University College London
Department of Computer Science

Cryptanalysis Exercises Lab 02

P. Spacek, N. Courtois,
J. Bootle

February 3, 2019

n.courtois@ucl.ac.uk
Version 1.2

1. Polynomials in SAGE

Quiz Answer each of the following.

1. Compute $x \cdot (x^3 + 1)$ modulo $x^4 + x - 1$. Answer $=$ ______ Ans

2. Suppose we represent $\mathbb{F}_{16}$ as $\mathbb{F}_2[x]/(x^4+x+1)$. Compute $x \cdot (x^3+1)$ in $\mathbb{F}_{16}$. Answer $=$ ______ Ans

Try out the following sequence of SAGE commands.

1. What is this line doing? Is this operation always defined?
   ZP.<x> = ZZ[]; ZP

2. $(x^\wedge 5 + 3 * x^\wedge 2 - 2 * x + 7)$ // (x + 1)
   $(x^\wedge 2)$.degree()
   $(x^\wedge 5 + 3 * x^\wedge 2 - 2 * x + 7)$.quo_rem(x + 1)

3. gcd$(3 * x^\wedge 2 + 6 * x - 9, 5 * x^\wedge 3 - 2 * x + 2)$
   factor$(3 * x^\wedge 5 + 5 * x - 8)$
   $(3 * x^\wedge 5 + 5 * x - 8)$.factor_mod(2)
   $(3 * x^\wedge 5 + 5 * x - 8)$.factor_mod(3)

2. Boolean Polynomials in SAGE

Execute the following commands and show that the result is correct.

1. from sage.crypto.boolean_function import BooleanFunction
2. F=BooleanFunction([0,0,1,0]); F(3);
   We define nonlinearity as the distance to the set of linear functions, or the minimum number of output 0s/1s inside the truth table needed to flip, in order to obtain a linear function. **Which entry can be flipped?**
3. F.nonlinearity();
   We define the Walsh-Hadamard transform as:
   $$W(j) = \sum_{i \in \{0,1\}^n} (-1)^{f(i) \oplus i \cdot j}$$
4. F.walsh_hadamard_transform();F.absolute_walsh_spectrum();
5. F.truth_table(format='hex');
6. Is this function linear? F=BooleanFunction("4"); F.truth_table(for

7. Show that the result is correct: F.algebraic_normal_form(); F.annih
8. R.<a,b,c,d,e,f> = BooleanPolynomialRing(6)
9. H=BooleanFunction(a*c); H.absolute_walsh_spectrum(); H.nonlinearity(); H.algebraic_normal_form()

1.
```
import itertools; letters = "abcdef"; var_list = []
for L in range(2, len(letters)+1):
 for subset in itertools.combinations(letters, L):
  var_list.append(subset)
mult_list = ['*'.join([x for x in v]) for v in var_list]
for i in range (0,len(var_list)):
 vars()[''.join(var_list[i])] = eval(''.join(mult_list[i
```
2.
```
U=BooleanFunction(1+abdf+d*ef+b+bcef);
(only 'def' does not work - due to Python limitation)
```
3. `max(U.absolute_walsh_spectrum()); U.algebraic_normal_for`
   This one is related to Differential Cryptanalysis and is defined by:
$$\Delta_f(j) = \sum_{i\in\{0,1\}^n} (-1)^{f(i)\oplus f(i\oplus j)}$$
   `min(U.autocorrelation()[1:]);max(U.autocorrelation()[1:]`

Some Boolean functions generated by students inside project T': https://docs.google.com/spreadsheets/d/19F28FbY5zZWsZkYweWs19KB_xsKLZVqcwGUg1_FpFlo/edit?usp=sharing

3. Polynomial Rings and Quotient Rings

Execute the following commands in SAGE and explain the result.

1. K=GF(4,'d4'); d4=K.gen(); K.modulus();
2. d4.minimal_polynomial(); d4^2+d4+1; d4^3
3. R = K[z]; R; z=R.gen(); R.cardinality();
4. R = PolynomialRing(K,'z'); R; z=S.gen(); R.cardinality();
5. S = R.quotient(x**2+x+1,'z'); S; z=S.gen(); S.cardinality();
6. for i,x in enumerate(S): print(" ".format(i, x))
   A list of all elements in another format is also shown on the next page.

7. z^2+z+(d4); z^4+z^2+(d4+1); z^6+(d4+1)*z^3+1

$GF(4^2) \equiv GF(4)[z]/z^2+z+2,\ p(z) = z^2+z+2$

Primitive polynomial over GF(4)

$\alpha = z$

$\alpha^{15} = 1$

Operate on GF(4)

Exponential Notation	Polynomial Notation	Binary Notation	Decimal Notation	Minimal Polynomial
0	0	00	0	
α^0	1	01	1	$x + 1$
α^1	z	10	4	$x^2 + x + 2$
α^2	$z + 2$	12	6	$x^2 + x + 3$
α^3	$3z + 2$	32	14	$x^2 + 3x + 1$
α^4	$z + 1$	11	5	$x^2 + x + 2$
α^5	2	02	2	$x + 2$
α^6	$2z$	20	8	$x^2 + 2x + 1$
α^7	$2z + 3$	23	11	$x^2 + 2x + 2$
α^8	$z + 3$	13	7	$x^2 + x + 3$
α^9	$2z + 2$	22	10	$x^2 + 2x + 1$
α^{10}	3	03	3	$x + 3$
α^{11}	$3z$	30	12	$x^2 + 3x + 3$
α^{12}	$3z + 1$	31	13	$x^2 + 3x + 1$
α^{13}	$2z + 1$	21	9	$x^2 + 2x + 2$
α^{14}	$3z + 3$	33	15	$x^2 + 3x + 3$

The exponential notation shows that the multiplicative group is cyclic. Each minimal polynomial divides $x^{15} - 1$.

Solutions to Quizzes

Solution to Quiz: We are working mod $x^4 + x - 1$, so we can add and subtract multiples of $x^4 + x - 1$ freely.

$$x \cdot (x^3 + 1) = x^4 + x \equiv 1 \mod (x^4 + x - 1) = \boxed{1}$$

Solution to Quiz: If we represent $\mathbb{F}_{16}$ as $\mathbb{F}_2[x]/(x^4+x+1)$, we are working mod x^4+x+1, so we can add and subtract multiples of x^4+x+1 freely. Also, because we are working in characteristic 2, we have $1=-1$.

$$x\cdot(x^3+1)=x^4+x\equiv -1 \mod (x^4+x+1)=\boxed{1}$$