ECE/CS 5745/6745: Testing and Verification of Digital Circuits
Hardware Verification using Symbolic Computation

Fall 2023, Homework # 6
Due Date: Mon, December 11, 2023
Topics: Gröbner Basis, The Nullstellensatz Concepts, & Circuit Verification

In this assignment, you will apply some definitions and concepts of Gröbner bases and the Weak Nullstellensatz over finite fields, that we have been studying over the past couple of weeks. For this assignment, you should make use of the Singular tool to solve the questions. Download and install the Singular tool, and *read the manual*. In the manual, you only need to glance through the following sections for now:

1) Section 2 on Introduction, of course.
2) Section 3.1 (usage), 3.3 (rings and orderings), 3.7 and 4.16 (procedures), and section 4.15 for all polynomial related operations and functions.
3) There are some standard procedures (or functions) already implemented in Singular that may be hard to find. So I am providing you with a list of procedures that you may find useful in learning the material.
4) Also uploaded on the class website, next to this HW is a `demo.sing` file with many examples that will be helpful for you to start programming this assignment.
5) For computing Radical ideals $\sqrt{J}$, include the library "LIB primdec.lib" and use the command `radical(J)`.

On a unix terminal, the way to load a singular script file is as follows:

```
prompt>> Singular
                     SINGULAR                                /
 A Computer Algebra System for Polynomial Computations   /   version 3-1-1
                                                       0<
     by: G.-M. Greuel, G. Pfister, H. Schoenemann        \   Feb 2010
FB Mathematik der Universitaet, D-67653 Kaiserslautern    \
```

```
> < "demo.sing";
```

In Singular, you can declare rings, term orderings, polynomials, ideals and compute their Gröbner bases. There are many algorithms implemented to compute a Gröbner basis: `std`, `groebner`, `slimgb` are three such commands. There is also a `reduce` command which reduces a polynomial modulo an ideal: i.e. if ideal $G = \langle g_1, \ldots, g_t \rangle$, then `f` $\xrightarrow{G}_+$ `r` is computed as `r = reduce(f, G)`, where ideal G is declared as "ideal $G = g_1, \ldots, g_t$;". See the "demo.sing" file on the class website.

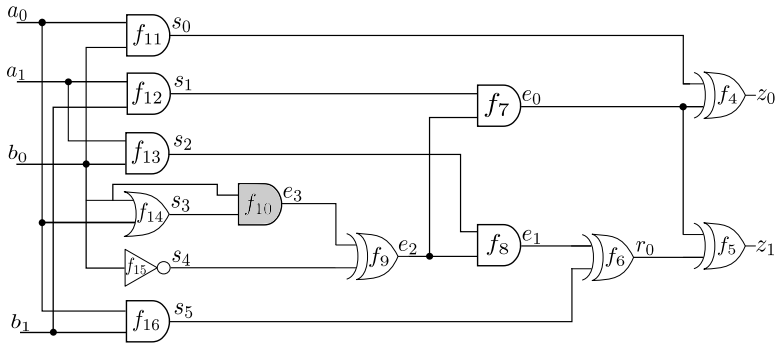

Fig. 1: The circuit for question 1

1) **(Formal verification of integer arithmetic circuits over $\mathbb{Q}[x_1, \ldots, x_n]$ using ideal membership testing – 40 points)** In class, we have seen how a circuit implementation C can be verified against a polynomial specification f_{spec} using an ideal membership testing approach. This approach works for finite field circuits as well as for integer arithmetic circuits. You will apply this concept to verify the circuit of Fig. 1 over $\mathbb{Q}[x_1, \ldots, x_n]$. You will, of course, have to make use of Singular. Perform the following steps:

   a) You are given a specification polynomial f_{spec} for an *integer arithmetic* circuit that takes two 2-bit words $\{a_0, a_1\}$, $\{b_0, b_1\}$ and produces a 2-bit output word $\{z_0, z_1\}$. The polynomial $f_{spec} \in \mathbb{Q}[z_0, z_1, a_0, a_1, b_0, b_1]$ is given as:

$$f_{spec} : (z_0 + 2z_1) - 2a_0a_1b_0b_1 + 4a_0a_1b_1 - a_0b_0 - 2a_0b_1 + 4a_1b_0b_1 - 2a_1b_0 - 3a_1b_1 \tag{1}$$

   b) Take the circuit of Fig. 1, and represent it as a set of 13 polynomials $F = \{f_1, \ldots, f_{13}\}$ with coefficients in $\mathbb{Q}$ for the 13 gates of the circuit. Denote the ideal $J = \langle f_1, \ldots, f_{13} \rangle \subset \mathbb{Q}[x_1, \ldots, x_n]$. By the way, the figure labels the gates as $\{f_4, \ldots, f_{16}\}$. Don't get confused by the labels. You could either re-label the gates from 1, ..., 13, or just keep the same labels for the gates/polynomials.

   c) *Note:* Modeling of logic gates over $\mathbb{Q}$ is given in the lecture slides of 11/22, https://my.ece.utah.edu/~kalla/ECE6745/verify-gf-ideal-membership.pdf, on page 24.

d) Generate J_0 as the ideal of all bit-level vanishing polynomials.

e) You will now perform formal verification using an ideal membership testing formulation. We have studied that verification can be solved by checking if $f_{spec} \in (J + J_0)$, for which we can compute a Gröbner basis $G = GB(J + J_0)$ and see if $f_{spec} \xrightarrow{G}_{+} 0$.

f) However, we have also seen that using reverse topological term order (RTTO) $>$, we can already represent the polynomials of $J + J_0$ as a minimal Gröbner basis.

g) Derive a RTTO-style term order $>$ for this circuit, and show what your term order is.

h) Using this term order, write a *minimal Gröbner basis* G_{min} of $J + J_0$. Note that you should not need to "compute" G_{min}, but should be able to write one just by looking at the circuit.

i) Is G_{min} also a reduced Gröbner basis? If not, then reduce G_{min} to G_{red}. You can use Singular to compute the reduced GB, by first loading the command `option(redSB)` in Singular, and then running "`ideal` G_{red} `= groebner(`G_{min}`)`". `option(redSB)` ensures that a reduced GB is computed.

j) How is G_{red} different from G_{min}?

k) Perform formal verification and check if the circuit C implements f_{spec} using ideal membership test.

l) Describe your procedure, and also attach a (well commented) Singular code that you executed to solve this problem.

2) **(Fundamentals of the Weak Nullstellensatz, and counting the number of solutions for zero-dimensional ideals using standard monomials of an ideal – 30 points)**. Consider the finite field of 5 elements $\mathbb{F}_5 = \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Let $\overline{\mathbb{Z}_5}$ be its algebraic closure. Let polynomials $f_1 = x^2 + y^2 + 1, f_2 = x^2y + 2xy + x$, where $f_1, f_2 \in \mathbb{Z}_5[x, y]$. Answer the following questions.

a) Describe in your own words: what is the algebraic closure ($\overline{\mathbb{Z}_5}$) of $\mathbb{Z}_5$?

b) Does the system of polynomial equations $\{f_1 = 0, f_2 = 0\}$ have common solutions over the closure $\overline{\mathbb{Z}_5}$? In other words, is the variety $V_{\overline{\mathbb{Z}_5}}(f_1, f_2) = \emptyset$? Answer this question without actually solving for the roots of f_1, f_2.

c) If the system of polynomial equations $\{f_1 = 0, f_2 = 0\}$ does have solutions over $\overline{\mathbb{Z}_5}$, is the number of solutions finite or infinite? If the number of solutions is finite, then count the number of solutions over $\overline{\mathbb{Z}_5}$. Once again, you have to apply Nullstellensatz concepts without actually solving for the roots.

d) You are now asked to find if the system of polynomial equations $\{f_1 = 0, f_2 = 0\}$ does

have solutions over the field $\mathbb{Z}_5$ itself? In other words, is $V_{\mathbb{Z}_5}(f_1, f_2)$ empty or non-empty? If non-empty, count the number of solutions in $\mathbb{Z}_5$, i.e. what is $|V_{\mathbb{Z}_5}(f_1, f_2)|$?

e) Explain how you arrived at your answers. Attach your (cleaned-up and well commented) Singular experiments to your solutions.

3) **This question is required for ECE/CS 6745 students; 5745 students can solve it for extra credit. (Radical Membership Testing – 30 points)** Consider the ring $R = \mathbb{Q}[x, y]$. Let $f_1 = xy^2 + 2y^2$, $f_2 = x^4 - 2x^2 + 1$ and let ideal $J = \langle f_1, f_2 \rangle \subset R$. Moreover, let $f = y - x^2 + 1$. Answer the following using the Singular tool:

a) Without computing the generators of radical of J ($\sqrt{J}$), find out whether $f \in \sqrt{J}$. Describe your formulation to test this problem. [*Hint:* Radical Membership Test given in the slides on Radical Ideals]

b) Now, compute the generators of $\sqrt{J} = \langle g_1, \ldots, g_t \rangle$, using the `radical(J)` command. Now, reconfirm your result by explicitly performing ideal membership test using the generators of $\sqrt{J}$. Make sure to load `LIB "primdec.lib"` in Singular which contains the `radical()` command.

c) Is the ideal J itself radical? In other words, is $J = \sqrt{J}$? How do you know?

d) Hilbert's Regular Nullstellensatz (and the definition of radical ideals) tells us that if $f \in \sqrt{J}$, then a power of f should be in J. In other words, $\exists m \in \mathbb{Z}_{\geqslant 1}$ such that $f^m \in J$. You are asked to find the value of m. [This will require some trial and error: First see if $f^1 \in J$ by checking if `reduce(f^1, groebner(J)) == 0`; if not, then see if $f^2 \in J$; if not, then see if $f^3 \in J$, and so on.]

e) Note: Since for the above decision problems, you will have to compute Gröbner bases, feel free to use any term order. Also, I am not certain whether the `radical(J)` command in Singular already returns a Gröbner basis of $\sqrt{J}$. Therefore, to be safe, you could use `groebner(radical(J))`, just to be sure.