INF 240 - Exercise problems - Boolean functions

Nikolay Kaleyski

1 Converting between different representations

Boolean functions and vectorial Boolean functions can be represented in a number of different ways, each of which has its advantages and disadvantages in terms of e.g. memory storage and the efficiency of performing different operations on the function. We have seen three representations of a Boolean function: via a *truth table*, via its *algebraic normal form (ANF)*, and via a *univariate polynomial*. A basic task involves converting between these representations.

1.1 Computing truth tables from the ANF

Computing the TT from the ANF is very simple and amounts to substituting concrete values for $x_1, x_2, \ldots, x_n$ into the ANF and simplifying the resulting expression.

Exercise 1. *Consider the* $(4, 1)$*-function given by the ANF*

$$f(x_1, x_2, x_3, x_4) = 1 + x_1 + x_3 + x_1x_2x_3 + x_1x_2x_3x_4.$$

Find the truth table of f*.*

Exercise 2. *Consider the* $(4, 3)$*-function given by the ANF*

$$F(x_1, x_2, x_3, x_4) = (0, 1, 1) + x_1(1, 0, 1) + x_2(1, 1, 1) + x_1x_2(1, 0, 0) + x_1x_3(0, 0, 1).$$

Find the truth table of F*.*

2 Computing the ANF from a truth table

The process of reconstructing the ANF from a truth table is slightly more involved, and there are several ways to do it. We have seen how to do this via the ANF's of the so-called atomic functions, which is a conceptually simple method. More sophisticated algorithms for solving this problem exist, but are outside the scope of the lecture. In some cases, it may even be possible to guess the ANF by intuitively reasoning about the TT.

Exercise 3. *Find the ANF of the* $(3, 1)$*-function with the following TT:*

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	1
1	0	0	0
0	1	0	0
1	1	0	1
0	0	1	1
1	0	1	0
0	1	1	0
1	1	1	0

Table 1: Truth table for Exercise 3

Exercise 4. *Find the ANF of the* $(4, 1)$*-function with the following TT:*

x_1	x_2	x_3	x_4	$f(x_1, x_2, x_3, x_4)$
0	0	0	0	0
1	0	0	0	1
0	1	0	0	0
1	1	0	0	0
0	0	1	0	0
1	0	1	0	1
0	1	1	0	0
1	1	1	0	1
0	0	0	1	1
1	0	0	1	0
0	1	0	1	1
1	1	0	1	1
0	0	1	1	1
1	0	1	1	0
0	1	1	1	1
1	1	1	1	0

Table 2: Truth table for Exercise 4

Exercise 5. *Find the ANF of the* $(3, 3)$*-function with the following truth table:*

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	$(0, 0, 0)$
0	0	1	$(0, 0, 0)$
0	1	0	$(0, 1, 0)$
0	1	1	$(1, 1, 1)$
1	0	0	$(1, 0, 1)$
1	0	1	$(1, 0, 1)$
1	1	0	$(0, 0, 0)$
1	1	1	$(0, 0, 0)$

Table 3: Truth table for Exercise 5

Exercise 6. *Find the ANF of the* $(3, 3)$*-function with the following truth table:*

x_1	x_2	x_3	$F(x_1, x_2, x_3)$
0	0	0	$(0, 1, 1)$
1	0	0	$(1, 1, 1)$
0	1	0	$(1, 0, 1)$
1	1	0	$(1, 1, 0)$
0	0	1	$(0, 1, 1)$
1	0	1	$(1, 1, 1)$
0	1	1	$(1, 0, 1)$
1	1	1	$(1, 1, 1)$

Table 4: Truth table for Exercise 5

2.1 Converting from and to univariate representation

Converting between the univariate representation of an (n, m)-function and its TT and ANF representations is slightly more involved as it requires performing computations (typically, both addition and multiplication) over a finite field. This process has not been covered at the lectures, and will therefore not be required for the exam. Despite this, we give a very brief description of how this works for the sake of completeness.

Recall that every extension field $\mathbb{F}_{2^n}$ can be seen as an n-dimensional vector space over its prime field $\mathbb{F}_2$. If α is a root of the irreducible polynomial used to define the extension field, then every element of $\mathbb{F}_{2^n}$ can be expressed as a linear combination of powers of α. For instance, if $p(x)$ is an irreducible polynomial of degree $\deg(p) = 3$, then every element of $\mathbb{F}_{2^3}$ can be represented as $a_0 + a_1\alpha + a_2\alpha^2$, for some $a_0, a_1, a_2 \in \mathbb{F}_2$. Then any element can be represented by the 3-dimensional vector (a_0, a_1, a_2) over $\mathbb{F}_2$. In this way, any element of $\mathbb{F}_{2^n}$ corresponds to an n-dimensional binary vector, and vice-versa.

To convert the univariate representation of a function, e.g. $F(x) = x^5 + \alpha x^2$, to a truth table, we simply take every binary input vector, e.g. $(0, 1, 1)$, find its corresponding finite field element, e.g. $\alpha + \alpha^2$, and evaluate the polynomial at $F(\alpha + \alpha^2)$. The resulting finite field element corresponds to the output vector.

To convert a truth table to univariate representation, one typically uses Lagrange interpolation, which is a method for constructing a polynomial having prescribed output values at given input points. An exposition of this method is outside the scope of the lecture, and we conclude this discussion with the note that Lagrange interpolation works in the same way over finite fields that it does over, say, the integers; if one is familiar with interpolation from a different context, applying it to the case of finite fields is straightforward.

If one needs to convert between ANF and univariate representation, the simplest way to do it would be to use the truth table as an intermediate step.

3 Cryptographic properties of Boolean functions

There are many statistics quantifying the security of Boolean functions against different kinds of cryptanalysis. Ones that we are familiar with are the differential uniformity, nonlinearity, algebraic degree, and polynomial degree of a function.

Exercise 7. *Determine the algebraic degree of the following* $(6, 6)$*-functions:*

1. $F_1(x) = a^{48}x^{55} + a^{21}x^{42} + a^{23}x^{40} + a^{14}x^{39} + a^{45}x^{36} + a^6x^{23} + a^{47}x^{17} + a^{46}x^{13} + a^{42}x^9 + a^{29}x^6$;
2. $F_2(x) = a^{35}x^{25} + a^4x^{19} + a^{26}x^{10}$;
3. $F_3(x) = a^{19}x^{63} + a^{61}x^{62} + a^{22}x^{40} + a^{53}x^{35} + a^{23}x^{29} + a^{51}x^{25} + a^{28}x$;
4. $F_4(x_1, \ldots, x_6) = (0,1,1,0,0,1)x_1x_2 + (1,1,1,0,1,1)x_1x_4x_5 + (0,0,0,0,0,1)x_1x_4x_5x_6$.

Exercise 8. *Determine the nonlinearity of the Boolean function with ANF*

$$f(x_1, x_2, x_3) = 1 + x_1x_2 + x_2x_3 + x_1x_2x_3.$$

Exercise 9. *Determine the nonlinearity of the Boolean function with ANF*

$$f(x_1, x_2, x_3, x_4) = 1 + x_1x_3 + x_2x_4 + x_1x_2x_3x_4.$$

Exercise 10. *The following table corresponds to a power $(4,4)$-function. Determine its differential uniformity.*

x_1	x_2	x_3	x_4	$F(x_1, x_2, x_3, x_4)$
0	0	0	0	$(0,0,0,0)$
1	0	0	0	$(1,0,0,0)$
0	1	0	0	$(0,1,1,0)$
0	0	1	0	$(1,1,1,0)$
0	0	0	1	$(1,0,0,0)$
1	1	0	0	$(0,1,1,0)$
0	1	1	0	$(1,1,1,0)$
0	0	1	1	$(1,0,0,0)$
1	1	0	1	$(0,1,1,0)$
1	0	1	0	$(1,1,1,0)$
0	1	0	1	$(1,0,0,0)$
1	1	1	0	$(0,1,1,0)$
0	1	1	1	$(1,1,1,0)$
1	1	1	1	$(1,0,0,0)$
1	0	1	1	$(0,1,1,0)$
1	0	0	1	$(1,1,1,0)$

Table 5: Truth table for Exercise 10

4 Equivalence relations on Boolean functions

There are several notions of equivalence that play a prominent role in the study and classification of cryptographic Boolean functions. Unfortunately, there is no simple way to check whether two given functions are equivalent with respect to most of these equivalence relations; in practice, the process of checking equivalence is usually handled by some sort of computer search.

In the case of power, or monomial functions, i.e. functions with a univariate representation of the form $F(x) = x^d$ for some positive integer d, it is enough to consider cyclotomic equivalence, which is simple enough to even be verified by hand for lower dimensions.

Exercise 11. *Consider the power functions*

$$x^{10}, \quad x^{17}, \quad x^{20}, \quad x^{30}, x^{43}, \quad x^{46}.$$

Partition them into cyclotomic equivalence classes:

1. *over* $\mathbb{F}_{2^6}$*;*
2. *over* $\mathbb{F}_{2^8}$*.*