A geometric interpretation of reduction of genus three curves.

J. Estrada Sarlabous
ICIMAF. Acad. Sci. Cuba.
matdis@cidet.icmf.inf.cu

J.-P. Cherdieu
UAG, France.
Jean-Pierre.Cherdieu@univ-ag.fr

R. Blache
UAG, France.
Regis.Blache@univ-ag.fr

The algorithmic aspects related to algebraic curves is an active field of interest in recent years.
Let C be a non hyperelliptic curve of genus three defined over a field k provided with a point $P \in C(k)$ (we assume it exists). In this talk we present an algorithm for the reduction of effective divisors on the Jacobian Variety of C. The algorithms may be geometrically interpreted as the intersection of a suitable projective model of C with low degree curves, resembling the classical reduction algorithm for elliptic curves.
The algorithm may be iterated, in such a way that the output of a loop serves as input for the next one, and all operations involved before the last step are defined in the ring of polynomials in several variables with coefficients in k . Only one factorization of a degree three polynomial with coefficients in k is needed.

:Jacobian Variety, reduction, genus three curves .

Let us denote the number of monomials x^α of total degree m in the homogeneous coordinates $(x_0 : ... : x_n)$ in ^{n} by

$$\vartheta_{n,m} = \binom{m+n}{m}$$

The monomials x^α of total degree m in the homogeneous coordinates $(x_0 : ... : x_n)$ in ^{n} define a one-to-one map

$$\begin{array}{rccc} \Psi_{m,n} : & {}^n & \to & {}^{\vartheta_{n,m}-1} \\ & (x_0 : ... : x_n) & \to & (... : x^\alpha : ...) \end{array}$$

Given a homogeneous polynomial $p_m(x_0 : ... : x_n)$ of degree m, the hypersurface in ^{n} defined as

$$H_m : p_m(x_0 : ... : x_n) = 0$$

is transformed in a hyperplane in the coordinates of $\Psi_{m,n}(x_0 : ... : x_n)$
Let C/k be a curve of genus three defined over a field k provided with a non singular point $P_\infty \in C(k)$ and let be $D = P_1 + ... + P_m$ a divisor on C, $P_i = P_i(x_i : y_i : z_i)$. The Chow form of D is the homogeneous polynomial of degree m in the projective variable $u = (u_x : u_y : u_z)$, defined as

$$Chow(D) = \prod (u_x x_i + u_y y_i + u_z z_i)$$

The $\vartheta_{2,m}$ coefficients of the hyperplane associated to $Chow(d)$ in the coordinates of $\Psi_{2,m}(u)$ are called the Chow coordinates of the divisor D. They are symmetric functions of the projective coordinates $(x_i : y_i : z_i)$ of P_i.
The linear system L_1 of plane conics V with coefficients in k such that

$$< V, C >_\infty \geq P_\infty$$

has dimension 4. Hence, the coefficients of V are linear homogeneous polynomials with coefficients in k, in the projective parameter $(l_0 : l_1 : l_2 : l_3 : l_4)$.
We may identify L_1 with ^{4}. By means of the Veronese map $\Psi_{4,m}(l_0 : ... : l_4)$, the homogeneous polynomials in the coefficients of V of degree m correspond one-to-one to the hyperplanes on $^{\vartheta_{4,m}-1}$.
The linear system L_2 of plane conics W with coefficients in k such that

$$< W, C >_\infty \geq 2P_\infty$$

has dimension 3. Hence, the coefficients of W are linear homogeneous polynomials with coefficients in k, in the projective parameter $(m_0 : m_1 : m_2 : m_3)$.
We may identify L_2 with ^{3}. By means of the Veronese map $\Psi_{3,s}(m_0 : ... : m_3)$, the homogeneous polynomials in the coefficients of W of degree s correspond one-to-one to the hyperplanes on $^{\vartheta_{3,s}-1}$.

Theorem 1 *Given P_1, P_2, P_3, P_4 points in $C(k)$ and assume that there exist a non degenerated conic $V \in L_1$, such that*

$$< V, C >_0 \geq P_1 + P_2 + P_3 + P_4 + P_\infty$$

Then, there exists a conic $W \in L_2$, such that:
1) The coordinates of $\Psi_{3,2}(W)$ are homogeneous polynomials in the Chow coordinates of the divisor $D = P_1 + P_2 + P_3 + P_4 + P_\infty$ and in the coordinates of $\Psi_{4,2}(V)$, with integer coefficients
2) $P_1 + P_2 + P_3 + P_4 - 4P_\infty$ is equivalent to $H_1 + H_2 + H_3 - 3P_\infty$ on $J(C)$ and the Chow coordinates of the divisor $D' = H_1 + H_2 + H_3$ are homogeneous polynomials in the coordinates of $\Psi_{3,2}(W)$, with integer coefficients

Theorem 2 *Given a point $P_5 in C(k)$ and the Chow coordinates of the divisor $D' = H_1 + H_2 + H_3$, if there is a non degenerated conic $W \in L_2$ with $< W, C >_0 \geq H_1 + H_2 + H_3 + 2P_\infty$, then there exists a conic $V' \in L_1$, such that:*
1) $< V', C >_0 \geq H_1 + H_2 + H_3 + P_5 + P_\infty$
2) The coordinates of $\Psi_{4,2}(V')$ are homogeneous polynomials with integer coefficients in the Chow coordinates of the divisor $D' + 2P_\infty$ and in the coordinates of $\Psi_{3,2}(W)$

The algorithm may be iterated, in such a way that the output of a loop serves as input for the next one, and all operations involved before the last step are defined in the ring of polynomials in several variables with coefficients in k . Only one factorization of a degree three polynomial with coefficients in k is needed in the last step, in order to recover the projective coordinates of the points in the support of the reduced divisor from its Chow form .