3: Finite Fields

Some Mathematical Foundations You Need to Remember

Goals:

- Recall basic algebraic structures
- Focus on finite fields of the form GF(2^n)
- Arithmetic over GF(2^n)
- Including the Gray-Code “trick” used in PMAC

Semi-Groups and Groups

We define:

- A non-empty set S
- An operation $'+'$: For all $a, b \in S : a + b \in S$
- $(S, +)$ is a **semi-group** iff it is **associative**:

$$\text{For all } a, b, c \in S : \quad a + (b + c) = (a + b) + c.$$

- A semi-group $(S, +)$ is a **monoid** iff there exists a **neutral element** $z \in S$:

$$\text{For all } a \in S : \quad a + z = z + a = a.$$

- A monoid $(S, +)$ is a **group** iff there exists an **inverse element**:

$$\text{For all } a \in S, \text{ there exists } \bar{a} \in S : \quad a + \bar{a} = z.$$

- A (semi-)group $(S, +)$ is **commutative** iff it holds:

$$\text{For all } a, b \in S : \quad a + b = b + a.$$

Semi-Groups and Groups: Examples

- $(\mathbb{Z}, -)$: No semi-group (not associative)
- $(\mathbb{N}, +)$: Only semi-group (no 0)
- $(\mathbb{N}_0, +)$: Only monoid (no inverse elements)
- $(\mathbb{Z}, *)$: Only monoid (no inverse elements)
- $(\mathbb{Z}, +)$: Group
- $(\mathbb{Z}_n, +)$: Group
- $(\mathbb{Z}_n, *)$: Only monoid (no inverse element for 0)
- In general: $(\mathbb{Z}_n \setminus \{0\}, *)$ is a group $\Leftrightarrow$ n is prime

Rings and Fields

(S a non-empty set with two operations "$+$" and "$*$")

- $(S, +, *)$ is a **ring** iff
  - $(S, +)$ is a commutative group,
  - $(S, *)$ is a semi-group, and
  - the **distributive law** holds: $\forall a, b, c \in S$:

$$a * (b + c) = a * b + a * c, \quad \text{and} \quad (a + b) * c = (a * c) + (b * c)$$

- A ring $(S, +, *)$ is a **field** iff $(S \setminus \{0\}, *)$ is a group

Examples:

- $(\mathbb{Z}, +, *)$: Ring, but no field.
- $(\mathbb{Z}_n, +, *)$: (Finite) Ring.
- $((\mathbb{Z}_n, +, *)$: (Finite) Field) $\Leftrightarrow$ (n is prime).

  (If $n = pq$, then $a = kp$ is a "zero-divisor", since $aq = kn \equiv 0$.)

Polynomials over $\mathbb{Z}_2$

- Unknown "x"
- Powers of x
- Coefficients in $\mathbb{Z}_2$; can be respresented as 0 or 1
- Examples:
  - 0
  - 1
  - x
  - $x + 1$
  - x^6
  - $x^6 + x + 1 = 1x^6 + 0x^5 + 0x^4 + 0x^3 + 0x^2 + 1x^1 + 1x^0$

Polynomials over $\mathbb{Z}_2$ (2)

- Examples: 0, 1, x, $x+1$, x^6, x^6+x+1, $\ldots$
- **Addition of coefficients** is **mod 2**:

$$0+0=1+1=0$$
$$0+1=1+0=1$$

- **Subtraction**: **same as addition**
- Both **addition** and **subtraction** are the same as the **logical xor** (We could replace both "$+$" and "$-$" by XOR: "$\oplus$")
- **Multiplication** of coefficients is the same as the **logical and**:

$$(a*b=1) \Leftrightarrow (a=b=1)$$

- Ring of polynomials over $\mathbb{Z}_2$, with the following operations:
  - Polynomial addition, e.g., $(x+1)+x=2x+1=1$
  - Polynomial multiplication, e.g., $(x+1)*x=x^2+x$

Modular Polynomial Arithmetic

- First choose irreducible polynomial over $\mathbb{Z}_2$, e.g, $P = x^3 + x + 1$
- Consider all polymomials over $\mathbb{Z}_2$, modulo P
- Example $(x^2 + x + 1) * (x^2 + 1)$ (mod P):

$$\begin{aligned}
(x^2 + x + 1) * (x^2 + 1) &\equiv (x^4 + x^3 + x^2) + (x^2 + x + 1) \\
&\equiv x^4 + x^3 + x + 1 \\
&\equiv x^4 + x^3 + x + 1 - xP \\
&\equiv x^3 + x^2 + 1 \\
&\equiv x^3 + x^2 + 1 - P \\
&\equiv \underline{\underline{x^2 + x}}
\end{aligned}$$

Natural Representation

The set of polynomials mod $P = x^3 + x + 1$ can be represented by the following **eight** polynomials, which are distinct (mod P):

- 0
- 1
- x
- $x + 1$
- x^2
- $x^2 + 1$
- $x^2 + x$
- $x^2 + x + 1$

We refer to this as GF(2^3). This is a field with eight elements.

The Field GF(2^3)

- GF(2^3) is a field.
- Consider the equation
$$ab + c = d$$
- Given a, b, and c, there is a unique solution for d.
- Given a, b, and d, there is a unique solution for c:
$$c = d - ab$$
- Given c, d and nonzero a or nonzero b, there is a unique solution for b resp a:
$$a = \frac{d-c}{b}, \qquad b = \frac{d-c}{a}.$$
- If a or b are nonzero, their multiplicative inverse is well-defined. I.e., we can actually divide by a nonzero a or b.

The Ring $\mathbb{Z}_8$

- Just like $\mathbb{Z}_8$ has eight eight distinct elements, which can be represented by $\{0, 1, \ldots, 7\}$.
- But consider the following equations:

$$a * 2 + 0 = 1, \qquad a * 2 + 0 = 2, \qquad a * 4 + 0 = 2.$$

  The first has no solutions, the second two: ($a = 3$ and $a = 7$), and the third has four solutions ($a \in \{1, 3, 5, 7\}$).
- The multiplicative inverse of 2 (or any even number) in $\mathbb{Z}_2$ is undefined.
- $\Longrightarrow$ $\mathbb{Z}_8$ is not a field.
- $\mathbb{Z}_8$ is still a ring.

On the Choice of the Modulus P

- Apart from P, there exists another irreducile degree-3 polynomial over $GF(2)$: $P' = x^3 + x^2 + 1$.
- Polynomial arithmetic modulo P' forms a field, as well.
- Nevertheless, mathematicans consider both as forming *the same field*, since both fields are *isomorphic*.
- This “single” field is denoted GF(2^3).

On the Choice of the Modulus P (2)

- Consider another polynomial, say $P'' = x^3 + x^2 + x + 1$.
- P'' is reducible: $P'' = (x^2 + 1)(x + 1)$.
- The factors $x + 1$ and $x^2 + 1$ of P'' are zero-divisors mod P''.
- Zero-divisors don't have multiplicative inverses. Consider $a, b \neq 0$ with $a * b = 0$ and assume inverses a^{-1} and b^{-1}:

$$a * a^{-1} * b * b^{-1} = 1 * 1 = 1,$$

but $a * a^{-1} * b * b^{-1} =$

$$a * b * a^{-1} * b^{-1} = 0 * a^{-1} * b^{-1} = 0.$$

- Thus, polynomial arithmetic modulo a reducible P'' does not form a field.

Representing Polynomials as Binary-Code Words

Recall the eight distinct polynomials in GF(2^3), and think of each x^i (including $x'0$) as the place-holder for one bit.
You can represent the polynomials as 3-bit strings:

- $000 = 0$
- $001 = 1$
- $010 = x$
- $011 = x + 1$
- $100 = x^2$
- $101 = x^2 + 1$
- $110 = x^2 + x$
- $111 = x^2 + x + 1$

Known Results from Mathematics

- For every $n \in \mathbb{N}$, a field GF(2^n) exists.
- GF(2^n) has distinct 2^n elements, which can be represented
  - by the polynomials of degree $n-1$ or smaller, or
  - by bit-strings of length n.
- Arithmetic over GF(2^n) is determined by an irreducible polynomial of degree n.
- Regardless of the polynomial, all instances of GF(2^n) are *isomorphic* (for fixed n, i.e., from the mathematical point of view, there exists exactly one field GF(2^n).

- These results generalize: For every prime p, up to isomorphism, there exists exactly one field GF(p^n) with p^n distinct elements.

Polynomial Addition

- In general, adding polynomials is done by adding the individual coefficients, e.g. $(x^2+1)+(x^2+x)=2x^2+x+1$.
- For polynomials over GF(2^n), the coefficients are in $\mathbb{Z}_2$, e.g., $(x^2+1)+(x^2+x)=x+1$.
- Thus, polyonmial addition and subtraction of polynomials of (max.) degree $n-1$ are the same as the bit-wise xor of n-bit strings, e.g. $101 \oplus 110 = 011$.

Multiply a Polynomial by a Monomial

Compute $p * x^i$

- A monomial is an expression of the form x^i.
- Each nonzero polynomial is the sum of one or more monomials.
- The multipication $p * x^i$ of a polynomial p with a monomial x^i is the same as replacing each monomial x^ℓ in p by $x^{i+\ell}$. Example:

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

- This is the same as shifting p to the left by i times (or as "multiplying" p by 2^i). Examples:

$$\begin{aligned} 101 * 001 &= 101, \\ 101 * 010 &= 1010, \\ 101 * 100 &= 10100. \end{aligned}$$

Multiply a Polynomial by Another Polynomial

compute $p * q$

- If $q = 0$, then $p * q = 0$.
- Otherwise, the polynomial q is the sum of one or more monomials, e.g., $q = x^i + x^j + x^k$, and then

$$p * q = p * (x^i + x^j + x^k) = p * x^i + p * x^j + p * x^k$$

(thanks to the distributive law).

- Thus, to compute the product $p * q$ of two polynomials in general

```
sum := 0
for all monomials x^i of q:
        sum := sum + p * x^i
return sum
```

- Example:

$$101 * 111 = 10100 + 1010 + 101 = 11011.$$

Efficient Computations mod p

- Let p be a polynomial of degree n.
- Efficiently compute $(a + b)$ mod p:
  - If a and b are natural representants, i.e., are of degree $\leq n - 1$, then $a + b$ is also of degree $\leq n - 1$.
- Efficiently compute $(a * b)$ mod p:
  - Consider multiplication by 2:

$$T := \begin{cases} T * 2 & \text{if T*2 is of degree} \leq n-1 \\ T * 2 - p & \text{otherwise} \end{cases}$$

  - Thus, T will always have degree $\leq n - 1$.
- Example: $(x^2 + 1) * (x^2 + x + 1)$ mod P, for $P = x^3 + x + 1 = 1011$:

$$\begin{aligned} 101 * 111 &\equiv 101 * 4 + 101 * 2 + 101 \\ &\equiv (1010 \bmod P) * 2 + (1010 \bmod P) + 101 \\ &\equiv (1010 - 1011) * 2 + (1010 - 1011) + 1 \\ &\equiv 001 * 2 + 001 + 101 \\ &\equiv 010 + 001 + 101 = 110 = x^2 + x^1 \end{aligned}$$

The Gray-Code Trick

- Recall that the hamming difference between g_{i-1} and g_i is exactly one, i.e., there exists some x_j, such that $g_{i-1} \oplus g_i = x_j$.
- Then, given $g_{i-1} * L$, it is easy to compute

$$\begin{aligned} g_i * L &= g_{i-1} * L \oplus x^i * L \\ &= g_{i-1} * L \oplus L * 2^i. \end{aligned}$$

- Thus, if we precompute $L, L * 2, L * 4, \ldots$, going from $g_{i-1} * L$ to $g_i * L$ costs a single addition over GF(2^n) (i.e., one n-bit xor).