INF 240 - Exercise problems - 12
Solutions

Nikolay Kaleyski

Exercise 1. *By the definition, the derivative $D_aF(x)$ of F in direction $a \in \mathbb{F}_{2^n}$ is given by*

$$D_aF(x) = F(a+x) + F(x).$$

We already have the univariate form of $F(x)$, viz.

$$F(x) = x^9 + \alpha x. \tag{1}$$

To find the univariate form of $F(a+x)$, we simply $(a+x)$ for x in (1) and get

$$F(a+x) = (a+x)^9 + \alpha(a+x).$$

To simplify this expression, we use the so-called "freshman's theorem", which states that

$$(A+B)^{2^k} = A^{2^k} + B^{2^k}$$

for any $A, B \in \mathbb{F}_{2^n}$ and any non-negative integer k. In particular, for $k = 3$, we have $(A+B)^8 = A^8 + B^8$, and thus we get

$$\begin{aligned} F(a+x) &= (a+x)^8(a+x) + \alpha a + \alpha x \\ &= (a^8 + x^8)(a+x) + \alpha a + \alpha x \\ &= x^9 + x^8 a + x a^8 + a^9 + \alpha x + \alpha a. \end{aligned}$$

We thus have

$$\begin{aligned} D_aF(x) &= F(a+x) + F(x) \\ &= x^9 + x^8 a + x a^8 + a^9 + \alpha x + \alpha a + x^9 + \alpha x \\ &= x^8 a + x a^8 + a^9 + \alpha a. \end{aligned}$$

To compute the second derivative, $D_bDaF(x)$, we simply compute the derivative of $D_aF(x)$. So, if we denote $G(x) = D_aF(x)$, we want to find $D_bG(x) = G(b+x) + G(x)$, which we do in the same way that we found $D_aF(x)$. We already have the univariate representation $G(x) = D_aF(x) = x^8 a + x a^8 + a^9 + \alpha a$, and by substituting $x + b$ for x, we get

$$G(x+b) = (x+b)^8 a + (x+b)a^8 + a^9 + \alpha a = x^8 a + x a^8 + b^8 a + b a^8 + a^9 + \alpha a.$$

Summing $G(x)$ and $G(x+b)$, we get

$$\begin{aligned} D_bG(x) &= D_bD_aF(x) \\ &= x^8 a + x a^8 + b^8 a + b a^8 + a^9 + \alpha a + x^8 a + x a^8 + a^9 + \alpha a \\ &= b^8 a + b a^8. \end{aligned}$$

¡++¿

Finally, we need to compute the algebraic degrees of F, D_aF and D_bD_aF. From (1), we have the exponents $9 = 1001$ and $1 = 1$, so $\deg(F) = 2$, i.e. F is a quadratic function. From $D_aF(x) = x^8 + ax^8 + a^9 + \alpha a$, we have the exponents $8 = 1000$ and $1 = 1$ (note that we only look at exponents of the indeterminate x so that e.g. a^9 does not affect the algebraic degree because a^9 is merely a coefficient) and thus $\deg(D_aF) = 1$, i.e. D_aF is an affine function (and it is not linear, as it has a constant term $a^9 + \alpha a$). Finally, $D_bDaF(x)$ does not contain the indeterminate x at all, so $\deg(D_bD_aF) = 0$.

This illustrates that each time a function is differentiated, its algebraic degree drops by (at least) 1.

Exercise 2. *The differential uniformity of an (n, n)-function F is defined to be the maximum number of solutions x to any equation of the form*

$$F(a + x) + F(x) = b \tag{2}$$

for any $0 \neq a \in \mathbb{F}_{2^n}$ and any $b \in \mathbb{F}_{2^n}$.

In the case when F is a power function, i.e. when F has univariate representation $F(x) = x^d$ for some positive integer d, then we know that the number of solutions to (2) does not depend on the value of a. Thus, we only have to find the number of solutions for some fixed values of a, say, $a = (0, 0, 1)$. Although it is difficult to decide whether the function represented by a given truth table is a power function or not, the assignment guarantees that the given table corresponds to a power function, which greatly simplifies our work.

Furthermore, for a fixed value of a, we do not have to go through all b in (2) and then through all x: since any value of b on the right-hand side of (2) must be of the form $F(a + x) + F(x)$ for some x, we can simply compute all possible b's by evaluating $F(a + x) + F(x)$ for all possible inputs x, and then count how many times each distinct output value occurs. To make the process more transparent, the results of this computation are given in Table 1.

x	$001 + x$	$F(x)$	$F(0001 + x)$	$F(x) + F(001 + x)$
000	001	000	101	101
001	000	101	000	101
010	011	110	111	001
011	010	111	110	001
100	101	100	011	111
101	100	011	100	111
110	111	001	010	011
111	110	010	001	011

Table 1: Derivation of differential uniformity

We can see that there are four distinct values of b that can be obtained as outputs, viz. 101, 001, 111, and 011. Each of them occurs twice, and so the differential uniformity of F (being the maximum frequency with which any value of b occurs) is $\delta_F = 2$.

Exercise 3. *By the definition, an APN function is one with differential uniformity equal to 2. To show that $F(x) = x^3$ is APN over $\mathbb{F}_{2^n}$, we thus need to*

show that the maximum number of solutions x to any equation of the form

$$F(a+x)+F(x)=b$$

for any $0 \neq a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^n}$ is 2. The left-hand side of the above equation is simply $F(a+x)+F(x)=D_aF(x)$, i.e. the derivative of F in direction a. We can find the univariate representation of this derivative in the same way as in the first exercise: substituting $x+a$ for x in $F(x)=x^3$, we get $F(a+x)=(a+x)^3$, which by the "freshman's theorem" simplifies to

$$(a+x)^3=(a+x)^2(a+x)=(a^2+x^2)(a+x)=a^3+a^2x+ax^2+x^3.$$

The derivative, therefore, has the form

$$D_aF(x)=F(a+x)+F(x)=a^3+a^2x+ax^2+x^3+x^3=x^2a+xa^2+a^3.$$

Now, take some element $b \in \mathbb{F}_{2^n}$. We need to show that the equation $x^2a+xa^2+a^3=b$ has no more than two solutions. If we define a polynomial $F'(x)=x^2a+xa^2+a^3+b$, then clearly x is a solution to $x^2a+xa^2+a^3=b$ if and only if it is a root of $F'(x)$. But since the degree of F' is 2, it cannot have more than two roots, and hence $x^2a+xa^2+a^3=b$ cannot have more than two solutions x. Since the same procedure can be applied for every possible value of $b \in \mathbb{F}_{2^n}$, we can conclude that $F(x)=x^3$ is indeed APN.

Exercise 4. *To determine the nonlinearity of the Boolean function f, we simply have to compute its Hamming distance to all affine $(2,1)$-functions, and take the minimum of these. Recall that the Hamming distance between two functions f and g is simply the number of inputs on which their values differ. It can thus be computed very easily, and so the only remaining obstacle is how to construct all affine $(2,1)$-functions.*

Recall that a linear function is an affine function with zero constant term; alternatively, an affine function is either a linear function, or a linear function plus a constant. In this case, all functions are from $\mathbb{F}_2^2$ to $\mathbb{F}_2$; since the output can only be 0 or 1, this means that the only non-zero constant is 1. Thus, an affine function $a(x)$ is either $a(x)=l(x)$ or $a(x)=l(x)+1$ for some linear function l.

We now discuss how to construct all linear $(2,1)$-functions. Recall that a linear function l must satisfy $l(x+y)=l(x)+l(y)$ for any x,y. In particular, this means that $L(00)=L(01+01)=L(01)+L(01)=0$, and thus any linear function must map the zero vector to 0. Furthermore, if we know $L(01)$ and $L(10)$, then we can derive the value of $L(11)=L(10+01)=L(10)+L(01)$. In other words, the values of L at $(0,1)$ and $(1,0)$ uniquely determine all values of L.

(In general, recall that a basis of the vector space $\mathbb{F}_2^n$ is a set of n elements $b_1,b_2,\ldots,b_n$ such that any element of $\mathbb{F}_2^n$ can be expressed as a sum of some of $b_1,b_2,\ldots,b_n$. Then, the values of a linear function L at $b_1,b_2,\ldots,b_n$ uniquely determine its values everywhere. For instance, if we are looking for linear $(4,1)$-functions, since the vectors $(1,0,0,0)$, $(0,1,0,0)$, $(0,0,1,0)$, $(0,0,0,1)$ form a basis of $\mathbb{F}_2^4$, then any linear function is uniquely specified by its values at these four points.)

In our case, we have two basis elements, viz. $(0,1)$ *and* $(1,0)$*, and since each of them can take either* 0 *or* 1 *as a value, there are* $2^2 = 4$ *possible combinations of values that we have to consider. We write down all four combinations in Table 2 (along with 0 for* $(0,0)$*) and derive the remaining value at* $(1,1)$ *as the sum of the values at* $(0,1)$ *and* $(1,1)$*.*

x	$l_1(x)$	$l_2(x)$	$l_3(x)$	$l_4(x)$
00	0	0	0	0
01	0	0	1	1
10	0	1	0	1
11	0	1	1	0

Table 2: Linear $(2,1)$-functions

Adding 1*'s to all entries in Table 2, we can obtain all non-linear functions, as shown in Table 3.*

x	$a_1(x)$	$a_2(x)$	$a_3(x)$	$a_4(x)$
00	1	1	1	1
01	1	1	0	0
10	1	0	1	0
11	1	0	0	1

Table 3: Affine but not linear $(2,1)$-functions

All that is left is to compute the Hamming distance between $f(x)$ *and the eight affine functions from Tables 2 and 3. The minimum distance turns out to be* 1*, which is then the nonlinearity of* f*.*

Exercise 5. *Substituting* $n = 7$ *in covering radius bound*

$$N_F \leq 2^{n-1} - 2^{n/2-1},$$

we obtain

$$N_F \leq 2^6 - 2^{2.5} = 64 - 2^{2.5} \approx 58.3.$$

We can thus conclude that the nonlinearity of a $(7,7)$*-function can never be greater than* 58 *by this bound.*

In the same way, we can substitute $n = 7$ *in the SCV bound*

$$N_F \leq 2^{n-1} - \frac{1}{2}\sqrt{3 \cdot 2^n - 2 - 2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1}}.$$

It is a bit more instructive to first substitute $m = n$ *to obtain a version of the SCV bound for* $n = m$*, i.e. for the case when the number of input and output bits is the same. We obtain*

$$
\begin{aligned}
N_F &\leq 2^{n-1} - \frac{1}{2}\sqrt{3 \cdot 2^n - 2 - 2\frac{(2^n-1)(2^{n-1}-1)}{2^n-1}} = \\
&= 2^{n-1} - \frac{1}{2}\sqrt{3 \cdot 2^n - 2 - 2(2^{n-1}-1)} = \\
&= 2^{n-1} - \frac{1}{2}\sqrt{3 \cdot 2^n - 2 - 2^n + 2} \\
&= 2^{n-1} - \frac{1}{2}\sqrt{2^{n+1}} = \\
&= 2^{n-1} - 2^{(n+1)/2-1} \\
&= 2^{n-1} - 2^{(n-1)/2}.
\end{aligned}
$$

Substituting $n = 7$, we get

$$N_F \leq 2^6 - 2^3 = 64 - 8 = 56.$$

Taking the smaller value from those provided by both the covering radius and SCV bounds, we see that $N_F \leq 56$ for any $(7,7)$-function F.

By the definition, an AB function is one whose nonlinearity is exactly equal to the value of the SCV bound. This means that any AB $(7,7)$-function F must have $N_F = 56$.

Finally, the bound $\deg(F) \leq (n+1)/2$ for the algebraic degree of an AB (n,n)-function implies (by substituting $n = 7$) that $\deg(F) \leq 4$ for any AB $(7,7)$-function.

Exercise 6. *To partition the given power functions into CCZ-equivalence classes, we first recall that CCZ-equivalence coincides with cyclotomic equivalence in the case of power functions (meaning that two power functions are CCZ-equivalent if and only if they are cyclotomic equivalent). By the definition, two power functions x^a and x^b over $\mathbb{F}_{2^n}$ are cyclotomic equivalent if and only if one of the following cases occurs:*

- *$a = 2^k b \mod (2^n - 1)$ for some positive integer k;*
- *$\gcd(a, 2^n - 1) = 1$ so that a is invertible modulo $2^n - 1$, and $a^{-1} = 2^k b \mod (2^n - 1)$.*

Note that $2^n = 1 \mod (2^n - 1)$, so only values of k up to $n - 1$ make sense above. In this case, $n = 7$, so we only need to consider $0 \leq k \leq 6$.

We can immediately see that $40 = 10 \cdot 2^4 \mod 127$ (although modulation here is not even needed), and so x^{10} and x^{40} are cyclotomic-, and hence also CCZ-equivalent. Similarly, we can see that $23 \cdot 2^5 = 736 = 101 \mod 127$, hence x^{23} and x^{101} are also CCZ-equivalent. By exhaustive search (which can be conveniently implemented as a simple computer program, for example), we can conclude that these are the only equivalences among the given functions. They can thus be partitioned into the classes $\{x^{10}, x^{40}\}$, $\{x^{23}, x^{101}\}$, and $\{x^{25}\}$.