Fields and Polynomials

Emil Straschil

ETH Zurich

2026

Remember Rings

A ring was an algebra $\langle R; +, -, 0, *, 1 \rangle$ where:

- $\langle R; +, -, 0 \rangle$ is a commutative group
- $\langle R; *, 1 \rangle$ is a monoid
- the distributive laws hold

If $ab = ba$ then the ring is called *commutative*.

Units

Unit

A **unit** is a ring element u which is invertible. So there is u^{-1} with $u * u^{-1} = u^{-1} * u = 1$

The set of units in R is denoted by R^*. R^* is a (multiplicative) group.

Integral Domains

Zerodivisor

A element $a \in R$ (where R is a commutative Ring) is called **zerodivisor** if $ab = 0$ for some $b \in R$ with $b \neq 0$.

Integral Domain

An **integral domain** is a (nontrivial) commutative ring without zerodivisors.

In an integral domain, if $ab = 0$ then either $a = 0$ or $b = 0$

Example: $\mathbb{Z}$ is an integral domain. But $\mathbb{Z}_6$ is not, since $3 * 2 = 0$.

Fields

Field

A **field** is a (nontrivial) *commutative* ring F in which every nonzero element is a unit.

In words: A field is commutative ring in which every element has an inverse (except 0).

Example: $\mathbb{Z}$ is not a field, since (for example) 3 has no inverse. $\mathbb{Q}$ is a field, since for any $a \in \mathbb{Q}$ with $a \neq 0$ we have $a^{-1} = \frac{1}{a}$

A field is an integral domain.

Notation

We denote a field with p elements with $GF(p)$. You can think of $GF(p)$ as $\mathbb{Z}_p$ for p prime. Note that $\mathbb{Z}_m$ is only a field if m is prime.

Polynomials over Rings

Polynomial

A polynomial $a(x)$ over a commutative ring R is:

$$a(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{d} a_i x^i$$

Degree

We call the greatest i with $a_i \neq 0$ the *degree* of $a(x)$.

$R[x]$ now denotes the set of all polynomials in x over R.

Polynomials over Rings

We can add and multiply polynomials as usual. For example, take the following calculations on polynomials over $\mathbb{Z}_5$:

$$(x^2 + 4x + 1) + (x + 7) = x^2 + 3$$

or

$$(x + 1)(x + 2) = x^2 + 3x + 2$$

Note that when multiplying polynomials a and b with $deg(a) = \alpha$ and $deg(b) = \beta$ then $deg(a * b) \leq \alpha + \beta$.

Polynomial Rings

Polynomial Rings

For any commutative ring R, $R[x]$ is a commutative ring.

Polynomials over Fields

Monic Polynomials

A polynomial is called **monic** if the leading coefficent is 1.

Example: $x^2 + 1$ is monic, but $2x^2 + 1$ is not.

Irreducible Polynomials

A polynomial $a(x) \in F[x]$ is called **irreducible** if it has degree at least 1 and is divisible only by constant polynomials and constant multiples of $a(x)$.

Note that constant polynomials are the elements of F and a constant multiple of $a(x)$ is $c * a(x)$ for $c \in F$.

Example: In $GF(2)[x]$, the polynomial $x^2 + 1$ is reducible since $(x + 1)(x + 1) = x^2 + 1$.

Division

Theorem 5.25

Let F be a field. For any $a(x)$ and $b(x) \neq 0$ inf $F[x]$ there are *unique* $q(x)$ and $r(x)$ with:

$$a(x) = b(x) * q(x) + r(x)$$

and $deg(r(x))deg(b(x))$

We can calculate those remainders using polynomial division.

Evaluating Polynomials

When working with polyonials it is useful to simply treat them as a vector. But we can also evaluate them (as we know from school).

Example: Consider $a(x) = x^2 + x + 2$ in $\mathbb{Z}_3$.
Then $a(1) = 1$ and $a(2) = 2$.

Roots

Roots

For a polymial $a(x) \in R[x]$ an element $\alpha \in R$ with $a(\alpha) = 0$ is called a **root** of $a(x)$.

Useful Fact

For a field F and $a(x) \in F[x]$, $\alpha \in F$ is a root of $a(x)$ if and only if $x - a$ divides $a(x)$.

This means that we can check irreducibiliy of a polynomial $a(x)$ with $deg(a(x)) \leq 3$ by checking if it has roots.

Modulo Polynomials

We can define congruence modulo a polynomial $m(x)$ similarly as we did with integers:

$$a(x) \equiv_{m(x)} b(x) \iff m(x)|(a(x) - b(x))$$

We can now define:

$$F[x]_{m(x)} = \{a(x) \in F[x] \mid deg(a) < deg(m)\}$$

So $F[x]_{m(x)}$ simply contains all the polynomials with a certain maximum degree in $F[x]$.

Example: $\mathbb{Z}_3[x]_{x^2+1}$ contains $0, 1, 2, x, x+1, x+2$. It contains the same elements as $\mathbb{Z}_3[x]_{x^2}$, but the modulus we are calculating with is different!

Polynomial Fields

Polynomial Fields

$F[x]_{m(x)}$ is a field if and only if $m(x)$ is irreducible.

Error Correcting Codes

Encoding

An *(n,k)-encoding function* maps some tuple A^k to a codeword A^n.

For example, over the alphabet $A = \{0, 1\}$ we could define a (8,4)-encoding function which maps $a_1a_2a_3a_4 \mapsto a_1a_2a_3a_4a_1a_2a_3a_4$.

Code

An *(n,k)-error-correcting* code over A with $|A| = q$ is a subset of A^n of cardinality q^k. (It is the image of the encoding function.)

Decoding

Decoding

A *decoding function* D for an *(n,k)-encoding function* is a function $A^n \to A^k$.

Hamming Distance

The *hamming distance* of two strings is the number of positions where they differ.

Minimum Distance

The *minimum distance* of a code C is the minimum hamming distance between any two codewords in C.

Good Codes

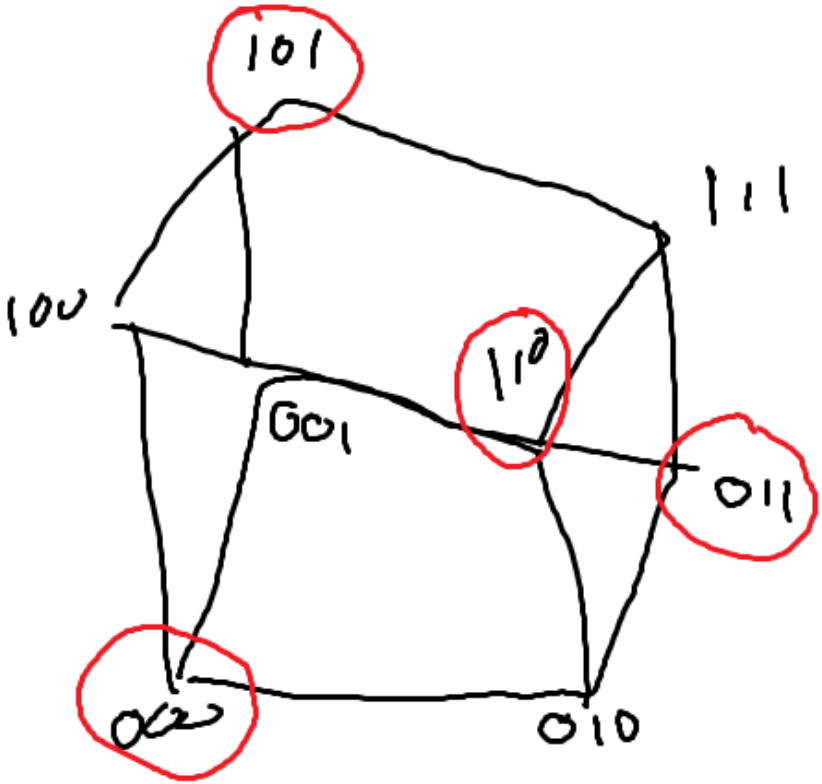
A decoding function D is *t-error correcting* for an encoding function E if it correctly decodes all strings with hamming distance at most t from $E(s)$ to s.

We want to correct as many errors as we can. Say we encode $0 \mapsto 00$ and $0 \mapsto 11$. What happens when one bit is corrupted to 01? If we encode $0 \mapsto 000$ and $1 \mapsto 111$ the we can correct one error.

Error Correction

A code C with minimum distance d is t error correcting if $d \geq 2t + 1$.

Cube



Polynomial Codes

Say we want to encode k values from $GF(q)$ into n new values. For the string $(a_0, a_1, \ldots, a_{k-1})$ we can calculate the new string $(a(\alpha_1), \ldots, a(\alpha_n))$. Here:

$$a(x) = a_{k-1}x^{k-1} + \cdots + a_0$$

and $\alpha_1, \ldots, \alpha_n$ are fixed and chosen in advance.

This code has minimum distance $n - k + 1$. Since the polynomial $a(x)$ is determined by k points, each encoded string can have at most $k - 1$ values in common.