

This document presents some of the details for deriving the polynomials needed for generating the SNARKs in the example code. The goal is to generate a strong *QAP* for the equation  $3 * x = 6$  as described here: <https://eprint.iacr.org/2012/215.pdf>

The starting set of polynomials is provided a priori, because they are relatively trivial to figure out with Lagrangian interpolation compared to the polynomial product calculated for:

$$(v_0 + \sum_{k=1}^2 a_k v_k)(w_0 + \sum_{k=1}^2 a_k w_k) - (y_0 + \sum_{k=1}^2 a_k y_k)$$

into the form  $h(x)t(x) = h(x)(x - r)$  for the SNARK.

Starting with the first set of polynomials the equations are:

$$\begin{aligned} v'_0(x) &= 1 * \frac{(x-r)(x-r_1)(x-r_2)(x-s_2)}{(s_1-r)(s_1-r_1)(s_1-r_2)(s_1-s_2)} \\ &\quad + 1 * \frac{(x-r)(x-r_1)(x-r_2)(x-s_1)}{(s_2-r)(s_2-r_1)(s_2-r_2)(s_2-s_1)} \\ &\quad + 3 * \frac{(x-r_1)(x-r_2)(x-s_1)(x-s_2)}{(r-r_1)(r-r_2)(r-s_1)(r-s_2)} \\ v'_1(x) &= 1 * \frac{(x-r)(x-r_2)(x-s_1)(x-s_2)}{(r_1-r)(r_1-r_2)(r_1-s_1)(r_1-s_2)} \\ v'_2(x) &= 1 * \frac{(x-r)(x-r_1)(x-s_1)(x-s_2)}{(r_2-r)(r_2-r_1)(r_2-s_1)(r_2-s_2)} \end{aligned}$$

With Lagrange basis polynomials:

$$\begin{aligned} l_r(x) &= \frac{(x-r_1)(x-r_2)(x-s_1)(x-s_2)}{(r-r_1)(r-r_2)(r-s_1)(r-s_2)} \\ l_{r_1}(x) &= \frac{(x-r)(x-r_2)(x-s_1)(x-s_2)}{(r_1-r)(r_1-r_2)(r_1-s_1)(r_1-s_2)} \\ l_{r_2}(x) &= \frac{(x-r)(x-r_1)(x-s_1)(x-s_2)}{(r_2-r)(r_2-r_1)(r_2-s_1)(r_2-s_2)} \\ l_{s_1}(x) &= \frac{(x-r)(x-r_1)(x-r_2)(x-s_2)}{(s_1-r)(s_1-r_1)(s_1-r_2)(s_1-s_2)} \\ l_{s_2}(x) &= \frac{(x-r)(x-r_1)(x-r_2)(x-s_1)}{(s_2-r)(s_2-r_1)(s_2-r_2)(s_2-s_1)} \end{aligned}$$

So that the first set can be rewritten as interpolation polynomials in Lagrange form:

$$\begin{aligned} v'_0(x) &= 1 * l_{s_1}(x) + 1 * l_{s_2}(x) + 3 * l_r(x) \\ v'_1(x) &= 1 * l_{r_1}(x) \\ v'_2(x) &= 1 * l_{r_2}(x) \end{aligned}$$

Next, in order to convert the set of polynomials that are part of the strong *QAP* into the form needed, each of the basis polynomials needs to be rewritten with a factor of  $x - r$ . Fortunately, only  $l_r(x)$  is not in that form, but is converted using the procedure outlined here:

$$\begin{aligned}
l_r(x) &= \frac{(x-r_1)(x-r_2)(x-s_1)(x-s_2)}{(r-r_1)(r-r_2)(r-s_1)(r-s_2)} \\
&= \frac{(x^2 + (-r_1-r_2)x + r_1r_2)(x^2 + (-s_1-s_2)x + s_1s_2)}{(r-r_1)(r-r_2)(r-s_1)(r-s_2)}
\end{aligned}$$

Taking the first term in the of the product of the numerator shows that:

$$(x + (-r_1-r_2)x + r_1r_2) = (x-r_1)(x-r_2)(x-r) + (r-r_1)(r-r_2)$$

And substituting back into the basis polynomial, expanding terms, and consolidating coefficients of  $x-r$  gives:

$$\begin{aligned}
l_r(x) &= \frac{(x-r_1)(x-r_2)(x-s_1)(x-s_2)}{(r-r_1)(r-r_2)(r-s_1)(r-s_2)} \\
&= \frac{(x^2 + (-r_1-r_2)x + r_1r_2)(x^2 + (-s_1-s_2)x + s_1s_2)}{(r-r_1)(r-r_2)(r-s_1)(r-s_2)} \\
&= \frac{((x-r_1)(x-r_2)(x-r) + (r-r_1)(r-r_2))((x-s_1)(x-s_2)(x-r) + (r-s_1)(r-s_2))}{(r-r_1)(r-r_2)(r-s_1)(r-s_2)} \\
&= A(x-r) + B(x-r) + C(x-r) + 1
\end{aligned}$$

With

$$\begin{aligned}
A &= (x-r_1)(x-r_2)(x-s_1)(x-s_2)(x-r) \\
B &= (r-r_1)(r-r_2)(x-s_1)(x-s_2) \\
C &= (x-r_1)(x-r_2)(r-s_1)(r-s_2)
\end{aligned}$$

then to make some of the manipulations that will need to be made later easier it is helpful to factor out the  $x-r$  term in the basis polynomials:

$$\begin{aligned}
v'_0(x) &= 1 * l'_{s_1}(x)(x-r) + 1 * l'_{s_2}(x)(x-r) + 3(A(x) + B(x) + C(x))(x-r) + 3 \\
v'_1(x) &= 1 * l'_{r_1}(x)(x-r) \\
v'_2(x) &= 1 * l'_{r_2}(x)(x-r)
\end{aligned}$$

Where the primed basis polynomials are easy to see, so no need to take up space rewriting them here. The other two sets of polynomials are:

$$\begin{aligned}
w'_0(x) &= 1 * \frac{(x-r)(x-r_2)(x-s_1)(x-s_2)}{(r_1-r)(r_1-r_2)(r_1-s_1)(r_1-s_2)} + 1 * \frac{(x-r)(x-r_1)(x-s_1)(x-s_2)}{(r_2-r)(r_2-r_1)(r_2-s_1)(r_2-s_2)} \\
&= 1 * l_{r_1}(x) + 1 * l_{r_2}(x) \\
&= 1 * l'_{r_1}(x)(x-r) + 1 * l'_{r_2}(x)(x-r) \\
w'_1(x) &= 1 * \frac{(x-r)(x-r_1)(x-r_2)(x-s_2)}{(s_1-r)(s_1-r_1)(s_1-r_2)(s_1-s_2)} + 1 * \frac{(x-r_1)(x-r_2)(x-s_1)(x-s_2)}{(r-r_1)(r-r_2)(r-s_1)(r-s_2)} \\
&= 1 * l_{s_1}(x) + 1 * l_r(x) \\
&= 1 * l'_{s_1}(x)(x-r) + (A(x) + B(x) + C(x))(x-r) + 1 \\
w'_2(x) &= 1 * \frac{(x-r)(x-r_1)(x-r_2)(x-s_1)}{(s_2-r)(s_2-r_1)(s_2-r_2)(s_2-s_1)} \\
&= 1 * l_{s_2}(x) \\
&= 1 * l'_{s_2}(x)(x-r)
\end{aligned}$$

And

$$y_0'(x) = 0$$

$$\begin{aligned} y_1'(x) &= 1 * \frac{(x-r)(x-r_2)(x-s_1)(x-s_2)}{(r_1-r)(r_1-r_2)(r_1-s_1)(r_1-s_2)} + 1 * \frac{(x-r)(x-r_1)(x-r_2)(x-s_2)}{(s_1-r)(s_1-r_1)(s_1-r_2)(s_1-s_2)} \\ &= 1 * l_{r_1}(x) + 1 * l_{s_1}(x) \\ &= 1 * l'_{r_1}(x)(x-r) + 1 * l'_{s_1}(x)(x-r) \end{aligned}$$

$$\begin{aligned} y_2'(x) &= 1 * \frac{(x-r_1) * (x-r_2) * (x-s_1) * (x-s_2)}{(r-r_1) * (r-r_2) * (r-s_1) * (r-s_2)} \\ &\quad + 1 * \frac{(x-r)(x-r_1)(x-s_1)(x-s_2)}{(r_2-r)(r_2-r_1)(r_2-s_1)(r_2-s_2)} \\ &\quad + 1 * \frac{(x-r)(x-r_1)(x-r_2)(x-s_1)}{(s_2-r)(s_2-r_1)(s_2-r_2)(s_2-s_1)} \\ &= 1 * l_r(x) + 1 * l_{r_2}(x) + 1 * l_{s_2}(x) \\ &= 1 * l'_{r_2}(x)(x-r) + 1 * l'_{s_2}(x)(x-r) + (A(x) + B(x) + C(x))(x-r) + 1 \end{aligned}$$

Now before calculating the polynomial product at the top simplify each of the terms:

$$\begin{aligned} v_0 + \sum_{k=1}^2 a_k v_k &= 1 * l_{s_1}(x) + 1 * l_{s_2}(x) + 3 * l_r(x) + a_1 * l_{r_1}(x) + a_2 * l_{r_2}(x) \\ &= 3(A(x) + B(x) + C(x))(x-r) + 3 \\ &\quad + a_1 * l'_{r_1}(x)(x-r) + a_2 * l'_{r_2}(x)(x-r) + 1 * l'_{s_1}(x)(x-r) + 1 * l'_{s_2}(x)(x-r) \\ &= (3A(x) + 3B(x) + 3C(x) + a_1 * l'_{r_1}(x) + a_2 * l'_{r_2}(x) + 1 * l'_{s_1}(x) + 1 * l'_{s_2}(x))(x-r) + 3 \\ &= f_v(x)(x-r) + 3 \end{aligned}$$

$$\begin{aligned} w_0 + \sum_{k=1}^2 a_k w_k &= 1 * l_{r_1}(x) + 1 * l_{r_2}(x) + a_1 * l_{s_1}(x) + a_1 * l_r(x) + a_2 * l_{s_2}(x) \\ &= a_1(A(x) + B(x) + C(x))(x-r) + a_1 \\ &\quad + 1 * l'_{r_1}(x)(x-r) + 1 * l'_{r_2}(x)(x-r) + a_1 * l'_{s_1}(x)(x-r) + a_2 * l'_{s_2}(x)(x-r) \\ &= (a_1A(x) + a_1B(x) + a_1C(x) + 1 * l'_{r_1}(x) + 1 * l'_{r_2}(x) + a_1 * l'_{s_1}(x) + a_2 * l'_{s_2}(x))(x-r) + a_1 \\ &= f_w(x)(x-r) + a_1 \end{aligned}$$

$$\begin{aligned} y_0 + \sum_{k=1}^2 a_k y_k &= a_1 * l_{r_1}(x) + a_1 * l_{s_1}(x) + a_2 * l_r(x) + a_2 * l_{r_2}(x) + a_2 * l_{s_2}(x) \\ &= a_2(A(x) + B(x) + C(x))(x-r) + a_2 \\ &\quad + a_1 * l'_{r_1}(x)(x-r) + a_1 * l'_{s_1}(x)(x-r) + a_2 * l'_{r_2}(x)(x-r) + a_2 * l'_{s_2}(x)(x-r) \\ &= f_y(x)(x-r) + a_2 \end{aligned}$$

The product is then:

$$\begin{aligned} (v_0 + \sum_{k=1}^2 a_k v_k)(w_0 + \sum_{k=1}^2 a_k w_k) - (y_0 + \sum_{k=1}^2 a_k y_k) &= (f_v(x)(x-r) + 3)(f_w(x)(x-r) + a_1) - (f_y(x)(x-r) + a_2) \\ &= f_v(x)f_w(x)(x-r)^2 + a_1f_v(x)(x-r) + 3f_w(x)(x-r) + 3a_1 \\ &\quad - f_y(x)(x-r) - a_2 \\ &= f_v(x)f_w(x)(x-r)^2 + 2f_v(x)(x-r) + 3f_w(x)(x-r) + 3 * 2 \\ &\quad - f_y(x)(x-r) - 6 \\ &= (f_v(x)f_w(x)(x-r) + 2f_v(x) + 3f_w(x) - f_{y(x)})(x-r) \end{aligned}$$

And clearly we have an expression for  $h(x)$  that is a composition of slightly modified Lagrange basis polynomials.