear combination to derive the equation \( 2 \rho (n, j) + \rho (n - 1, j) \):

\[
2 t_{n, j}^z + t_{n, j}^x = t_{n, j}^z + t_{n, j}^y + c_{n-1}^x y_j z_j.
\]

Repeating this step for \( \rho (n - 2, j), \ldots, \rho (0, j) \) gives \( \rho (j) \).

The rest of the proof combines equations \( \rho (j) \) given by Lemma V.2 with the conservation of weight equations. We first observe that combining the conservation of weight equations gives us, in a constant number of steps, the two equations

\[
\sum i=0 \sigma i 2^i \cdot (x z + y z)_i = \sum j=0 \sigma j 2^{i+j} \cdot (t_{i, j}^z + t_{i, j}^y) \quad (1)
\]

\[
\sum i=0 \sigma i 2^i \cdot ((x + y) z)_i = \sum j=0 \sigma j 2^{i+j} \cdot t_{i, j} \cdot (x + y) z_i. \quad (2)
\]

Sum all of the equalities \( \rho (j) \) to derive the equation \( \rho \), stating that both sides have equal weight in their tableau variables:

\[
\sum \sigma i, j 2^i + 1 t_{i, j}^z = \sum \sigma i, j 2^i + 1 t_{i, j}^y + t_{i, j} \cdot \rho (i, j) \cdot \rho (i, j)
\]

**B. 2-Colorable identities**

In this section we state some theorems that we can obtain by generalizing the ideas behind the proofs for the identity \((x + y) z = x z + y z\) to provide \( O(n^2) \) length cutting planes proofs for larger instances of distributivity. The proofs of these theorems may be found in [34].

**Theorem V.3.** Let \( x_1, x_2, \ldots, x_n \) and \( y_1, y_2, \ldots, y_n \) be length \( n \) bit-vectors. Define the circuit \( L \) as \((x_1 + x_2 + \ldots + x_n)(y_1 + y_2 + \ldots + y_n)\). Also define the circuit \( R \) as \((\sum_{\alpha, \beta} x_{\alpha} Y_{\beta})\), representing the fully expanded version of \( L \). There is a length \( O(n^2) \) cutting planes proof that circuits \( L \) and \( R \) have equal outputs.

**Theorem V.3** gives us \( O(n^2) \) cutting planes proofs for fixed ring identities that can be written as sum of independent bivector distributing or factoring steps. However, there exist identities such as \( x(y + z) + wz = xy + (x + w)z \) which cannot be decomposed into a sum of independent distributing and factoring components. Nevertheless, we can still give an \( O(n^2) \) length proof of this identity. We define the notion of a 2-colorable degree two identity to identify the general class of ring identities for which our technique can derive \( O(n^2) \) length proofs.

**Definition** Let \( L = R \) be a degree two ring identity. A 2-coloring for \( L = R \) is an assignment of either the color red or
blue to each bit-vector, with multiplicity (so a bit-vector may appear twice with different colors), such that: (1) each bit-vector in a sub-expression \((x_1 + x_2 + \ldots + x_r)\) has the same color as the bit-vector representing the sub-expression, (2) two sub-expressions that are multiplied together have opposite colors, and (3) the colored version of \(L = R\), where a blue input bit-vector colored blue \(x_i\) is distinguished from its red counterpart \(x_i\), is still a valid ring identity.

For example, \((x + y)z = xz + yz\) has the 2-coloring \((x + y)z = xz + yz\). The more general form of distributivity in Theorem V.3 clearly always has a 2-coloring. Lastly, the identity \(x(y + z) + wz = xy + z(x + w)\) has the 2-coloring \(x(y + z) + wz = xy + z(x + w)\). An example of an identity without a 2-coloring is \(x(y + z) + w(x + y) = y(x + w) + x(z + w)\).

**Theorem V.4.** Let \(L = R\) be a 2-colorable degree two ring identity on length \(n\) bit-vectors \(x_1, \ldots, x_n\). There is a length \(O(n^2)\) cutting planes proof that the circuits \(L\) and \(R\) have equivalent outputs.

**VI. Experiments**

The goal of our experiments was to evaluate the potential of using cutting planes solvers to reason with mixtures of multiplication and bit-level logic. Such problems are a key weakness of using a SAT-based approach to “bit-blasting”. We found several types of problems where pseudo-Boolean solvers performed well out-of-the-box. These include checking the word-level equivalence, commutativity, or correctness of different multipliers, extracting bit-equalities from word-level equalities, and verifying nonlinear bit-vector inequalities.

In our experiments, we used an Intel Core i7-6700K CPU at 4.00GHz with a memory limit of 8GB. The wall-clock time limit was set to 1200 seconds. We list experiment times in seconds (wall-clock time) and write TO if the time limit of 1200 seconds was exceeded. Our benchmarks are available at [35].

We used two pseudo-Boolean solvers, each equipped with a different form of cutting planes reasoning. The first, Sat4j-CP [33], employs saturation in its conflict analysis. The second solver, RoundingSat [21], [48], instead uses division; we used the new multi-precision version of the solver for which we could also log and separately verify the derivations it used.

Our experiments focused on integer multipliers with \(n\)-bit inputs and \(2n\) bits of output. We report results on three different circuits to represent multiplication: array, diagonal, and Wallace-tree multipliers with final stage ripple-carry adder. As noted in the introduction, we directly represent the adder constraints as two inequalities instead of as a set of clauses and define a “spec-equation multiplier” without a circuit by simply using the specification equation

\[
\sum_{i,j=0}^{n-1} 2^{i+j} t^{x}_{i,j} + \sum_{i=0}^{2n-1} 2^i (xy)_i = 0
\]

along with the partial product constraints \(t^{xy}_{i,j} = x_i y_j\). In these two ways, the pseudo-Boolean format allows us to “bit-blast” multiplication, along with other word-level functions, to a higher-level description than CNF while maintaining full bit-precision.

Our first set of experiments, presented in Table I, uses...
the pseudo-Boolean solvers Sat4j-CP and RoundingSat to verify the word-level and bit-level equivalence of different multiplier circuits. More precisely, we use Sat4j-CP to prove an equation of the form \( \sum_{i=0}^{n-1} 2^i (s_i - s'_i) = 0 \) stating that the total weight of the outputs \( s, s' \) is the same for the two multipliers. Then we have RoundingSat deduce, from this equation, each equality \( s_i = s'_i \) individually in order to prove equivalence at the bit-level. Performance on bit-extraction scaled particularly well with the right choice of pseudo-Boolean solver, as shown in Table III, which also includes a comparison with the theoretical lower bound we showed for algebraic methods. Using these two steps, we can efficiently check the commutativity of array, diagonal, and Wallace-tree multipliers, as well as several equivalences between array, diagonal, and spec-equation multipliers. We can also check some of these properties of Wallace-tree multipliers for up to 32 or 64 bits.

An important step for showing word-level equivalence was to do some basic pre-processing to find equivalent partial products (\( t_{xy}^{i,j} \) variables). Adding these equivalences was key to obtaining efficient solve times in Sat4j-CP. In contrast, we found that adding these equivalences did not help SAT-based solvers. We note that most bit-vector solvers, and many SAT solvers, already perform similar pre-processing to find equivalent variables; current pseudo-Boolean solvers based on cutting planes do not yet have such pre-processing.

To provide some context for these results, we compared the performance of our pseudo-Boolean approach to the algebraic approach of [28], which is currently the fastest method for verifying these properties. We replicated their verification of the commutativity and correctness of a simple gate-level array multiplier “\( \text{btor} \)”, generated by Boolector, by using their tool, AMulet, in our environment to obtain the solve times at the bottom of Table I. We note that AMulet, is also capable of similarly fast solve times for more complicated gate-level multipliers such as Booth-encoded Wallace-tree multipliers. We direct interested readers to [28] for further experiments using the algebraic approach to verify commutativity, correctness, and equivalence of these other gate-level multiplier architectures.

Current pseudo-Boolean solvers have limited reasoning capabilities for these lower level multipliers. In particular, these solvers degenerate to SAT-based reasoning when given a CNF input. Our focus is not so much on verifying a large spectrum of multiplier circuits as on bit-vector solving, where we are free to choose the most efficient way to represent bit-vector multiplication.

We see that for simple array and diagonal multipliers, our approach (on adder-level multipliers) achieves comparable times to the algebraic approach (on gate-level multipliers) for proving commutativity and word-level equivalence. Furthermore, we are able to efficiently extract each of the individual bit-level equalities that a word-level equality implies.

For Wallace-tree multipliers with a final stage ripple-carry adder (\( \text{wt-rca} \)), we could check its equivalence with an array for 64 bits within 1 minute. We could also check commutativity for 32 bits in 5 seconds. However, we hit time-out on larger instances of 48 or 64 bits. We were also unable to completely verify the equivalence of a wt-rca and spec equation multiplier for 32-bit instances, though we could show that the output of the wt-rca is at least as large as the output of the spec equation in 5 seconds. We see that Sat4j-CP has a harder time with these more complicated multiplier architectures.

Our other experiments, presented in Table IV, use the solver RoundingSat to verify some nonlinear bit-vector inequalities involving untruncated multiplication and the operations \( \| \) for bit-wise OR, \( \& \) for bit-wise AND. We use these bit-wise operations to apply the bit masks \( \| k \)" and \( \& k \), where \( k \) is set to the constant alternating bit-string \( (10)^{(n/2)} \). (This value was an arbitrary choice that contains a mix of 1s and 0s; we observed similar performance across all solvers with other values of \( k \).) The inequalities listed follow from thinking of \( || \) and \( \& \) as, respectively, computing the bit-wise maximum and minimum of their inputs.

We compare RoundingSat’s performance on these inequalities against the bit-vector solvers Boolector, Yices2, Z3 and CVC4. Our inputs to these bit-vector solvers used the word-level format SMT-LIB2 [3] to allow for full use of word-level reasoning and other non-SAT capabilities. We found that these bit-vector solvers (with the exception of Boolector) generally exceeded the time limit at 20 bits. On the other hand, when we “bit-blasted” multiplication using the spec-equation, RoundingSat outperformed all of the bit-vector solvers, with the exception of last inequality \( (x \mid k)(y+1) \geq k y + x \), where Boolector won out by a few bits.

VII. CONCLUSIONS & DIRECTIONS

In this paper, we have described a new approach to deciding nonlinear bit-vector formulas: include 1-bit adders among the set of essential building blocks along with the usual Boolean operations and express properties using pseudo-Boolean formulas rather than CNF formulas during “bit-blasting”. We have shown, both experimentally and in principle, how pseudo-Boolean solvers based on cutting planes reasoning, when given these new bit-blasted formulas, can achieve levels of performance comparable to, or better than, the best altern-
such as associativity. Although word-level associativity has an

<table>
<thead>
<tr>
<th>Inequality</th>
<th>n</th>
<th>RS</th>
<th>Btor</th>
<th>Z3</th>
<th>Yices2</th>
<th>CVC4</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(x \mid k)z \geq k z$</td>
<td>16</td>
<td>17</td>
<td>14</td>
<td>21</td>
<td>31</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>11</td>
<td>16</td>
<td>TO</td>
<td>TO</td>
<td>TO</td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>16</td>
<td>501</td>
<td>TO</td>
<td>TO</td>
<td>TO</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$k z \geq (x &amp; k)z$</td>
<td>16</td>
<td>.06</td>
<td>10</td>
<td>172</td>
<td>31</td>
<td></td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>.7</td>
<td>117</td>
<td>TO</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>.6</td>
<td>1154</td>
<td>TO</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>.6</td>
<td>1154</td>
<td>TO</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$(x \mid z)(z \mid k) \geq k x$</td>
<td>16</td>
<td>.088</td>
<td>14</td>
<td>22</td>
<td>31</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>.05</td>
<td>14</td>
<td>TO</td>
<td>31</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>.7</td>
<td>351</td>
<td>TO</td>
<td>43</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$k x \geq (x &amp; z)(z &amp; k k)$</td>
<td>16</td>
<td>.04</td>
<td>10</td>
<td>32</td>
<td>100</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>.07</td>
<td>10</td>
<td>243</td>
<td>32</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>.1</td>
<td>243</td>
<td>TO</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>.1</td>
<td>243</td>
<td>TO</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>.7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$(x \mid k)(y + 1) \geq k y + x$</td>
<td>16</td>
<td>.4</td>
<td>25</td>
<td>29</td>
<td>38</td>
<td>118</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>TO</td>
<td>25</td>
<td>29</td>
<td>38</td>
<td>118</td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>TO</td>
<td>25</td>
<td>29</td>
<td>38</td>
<td></td>
</tr>
</tbody>
</table>

Bit-vector $k$ is the value $(10)^{(n/2)}$. & is bit-wise AND, | is bit-wise OR.

The idea of using pseudo-Boolean solving for verifying nonlinear bit-vector formulas appears not to have been explored previously. One possible explanation for this is that when pseudo-Boolean solvers are run purely on CNF inputs, their reasoning collapses to that of CDCL SAT solvers, only much less efficient ones because of the more involved data structures and algorithms required in the pseudo-Boolean case. Our use of 1-bit adders as fundamental structures is critical to achieving the performance that we obtain.

Conflict-driven pseudo-Boolean solvers are still at a relatively early stage of development, especially compared to the 25+ years of concerted effort directed at optimizing Gröbner basis algorithms and CDCL solvers. In particular, there is quite some variation in the different forms of conflict analysis methods used, and some of these methods have been shown to be quite weak. In fact, many solvers, such as NaPS [49] and Open-WBO [40], do not use any cutting planes reasoning and instead reduce the problem to SAT. Other shortcomings in the cutting planes reasoning used in current solvers are discussed in ([20], [23], [53]). In our experiments, different conflict analysis methods worked best on different problems. For example, we found that the saturation-based solver Sat4j-CP worked much better than RoundingSat for checking word-level equalities. On the other hand, the division-based solver RoundingSat significantly outperformed Sat4j-CP when tasked with extracting bit-equalities, and also for checking bit-vector inequalities. This is in contrast with CDCL solvers where the best ideas for conflict analysis have largely converged on a single method that is used by all of the currently best solvers.

We view this work as providing a “call to arms” for pseudo-Boolean solver development, focusing especially on features that will be useful in verification of these kinds of bit-vector problems. In particular, though our experiments validate the pseudo-Boolean approach in principle, none of the solvers we used allowed us to verify the properties for which we provided more complex cutting planes proofs in Section V. Thus, there is substantial scope for developing new methods and heuristics for pseudo-Boolean solving that can carry out much more of this cutting planes reasoning in practice.

ACKNOWLEDGMENTS

Paul Beame and Vincent Liew’s research was supported in part by NSF-SHF grant CCF-1714593. Jo Devriendt, Jan Eliffers, and Jakob Nordström were funded by the Swedish Research Council (VR) grant 2016-00782, and Jakob Nordström was also supported by the Independent Research Fund Denmark (DFF) grant 9040-00389B. Some development work on RoundingSat was done using computational resources provided by the Swedish National Infrastructure for Computing (SNIC) at the High Performance Computing Center North (HPC2N) at Umeå University.


