Small Circuits for Boolean Functions

Rene C. Peralta
NIST, Computer Security Division *

We consider the problem of building efficient circuits using arithmetic modulo 2. In this type of arithmetic, the only possible values are 0 and 1. Addition and multiplication are defined by x + x = 0 and $x \cdot x = x$. If we identify the Boolean constants (TRUE,FALSE) with (1,0), then all Boolean logic can be encoded using arithmetic modulo 2: addition corresponds to logical XOR, multiplication to AND, and negation is given by NOT(x) = x + 1. This problem is highly intractable for any meaningful measure of "efficiency". Thus, we can only hope to develop heuristics. We propose the following approach:

1. find a circuit with as few multiplications as possible; then
2. optimize the linear pieces of this circuit.

The *multiplicative complexity* of a function is the number of multiplications necessary and sufficient to compute it.

For example, the function: $f(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3$ can be computed using only one multiplication:

$$x_1x_2 + x_1x_3 + x_2x_3 = (x_1 + x_2)(x_1 + x_3) + x_1.$$

Too easy? Then try the following one using 3 multiplications only:

$$x_1x_2x_3x_4 + x_1x_2x_3 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4.$$

I will discuss known bounds on the multiplicative complexity of functions. Some of these results are constructive, and thus can be used in the first step of our circuit optimization method.

The second part of the talk considers the problem of optimizing the linear parts of a circuit. In this problem, we are given a binary m-by-n matrix M, and the task is to build a circuit for computing Mx (where x is an n-bit input). It turns out most work in this area makes an implicit assumption that turns out to be false. When one sheds this assumption, it becomes clear that new heuristics are needed. We have coded one such heuristic. I will report on how it fares compared to traditional methods. [1]

*Homepage: `http://cs-www.cs.yale.edu/homes/peralta/`

[1] Joint work with Joan Boyar, University of Southern Denmark.