Proof of Lemma 3.3 Using S-Polynomials

Max Comstock

June 16, 2014

1 Directed Case

Lemma. *The cycle encoding polynomials $F = \{g_1, \ldots, g_k\}$, where*

$$g_i = \begin{cases} x_{v_{k-i}} - \omega^{k-i} x_{v_k} & i = 1, \ldots, k-1, \\ x_{v_k}^k - 1 & i = k \end{cases},$$

are a reduced Gröbner basis for the cycle ideal $H_{G,C}$ with respect to any term order $\prec$ with $x_{v_k} \prec \cdots \prec x_{v_1}$.

Proof. We will show that every combination of g_i satisfies Buchberger's Criterion. First, we will consider arbitrary $n' < k$ and $m' < k$, corresponding to n and m such that $n = k - n'$ and $m = k - m'$. Then we find

$$\begin{aligned} g_{n'} &= x_n - \omega^n x_k \\ g_{m'} &= x_m - \omega^m x_k. \end{aligned}$$

Suppose, without loss of generality, that $n < m$. Taking the S-polynomial, we find

$$\begin{aligned} S(g_{n'}, g_{m'}) &= \frac{x_n x_m}{x_n} g_{n'} - \frac{x_n x_m}{x_m} g_{m'} \\ &= x_m g_{n'} - x_n g_{m'} \\ &= x_m(x_n - \omega^n x_k) - x_n(x_m - \omega^m x_k) \\ &= x_n x_m - \omega^n x_m x_k - (x_n x_m - \omega^m x_n x_k) \\ &= \omega^m x_n x_k - \omega^n x_m x_k. \end{aligned}$$

Using the division algorithm, we find

$$S(g_{n'}, g_{m'}) = \omega^m x_n x_k - \omega^n x_m x_k = \omega^m x_k g_{n'} - \omega^n x_k g_{m'}.$$

The only remaining case is an S-polynomial including g_k. Then we find

$$\begin{aligned} S(g_{n'}, g_k) &= \frac{x_n x_k^k}{x_n} g_{n'} - \frac{x_n x_k^k}{x_k^k} g_k \\ &= x_k^k g_{n'} - x_n g_k \\ &= x_k^k(x_n - \omega^n x_k) - x_n(x_k^k - 1) \\ &= x_n x_k^k - \omega^n x_k^{k+1} - (x_n x_k^k - x_n) \\ &= x_n - \omega^n x_k^{k+1}. \end{aligned}$$

Using the division algorithm here, we find

$$S(g_{n'}, g_k) = x_n - \omega^n x_k^{k+1} = g_{n'} - \omega^n x_k g_k.$$

Hence F is a Gröbner basis for the cycle ideal $H_{G,C}$. The fact that F is a reduced Gröbner basis follows from inspection of F.

2 Undirected Case

Lemma. *The cycle encoding polynomials $F = \{g_1, \dots, g_k\}$, where*

$$g_i = \begin{cases} x_{v_i} + \frac{\omega^{2+i}-\omega^{2-i}}{\omega^3-\omega} x_{v_{k-1}} + \frac{\omega^{1-i}-\omega^{3+i}}{\omega^3-\omega} x_{v_k} & i = 1, \dots, k-2, \\ (x_{v_{k-1}} - \omega x_{v_k})(x_{v_{k-1}} - \omega^{-1} x_{v_k}) & i = k-1 \\ x_{v_k}^k - 1 & i = k \end{cases},$$

are a reduced Gröbner basis for the cycle ideal $H_{G,C}$ with respect to any term order $\prec$ with $x_{v_k} \prec \cdots \prec x_{v_1}$.

Proof. We will use the same method as before to show that the set F satisfies Buchberger's Criterion. We will begin by choosing n and m, where $0 < n < m < k-1$. Then we find

$$g_n = x_n + \frac{\omega^{2+n}-\omega^{2-n}}{\omega^3-\omega} x_{k-1} + \frac{\omega^{1-n}-\omega^{3+n}}{\omega^3-\omega} x_k$$
$$g_m = x_m + \frac{\omega^{2+m}-\omega^{2-m}}{\omega^3-\omega} x_{k-1} + \frac{\omega^{1-m}-\omega^{3+m}}{\omega^3-\omega} x_k.$$

The resulting S-polynomial is

$$\begin{aligned} S(g_n, g_m) &= \frac{x_n x_m}{x_n} g_n - \frac{x_n x_m}{x_m} g_m \\ &= x_m g_n - x_n g_m \\ &= x_m \left(x_n + \frac{\omega^{2+n}-\omega^{2-n}}{\omega^3-\omega} x_{k-1} + \frac{\omega^{1-n}-\omega^{3+n}}{\omega^3-\omega} x_k \right) \\ &\quad - x_n \left(x_m + \frac{\omega^{2+m}-\omega^{2-m}}{\omega^3-\omega} x_{k-1} + \frac{\omega^{1-m}-\omega^{3+m}}{\omega^3-\omega} x_k \right) \\ &= x_n x_m + \frac{\omega^{2+n}-\omega^{2-n}}{\omega^3-\omega} x_m x_{k-1} + \frac{\omega^{1-n}-\omega^{3+n}}{\omega^3-\omega} x_m x_k \\ &\quad - \left(x_n x_m + \frac{\omega^{2+m}-\omega^{2-m}}{\omega^3-\omega} x_n x_{k-1} + \frac{\omega^{1-m}-\omega^{3+m}}{\omega^3-\omega} x_n x_k \right) \\ &= -\frac{\omega^{2+m}-\omega^{2-m}}{\omega^3-\omega} x_n x_{k-1} - \frac{\omega^{1-m}-\omega^{3+m}}{\omega^3-\omega} x_n x_k + \frac{\omega^{2+n}-\omega^{2-n}}{\omega^3-\omega} x_m x_{k-1} + \frac{\omega^{1-n}-\omega^{3+n}}{\omega^3-\omega} x_m x_k. \end{aligned}$$

Using the division algorithm, we find

$$S(g_n, g_m) = -\left(\frac{\omega^{2+m}-\omega^{2-m}}{\omega^3-\omega} x_{k-1} + \frac{\omega^{1-m}-\omega^{3+m}}{\omega^3-\omega} x_k \right) g_n + \left(\frac{\omega^{2+n}-\omega^{2-n}}{\omega^3-\omega} x_{k-1} + \frac{\omega^{1-n}-\omega^{3+n}}{\omega^3-\omega} x_k \right) g_m.$$

Next, we will consider the case where $m = k-1$. Then we have the S-polynomial

$$\begin{aligned} S(g_n, g_{k-1}) &= \frac{x_n x_{k-1}^2}{x_n} g_n - \frac{x_n x_{k-1}^2}{x_{k-1}^2} g_{k-1} \\ &= x_{k-1}^2 g_n - x_n g_{k-1} \\ &= x_{k-1}^2 \left(x_n + \frac{\omega^{2+n}-\omega^{2-n}}{\omega^3-\omega} x_{k-1} + \frac{\omega^{1-n}-\omega^{3+n}}{\omega^3-\omega} x_k \right) - x_n \left(x_{k-1}^2 - (\omega + \omega^{-1}) x_{k-1} x_k + x_k^2 \right) \\ &= x_n x_{k-1}^2 + \frac{\omega^{2+n}-\omega^{2-n}}{\omega^3-\omega} x_{k-1}^3 + \frac{\omega^{1-n}-\omega^{3+n}}{\omega^3-\omega} x_{k-1}^2 x_k \\ &\quad - \left(x_n x_{k-1}^2 - (\omega + \omega^{-1}) x_n x_{k-1} x_k + x_n x_k^2 \right) \\ &= (\omega + \omega^{-1}) x_n x_{k-1} x_k - x_n x_k^2 + \frac{\omega^{2+n}-\omega^{2-n}}{\omega^3-\omega} x_{k-1}^3 + \frac{\omega^{1-n}-\omega^{3+n}}{\omega^3-\omega} x_{k-1}^2 x_k. \end{aligned}$$

Using the division algorithm, we find

$$S(g_n, g_{k-1}) = \left((\omega + \omega^{-1}) x_{k-1} x_k - x_k^2 \right) g_n + \left(\frac{\omega^{2+n}-\omega^{2-n}}{\omega^3-\omega} x_{k-1} + \frac{\omega^{1-n}-\omega^{3+n}}{\omega^3-\omega} x_k \right) g_{k-1}.$$

The next possibility is that $m = k$. Then we find

$$\begin{aligned}
S(g_n, g_k) &= \frac{x_n x_k^k}{x_n} g_n - \frac{x_n x_k^k}{x_k^k} g_k \\
&= x_k^k g_n - x_n g_k \\
&= x_k^k \left(x_n + \frac{\omega^{2+n} - \omega^{2-n}}{\omega^3 - \omega} x_{k-1} + \frac{\omega^{1-n} - \omega^{3+n}}{\omega^3 - \omega} x_k \right) - x_n(x_k^k - 1) \\
&= x_n x_k^k + \frac{\omega^{2+n} - \omega^{2-n}}{\omega^3 - \omega} x_{k-1} x_k^k + \frac{\omega^{1-n} - \omega^{3+n}}{\omega^3 - \omega} x_k^{k+1} - (x_n x_k^k - x_n) \\
&= x_n + \frac{\omega^{2+n} - \omega^{2-n}}{\omega^3 - \omega} x_{k-1} x_k^k + \frac{\omega^{1-n} - \omega^{3+n}}{\omega^3 - \omega} x_k^{k+1}.
\end{aligned}$$

The division algorithm allows us to write

$$S(g_n, g_k) = g_n + \left(\frac{\omega^{2+n} - \omega^{2-n}}{\omega^3 - \omega} x_{k-1} + \frac{\omega^{1-n} - \omega^{3+n}}{\omega^3 - \omega} x_k \right) g_k.$$

The only remaining case is where $n = k - 1$ and $m = k$. This produces the S-polynomial

$$\begin{aligned}
S(g_{k-1}, g_k) &= \frac{x_{k-1}^2 x_k^k}{x_{k-1}^2} g_{k-1} - \frac{x_{k-1}^2 x_k^k}{x_k^k} g_k \\
&= x_k^k g_{k-1} - x_{k-1}^2 g_k \\
&= x_k^k \left(x_{k-1}^2 - (\omega + \omega^{-1}) x_{k-1} x_k + x_k^2 \right) - x_{k-1}^2 (x_k^k - 1) \\
&= x_{k-1}^2 x_k^k - (\omega + \omega^{-1}) x_{k-1} x_k^{k+1} + x_k^{k+2} - (x_{k-1}^2 x_k^k - x_{k-1}^2) \\
&= x_{k-1}^2 - (\omega + \omega^{-1}) x_{k-1} x_k^{k+1} + x_k^{k+2}.
\end{aligned}$$

From the division algorithm, we find

$$S(g_{k-1}, g_k) = g_{k-1} - \left((\omega + \omega^{-1}) x_{k-1} x_k - x_k^2 \right) g_k.$$

Hence F is a Gröbner basis for the cycle ideal $H_{G,C}$. The fact that F is a reduced Gröbner basis follows from inspection of F.