Algebraic computations over field of fractions

A. *Problem*

In [1], the authors showed that verification of integer multipliers can be formulated as a decision procedure and solved over polynomial rings with coefficients from the field of fractions $\mathbb{Q}$, as opposed to solving over integers $\mathbb{Z}$. As most algebraic geometry results are valid over fields (and $\mathbb{Z} \subset \mathbb{Q}$ is not a field), their approach leveraged theory as well as efficient computational techniques over fields to solve this verification problem. We utilize this algebraic setup and present techniques to perform rectification of integer multipliers. The rectification function computation is modeled as a quantification procedure. However, since the operations are modeled over $\mathbb{Q}$, our computations may result in functions (f) which may evaluate to non-Boolean (non-synthesizable) values in $\mathbb{Q}$. To overcome this issue, we conjecture that a polynomial f^b can be computed such that $V(f) = V(f^b)$, and f^b evaluates to only Boolean values $\{0,1\} \subset \mathbb{Q}$.

B. *Notation*

- Let $\mathbb{Q}$ be the field of fractions. Let $R = \mathbb{Q}[X]$ be the polynomial ring in variables X with coefficients in $\mathbb{Q}$. For the examples illustrated below, let $X = \{a_0, a_1, b_0, b_1\}$.
- In our work, we only make use of lexicographic (lex) ordering. Impose a lex monomial order on ring R with following variable order $a_0 > a_1 > b_0 > b_1$.
- Let $F_0 = \{a_0^2 - a_0, a_1^2 - a_1, b_0^2 - b_0, b_1^2 - b_1\}$ be a set of polynomials over R and J_0 be the ideal generated by F_0, $J_0 = \langle F_0 \rangle \subset \mathbb{Q}[X]$.
  - Consider the polynomial $f_0 = a_0^2 - a_0 \in R$. The solution to this polynomial over $\overline{\mathbb{Q}}$, and over $\mathbb{Q}$, is $\{0,1\}$. Therefore, $V(J_0) = V_{\mathbb{Q}}(J_0) = \{0,1\}^{|X|}$. Thus we can include ideal J_0 in our computations to restrict the solutions of polynomials to Boolean values.

Conjecture .1. Let $f(X)$ be a polynomial in R with coefficients from $\mathbb{Q}$, and $V(f(X)) \subseteq \{0,1\}^{|X|}$. Let $G = \{g_1, \dots, g_t\}$ denote the set of generators of the reduced Gröbner basis (redGB) computation of the ideal $J = \langle f(X) \rangle + J_0$. Then, $\forall g_i \in G$ the coefficients of g_i will only be in $\{0,1,-1\} \subset \mathbb{Q}$.

- Since we write and operate only on non-zero terms of a polynomial, can we rewrite the coefficient set of g_i to $\{1,-1\}$?

Example .1. Let $f_1 = 4 \cdot a_0a_1b_0b_1 - 2 \cdot a_0b_0b_1 - 2 \cdot a_1b_0$ be a polynomial in R with coefficients in $\mathbb{Z} \subset \mathbb{Q}$.

$$\begin{aligned} G_1 = redGB(\{f_1, J_0\}) = \{&b_1^2 - b_1,\ b_0^2 - b_0,\ a_1^2 - a_1,\ a_0^2 - a_0, \\ &a_1b_0b_1 - a_1b_0,\ a_0b_0b_1 - a_1b_0,\ a_0a_1b_0 - a_1b_0\} \end{aligned}$$

Let $f_2 = (4/3) \cdot a_0a_1b_0b_1 - 2 \cdot a_0b_0b_1 - (2/7) \cdot a_1b_0$ be a polynomial in R with coefficients in $\mathbb{Q}$.

$$G_2 = redGB(\{f_2, J_0\}) = \{b_1^2 - b_1,\ b_0^2 - b_0,\ a_1^2 - a_1,\ a_0^2 - a_0,\ a_0b_0b_1,\ a_1b_0\}$$

Conjecture .2. Assuming Conjecture .1 holds, let $G = redGB(\{f(X), J_0\}) = \{g_1, \dots, g_t\}$ denote the non-zero generators such that, $\forall g_i \in G$, coefficients of $g_i \in \{1, -1\}$. We want a polynomial $f^b(X)$ with variables in X and coefficients in $\{1\}$, such that, $V(f(X)) = V(G) = V(f^b(X))$ and $f^b : \{0,1\}^{|X|} \mapsto \{0,1\}$. A polynomial constructed as $f^b(X) = ((1+g_1)\cdot(1+g_2)\cdots(1+g_t)) + 1 \pmod 2$ will always satisfy the above requirements.

Example .2. Continuing with the Ex. .1:

$$\begin{aligned} f_{G_1} &= ((1 + a_1b_0b_1 - a_1b_0)\cdots(1 + a_0a_1b_0 - a_1b_0)) + 1 \\ &= a_0b_0b_1 - a_1b_0 + 2 \\ f^b_{G_1} &= a_0b_0b_1 + a_1b_0 \pmod 2 \end{aligned}$$

$$\begin{aligned} f_{G_2} &= ((1 + a_0b_0b_1)\cdot(1 + a_1b_0)) + 1 \\ &= a_0a_1b_0b_1 + a_0b_0b_1 + a_1b_0 + 2 \\ f^b_{G_2} &= a_0a_1b_0b_1 + a_0b_0b_1 + a_1b_0 \pmod 2 \end{aligned}$$

Table I presents the evaluations of the polynomials $f_1, f_2, f^b_{G_1}$, and $f^b_{G_2}$ for all the input assignments.

$\{a_1a_0b_1b_0\}$	f_1	$f^b_{G_1} \pmod 2$	f_2	$f^b_{G_2} \pmod 2$
0000	0	0	0	0
0001	0	0	0	0
0010	0	0	0	0
0011	0	0	0	0
0100	0	0	0	0
0101	0	0	0	0
0110	0	0	0	0
0111	-2	1	-2	1
1000	0	0	0	0
1001	-2	1	-2/7	1
1010	0	0	0	0
1011	-2	1	-2/7	1
1100	0	0	0	0
1101	-2	1	-2/7	1
1110	0	0	0	0
1111	0	0	-20/21	1

TABLE I: Evaluation of the polynomials

References

[1] D. Ritirc, A. Biere, and M. Kauers, "Column-Wise Verification of Multipliers Using Computer Algebra," in *Formal Methods in Computer-Aided Design (FMCAD)*, 2017, pp. 23–30.