CS 290T Computational Algebra
Winter Term 2016

Homework Assignment 02:

- Let $T_f = (0,1,0,1,0,1,1,1,1,1,0,1,0,1,1,1)$ be the truth table of $f : \mathbf{F}_2^4 \to \mathbf{F}_2$.
  1. Find the ANF (Algebraic Normal Form) of f.
  2. Find the degree of f.
  3. What is the distance between f and $x_1 + x_3 + x_4$?
  4. Find the nonlinearity of f.
  5. Is f satisfies $PC(1)$?
- Let $f(x_1, x_2, x_3, x_4) = x_1 + x_2x_3 + x_1x_4$ be a Boolean function over $\mathbf{F}_2^4$.
  1. Find the truth table of f.
  2. What is the distance between f and $x_1 + x_2$?
  3. Find the nonlinearity of f.
  4. Is f satisfies SAC?
- Let f be any Boolean function from $\mathbf{F}_2^8$ to F_2 and let $W_f(a) = \sum_{x \in \mathbf{F}_2^8} (-1)^{f(x)+a\cdot x}$ denote its Walsh transform $\left(a \cdot x = \sum_{i=1}^{8} a_i x_i\right)$. Then find the maximum and minimum value of

$$\sum_{a \in \mathbf{F}_2^8} \left(W_f(a)\right)^2 \ .$$

- The *linear complexity* of a given binary sequence is the length of the smallest LFSR (one with the fewest states) that produces the sequence. Compute the linear complexity of the following sequence:

$$0001001000110100010101100111100010 01$$

Due 5pm Wednesday February 10
Either, email an electronic copy to me (koc@cs.ucsb.edu) or bring a paper copy to the class. Electronic copy of your homework can be in Text or PDF. You could also scan/pdf your handwritten work; however, do not send (low-resolution or small) phone-camera images under any circumstances! Put your name inside the file. Also make the attached file name as your last name, followed by homework number, for example: green-hw01.pdf