QAP (Quadratic Arithmetic Program)

Sample calculations in deriving some of the polynomials used in constructing a *SNARK* for the equation $3 * x = 6$. The equation

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

is guaranteed to have the form $h(x)t(x) = h(x)(x - r)$ by the *Polynomial remainder theorem* and more specifically the *Factor theorem*. The first set of polynomials are the equations:

$$\begin{aligned} v_0^{'}(x) = 1 * &\frac{(x-r)(x-r_1)(x-r_2)(x-s_2)}{(s_1-r)(s_1-r_1)(s_1-r_2)(s_1-s_2)} \\ &+ 1 * \frac{(x-r)(x-r_1)(x-r_2)(x-s_1)}{(s_2-r)(s_2-r_1)(s_2-r_2)(s_2-s_1)} \\ &+ 3 * \frac{(x-r_1)(x-r_2)(x-s_1)(x-s_2)}{(r-r_1)(r-r_2)(r-s_1)(r-s_2)} \end{aligned}$$

$$v_1^{'}(x) = 1 * \frac{(x-r)(x-r_2)(x-s_1)(x-s_2)}{(r_1-r)(r_1-r_2)(r_1-s_1)(r_1-s_2)}$$

$$v_2^{'}(x) = 1 * \frac{(x-r)(x-r_1)(x-s_1)(x-s_2)}{(r_2-r)(r_2-r_1)(r_2-s_1)(r_2-s_2)}$$

With Lagrange basis polynomials:

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

So, 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, rewrite each of the basis polynomials in a form that has a factor of $x - r$:

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

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

$$(x + (-r_1 - r_2)x + r_1 r_2) = (x - r1)(x - r2)(x - r) + (r - r1)(r - r2)$$

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

$$
\begin{aligned}
l_r(x) &= \frac{(x-r_1)(x-r_2)(x-s_1)(x-s_2)}{(r-r_1)(r-r_2)(r-s_1)(r-s_2)} \\
&= \frac{(x^2+(-r_1-r_2)x+r_1r_2)(x^2+(-s_1-s_2)x+s_1s_2)}{(r-r_1)(r-r_2)(r-s_1)(r-s_2)} \\
&= \frac{((x-r1)(x-r_2)(x-r)+(r-r_1)(r-r_2))((x-s_1)(x-s_2)(x-r)+(r-s_1)(r-s_2))}{(r-r_1)(r-r_2)(r-s_1)(r-s_2)} \\
&= A(x-r)+B(x-r)+C(x-r)+1
\end{aligned}
$$

Where:

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

To make the algebra easier factor out the $x-r$ term in the basis polynomials:

$$
\begin{aligned}
v_0^{'}(x) &= 1*l_{s_1}^{'}(x)(x-r)+1*l_{s_2}^{'}(x)(x-r)+3(A(x)+B(x)+C(x))(x-r)+3 \\
v_1^{'}(x) &= 1*l_{r_1}^{'}(x)(x-r) \\
v_2^{'}(x) &= 1*l_{r_2}^{'}(x)(x-r)
\end{aligned}
$$

The other two sets of polynomials become:

$$
\begin{aligned}
w_0^{'}(x) &= 1*\frac{(x-r)(x-r_2)(x-s_1)(x-s_2)}{(r_1-r)(r_1-r_2)(r_1-s_1)(r_1-s_2)}+1*\frac{(x-r)(x-r_1)(x-s_1)(x-s_2)}{(r_2-r)(r_2-r_1)(r_2-s_1)(r_2-s_2)} \\
&= 1*l_{r_1}(x)+1*l_{r_2}(x) \\
&= 1*l_{r_1}^{'}(x)(x-r)+1*l_{r_2}^{'}(x)(x-r)
\end{aligned}
$$

$$
\begin{aligned}
w_1^{'}(x) &= 1*\frac{(x-r)(x-r_1)(x-r_2)(x-s_2)}{(s_1-r)(s_1-r_1)(s_1-r_2)(s_1-s_2)}+1*\frac{(x-r1)(x-r_2)(x-s_1)(x-s_2)}{(r-r_1)(r-r_2)(r-s_1)(r-s_2)} \\
&= 1*l_{s_1}(x)+1*l_r(x) \\
&= 1*l_{s_1}^{'}(x)(x-r)+(A(x)+B(x)+C(x))(x-r)+1
\end{aligned}
$$

$$
\begin{aligned}
w_2^{'}(x) &= 1*\frac{(x-r)(x-r_1)(x-r_2)(x-s_1)}{(s_2-r)(s_2-r1)(s_2-r_2)(s_2-s_1)} \\
&= 1*l_{s_2}(x) \\
&= 1*l_{s_2}^{'}(x)(x-r)
\end{aligned}
$$

and

$$
y_0^{'}(x) = 0
$$

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

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

Now, before calculating the full expression simplify each of the terms with a factor $x - r$:

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

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

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

The product is then:

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

An expression of the form $h(x)(x-r)$ as needed.

Zero Knowledge Set Membership

Derivation showing the equality between what the prover generates and what the verifier checks. From the construction:

$$
y = g^x, \quad A_i = g^{\frac{1}{x+i}}, \quad V = A_\delta^\tau = g^{\frac{\tau}{x+\delta}}
$$

Prover claims to send:

$$a = e(V, g)^{-s} \cdot e(g, g)^t$$

and to validate this the verifier send c for which if they recieve (supposedly) $z_\delta = s - \delta c$, $z_\tau = t - \tau c$, and $z_\gamma = m - \gamma c$. So they can check the validity of a because:

$$\begin{aligned} e(V, y)^c \cdot e(V, g)^{-z_\delta} \cdot e(g, g)^{z_\tau} &= e\left(g^{\frac{\tau}{x+\delta}}, g^x\right)^c \cdot e\left(g^x, g\right)^{-z_\delta} \cdot e(g, g)^{z_\tau} \\ &= e(g, g)^{\frac{c\tau x}{x+\delta}} \cdot e(g, g)^{-z_\delta x} \cdot e(g, g)^{z_\tau} \\ &= e(g, g)^{\frac{c\tau x}{x+\delta} - z_\delta x + z_\tau} \end{aligned}$$

the prover had sent:

$$\begin{aligned} e(V, g)^{-s} \cdot e(g, g)^t &= e\left(g^{\frac{\tau}{x+\delta}}, g\right)^{-s} \cdot e(g, g)^t \\ &= e(g, g)^{\frac{-s\tau}{x+\delta}} \cdot e(g, g)^t \\ &= e(g, g)^{\frac{-s\tau}{x+\delta} + t} \end{aligned}$$

So, if the prover did in fact supply correct z_δ, z_τ, and z_γ after the verifier shared c the two expressions should be equal because the exponent of the verifier's calculation would evaluate to:

$$\begin{aligned} \frac{c\tau x}{x+\delta} - z_\delta x + z_\tau &= \frac{c\tau x - \tau z_\delta + (x+\delta) z_\tau}{x+\delta} \\ &= \frac{c\tau x - \tau(s - \delta c) + (x+\delta)(t - \tau c)}{x+\delta} \\ &= \frac{c\tau x - \tau s + \tau\delta c + t(x+\delta) - \tau c(x+\delta)}{x+\delta} \\ &= \frac{t(x+\delta) - \tau s}{x+\delta} \\ &= \frac{-s\tau}{x+\delta} + t \end{aligned}$$