Proofs, Arguments, and Zero-Knowledge
Solutions by L. Russo

1 Definitions and Technical Preliminaries

Exercise 3.2

Let $p = 11$. Consider the function $f : \{0,1\}^2 \to \mathbb{F}_p$ given by $f(0,0) = 3$, $f(0,1) = 4$, $f(1,0) = 1$ and $f(1,1) = 2$. Write out an explicit expression for the multilinear extension $\tilde{f}$ of f. What is $f(2,4)$?

Solution

We first write the Lagrange interpolation for f as $\tilde{f}(x_1, x_2) = \sum_{w \in \{0,1\}^2} f(w)\mathrm{X}_w(x_1, x_2)$, where $\mathrm{X}_w(x_1, x_2) = \prod_{i=1}^{2}(x_i w_i + (1 - x_i)(1 - w_i)$. We easily determine:

- $\mathrm{X}_{00}(x_1, x_2) = (1 - x_1)(1 - x_2)$
- $\mathrm{X}_{01}(x_1, x_2) = (1 - x_1)x_2$
- $\mathrm{X}_{10}(x_1, x_2) = x_1(1 - x_2)$
- $\mathrm{X}_{11}(x_1, x_2) = x_1 x_2$

Then we only need to compute $\tilde{f}(x_1, x_2) = 3(1-x_1)(1-x_2)+4(1-x_1)x_2+x_1(1-x_2)+2x_1x_2$ in $(x_1, x_2) = (2, 4)$.
$\tilde{f}(2,4) = 3(1-2)(1-4) + 4(1-2)4 + 2 \cdot 4 + 2 \cdot 2 \cdot 4 = 3$