ECE/CS 5745/6745: Testing and Verification of Digital Circuits

Verification over Galois fields using Gröbner Bases

Fall 2014, Homework # 4
Due Date: Fri, November 14, 2014

1) (30 points) Design a 3-bit Mastrovito multiplier over the Galois field $\mathbb{F}_8 = \mathbb{F}_2[x] \pmod{P(x)}$ using any appropriate irreducible polynomial of degree 3. Then, using the Gröbner basis engine that you developed in the previous HW assignment, verify that the designed circuit is indeed a multiplier (i.e. no bugs in the design).
   - Show your design using either a circuit schematic or describe it using polynomial equations, as described in the lecture slides or my book-chapter.
   - You will perform verification of the circuit using the Weak Nullstellensatz. Describe your verification problem formulation and your approach. Be mathematically precise: What is the specification? What is the implementation? Over which ring are you operating? What is the ideal composed of? The varieties are being analyzed over which field?
   - Setup the problem in SINGULAR and prove that the circuit is correct.
   - Introduce a bug in the design and show that your approach can prove dis-equivalence.
2) (30 points) Consider the function (mapping) shown in the truth-table below.

$A = \{a_2 a_1 a_0\}$	$\mapsto$	$Z = \{z_2 z_1 z_0\}$
000	$\mapsto$	000
001	$\mapsto$	001
010	$\mapsto$	111
011	$\mapsto$	111
100	$\mapsto$	101
101	$\mapsto$	011
110	$\mapsto$	101
111	$\mapsto$	101

   - Using Karnaugh-maps (or any other method) design a Boolean logic circuit that implements the function.
   - Now you will verify that the implementation circuit is equivalent to the truth-table specification using Gröbner bases over Galois fields. Interpreting this function $f : \mathbb{B}^3 \rightarrow \mathbb{B}^3$ as

a function $f : \mathbb{F}_{2^3} \to \mathbb{F}_{2^3}$, derive a unique minimal canonical polynomial representation of the function as $Z = \mathcal{F}A$ over $\mathbb{F}_{2^3}$.

- Subsequently, using the Weak Nullstellensatz, prove the equality of the functions of the specification and the implementation.

3) (10 points) Let $\alpha_1, \alpha_2, \ldots, \alpha_t$ be arbitrary elements in $\mathbb{F}_{2^k}$. Prove or disprove:

$$(\alpha_1 + \alpha_2 + \cdots + \alpha_t)^{2^i} = \alpha_1^{2^i} + \alpha_2^{2^i} + \cdots + \alpha_t^{2^i}$$

for $i = 1, 2, \ldots$

4) (10 points) Design $\mathbb{F}_{16} = \mathbb{F}_2[x] \pmod{P(x)}$ where $P(x) = x^4 + x^3 + x^2 + x + 1$, and let $P(\alpha) = 0$. Identify a primitive element of the field. In other words, find an element β such that $\beta = \alpha^n$ for some n, and that $\mathbb{F}_{16} = \{0, 1, \beta, \beta^2, \ldots, \beta^{14}\}$.

5) (20 points) On the class website, along with this HW, I have uploaded two BLIF files. They correspond to a 16-bit Mastrovito GF multiplier and another 16-bit Montgomery GF multiplier. As described in my book chapter, these architectures are based on different mathematical concepts; due to which these designs do not exhibit any internal structural or functional equivalences. As a result, SAT/BDD/AIG-based techniques are unable to prove equivalence between them. Instead of taking my word for it, you will gain a first-hand experience for yourself.

- Input the two designs into the ABC tool, and miter them.
- Using `print_stats, strash, ifraig, print_stats`, identify the structural similarity in the design. Let N_1 be the number of AIG nodes in the miter before *fraiging*, and N_2 be the number of AIG nodes after *fraiging*. Then $\frac{N_1 - N_2}{N_1}$ roughly depicts the structural similarity as a percentage.
- Solve sat on the miter to perform the combinational equivalence check. How many years does it take to prove equivalence of just a 16-bit datapath circuits?
- I am going to upload (very soon) a 16-bit miter of Mastrovito and Montgomery multipliers in SINGULAR format. You can experiment with it and compare the execution time with that of AIGs. [I will send you an email as soon as this file is generated. Until then, work on the rest of the HW.]

For any computations that you need to perform, you are free to use SINGULAR, or any other CAD tool that you may need. Have fun.