Lagrange bases in subgroups of $\mathbb{F}_p^*$: a hands-on introduction

Aragon Research - Math Seminar Note #1

Alex Kampa

April 2022

This seminar note aims to provide an easy to follow introduction to Lagrange bases in the particular context of subgroups of $\mathbb{F}_p^*$. Readers are encouraged to redo some of the examples by hand.

1 Setting and Motivation

We are in the field $\mathbb{F}_p$ where p is prime. The element $\omega \neq 0$ is a generator of order n of a multiplicative subgroup H of $\mathbb{F}_p^*$. Obviously, n divides $p-1$, which is the order of $\mathbb{F}_p^*$, and we have:

$$H = \{1, \omega, \omega^2, ..., \omega^{n-1}\} \tag{1}$$

We seek to represent a polynomial $P(x)$ over H that takes a set of predefined values v_i over the elements of H. In other words, given a set $V = \{v_0, v_1, ..., v_{n-1}\}$, we seek a polynomial P such that:

$$\forall\, \omega^i \in H,\ P(\omega^i) = v_i \tag{2}$$

Lagrange polynomials L_i provide an easy way to do this. The desired P is simply expressed as:

$$P(x) = v_0 L_0(x) + v_1 L_1(x) + ... + v_{n-1} L_{n-1}(x) \tag{3}$$

Lagrange polynomials, also called Lagrange bases, provide an alternative and useful approach to polynomials: instead of defining them by their coefficients, they are defined by their values. Lagrange polynomials have recently been used in the construction of a popular zk-SNARK scheme called PLONK [1].

2 Definitions

The Lagrange polynomials on H are a set of polynomials L_i defined for $0 \leq i < n-1$ as follows:

$$\forall x \in H, \quad L_i(x) = \begin{cases} 1 \text{ for } x = \omega^i \\ 0 \text{ otherwise} \end{cases} \tag{4}$$

It should be clear that we can write $L_i(x)$ as:

$$L_i(x) = \alpha_i \prod_{\substack{j=0 \\ j \neq i}}^{n-1} (x - \omega^j) \tag{5}$$

It is also useful to define the polynomial $L(x)$ which has roots at exactly all the element of H:

$$L(x) = \prod_{j=0}^{n-1} (x - \omega^j) \tag{6}$$

Our principal aim is to show that:

$$L(x) = x^n - 1 \tag{7}$$

and that:

$$L_i(x) = \frac{\omega^i}{n} \cdot \frac{x^n - 1}{x - \omega^i} = \frac{1}{n} \cdot \sum_{k=0}^{n-1} \omega^{-ik} x^k \tag{8}$$

2.1 Example 1

We place ourselves in $\mathbb{F}_3^*$, with $\omega = 2$, $H = \{1, 2\}$ and therefore $n = 2$. The two Lagrange polynomials in this case can be written:

$$
\begin{aligned}
L_0(x) &= a_0(x-2) \\
L_1(x) &= a_1(x-1)
\end{aligned}
\tag{9}
$$

As a result, and remembering that we are computing modulo 3, we find that:

$$
\begin{aligned}
L_0(1) = a_0(1-2) = 2a_0 = 1 &\implies a_0 = 2 = {}^1\!/_2 \\
L_1(2) = a_1(2-1) = 1a_1 = 1 &\implies a_1 = 1 = {}^2\!/_2
\end{aligned}
\tag{10}
$$

Now let's compute $L(x)$, noting that we have $2 = -1$ in modulo 3:

$$
\begin{aligned}
L(x) &= (x-1)(x-2) \\
&= x^2 - x(1+2) + 1 \cdot 2 \\
&= x^2 - 3x + 2 \\
&= x^2 - 1
\end{aligned}
\tag{11}
$$

2.2 Example 2

We place ourselves in $\mathbb{F}_7^*$, with $\omega = 2$, $H = \{1, 2, 4\}$ and therefore $n = 3$. The three Lagrange polynomials in this case can be written:

$$
\begin{aligned}
L_0(x) &= a_0(x-2)(x-4) \\
L_1(x) &= a_1(x-1)(x-4) \\
L_2(x) &= a_2(x-1)(x-2)
\end{aligned}
\tag{12}
$$

As a result, and remembering that we are computing modulo 7, we find:

$$
\begin{aligned}
L_0(1) = a_0(1-2)(1-4) = 3a_0 = 1 &\implies a_0 = 5 = {}^1\!/_3 \\
L_1(2) = a_1(2-1)(2-4) = 5a_1 = 1 &\implies a_0 = 3 = {}^2\!/_3 \\
L_2(4) = a_2(4-1)(4-2) = 6a_2 = 1 &\implies a_0 = 6 = {}^4\!/_3
\end{aligned}
\tag{13}
$$

Now let's compute $L(x)$:

$$
\begin{aligned}
L(x) &= (x-1)(x-2)(x-4) \\
&= x^3 - x^2(1+2+4) + x(1 \cdot 2 + 1 \cdot 4 + 2 \cdot 4) - 1 \cdot 2 \cdot 4 \\
&= x^3 - 7x^2 + 14x - 8 \\
&= x^3 - 1
\end{aligned}
\tag{14}
$$

3 More Definitions

We assume that p and ω are fixed, and therefore also n. We define I to be the set containing all n integers between 0 and $n-1$.

$$I = \{0, 1, ..., n-1\} \tag{15}$$

For $i \in I$, we define I_i as the set of all integers between 0 and $n-1$, with the exception of i.

$$I_i = \{0, 1, ..., n-1\} \setminus \{i\} \tag{16}$$

For $0 < k \leq n-1$, We define $C(k)$ as the set of all strictly increasing sequences of length k contained in I^k.

$$C(k) = \{\{j_1, ..., j_k\} \in I^k : j_1 < .. < j_k\} \tag{17}$$

Clearly, $C(k)$ represents the number of k-element subsets of I, and $|C(k)| = \binom{n}{k}$. We similarly define $C_i(k)$ as the set of all strictly increasing sequences of length k contained in I_i^k.

$$C_i(k) = \{\{j_1, ..., j_k\} \in I_i^k : j_1 < .. < j_k\} \tag{18}$$

We can now define the following sums over elements of $C(k)$ and $C_i(k)$, with $k > 0$:

$$S(k) = \sum_{\vec{j} \in C(k)} \omega^{j_1 + .. + j_k} \tag{19}$$

$$S_i(k) = \sum_{\vec{j} \in C_i(k)} \omega^{j_1 + .. + j_k} \tag{20}$$

Finally, it is useful to define these sums for $k = 0$ as follows:

$$S(0) = S_i(0) = 1 \tag{21}$$

Note that in all the above definitions, n is considered as fixed. If necessary the sets/sums defined above could be denoted more explicitly as $I(n)$, $I_i(n)$, $C(k,n)$, $C_i(k,n)$, $S(k,n)$ and $S_i(k,n)$.

3.1 Example 3

Let's assume our subgroup is of order 5. This would be the case if we took $\omega = 3$ in $\mathbb{F}_{11}^*$, with $\{1, \omega, \omega^2, \omega^3, \omega^4\} = \{1, 3, 9, 5, 4\}$. The polynomial $L(x)$ can be written as:

$$\begin{aligned} L(x) &= (x - \omega^0)(x - \omega^1)(x - \omega^2)(x - \omega^3)(x - \omega^4) \\ &= a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \end{aligned} \tag{22}$$

The coefficients of this polynomial are:

$$\begin{aligned} a_5 &= 1 \\ &= (-1)^0 \cdot S(0) \\[1em] a_4 &= -(\omega^0 + \omega^1 + \omega^2 + \omega^3 + \omega^4) \\ &= (-1)^1 \cdot S(1) \\[1em] a_3 &= \omega^0\omega^1 + \omega^0\omega^2 + \omega^0\omega^3 + \omega^0\omega^4 + \omega^1\omega^2 \\ &\quad + \omega^1\omega^3 + \omega^1\omega^4 + \omega^2\omega^3 + \omega^2\omega^4 + \omega^3\omega^4 \\ &= (-1)^2 \cdot S(2) = 2 \cdot (\omega^0 + \omega^1 + \omega^2 + \omega^3 + \omega^4) \\[1em] a_2 &= -(\omega^0\omega^1\omega^2 + \omega^0\omega^1\omega^3 + \omega^0\omega^1\omega^4 + \omega^0\omega^2\omega^3 + \omega^0\omega^2\omega^4 \\ &\quad + \omega^0\omega^3\omega^4 + \omega^1\omega^2\omega^3 + \omega^1\omega^2\omega^4 + \omega^1\omega^3\omega^4 + \omega^2\omega^3\omega^4) \\ &= (-1)^3 \cdot S(3) = -2 \cdot (\omega^0 + \omega^1 + \omega^2 + \omega^3 + \omega^4) \\[1em] a_1 &= \omega^0\omega^1\omega^2\omega^3 + \omega^0\omega^1\omega^2\omega^4 + +\omega^0\omega^1\omega^3\omega^4 \\ &\quad + \omega^0\omega^2\omega^3\omega^4 + \omega^1\omega^2\omega^3\omega^4 \\ &= (-1)^4 \cdot S(4) = \omega^0 + \omega^1 + \omega^2 + \omega^3 + \omega^4 \\[1em] a_0 &= -\omega^0\omega^1\omega^2\omega^3\omega^4 \\ &= (-1)^5 \cdot S(5) \end{aligned} \tag{23}$$

Note that a_4 is a sum of $5 = \binom{5}{1}$ elements, a_3 a sum of $10 = \binom{5}{2}$ elements etc.

Also note that, because $\omega^5 = \omega^0 = 1$, we have:

$$\begin{aligned} \omega \cdot a_4 &= \omega \cdot (\omega^0 + \omega^1 + \omega^2 + \omega^3 + \omega^4) \\ &= \omega^1 + \omega^2 + \omega^3 + \omega^4 + \omega^0 \\ &= a_4 \end{aligned} \tag{24}$$

Now $\omega \cdot a_4 = a_4$ implies $a_4 = 0$ because $\omega \neq 0$. As a result, it is clear that $a_1 = a_2 = a_3 = a_4 = 0$. As to a_0, we have:

$$a_0 = -\omega^{0+1+2+3+4} = -\omega^{10} = -1 \tag{25}$$

This conforms to our expectation that:

$$L(x) = x^5 - 1 \tag{26}$$

3.2 Example 4

In the same setting as the preceding example, with $n = 5$, the Lagrange polynomial $L_3(x)$ can be written as:

$$\begin{aligned} \frac{L_3(x)}{\alpha_3} &= (x - \omega^0)(x - \omega^1)(x - \omega^2)(x - \omega^4) \\ &= b_4 x^4 + b_3 x^3 + b_2 x^2 + b_1 x + b_0 \end{aligned} \tag{27}$$

The coefficients of this polynomial are:

$$\begin{aligned} b_4 &= 1 \\ &= (-1)^0 \cdot S_3(0) \\ \\ b_3 &= -(\omega^0 + \omega^1 + \omega^2 + \omega^4) \\ &= (-1)^1 \cdot S_3(1) = \omega^3 \\ \\ b_2 &= \omega^0\omega^1 + \omega^0\omega^2 + \omega^0\omega^4 + \omega^1\omega^2 + \omega^1\omega^4 + \omega^2\omega^4 \\ &= (-1)^2 \cdot S_3(2) = \omega \\ \\ b_1 &= -(\omega^0\omega^1\omega^2 + \omega^0\omega^1\omega^4 + \omega^0\omega^2\omega^4 + \omega^1\omega^2\omega^4) \\ &= (-1)^3 \cdot S_3(3) = \omega^4 \\ \\ b_0 &= \omega^0\omega^1\omega^2\omega^4 \\ &= (-1)^4 \cdot S_3(4) = \omega^2 \end{aligned} \tag{28}$$

Therefore:

$$\frac{L_3(x)}{\alpha_3} = x^4 + \omega^3 x^3 + \omega x^2 + \omega^4 x + \omega^2 \tag{29}$$

By definition, $L_3(\omega^3) = 1$. Plugging this in the above equation, we obtain:

$$\frac{L_3(\omega^3)}{\alpha_3} = \frac{1}{\alpha_3} = 5\omega^2 \implies \alpha_3 = \frac{1}{5\omega^2} = \frac{\omega^3}{5} \tag{30}$$

So finally:

$$L_3(x) = \frac{\omega^3}{5} \cdot \frac{x^5 - 1}{x - \omega^3} = \frac{1}{5} \cdot (\omega^3 x^4 + \omega x^3 + \omega^4 x^2 + \omega^2 x + 1) \tag{31}$$

4 Explicit representations of $L(x)$ and $L_i(x)$

The preceding examples have hopefully made it clear that we can write $L(x)$ and $L_i(x)$ as:

$$L(x) = \prod_{k=0}^{n-1} (x - \omega^k) = \sum_{k=0}^{n} (-1)^{n-k} S(n-k) x^k \tag{32}$$

$$\frac{L_i(x)}{\alpha_i} = \prod_{\substack{j=0 \\ j \neq i}}^{n-1} (x - \omega^k) = \sum_{k=0}^{n-1} (-1)^{n-1-k} S_i(n-1-k) x^k \tag{33}$$

In fact, $S(k)$ and $S_i(k)$ have specifically been defined for this to be true. The proof of this fact is simple and left to the reader.

4.1 Values of $S(k)$ and $S_i(k)$ for $0 < k < n$

We want to show that for $0 < k < n$, we have:

$$\begin{aligned} S(k) &= 0 \\ S_i(k) &= (-1)^k \omega^{ik} \end{aligned} \tag{34}$$

We proceed by induction.

We have $S(1) = \omega^0 + \omega^1 + ... + \omega^{n-1} = 0$ because $\omega \cdot S(1) = S(1)$. We also have $S_i(1) = S(1) - \omega^i = -\omega^i$. The relation therefore holds for $k = 1$.

Let us now express $S(k)$ in n different ways:

$$
\begin{aligned}
S(k) &= \omega^0 S_0(k-1) + S_0(k) \\
&= \omega^1 S_1(k-1) + S_1(k) \\
&= \ldots \\
&= \omega^{n-1} S_{n-1}(k-1) + S_{n-1}(k)
\end{aligned}
\tag{35}
$$

Adding all of these up, we obtain:

$$
\begin{aligned}
nS(k) &= \sum_{i=0}^{n-1} \omega^i S_i(k-1) + \sum_{i=0}^{n-1} S_i(k) \\
&= A(k) + B(k)
\end{aligned}
\tag{36}
$$

By the induction hypothesis, we have $S_i(k-1) = (-1)^{k-1}\omega^{i(k-1)}$ and therefore:

$$
A(k) = \sum_{i=0}^{n-1} \omega^i (-1)^{k-1} \omega^{i(k-1)} = (-1)^{k-1} \sum_{i=0}^{n-1} \omega^{ik} \tag{37}
$$

Notice that $\omega^k A(k) = A(k)$ and therefore $A(k) = 0$.

As to $B(k)$, it has to be a multiple of S(k). To see why, take an arbitrary term $\omega^{j_1+..+j_k}$ of $S(k)$. This term cannot appear in any of the k sums $S_{j_1}(k)$, $S_{j_2}(k)$ ... $S_{j_k}(k)$, but will appear in all of the $n-k$ other groups. Therefore $B(k) = (n-k)S(k)$.

A second way to looks at this is by invoking symmetry. Taking some arbitrary term of $S(k)$, it will appear in $B(k)$ a certain number of times. There is no reason why one term would appear more or less often than another, meaning they all appear with the same frequency. As $nS(k)$ has $n\binom{n}{k}$ terms and $B(k)$ has $n\binom{n-1}{k}$ terms, we again conclude that $B(k) = (n-k)S(k)$. As a result:

$$
\begin{aligned}
nS(k) &= A(k) + B(k) = 0 + (n-k)S(k) \\
&\implies kS(k) = 0 \\
&\implies S(k) = 0
\end{aligned}
\tag{38}
$$

We now use this fact to determine the value of $S_i(k)$.

$$
\begin{aligned}
S(k) &= \omega^i S_i(k-1) + S_i(k) = 0 \\
&\implies S_i(k) = -\omega^i S_i(k-1)
\end{aligned}
\tag{39}
$$

Again using the induction hypothesis, we obtain:

$$
S_i(k) = -\omega^i (-1)^{k-1} \omega^{i(k-1)} = (-1)^k \omega^{ik} \tag{40}
$$

This completes the proof.

4.2 An example

Let's take the example of $S(2)$ with $n = 4$:

$$S(2) = \omega^0\omega^1 + \omega^0\omega^2 + \omega^0\omega^3 + \omega^1\omega^2 + \omega^1\omega^3 + \omega^2\omega^3$$

$$\begin{aligned}
&= \omega^0(\omega^1 + \omega^2 + \omega^3) + (\omega^1\omega^2 + \omega^1\omega^3 + \omega^2\omega^3) = \omega^0 S_0(1) + S_0(2) \\
&= \omega^1(\omega^0 + \omega^2 + \omega^3) + (\omega^0\omega^2 + \omega^0\omega^3 + \omega^2\omega^3) = \omega^1 S_1(1) + S_1(2) \\
&= \omega^2(\omega^0 + \omega^1 + \omega^3) + (\omega^0\omega^1 + \omega^0\omega^3 + \omega^1\omega^3) = \omega^2 S_2(1) + S_2(2) \\
&= \omega^3(\omega^0 + \omega^1 + \omega^2) + (\omega^0\omega^1 + \omega^0\omega^2 + \omega^1\omega^2) = \omega^3 S_3(1) + S_3(2)
\end{aligned} \tag{41}$$

So we can write $4S(2) = A(2) + B(2)$, with:

$$\begin{aligned}
A(2) &= \omega^0 S_0(1) + \omega^1 S_1(1) + \omega^1 S_1(1) + \omega^2 S_2(1) + \omega^3 S_3(1) \\
B(2) &= S_0(2) + S_1(2) + S_2(2) + S_3(2)
\end{aligned} \tag{42}$$

Remembering that $0 = \omega^0 + \omega^1 + \omega^2 + \omega^3 \implies \omega^1 + \omega^2 + \omega^3 = -\omega^0$ etc:

$$\begin{aligned}
A(2) &= \omega^0(-\omega^0) + \omega^1(-\omega^1) + \omega^2(-\omega^2) + \omega^3(-\omega^3) \\
&= -2(\omega^0 + \omega^2) \\
&= 0
\end{aligned} \tag{43}$$

Now note that every term of $S(2)$ appears in $B(2)$ exactly twice, which means that $B(2) = 2S(2)$.

$$4S(2) = A(0) + B(2) = 0 + 2S(2) \implies S(2) = 0 \tag{44}$$

Finally, we find $S_0(2) = S_2(2) = \omega^0 = 1$ and $S_1(2) = S_3(2) = \omega^2 = -1$.

4.3 The value of $S(n)$

We have $S(n) = \omega^0\omega^1 ... \omega^{n-1}$ and therefore $S(n) = \omega^{0+1+...+(n-1)} = \omega^{n(n-1)/2}$.

When n is even, we can write $n = 2m$ and $S(n) = \omega^{m(2m-1)} = \omega^{-m} = \omega^m = -1$. To see why $\omega^m = -1$, note that $\omega^m(1 + \omega^m) = 1 + \omega^m$.

When n is odd, we can write $n = 2m + 1$ and thus $S(0) = \omega^{nm} = 1$.

We can therefore write:

$$S(n) = (-1)^{n+1} \tag{45}$$

4.4 The formula for $L(x)$

Let us summarise what we have found out so far. We have first converted $L(x)$ from a product to a sum (equation 32). We know that $S(0) = 1$ (equation 21) and we also found that $S(k) = 0$ for $0 < k < n$ (equation 38) and that $s(n) = (-1)^{n+1}$ (equation 45). We can therefore write:

$$\begin{aligned} L(x) &= \sum_{k=0}^{n} (-1)^{n-k} S(n-k) x^k \\ &= (-1)^n S(n) + \sum_{k=1}^{n-1} (-1)^{n-k} S(n-k) x^k + S(0) x^n \\ &= (-1)^n (-1)^{n+1} + 0 + 1 \cdot x^n \\ &= -1 + x^n \end{aligned} \tag{46}$$

As a result, we have:

$$L(x) = \prod_{k=0}^{n-1} (x - \omega^k) = x^n - 1 \tag{47}$$

4.5 The value of α_i

We have found that $S_i(k) = (-1)^k \omega^{ik}$ (equation 40), equation 33 can therefore be restated as follows:

$$\begin{aligned} \frac{L_i(x)}{\alpha_i} &= \sum_{k=0}^{n-1} (-1)^{n-1-k} S_i(n-1-k) x^k \\ &= \sum_{k=0}^{n-1} (-1)^{n-1-k} (-1)^{n-1-k} \omega^{i(n-1-k)} x^k \\ &= \sum_{k=0}^{n-1} \omega^{-i(k+1)} x^k \end{aligned} \tag{48}$$

By definition, $L_i(\omega^i) = 1$, so we can write:

$$\frac{L_i(\omega^i)}{\alpha_i} = \frac{1}{\alpha_i} = \sum_{k=0}^{n-1} \omega^{-i(k+1)}\omega^{ik} = n \cdot \omega^{-i} \tag{49}$$

So we finally have $\alpha_i = \omega^i/n$.

4.6 The formula for $L_i(x)$

Now that we have α_i, we can write:

$$L_i(x) = \frac{\omega^i}{n} \cdot \sum_{k=0}^{n-1} \omega^{-i(k+1)} x^k = \frac{1}{n} \cdot \sum_{k=0}^{n-1} \omega^{-ik} x^k \tag{50}$$

Final formula:

$$\begin{aligned} L_i(x) &= \frac{\omega^i}{n} \cdot \prod_{\substack{j=0 \\ j \neq i}}^{n-1} (x - \omega^k) \\ &= \frac{\omega^i}{n} \cdot \frac{x^n - 1}{x - \omega^i} \\ &= \frac{1}{n} \cdot \sum_{k=0}^{n-1} \omega^{-ik} x^k \end{aligned} \tag{51}$$

References

[1] Ariel Gabizon, Zachary J. Williamson, and Oana Ciobotaru. PLONK: permutations over lagrange-bases for oecumenical noninteractive arguments of knowledge. *IACR Cryptol. ePrint Arch.*, page 953, 2019.