Illustration on my write-up and some issues to address

Xiaojun Sun

March 8, 2014

1 About my write-up

My write-up (attached in same tar) is the theory part of proposed ICCAD paper with examples in details. I think the essence of our theory should focus on the state space traversal on general FSM part, because this part introduces algebraic geometry concepts (sum, product and quotient of ideals). The quotient of ideal concept has never been used to describe state transition (including complement) based on my survey, and its soundness has been validated by Florian's proof.

A general example circuit/FSM, please refer to **Part 2.1, 2.2** and **2.3**, basically I had done a step-by-step comment on this example. Also I attach the *Singular* file with full comments, please try to run this *traversal.sing*.

There are limitations on my technique, one is that the polynomial (ideal generator) must be univariate, so using Tim's abstraction is necessary. As to the normal basis multiplier, since this implementation is like a one-way FSM, the state transition graph is a chain, there is no need to use techniques like ideal sum/product/quotient. Thus the main contribution of this multiplier is providing an sequential application of Tim's abstraction technique, but it can still fit our state-space-traversal framework (see last paragraph of **Part 3.1**, then **Part 3.2**).

Still, in this multiplier example, I can propose another contribution on fast Gröbner basis computing (see **Part 4.2**), it is originally from Tim's idea, but not exactly the same, because the property of Normal Basis allows us to square the polynomial conveniently.

2 Soundness of Optimal Normal Basis Theory

This is more likely related to mathematical stuff rather than computer engineering. My following questions are necessary to prove the soundness of the SAT based technique to compute optimal normal element.

(a) We know how to get the λ-Matrix from a set of criteria C such as

$$\begin{cases} 2^i + 2^j = 1 \mod 2n+1 \\ 2^i + 2^j = -1 \ mod \ 2n+1 \\ 2^i - 2^j = 1 \ mod \ 2n+1 \\ 2^i - 2^j = -1 \ mod \ 2n+1 \end{cases} \tag{1}$$

but a formal proof of following equivalence is needed:

N is type-II optimal normal basis $\Leftrightarrow$ N is the only solution of λ-Matrix M^0generated by C

Considering Rosing's book already proved the sufficiency, we want to confirm the necessity:

$$N \text{ is one solution of } \lambda\text{-Matrix } M^0 \text{generated by } C \implies N \text{ is type-II optimal normal basis}$$

(b) This relates to the approach from Florian's student: to convert the λ-Matrix satisfiability problem to solving system of boolean equations (then we can solve the system using SAT/BDD). I also include my questions in **Part B.2** last paragraph of my write-up, here I state more formally:

Prove: solutions to system of boolean equations are always conjugates;

Prove: choosing equation on β^3 is sufficient to cover all solutions to original λ-Matrix.

If we proved all above, then it is sufficient to write a paper on "methodology to compute optimal normal basis".

3 Challenges on 32/64-bit multiplier experiment

I think the main thing lagging my tool is the bad performance for *Singular* to convert a high-degree power representation ring variable to its standard basis representation. For example, if the minimal polynomial is

$$p(\alpha) = \alpha^{33} + \alpha^{27} + \alpha^{20} + \alpha^{19} + \alpha^{17} + \alpha^{11} + \alpha^5 + \alpha + 1$$

and the normal element (in std basis) is

$$\beta = 1 + \alpha^2 + \alpha^4 + \alpha^6 + \alpha^7 + \alpha^9 + \alpha^{14} + \alpha^{15} + \alpha^{16} + \alpha^{19} + \alpha^{21} + \alpha^{22} + \alpha^{26} + \alpha^{27} + \alpha^{29} + \alpha^{30} + \alpha^{32}$$

Compute $\beta^{4294967296}$ (in std basis).