The Proof for the Formula of the Lagrange Basis Polynomials for Cyclic Multiplicative Subgroups of Galois Fields

Aleksei Vambol

December 2022

1 Introduction

The Lagrange basis polynomials for cyclic multiplicative subgroups of finite fields are of great importance for the PlonKish zk-SNARK protocols. Indeed, the abbreviation "PlonK" stands for "Permutations over Lagrange-bases for Oecumenical Noninteractive Arguments of Knowledge" [GWC19].

Let H be a cyclic multiplicative subgroup of some finite field F. For a fixed ω, which is a generator of H, $n = |H|$ and $i \in [0..n-1]$ the i-th Lagrange basis polynomial $L_i(x)$ is $(n-1)$-degree polynomial, which equals 1 at ω^i and 0 at all other elements of H.

It is easy to see that the aforesaid polynomial is unique. In [PFM22] one can find the following formula:

$$L_i(x) = \frac{\omega^i(x^n - 1)}{n(x - \omega^i)}. \tag{1.1}$$

Since ω is of order n, it is obvious that $L_i(x)$ defined by (1.1) equals 0 at all other elements of H except for ω^i. However, it is harder to verify that the statement $L_i(\omega^i) = 1$ follows from (1.1). We have failed to find the proof of this statement in any source, so in the next section we give our own one, which accomplishes the proof of (1.1).

2 Proof for the Non-zero Case

Statement. $L_i(\omega^i) = 1$ for $L_i(x)$ defined by (1.1).

Proof. Since ω is a generator of H and $n = |H|$, all n elements of H are roots of the monic polynomial $x^n - 1$. This justifies the following identity:

$$x^n - 1 = (x-1)(x-\omega)(x-\omega^2)...(x-\omega^{n-1}). \tag{2.1}$$

Therefore, $L_i(\omega^i)$ can be rewritten as follows:

$$L_i(\omega^i) = \frac{\omega^i}{n} \prod_{k=0, k\neq i}^{n-1} (\omega^i - \omega^k). \tag{2.2}$$

Taking ω^i out of each bracket, we obtain the following formula:

$$L_i(\omega^i) = \frac{(\omega^i)^n}{n} \prod_{k=0, k\neq i}^{n-1} (1 - \omega^{k-i}). \tag{2.3}$$

Since ω is of order n, $\omega^{j+kn} = \omega^j$ for $j \in [0..n-1]$, so (2.3) implies the following identity:

$$L_i(\omega^i) = \frac{1}{n} \prod_{k=1}^{n-1} (1 - \omega^k). \tag{2.4}$$

Using (2.1) and the well-known formula $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + ... + 1)$, we obtain the following identity:

$$\sum_{k=0}^{n-1} x^k = \prod_{k=1}^{n-1} (x - \omega^k). \tag{2.5}$$

Combining (2.5) for $x = 1$ with (2.4), we obtain the formula

$$L_i(\omega^i) = \frac{1}{n} \sum_{k=0}^{n-1} 1^k, \tag{2.6}$$

which implies that $L_i(\omega^i) = 1$. ■

References

[GWC19] A. Gabizon, Z. Williamson, O. Ciobotaru. "PlonK: Permutations over Lagrange-bases for Oecumenical Noninteractive Arguments of Knowledge", Cryptology ePrint Archive, Report 2019/953, 2019.

https://eprint.iacr.org/2019/953

[PFM22] L. Pearson, J. Fitzgerald, H. Masip, M. Bellés-Muñoz, J. Muñoz-Tapia. "PlonKup: Reconciling PlonK with plookup", Cryptology ePrint Archive, Paper 2022/086, 2022.

https://eprint.iacr.org/2022/086