Hyperelliptic Curves

Rong-Jaye Chen

Department of Computer Science, National Chiao Tung University

ECC 2008
Outline

- Basic definitions and properties
- Polynomial and rational functions
- Divisors
- HCDLP on $J_C(K)$
- Representing divisors
- Adding reduced divisors
Basic definitions and properties [1/3]

- Def (hyperelliptic curve):
  - Let $\mathbb{K}$ be a field and $\overline{\mathbb{K}}$ be the algebraic closure of $\mathbb{K}$.
  - A hyperelliptic curve $C$ of genus $g$ over $\mathbb{K}$ ($g \geq 1$) is an equation of the form in $\mathbb{K}[x, y]$
    
    $C : y^2 + h(x)y = f(x)$  .................................................................(1)

    where

    - $h(x) \in \mathbb{K}[x]$ is a polynomial of degree at most $g$,
    - $f(x) \in \mathbb{K}[x]$ is a monic polynomial of degree $2g+1$,
    - No solution $(u,v) \in \overline{\mathbb{K}} \times \overline{\mathbb{K}}$ simultaneously satisfies the equation $y^2 + h(x)y = f(x)$ and the partial derivative equations $2y + h(x) = 0$, $h'(x)y - f'(x) = 0$. 
Basic definitions and properties [2/3]

- Def (rational points, point at infinity, finite points)
  - The set of $\overline{K}$-rational points on $C$, denoted $C(\overline{K})$, is the set of all points $(x, y) \in \overline{K} \times \overline{K}$ satisfy the equation (1) of the curve $C$, together with a special point at infinity denoted $\infty$.
  - The set of points $C(\overline{K})$ will simply be denoted by $C$.
  - The points in $C$ other than $\infty$ are called finite points.
Basic definitions and properties [3/3]

- Def (opposite, special and ordinary points)
  - Let $P = (x, y)$ be a finite point on a curve $C$.
  - The opposite of $P$ is the point $\tilde{P} = (x, -y - h(x))$ ($\tilde{P}$ is indeed on $C$).
  - Define $\infty = \infty$.
  - If a finite point $P$ satisfies $P = \tilde{P}$ then the point is said to be special; otherwise, the point is said to be ordinary.
Polynomial and rational functions [1/2]

- Def (coordinate ring, polynomial function)
  - The coordinate ring of $C$ over $\overline{K}$, denoted $\overline{K}[C]$, is the quotient ring
    \[
    \overline{K}[C] = \overline{K}[x, y]/(y^2 + h(x)y - f(x))
    \]
    where $(y^2 + h(x)y - f(x))$ denotes the ideal in $\overline{K}[x, y]$ generated by the polynomial $y^2 + h(x)y - f(x)$.
  - An element of $\overline{K}[C]$ is called a polynomial function on $C$.

- Lemma
  - The polynomial $y^2 + h(x)y - f(x)$ is irreducible over $\overline{K}$, and hence $\overline{K}[C]$ is an integral domain.
Polynomial and rational functions [2/2]

- Def (function field, rational functions)
  - The function field $\overline{K}(C)$ of $C$ over $\overline{K}$ is the field of fractions of $\overline{K}[C]$.
  - The elements of $\overline{K}(C)$ are called rational functions on $C$. 

...
Divisors [1/8]

- Def (divisor, degree, order):
  - A divisor $D$ is a formal sum of points in $C$, $D = \sum_{P \in C} m_P P$, $m_P \in \mathbb{Z}$
  - The degree of $D$, $\deg D = \sum_{P \in C} m_P$
  - The order of $D$ at $P$ is the integer $m_P$, we write $\text{ord}_P(D) = m_P$

- The set of all divisors, denoted $\mathcal{D}$, forms an additive group under the addition rule:
  $$\sum_{P \in C} m_P P + \sum_{P \in C} n_P P = \sum_{P \in C} (m_P + n_P)P$$
  - The set of all divisors of degree 0, denote $\mathcal{D}^0$, is the subgroup of $\mathcal{D}$. 
Divisors [2/8]

- **Def (gcd of divisors):**
  - Let \( D_1 = \sum_{P \in C} m_P P \) and \( D_2 = \sum_{P \in C} n_P P \) be two divisors.

\[
gcd(D_1, D_2) = \sum_{P \in C} \min(m_P, n_P) P - \left( \sum_{P \in C} \min(m_P, n_P) \right)_\infty
\]

- \( \text{Gcd}(D_1, D_2) \in D^0 \)

- **Def (divisor of a rational function):**
  - Let \( R \in K(C)^* \). The divisor of \( R \) is

\[
div(R) = \sum_{P \in C} (\text{ord}_P R) P
\]
Divisors [3/8]

- Example
  - If $P = (x_1, y_1)$ is an ordinary point on $C$, then
    $$\text{div}(x - x_1) = P + \tilde{P} - 2\infty$$
  - If $Q = (x_2, y_2)$ is a special point on $C$, then
    $$\text{div}(x - x_2) = 2Q - 2\infty$$
Divisors [4/8]

- Def (principal divisors, jacobian, support):
  - A divisor $D \in D^0$ is called a principal divisor if $D = \text{div}(R)$ for some rational function $R \in \overline{K(C)}^*$.
  - The set of all principal divisors, denoted $P$, is a subgroup of $D^0$.
  - The quotient group $J = D^0/P$ is called the jacobian of the curve $C$.
  - If $D_1, D_2 \in D^0$ and $D_1 - D_2 \in P$, then $D_1$ and $D_2$ are said to be equivalent divisors; we write $D_1 \sim D_2$.
  - Let $D = \sum_{P \in C} m_P P$ be a divisor. The support of $D$ is the set $\text{supp}(D) = \{P \in C | m_P \neq 0\}$. 

Rong-Jaye Chen

Hyperelliptic Curves

ECC 2008

11 / 29
Divisors [5/8]

- A divisor $D$ is said to be defined over $K$, if
  
  $$D^\sigma = \sum m_P P^\sigma = D$$
  
  for all automorphisms $\sigma$ of $\overline{K}$ over $K$, where
  
  $P^\sigma = (\sigma(x), \sigma(y))$ if $P = (x, y)$, and $\infty^\sigma = \infty$.

- This implies that a divisor defined over $K$ can include
  some points $P_i$ in its support which are not defined over $K$.

- The Jacobian defined over a finite field $K$ is a finite
  abelian group $J_C(K)$. 

Divisors [6/8]

- Def (semi-reduced divisor):
  - A semi-reduced divisor is a divisor of the form \( D = \sum m_i P_i - (\sum m_i) \infty \), where
    - \( m_i \geq 0 \)
    - \( P_i \)'s are finite points s.t. when \( P_i \in \text{supp}(D) \) then \( \tilde{P}_i \not\in \text{supp}(D) \), unless \( P_i = \tilde{P}_i \), in which case \( m_i = 1 \).

- Lemma:
  - For each divisor \( D \in D^0 \) there exists a semi-reduced divisor \( D_1 \in D^0 \) such that \( D \sim D_1 \).
Divisors [7/8]

- **Def (reduced divisor):**
  - Let $D = \Sigma m_i P_i - (\Sigma m_i)\infty$ be a semi-reduced divisor. If $\Sigma m_i \leq g$ (where $g$ is the genus of $C$) then $D$ is called a reduced divisor.
  - The weight of a reduced divisor $D = \text{div}(a, b)$ is the degree of the polynomial $a$.

- **Theorem:**
  - For each divisor $D \in D^0$ there exists a unique reduced divisor $D_1$ such that $D \sim D_1$. 
Divisors [8/8]

- **Theorem:**
  - Let $C$ be a hyperelliptic curve of genus $g$ defined over a finite field $F_q$ with $q$ elements. Then

  \[(\sqrt{q} - 1)^{2g} \leq \# J_C(F_q) \leq (\sqrt{q} + 1)^{2g}\]

  and

  \[|\# C(F_q) - (q + 1)| \leq 2g \sqrt{q}\]

- **Hasse theorem:**

  \[\# E(F_q) = q + 1 - t, \quad |t| \leq 2\sqrt{q}\]
HCDLP on $J_C(K)$ [1/2]

- **HCDLP**: (Hyperelliptic curve discrete logarithm problem)
  - Let a divisor $D_1$ in $J_C(F_q)$ with known order $N$, and $D_2$ in $<D_1>$
  - To find an integer $\lambda$ s.t. $D_2 = \lambda D_1$ is hard.
HCDLP on $J_C(K)$ [2/2]

- A genus 2 hyperelliptic curve over $R$:
  
  \[ C: y^2 = x^5 - 5x^3 + 4x \]

- \[ y = a_3x^3 + a_2x^2 + a_1x + a_0 \]

\[
(P_1 + P_2 - 2\infty) + (P_3 + P_4 - 2\infty) = (P_5 + P_6 - 2\infty)
\]
Representing divisors [1/5]

- **Theorem:**
  - \( D = \sum m_i P_i - (\sum m_i)^\infty \) be a semi-reduced divisor, where \( P_i = (x_i, y_i) \).
  - Let \( a(x) = \Pi (x-x_i)^{m_i} \).
  - Let \( b(x) \) be the unique polynomial satisfying:
    - \( \deg_x b < \deg_x a \)
    - \( b(x_i) = y_i \) for all \( i \) for which \( m_i \neq 0 \).
    - \( a(x) | (b(x)^2 + b(x)h(x) - f(x)) \).
  - Then \( D = \gcd (\text{div}(a(x)), \text{div}(b(x)-y)) \).
  - \( \gcd (\text{div}(a(x)), \text{div}(b(x)-y)) \) will usually abbreviated to \( \text{div}(a(x)), b(x)-y) \) or, more simply, to \( \text{div}(a, b) \).
Representing divisors [2/5]

- Lemma
  - Let $a(x), b(x) \in \overline{K}[x]$ be such that $\deg_x b < \deg_x a$. If $a \mid (b^2 + bh - f)$ then $\text{div}(a, b)$ is semi-reduced.

- The neutral element of $J_C$ is the unique weight zero divisor $\text{div}(1, 0)$
Representing divisors [3/5]

- Genus 2 curve in $\mathbb{F}_3[x, y]$
  
  $C: y^2 = x^5 + 2x^4 + 1$

- $F_{3^2} \cong \mathbb{F}_3[x]/(x^2 + 1) = \{0, 1+i, 2i, 1+2i, 2, 2+2i, i, 2+i, 1\}$

- The $F_{3^2}$ rational points $C_{F_{3^2}}$:
  - $P_1 = (0, 1)$, $P_2 = (1, 2)$, $P_3 = (1, 1)$, $P_4 = (0, 2)$,
  - $P_5 = (2+i, 2+2i)$, $P_6 = (2+2i, 2+i)$, $P_7 = (i, 2+i)$,
  - $P_8 = (2i, 2+2i)$, $P_9 = (i, 1+2i)$, $P_{10} = (2i, 1+i)$,
  - $P_{11} = (2+i, 1+i)$, $P_{12} = (2+2i, 1+2i)$, $\infty$

- $\#J(\mathbb{F}_3) = 17$

- Let $D_1 = \text{div}(x, 1-y) = \text{div}(x, 1)$
Representing divisors [4/5]

- $1D_1 = \text{div}(x, 1) = P_1 - \infty$
- $2D_1 = \text{div}(x^2, 1) = P_1 + P_1 - 2\infty$
- $3D_1 = \text{div}(x^2+2x, 2) = P_2 + P_4 - 2\infty$
- $4D_1 = \text{div}(x+2, 2) = P_2 - \infty$
- $5D_1 = \text{div}(x^2+2x, x+1) = P_1 + P_2 - 2\infty$
- $6D_1 = \text{div}(x^2+2x+2, 2x+1) = P_5 + P_6 - 2\infty$
- $7D_1 = \text{div}(x^2+1, x+2) = P_7 + P_8 - 2\infty$
- $8D_1 = \text{div}(x^2+x+1, x+1) = P_2 + P_2 - 2\infty$
- $9D_1 = \text{div}(x^2+x+1, 2x+2) = P_3 + P_3 - 2\infty$
- $10D_1 = \text{div}(x^2+1, x+1) = P_9 + P_{10} - 2\infty$
Representing divisors [5/5]

- $11D_1 = \text{div}(x^2+2x+2, x+2) = P_{11} + P_{12} - 2\infty$
- $12D_1 = \text{div}(x^2+2x, 2x+2) = P_3 + P_4 - 2\infty$
- $13D_1 = \text{div}(x^2+2, 1) = P_3 - \infty$
- $14D_1 = \text{div}(x^2+2x, 1) = P_1 + P_3 - 2\infty$
- $15D_1 = \text{div}(x^2, 2) = P_4 + P_4 - 2\infty$
- $16D_1 = \text{div}(x, 2) = P_4 - \infty$
- $17D_1 = \text{zero} = \Phi$
Adding reduced divisors [1/7]

- Cantor’s algorithm: (composition)
  - Input: Reduced divisor $D_1 = \text{div}(a_1, b_1)$ and $D_2 = \text{div}(a_2, b_2)$ both defined over $K$.
  - Output: A semi-reduced divisor $D = \text{div}(a, b)$ defined over $K$ such that $D \sim D_1 + D_2$.
    - Find polynomials $d_1, e_1, e_2 \in K[x]$ where $d_1 = \gcd(a_1, a_2) = e_1 a_1 + e_2 a_2$.
    - Find polynomials $d, c_1, c_2 \in K[x]$ where $d = \gcd(d_1, b_1 + b_2 + h) = c_1 d_1 + c_2 (b_1 + b_2 + h)$.
    - Let $s_1 = c_1 e_1$, $s_2 = c_2 e_2$, and $s_3 = c_2$, so that $d = s_1 a_1 + s_2 a_2 + s_3 (b_1 + b_2 + h)$.
    - Set $a = a_1 a_2 / d^2$, and
      \[
      b = \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3 (b_1 b_2 + f)}{d} \mod a
      \]
Adding reduced divisors [2/7]

- Cantor’s algorithm: (reduction)
  - Input: A semi-reduced divisor \( D = \text{div}(a, b) \) defined over \( K \).
  - Output: The (unique) reduced divisor \( D' = \text{div}(a', b') \) such that \( D' \sim D \).
  - Set \( a' = (f - bh - b^2)/a \)
  - \( b' = (-h - b) \mod a' \).
  - If \( \deg_u a > g \) then set \( a \leftarrow a', b \leftarrow b' \) and go to previous step.
  - Let \( c \) be the leading coefficient of \( a' \), and set \( a' \leftarrow c^{-1}a' \).
  - Output \( (a', b') \).
Adding reduced divisors [3/7]

- In previous example, use Cantor’s algorithm to compute

\[ 4D_1 + 5D_1 = \operatorname{div}(x+2, 2) + \operatorname{div}(x^2+2x, x+1) = \operatorname{div}(x^2+x+1, 2x+2) = 9D_1 \]

- \[ d_1 = \gcd(a_1, a_2) = e_1 a_1 + e_2 a_2 \]
  - \[ d_1 = x+2, \quad e_1 = 1, \quad e_2 = 0 \]

- \[ d = \gcd(d_1, b_1 + b_2 + h) = c_1 d_1 + c_2 (b_1 + b_2 + h) \]
  - \[ d = 1, \quad c_1 = 2, \quad c_2 = 1 \]

- \[ s_1 = c_1 e_1, \quad s_2 = c_1 e_2, \quad \text{and} \quad s_3 = c_2 \]
  - \[ s_1 = 2, \quad s_2 = 0, \quad s_3 = 1 \]

- \[ a = a_1 a_2 / d^2 \]
  - \[ a = x^3 + x^2 + x \]

\[ b = \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3 (b_1 b_2 + f)}{d} \mod a \]

\[ = (x^5 + 2x^4 + 2x^2 + 2x + 1) \mod (x^3 + x^2 + x) \]

\[ = x + 1 \]
Adding reduced divisors [4/7]

- \(a' = \frac{f - bh - b^2}{a}\)
  \[= \frac{x^5 + 2x^4 + 2x^2 + x + 1}{x^3 + x^2 + x}\]
  \[= x^2 + x + 1\]

- \(b' = (-h - b) \mod a'\)
  \[= (2x + 2) \mod (x^2 + x + 1)\]
  \[= 2x + 2\]
\( F_{25} = F_2[x]/(x^5+x^2+1) \)

<table>
<thead>
<tr>
<th>n</th>
<th>( \alpha^n )</th>
<th>n</th>
<th>( \alpha^n )</th>
<th>n</th>
<th>( \alpha^n )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>11</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>22</td>
<td>( \alpha^4 + \alpha^2 + 1 )</td>
</tr>
<tr>
<td>1</td>
<td>( \alpha )</td>
<td>12</td>
<td>( \alpha^3 + \alpha^2 + \alpha )</td>
<td>23</td>
<td>( \alpha^3 + \alpha^2 + \alpha + 1 )</td>
</tr>
<tr>
<td>2</td>
<td>( \alpha^2 )</td>
<td>13</td>
<td>( \alpha^4 + \alpha^3 + \alpha^2 )</td>
<td>24</td>
<td>( \alpha^4 + \alpha^3 + \alpha^2 + \alpha )</td>
</tr>
<tr>
<td>3</td>
<td>( \alpha^3 )</td>
<td>14</td>
<td>( \alpha^4 + \alpha^3 + \alpha^2 + 1 )</td>
<td>25</td>
<td>( \alpha^4 + \alpha^3 + 1 )</td>
</tr>
<tr>
<td>4</td>
<td>( \alpha^4 )</td>
<td>15</td>
<td>( \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 )</td>
<td>26</td>
<td>( \alpha^4 + \alpha^2 + \alpha + 1 )</td>
</tr>
<tr>
<td>5</td>
<td>( \alpha^2 + 1 )</td>
<td>16</td>
<td>( \alpha^4 + \alpha^3 + \alpha + 1 )</td>
<td>27</td>
<td>( \alpha^3 + \alpha + 1 )</td>
</tr>
<tr>
<td>6</td>
<td>( \alpha^3 + \alpha )</td>
<td>17</td>
<td>( \alpha^4 + \alpha + 1 )</td>
<td>28</td>
<td>( \alpha^4 + \alpha^2 + \alpha )</td>
</tr>
<tr>
<td>7</td>
<td>( \alpha^4 + \alpha^2 )</td>
<td>18</td>
<td>( \alpha + 1 )</td>
<td>29</td>
<td>( \alpha^3 + 1 )</td>
</tr>
<tr>
<td>8</td>
<td>( \alpha^3 + \alpha^2 + 1 )</td>
<td>19</td>
<td>( \alpha^2 + \alpha )</td>
<td>30</td>
<td>( \alpha^4 + \alpha )</td>
</tr>
<tr>
<td>9</td>
<td>( \alpha^4 + \alpha^3 + \alpha )</td>
<td>20</td>
<td>( \alpha^3 + \alpha^2 )</td>
<td>31</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>( \alpha^4 + 1 )</td>
<td>21</td>
<td>( \alpha^4 + \alpha^3 )</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Adding reduced divisors [5/7]

- Example 2:
  Consider the hyperelliptic curve $C$: $y^2 + (x^2 + x)y = x^5 + x^3 + 1$ of genus 2 over the finite field $F_{2^5}$. $P = (\alpha^{30}, 0)$ is an ordinary point in $C(F_{2^5})$ and the opposite of $P$ is $\tilde{P} = (\alpha^{30}, \alpha^{16})$. $Q_1 = (0, 1)$ and $Q_2 = (1, 1)$ are special points in $C(F_{2^5})$.

- Let $D_1 = P + Q_1 - 2\infty = \text{div}(a_1, b_1)$ where $a_1 = x(x + \alpha^{30})$, $b_1 = \alpha x + 1$.
  
  $D_2 = \tilde{P} + Q_2 - 2\infty = \text{div}(a_2, b_2)$ where $a_2 = (x + 1)(x + \alpha^{30})$, $b_2 = \alpha^{23} x + \alpha^{12}$.

- $d_1 = \gcd(a_1, a_2) = x + \alpha^{30}$; $d_1 = a_1 + a_2$.

- $d_2 = \gcd(d_1, b_1 + b_2 + h) = x + \alpha^{30}$; $d = 1 \cdot d_1 + 0 \cdot (b_1 + b_2 + h)$
Adding reduced divisors [6/7]

- \( d = a_1 + a_2 + 0 \cdot (b_1 + b_2 + h) \).
- Set \( a = a_1 a_2 / d^2 = x(x+1) = x^2 + x \),

\[
\begin{align*}
  b &= \frac{1 \cdot a_1 b_2 + 1 \cdot a_2 b_1 + 0 \cdot (b_1 b_2 + f)}{d} \mod a \\
  &\equiv 1 \pmod{a}.
\end{align*}
\]

- Check:

\[
\begin{align*}
  \text{div}(a) &= 2Q_1 + 2Q_2 - 4\infty \\
  \text{div}(b - y) &= Q_1 + Q_2 + \sum_{i=1}^{3} P_i - 5\infty, \text{ where } P_i \neq Q_1, Q_2 \\
  \text{div}(a, b) &= Q_1 + Q_2 - 2\infty
\end{align*}
\]
Adding reduced divisors [7/7]

- Example:
Consider the semi-reduced divisor
\[ D = (0,1) + (1,1) + (\alpha^5, \alpha^{15}) - 3\infty = \text{div}(a,b), \]
where

\[ a(x) = x(x+1)(x+\alpha^5) = x^3 + \alpha^2 x^2 + \alpha^5 x \]
\[ b(x) = \alpha^{17} x^2 + \alpha^{17} x + 1 \]

Reduction algorithm yields

\[ a'(x) = x^2 + \alpha^{15} x + \alpha^{26} \]
\[ b'(x) = \alpha^{23} x + \alpha^{21} \]

Hence \[ D \sim \text{div}(a', b') = (\alpha^{28}, \alpha^7) + (\alpha^{29}, 0) - 2\infty \]