Riemann-Roch and algebraic geometry codes

1 Riemann-Roch: statement

Theorem 1.1 [Riemann] *Let D be a divisor on a nonsingular projective curve X of genus g. Then*
$$l(D) \geq \deg(D) + 1 - g.$$

Theorem 1.2 [Roch] *In fact,*
$$l(D) - l(W - D) = \deg(D) + 1 - g$$
where W is a canonical divisor of X.

This theorem says something about the dimensions $l(D)$ of linear spaces $L(D)$ associated with the curve X. All required definitions follow.

2 Divisors

A *divisor* on a smooth (i.e., nonsingular) projective curve X is a formal sum of points:
$$D = \sum n_P P$$
where $P \in X$, $n_P \in \mathbf{Z}$, only finitely many nonzero.

The *degree* of the divisor D is
$$\deg D = \sum n_P.$$

Clearly, divisors form an Abelian group under addition, and deg is a homomorphism from this group to $\mathbf{Z}$.

(If k is not algebraically closed, one uses sums of *closed points*, where a closed point is a minimal 0-dimensional subvariety defined over k, that is, the orbit of a point defined over $\bar{k}$ under the Galois group.)

(If X is not necessarily a curve, a divisor is a formal sum of subvarieties of codimension 1.)

One writes
$$D \geq 0$$
if $n_P \geq 0$ for all P.

3 Principal divisors

Given $f \in k(X)$, $f \neq 0$, the *principal divisor* (f) is defined by

$$(f) = \sum v_P(f)P$$

where $v_P(f) = \#\text{zeros} - \#\text{poles of } f \text{ at } P$.

Now $\deg(f) = 0$.

The principal divisors form a subgroup of the group of divisors: $(f)+(g) = (fg)$. The *Picard group* (or *divisor class group*) is the quotient group

$$\mathrm{Pic}(X) = \{\text{divisors}\}/\{\text{principal divisors}\}.$$

4 The spaces $L(D)$

Given a divisor D on a curve X, define

$$L(D) = \{0\} \cup \{f \in k(X), f \neq 0 \mid (f) + D \geq 0\}.$$

These spaces are finite-dimensional. Let $l(D) = \dim_k L(D)$.

Now we can read the statement of Riemann's theorem. It says that the dimension of the space $L(D)$ is at least $1 - g + \sum n_P$, where $L(D)$ is the space of of rational functions f on X where if $n_P < 0$ the function f is required to have a zero of multiplicity at least $-n_P$ at P, and if $n_P = 0$ the function f must be regular at P (that is, have no pole there), and if $n_P > 0$ the function f is allowed to have an n_P-fold pole at P.

5 Canonical divisors

Let ω be a rational differential form. Then $W = (\omega) = \sum v_P(\omega)P$ is called a canonical divisor. Here $v_P(\omega) = \#\text{zeros} - \#\text{poles of } \omega \text{ at } P$, where by definition $v_P(\omega) = v_P(f)$ if $\omega = f dt$ locally at P.

Any two canonical divisors differ by a principal divisor.

6 Genus

We have $g = l(W) = \dim_k L(W)$.

Indeed, $L(W) = \{f \mid (f) + (\omega) \geq 0\} = \{f \mid f\omega \text{ is a regular diff. form}\}$, so $l(W) = \dim_k L(W) = \dim_k \Omega[X] = g$.

7 Corollaries

We saw that when g is defined as $\dim_k \Omega[X]$ then $g = l(W)$. But when g is defined by the statement of Riemann-Roch, $l(D) - l(W - D) = \deg(D) + 1 - g$, then the same conclusion holds.

Corollary 7.1 $l(W) = g$.

Proof Pick $D = 0$ and use $l(0) = 1$. $\square$

Corollary 7.2 $\deg(W) = 2g - 2$.

Proof Pick $D = W$. $\square$

Corollary 7.3 *If* $\deg(D) > 2g - 2$ *then* $l(D) = \deg(D) + 1 - g$.

Proof If $\deg(D) < 0$ then $l(D) = 0$. $\square$

8 Algebraic Geometry Codes

Pick a divisor D, say with $2g - 1 < \deg D < n$, and let P_1, ..., P_n be points outside the support of D.

Make a code

$$C = \{(f(P_1), ..., f(P_n)) \mid f \in L(D)\}.$$

Theorem 8.1 *The code C has word length n, dimension $k = l(D) = \deg(D) + 1 - g$ and minimum distance $d \geq n - \deg(D)$.*

Proof That C has word length n is clear. The statement about the dimension was a corollory above. If C has minimum distance d, then there is a function f such that $f \in L(D')$ where $D' = D - \sum_{f(P_i)=0} P_i$, with $\deg(D') = \deg(D) - (n - d) \geq 0$. $\square$

This means that if g is small we get reasonably good codes: the Singleton bound says $k + d \leq n + 1$ and the codes constructed here have $k + d \geq n + 1 - g$.