# Lecture 10

# AG Codes II

In the last lecture we saw how to construct AG codes defined as evaluation of bivariate polynomials on a curve in the plane $\mathbb{F}_q^2$. The block length of such codes does not exceed $q^2$, so for constructing longer codes, we need to generalize the construction. This is going to be the topic of this lecture.

## 10.1. Irreducible Curves and Bézout's Theorem

For what follows, the following informal definition of a curve is sufficient: a curve in $\mathbb{F}_q^m$ is the common zeroset of $m-1$ nonconstant polynomials $f_1(x_1,x_2), f_2(x_2,x_3), \ldots, f_{m-1}(x_{m-1},x_m) \in \mathbb{F}_q[x_1,\ldots,x_m]$. The *degree* of this curve is defined as the product of the total degrees of $f_1, f_2, \ldots, f_{m-1}$. The curve is called *irreducible* if all the $f_i$ are irreducible polynomials.

Crucial for the construction of AG codes in this more general setting is the following theorem of Bézout:

**Theorem 10.1** (Bézout's Theorem)**.** *Suppose that the curve given by*

$$\begin{aligned} f_1(x_1,x_2) &= 0 \\ f_2(x_2,x_3) &= 0 \\ \vdots &\quad \vdots \\ f_{t-1}(x_{t-1},x_t) &= 0 \end{aligned}$$

*is irreducible, and that $g \in \mathbb{F}_q[x_1,\ldots,x_t]$ is a polynomial that cannot be expressed in the form $h_1f_1+\cdots+h_{t-1}f_{t-1}$ for $h_1,\ldots,h_{t-1} \in \mathbb{F}_q[x_1,\ldots,x_t]$. Then the number of intersection points of the zeroset of $g$ and the curve is at most* $\deg(g)\deg(f_1)\cdots\deg(f_{t-1})$.

A proof of a more general version of this theorem can be found, e.g., in Chapter 1 of "Algebraic Geometry" by Hartshorne, or in Chapter 8 of "Algebraic Complexity Theory" by Bürgisser et al.

It remains to be show how to test whether a polynomial $g \in \mathbb{F}_q[x_1,\ldots,x_m]$ has the property that it cannot be expressed in the form $h_1f_1+\cdots+h_{m-1}f_{m-1}$ for $h_1,\ldots,h_{m-1} \in \mathbb{F}_q[x_1,\ldots,x_m]$. As in the last section, we can assume w.l.o.g. that each $f_i$ is of the form $ax_{i+1}^{d_{i+1}}+h_i$, wherein $\deg_{x_{i+1}}(h_i) < d_{i+1}$, and $d_{i+1}$ is the total degree of $f_i$. Consider the vector space

$$\Gamma := \bigoplus_{i_2=0}^{d_2-1}\bigoplus_{i_3=0}^{d_3-1}\cdots\bigoplus_{i_t=0}^{d_t-1}\mathbb{F}_q[x_1]x_2^{i_2}\cdots x_t^{i_t}.$$

If $g \in \Gamma$ and it is nonzero, then it cannot be represented as $h_1f_1+\cdots h_{t-1}f_{t-1}$, since the local degrees of $g$ in $x_2,\ldots,x_t$ is smaller than the maximum of the local degrees of the $f_j$ in these variables. Moreover, any $g \in \mathbb{F}_q[x_1,\ldots,x_t]$ has the property that there exist $h_1,\ldots,h_{t-1}$ such that $g+h_1f_1+\cdots+h_{t-1}f_{t-1} \in \Gamma$.

---

Lecture and scribes by Amin Shokrollahi

For $m > (t-1)q$, let

$$\Gamma_{<m} := \bigoplus_{i_2=0}^{d_2-1} \bigoplus_{i_3=0}^{d_3-1} \cdots \bigoplus_{i_t=0}^{d_t-1} \mathbb{F}_q[x_1]_{m-(i_2+\cdots+i_t)} x_2^{i_2} \cdots x_t^{i_t}.$$

Then any nonzero $g \in \Gamma_{<m}$ satisfies the property of Bézout's Theorem. Moreover, the dimension of $\Gamma_{<m}$ is

$$\sum_{i_2=0}^{d_2-1} \cdots \sum_{i_t=0}^{d_t-1} m - (i_2 + \cdots + i_t) = (m-1)D - D\frac{d_2 + \cdots + d_t - t - 1}{2},$$

where $D = d_2 \cdots d_t$.

Suppose now that $g \in \Gamma_{<m}$, that $X$ has $n$ points, and that $d_2 \cdots d_t(m-1) < n$, and consider the evaluation code via $(\Gamma_{<m}, X; \mathbb{F}_q)$. By Bézout's theorem, we obtain a code with parameters

$$\left[ n, (m-1)D - D\frac{\sum_2^t d_t - t - 1}{2}, n - (m-1)D \right]_q. \tag{10.1}$$

## 10.2. Example: Hermitian Towers

Consider the curve $X$ in $\mathbb{F}_{q^2}^3$ given by

$$\begin{aligned} y^{q+1} &= x^q - x \\ x^{q+1} &= z^q - z. \end{aligned}$$

The number of points of this curve, i.e., the number of $(x, y, z) \in \mathbb{F}_{q^2}^3$ satisfying the above equations, is $q^4$: For each of the $q^2$ possible values for $y$, there are $q$ values for $x$, and for each of these $x$-values there are $q$ values for $z$. Each of the equations in the curve is irreducible (by Eisenstein's Criterion) and hence the curve is irreducible. Applying the machinery of the last section with $d_2 = d_3 = q+1$, we obtain a code with parameters

$$\left[q^4, (q+1)^2 (m-q), q^4 - (q+1)^2(m-1)\right]_{q^2}.$$

In general, let us look at the Hermitian tower

$$\begin{aligned} x_2^{q+1} &= x_1^q - x_1 \\ x_3^{q+1} &= x_2^q - x_2 \\ &\vdots \quad\quad \vdots \\ x_t^{q+1} &= x_{t-1}^q - x_{t-1}. \end{aligned}$$

This tower defines a set $X$ of $q^{t+1}$ points in $\mathbb{F}_{q^2}^t$. The curve is irreducible, since at every step the polynomial used is irreducible (use Eisenstein's Criterion). If $m > (t-1)q$ and $(m-1)(q+1)^{t-1} < q^{t+1}$, we obtain a code with parameters

$$\left[q^{t+1}, (q+1)^{t-1}\left(m - q\frac{t-1}{2}\right), q^{t+1} - (m-1)(q+1)^{t-1}\right]_{q^2}.$$

Asymptotically, when we let $t$ go to infinity, we obtain codes for which the relative minimum distance $\delta$ and the rate $R$ satisfy the following relation

$$\begin{aligned} \delta + R &\geq 1 - \frac{(q+1)^{t-1}}{q^{t+1}}\left(\frac{q(t-1)}{2} - 1\right) \\ &= 1 - \left(1 + \frac{1}{q}\right)^{t-1} \frac{1}{q^2}\left(\frac{q(t-1)}{2} - 1\right). \end{aligned}$$

Unfortunately, the right hand side of the above inequality converges to $-\infty$, so that we do not get obtain asymptotically good codes (or at least, we cannot prove that we do).

**Figure 10.1**: Construction of codes beyond the GV bound. The line corresponds to the equation $x + y = 1 - \gamma_q$, and the curve corresponds to the GV bound.

## 10.3. Codes Beyond the GV-Bound

Fundamentally, a construction like the one described above is not sufficient to find asymptotically good codes, though it is a first step in this direction. Let us see, why: Suppose that for any of the $qx$ possibilities for $x_1$, we can find $d_2$ possibilities for $x_2$, $d_3$ possibilities for $x_3$, and finally $d_t$ possibilities for $x_t$. Altogether, this would give rise to $qd_1d_2 \cdots d_t$ points, i.e., in 10.1, we have $n \leq qd_1d_2 \cdots d_t$. Referring to (10.1), let

$$g := \frac{d_2 + \cdots + d_t - t - 1}{2}.$$

Then, we obtain a code with parameters $[qD, (m-1)D - gD, qD - (m-1)D]_q$. Asymptotically, this gives a code for which the rate $R$ and the relative distance $\delta$ satisfy $R + \delta \geq 1 - g/q$. But, $g$ goes to infinity as the tower grows, so this does not give asymptotically good codes.

The presentation we have given here is a very restricted view of AG codes. In fact, the actual construction of such codes uses a different approach for which we would have to develop some parts of the language of algebraic geometry, which we are not going to do here.

Given a curve $X$ defined over $\mathbb{F}_q$, we can associate to $X$ an invariant, called the (geometric) *genus* of the curve. In the case of a plane algebraic curve with no singularities defined by a bivariate polynomial of degree $d$, this quantity is simply $(d-1)(d-2)/2$, a number we encountered in the last lecture.

We can introduce the notion of irreducibility of a curve: for a curve defined by polynomial equations in many variables, irreducibility coincides with the notion of the ideal generated by the polynomials to be prime. Moreover, we can associate with arbitrarily defined irreducible curves an analogue of the vector space $\Gamma_{<m}$, and the notion of *degree*. The dimension of $\Gamma_{<m}$, the degree $d$, and the genus $g$ of nonsingular curves are intimately related: if $m$ is large enough, then the dimension of $\Gamma_{<m}$ is $(m-1)d - g + 1$. This is often called the *Theorem of Riemann*. Putting things together, this would give us a code with parameters

$$[n, (m-1)d - g + 1, n - (m-1)d]_q,$$

where $n$ is the number of points of the curve over $\mathbb{F}_q$. The rate and the relative distance of the code satisfy

$$R + \delta \geq 1 - \frac{g-1}{n}.$$

Let us define $\gamma_q$ as the lower limit, taken over all curves for which the number of points goes to infinity, of the quantity $g/n$. Then we know that, asymptotically, the points $(R, \delta)$ with $R + \delta = 1 - \gamma_q$ are achievable in the sense that there are sequences of codes of rate $R$ and relative distance at least $\delta$ for which the block length goes to infinity. If the point $(R, \delta)$ lies above the GV bound, then we have shown the existence of codes beyond the GV bound. (Technically, we need also to show that the rate $R$ is achievable for the code, since for the codes we have built the dimension is of the form $(m-1)d - g + 1$, but if $d = o(g)$, then this is will be OK.)

When does the line $1 - \gamma_q - x$ intersect the GV curve

$$f(x) = 1 - x\log_q(q-1) + x\log_q(x) + (1-x)\log_q(1-x)?$$

For this, we calculate the derivative of $f(x)$ which is

$$f'(x) = \log_q\left(\frac{x}{1-x}\right) - \log_q(q-1).$$

This value is $-1$ if $x = x_0 = (q-1)/(2q-1)$. The equation of the tangent line to the GV bound at $x_0$ is

$$x + y = x_0 + f(x_0).$$

It turns out that if $1 - \gamma_q > x_0 + f(x_0)$, then we obtain codes beyond the GV bound.

Tsfasman, Vladut, and Zink were the first to show that if $q$ is a square, then $\gamma_q \leq \frac{1}{\sqrt{q}-1}$. They used a special class of curves, called "modular curves" to show this result. Using this result, they showed that if $q$ is a square and

$$x_0 + f(x_0) \leq 1 - \frac{1}{\sqrt{q}-1},$$

then their codes are above the GV bound. The situation is depicted in Figure 10.1: Between the intersection points of the line $x + y = 1 - \gamma_q$ and the GV bound we obtain codes that are genuinely above the GV bound. Solving the above equation, it turns out that $q$ has to be larger than or equal to $49$.

**Theorem 10.2** (Tsfasman, Vladut, and Zink)**.** *If $q$ is a square larger than or equal to $49$, then one can construct AG codes over $\mathbb{F}_q$ that are beyond the GV bound.*

Later, Drinfeld and Vladut showed that $\gamma_q \geq \frac{1}{\sqrt{q}-1}$, thereby showing the optimality of the curves constructed by Tsfasman et al.

A description of codes derived from such curves has been vastly simplified by Garcia and Stichtenoth. They have provided an explicit tower of "function fields" and calculated the genus and and the number of points explicitly. The tower is given by

$$\begin{array}{rcl} z_2^q + z_2 & = & x_1^{q+1} \\ z_3^q + z_3 & = & x_2^{q+1} \\ \vdots & & \vdots \end{array}$$

where at each step, $x_n = z_n / x_{n-1}$.