# BACHELOR PROJECT: AG CODES

PROPOSED BY: YAJNASENI DUTTA

Many results in this field hinge on the fundamental theorem of algebra: a polynomial of degree $d$ has at most $d$ roots.

**Prerequisite.** This project follows naturally from the algebraic curves course as the first step to the thesis will be to understand the Riemann–Roch theorem for curves. We will work with several explicit equations of curves, so some knowledge of computational algebra systems will be helpful (though I will not be able to help much there).

**Overview.** Suppose we want to send a message of length $k$; say $k$ points lying on some curve of genus $g$ over a finite field $\mathbb{F}_q$. We pick $n - k$ more rational points (i.e., $\mathbb{F}_q$-zeroes of the defining equations)so that all in all we have $n$-points, $p_1, \ldots, p_n$ on the curve, where $n > k$. If the channel through which we send the message is noisy, it will distort some of these $n$ points, but hopefully not too many so that the original $k$ is easily retrievable.

We pick another set $G$ of points, apart form the $n$ we already chose, and consider the space of all functions $f$ that vanish along these points with certain specified multiplicity. Instead of sending the message directly, we evaluate this function at our $n$ code points and create a codeword $c = (f(p_1), \ldots, f(p_n))$.

For different choices of $f$, the difference between these codewords can also be bound (asymptotically) via Riemann–Roch theorem. After receiving a corrupted message, the receiver looks for the unique function $f$ whose values at the points $p_i$ most closely match the received data. The receiver can then reconstruct the original curve from these received codewords.

**Goals.** After revising basics of finite fields, and the Riemann–Roch theorem, the main goal will be to understand how to most efficiently choose $n$ and the functions $f$, i.e. the TVZ theorem from 1982. We will follow Chapter 2,3 of these notes, as well as the textbook `https://link.springer.com/book/10.1007/978-3-0348-9286-5` by van Lint and van der Geer.