Algebraic Geometry for Theoretical Computer Science

Assignment 8

Lecturer: Gil Cohen *Hand in date: January 1, 2015*

Instructions: Please write your solutions in LaTeX / Word or exquisite handwriting. Submission can be done individually or in pairs.

The AG codes introduced in class can only yield meaningful results when the field size is larger than 4. In this assignment we will construct codes from algebraic function fields in a different way than was used by Goppa. This will give us a chance to practice working with divisors and Riemann-Roch spaces while obtaining codes even for the binary field.

Let $F/\mathbb{F}_q$ be an algebraic function field with genus g. let $G_1, \dots, G_r$ be effective divisors of F with pairwise disjoint supports, where $\deg(G_i) = d_i$. Let $n = \sum_{i=1}^r d_i$. This will be the length of the code. Let E be an effective divisor with a support that does not intersect any of the supports of the G_i's. Let D be any divisor with $\deg(D) \geq 2g - 1$. Assume further that $1 \leq m \leq n - g$, where $m = \deg(E - D)$.

1. Prove that $\ell(D + G_i) = \ell(D) + d_i$ for all $i \in [r]$.

For each $i \in [r]$, let

$$\{f_{i,j} + \mathcal{L}(D) \ \mid \ 1 \leq j \leq d_i\}$$

be an $\mathbb{F}_q$-basis for the quotient space $\mathcal{L}(D + G_i)/\mathcal{L}(D)$.

2. Prove that $\{f_{i,j} + \mathcal{L}(D) \ \mid \ 1 \leq i \leq r,\ 1 \leq j \leq d_i\}$ is an $\mathbb{F}_q$-basis for the n-dimensional quotient space $\mathcal{L}(D + \sum_{i=1}^r G_i)/\mathcal{L}(D)$. To this end, show that if $h_1, \dots, h_r$ are such that $h_i \in \mathcal{L}(D + G_i)$ for all $i \in [r]$ and $h_1 + \cdots + h_r \in \mathcal{L}(D)$, then it holds that $h_i \in \mathcal{L}(D)$ for all $i \in [r]$.

By the above item, it follows that every

$$f \in \mathcal{L}\left(D + \sum_{i=1}^r G_i - E\right) \subseteq \mathcal{L}\left(D + \sum_{i=1}^r G_i\right)$$

has a unique representation

$$f = \sum_{i=1}^r \sum_{j=1}^{d_i} c_{i,j} f_{i,j} + u,$$

with $c_{i,j} \in \mathbb{F}_q$ and $u \in \mathcal{L}(D)$. With this, we define the code to be the image of the $\mathbb{F}_q$-linear map

$$C\colon \mathcal{L}\left(D + \sum_{i=1}^r G_i - E\right) \to \mathbb{F}_q^n$$

given by

$$C(f) = (c_{1,1}, \ldots, c_{1,d_1}, \ldots, c_{r,1}, \ldots, c_{r,d_r}) .$$

Let

$$\Delta = \min_{R \subseteq [r]} \left(|R| \;\middle|\; \sum_{i \in R} d_i \geq m \right) .$$

3. Prove that the code C above is an $[n, k, d]_q$-linear code with dimension $k \geq n - m - g + 1$ and distance $d \geq \Delta$. *Guidance: given $f \in \mathcal{L}\left(D + \sum_{i=1}^{r} G_i - E\right)$, consider the subset $R \subseteq [r]$ such that $i \in R$ if and only if $c_{i,j} \neq 0$ for some $j \in [d_i]$.*

We now illustrate the power of this general construction of codes, by constructing a specific code over the binary field. To this end, consider the rational function field $\mathbb{F}_2(x)/\mathbb{F}_2$.

4. Please specify 3 rational places of this function field, a degree 2 place, two degree 3 places, and one place of degree 7 (for the latter you can use the fact that $x^7 + x + 1$ is irreducible over $\mathbb{F}_2$).

We denote the first six places you wrote down as an answer to the above item by $P_1, \ldots, P_6$, and the latter, degree 7 place, by E. Furthermore, for $i \in [6]$, let G_i denote the principal divisor P_i. Finally, we take D to be the zero divisor (why does this choice of D satisfy the hypothesis of the general construction described above?).

5. What are the parameters of the code resulted by these choices of $G_1, \ldots, G_6, D$ and E?

6. Write down a basis for $\mathcal{L}(G_1 + \cdots + G_6 - E)$. Don't use a computer – be brave.

7. Write down the generating matrix for C. Again, don't use a computer.