Heads and tails, summer 2015

PROF. DR. JOACHIM VON ZUR GATHEN AND DR. DANIEL LOEBENBERGER

5. Exercise sheet
Hand in solutions until Sunday, 17 May 2015, 23:59:59

Exercise 5.1 (Enhancing distinguishers). (14 points)

Let $\mathcal{A}$ be a ε-distinguisher between a distribution X and the uniform distribution U on bit strings in $\{0,1\}^n$ of length n. The following algorithm $\mathcal{B}$ receives as input three bit strings y_1, y_2, y_3 and returns the majority of $\mathcal{A}$'s three answers. Is this algorithm $\mathcal{B}$ a better distinguisher between X and U?

(i) Specify the definition. For which distributions does the new algorithm $\mathcal{B}$ give an exact distinction? [3]

(ii) Is the new algorithm better?

(a) Prove that the following holds with $q = \mathcal{E}_{\mathcal{A}}(X)$ and $r = \mathcal{E}_{\mathcal{A}}(U)$: [4]

$$\delta_{\mathcal{B}} = \Delta_{\mathcal{B}}(X^3, U^3) = \left|E_{\mathcal{B}}(X^3) - E_{\mathcal{B}}(U^3)\right| = \left|(3q^2 - 2q^3) - (3r^2 - 2r^3)\right|.$$

(b) Find the best lower bound for $\delta_{\mathcal{B}}$ that only depends on ε. Compare with ε. [4]

(c) Compare the old and the new distinction power by plotting [3]

$$\left|\Delta_{\mathcal{B}}(X^3, U^3)\right| / \left|\Delta_{\mathcal{A}}(X, U)\right|.$$

Concerning the lower bound: Under the side conditions $|q - r| \geq \varepsilon$, $q, r \in [0,1]$ minimize $f(q,r) = |(3q^2 - 2q^3) - (3r^2 - 2r^3)|$. The minimum is $3\varepsilon^2 - 2\varepsilon^3$. (This is how to find this answer: to start with search for the extreme value of f in $\mathbb{R}^2$. There are none within the area that is of interest for us. Thus we continue our search on the boundary. This consists of six segments. As soon as we realize that $f(q,r) = f(r,q) = f(1-p, 1-q)$, we only have to consider two of them. All extreme points on these segments are maximum points, thus we continue to search on the edges: There are only six (and only two up to symmetry) and the smallest value of f on these edges is the minimum we wanted to find. It is useful to plot f.)

Exercise 5.2 (Design from lines). (9+8 points)

Let p be a prime number and $\mathbb{F}_p$ the field with p elements. Consider:

- $S = \mathbb{F}_p^2$,
- $S_{a,b} = \{(x, ax + b) \colon x \in \mathbb{F}_p\} \subseteq S$, for $a, b \in \mathbb{F}_p$,
- $D' = \{S_{a,b} \colon a, b \in \mathbb{F}_p\}$.

2 (i) Arrange the elements of D' into a sequence D.

3 (ii) Determine the uniquely determined values $k, n, s \in \mathbb{N}$ and the *smallest possible value* $t \in \mathbb{N}$ such that D is a (k, n, s, t)-design.

4 (iii) Consider the function

$$f \colon \begin{array}{ccc} \mathbb{B}^3 & \longrightarrow & \mathbb{B}, \\ x & \longmapsto & (x_1 \vee \neg x_2) \oplus (x_2 \wedge x_3) \end{array}$$

and compute $f_D(x)$ for $x = 101010101$ and $x = 110010011$.

+8 (iv) Generalize from lines to arbitrary degree polynomials. Which kind of designs do you obtain? Explain detailed.