Hyperelliptic Curves

Rong-Jaye Chen

Department of Computer Science, National Chiao Tung University

ECC 2008
Outline

1. Lemma 39
2. Lemma 40
3. Lemma 41
4. Theorem 42
Lemma 39

- A semi-reduced divisor can be expressed by \((a(u), b(u))\)
  
i.e. \(D = \text{div}(a, b)\)

Lemma 39 (p:17)

\[ D \in D^0 \]
\[ \rightarrow \exists \; D_1 \in D^0 \; , \; D_1 \; \text{is a semi-reduced divisor such that} \; D \sim D_1 \]

Proof:

- Let \(D = \sum_{P \in C} m_P P\)
  
  Let \((C_1, C_2)\) : partition of ordinary points on \(C\), such that
  
  (i) \(P \in C_1\) if and only if \(\tilde{P} \in C_2\)
  
  (ii) \(P \in C_1 \rightarrow m_P \geq m_{\tilde{P}}\)

Let \(C_0\) : set of special points

\[ C = C_0 \cup C_1 \cup C_2 \cup \{\infty\} \]
Proof of Lemma 39

Proof (continue):

\[ D = \sum_{P \in C_1} m_P P + \sum_{P \in C_2} m_P P + \sum_{P \in C_0} m_P P - m\infty \]

Consider

\[ D_1 = D - \sum_{P=(x, y) \in C_2} m_P \text{div}(u - x) - \sum_{P=(x, y) \in C_0} \left\lfloor \frac{m_P}{2} \right\rfloor \text{div}(u - x) \]

Then \( D_1 \sim D \)

\[ D_1 = \sum_{P=(x, y) \in C_1} (m_P - m\bar{P})P + \sum_{P \in C_0} \left( m_P - 2 \left\lfloor \frac{m_P}{2} \right\rfloor \right) P - m_1\infty \]

for some \( m_1 \in \mathbb{Z} \)

and hence \( D_1 \) is a semi-reduced divisor
Lemma 40

Let $P = (x, y)$ be an ordinary point on $C$. Then $R \in \overline{K}(C)$, $R$ does not have a pole at $P$, $\forall k \geq 0$ there exist $c_0, c_1, \ldots, c_k \in \overline{K}$ and $R_k \in \overline{K}(C)$ such that

$$R = \sum_{i=0}^{k} c_i (u - x)^i + (u - x)^{k+1} R_k$$

where $R_k$ does not have a pole at $P$. 
Proof of Lemma 40

Proof:

\( \exists! \ c_0 \in \overline{K} , \ \text{i.e.} \ c_0 = R(x, y) \) , \( P \) is a zero of \( R - c_0 \)

\( \therefore (u - x) \) is a uniformizing parameter for \( P \)

\( \therefore R - c_0 = (u - x)R_1 , \ R_1 \in \overline{K}(C) \) with \( \operatorname{ord}_P(R_1 \geq 0) \).

Hence \( R = c_0 + (u - x)R_1 \)

The Lemma now follows by induction.
Lemma 41

\[ P = (x, y) : \text{ordinary point on } C \]
\[ \rightarrow \exists! b_k(u) \in \overline{K}[u] \text{ such that} \]
\[ (i) \ \deg_u b_k < k \]
\[ (ii) \ b_k(x) = y \]
\[ (iii) \ b_k^2(u) + b_k(u)h(u) \equiv f(u) \pmod{(u - x)^k} \]
Proof of Lemma 41

Proof:

Let

\[ v = \sum_{i=0}^{k-1} c_i(u - x)^i + (u - x)^k R_{k-1} \quad \text{where} \quad c_i \in \overline{K}, \ R_{k-1} \in \overline{K}(C) \]

Define

\[ b_k(u) = \sum_{i=0}^{k-1} c_i(u - x)^i \]

\[ c_0 = y \quad \text{and hence} \quad b_k(x) = y \]

Since \[ v^2 + h(u)v = f(u) \]
\[ \rightarrow b_k(u)^2 + b_k(u)h(u) \equiv f(u) \pmod{(u - x)^k} \]

Uniqueness is easily prove by induction on \( k \)
Theorem 42

Let
\[ D = \sum m_i P_i - (\sum m_i) \infty \quad : \text{semi-reduced}, \]
\[ P_i = (x_i, y_i) \]
Let \( a(u) = \prod (u - x_i)^{m_i} \)
Let \( b(u) \) be the unique polynomial satisfying
(i) \( \deg_u b < \deg_u a \)
(ii) \( b(x_i) = y_i \quad \forall \ i \quad \text{with} \quad m_i \neq 0 \)
(iii) \( a(u) \mid (b(u)^2 + b(u)h(u) - f(u)) \)
Then \( D = \gcd(\text{div}(a(u)), \text{div}(b(u) - v)) \)
Proof of Theorem 42 - (1)

Proof:

Let

\[ C_1 : \text{ordinary points in } supp(D) \]
\[ C_0 : \text{special points in } supp(D) \]

(1) By Lemma 41,
\[ \forall P_i \in C_1 \quad \exists! \ b_i(u) \in \overline{K}[u] \text{ satisfying} \]
(i) \( \deg_u b_i < m_i \)
(ii) \( b_i(x_i) = y_i \)
(iii) \( (u - x)^{m_i} | b_i^2(u) + b_i(u)h(u) - f(u) \)

(2) It can be easily verified that \( \forall P_i \in C_0, b_i(u) = y_i \) is the unique polynomial satisfying
(i) \( \deg_u b_i < 1 \)
(ii) \( b_i(x_i) = y_i \)
(iii) \( (u - x_i) | b_i^2(u) + b_i(u)h(u) - f(u) \)
Proof of Theorem 42 - (2)

Proof (continue):

(3) By CRT for polynomials, \( \exists! b(u) \in \overline{K}[u], \ \deg_u b < \sum m_i \), such that

\[
b(u) \equiv b_i(u) \pmod{(u - x_i)^{m_i}} \quad \forall \ i
\]

It can now be verified that \( b(u) \) satisfies conditions (i), (ii), (iii) of the statement of the theorem.

(4) Now

\[
div(a(u)) = div \left( \prod (u - x_i)^{m_i} \right)
\]

\[
= \sum_{D_i \in C_0} 2P_i + \sum_{P_i \in C_1} m_i P_i + \sum_{P_i \in C_1} m_i \tilde{P}_i - (*)\infty
\]
Proof of Theorem 42 - (3)

Proof (continue):

(5) and

\[
\text{div}(b(u) - v) = \sum_{P_i \in C_0} t_i P_i + \sum_{P_i \in C_1} s_i P_i + \sum_{P_i \in C} m_i P_i - (*)^\infty
\]

where each \( s_i \geq m_i \)

\( \therefore (u - x_i)^m \) divides \( N(b - v) = b^2 + hb - f \)

Now if \( P = (x, y) \in C_0 \) then \( (u - x) \) divides \( b^2 + hb - f \)

\( (b^2 + bh - f)' \mid_{u=x} \neq 0 \)
Proof of Theorem 42 - (4)

Proof (continue):

(5) (Continue):

\[
\begin{align*}
\therefore & \quad 2b(x)b'(x) + b'(x)h(x) + b(x)h'(x) - f'(x) \\
& = b'(x)(2y + h(x)) + (h'(x)y - f'(x)) \\
& = h'(x)y - f'(x) \quad \text{since} \ 2y + h(x) = 0 \neq 0
\end{align*}
\]

Hence \( u = x \) is a simple root of \( N(b - v) = b^2 + bh - f \), and hence \( t_i = 1, \forall i \)

Therefore

\[
div(a(u), b(u) - v) = \sum_{P_i \in C_0} P_i + \sum_{P_i \in C_1} m_i P_i - (*)\infty
\]
Proof of Theorem 42 - (5)

Proof (continue):

(5) (Continue):

Notation:

\[
\gcd(\text{div}(a(u), \text{div}(b(u) - v)))
= \text{div}(a(u), b(u) - v)
= \text{div}(a, b)
\]