# Finite Fields

In practice most finite field applications e.g. cryptography and error correcting codes utilizes a specific type of finite fields, namely the *binary extension fields*. The following exercises will introduce you to calculations in binary extension fields.

**Exercise 1: The Binary Field** .....

The binary field $\mathbb{F}_2$ consists of two elements $\{0, 1\}$ and is of particular interest since the binary operations are easily implemented and represented in software and hardware. In the case of the binary fields, arithmetic operations are performed modulo-2. For addition and multiplication this corresponds to the bitwise exclusive or (XOR) and the bitwise and (AND) operations.

(a) Fill in the missing values in the below table.

| $XOR$ | 0 | 1 |
|---|---|---|
| 0 | | |
| 1 | | |

| $AND$ | 0 | 1 |
|---|---|---|
| 0 | | |
| 1 | | |

Table 1: The finite field $\mathbb{F}_2$ consists of elements 0 and 1 which satisfy the addition(XOR) and multiplication(AND) tables.

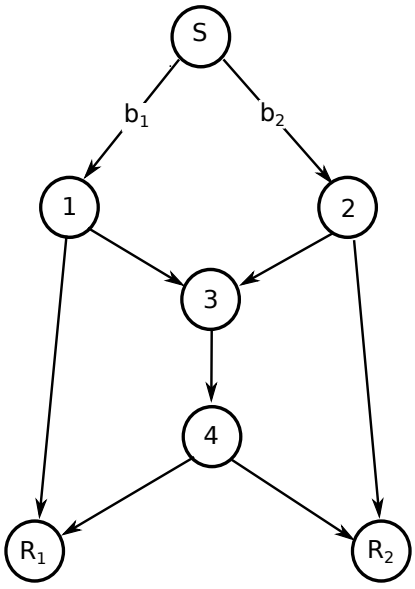
**Solution:**

| $XOR$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

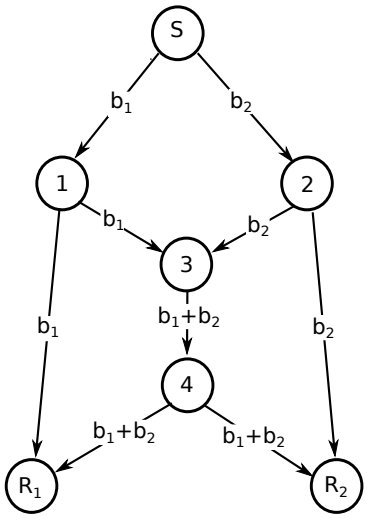
| $AND$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

**Exercise 2: The Butterfly Network** .....

(a) The butterfly network shown in the below figure is a famous example of Network Coding. Show how the two bits $b_1$ and $b_2$ may be delivered at the two receivers $R_1$ and $R_2$ simultaneously using the operations from the binary field (hint: the XOR operation is enough). Each edge may carry 1 bit per time unit.



**Solution:**




**Exercise 3: Binary Field Calculations**

In practice calculations are typically performed $w$-bits at a time, where $w$ corresponds to the word size of the hardware used. Typical values of $w$ are $\{16, 32, 64\}$ bits. The below table shows an example of XOR and AND between two 8-bit words.

| | | | |
|---|---|---|---|
| | 01011001 | | 00011101 |
| $XOR$ | 00100110 | $AND$ | 01100111 |
| $=$ | 01111111 | $=$ | 00000101 |

(a) Fill in the missing values in the tables.

| | | | |
|---|---|---|---|
| | 11101001 | | 01111000 |
| $XOR$ | 10100110 | $AND$ | 01100111 |
| $=$ | | $=$ | |

Table 2: Addition and multiplication in $\mathbb{F}_2$ with 8-bit words.

**Solution:**

| | |
|---|---|
| | 11101001 |
| $XOR$ | 10100110 |
| $=$ | 01001111 |

| | |
|---|---|
| | 01111000 |
| $AND$ | 01100111 |
| $=$ | 01100000 |

**Exercise 4: The Binary Extension Field**

In a previous exercise we found a solution for the butterfly network using the binary field. However, when implementing Network Coding it can in certain cases be necessary to increase the field size in order to find a solution (i.e. the number of elements contained in the field). In the binary field $\mathbb{F}_2$ the field size was 2, i.e. there are two elements $0, 1$. Binary extension fields have the form $\mathbb{F}_{2^m}$, where $m \geq 1$. A binary extension field contains $2^m$ elements, all field elements may be represented as binary polynomials of degree at most $m-1$:

$$\mathbb{F}_{2^m} = \{f_{m-1}x^{m-1} + \ldots + f_2x^2 + f_1x + f_0 : f_i \in \{0, 1\}\} \tag{1}$$

As an example consider the field given by $\mathbb{F}_{2^3}$ in the below table, in this case the field will consist of $2^3 = 8$ polynomial elements of degree $< m$.

In the binary extension field all polynomial elements can be represented as $m$ bit binary numbers. It is important to notice the correspondence between the binary and polynomial representation. The bits from left to right are the coefficients of the powers of $x$ in increasing order.

| $GF2^3$ | | |
|---|---|---|
| Polynomial | Binary | Decimal |
| 0 | 000 | 0 |
| 1 | 001 | 1 |
| $x$ | 010 | 2 |
| $x+1$ | 011 | 3 |
| $x^2$ | 100 | 4 |
| $x^2+1$ | 101 | 5 |
| $x^2+x$ | 110 | 6 |
| $x^2+x+1$ | 111 | 7 |

(a) Fill in the missing values in the below table.

| $GF2^m$ | | |
|---|---|---|
| Polynomial | Binary | Decimal |
| $x^7+x^6+x^4+x+1$ | | |
| | 11001001 | |
| | | 133 |
| $x^4+x^2+x$ | | |
| | 00011001 | |
| | | 10 |

**Solution:**

| $GF2^m$ | | |
|---|---|---|
| Polynomial | Binary | Decimal |
| $x^7+x^6+x^4+x+1$ | 11010011 | 211 |
| $x^7+x^6x^3+1$ | 11001001 | 201 |
| $x^7+x^2+1$ | 10000101 | 133 |
| $x^4+x^2+x$ | 00010110 | 22 |
| $x^4+x^3+1$ | 00011001 | 25 |
| $x^3+x$ | 00001010 | 10 |

(b) In the table what is the required value for $m$ in order to represent the field elements.

**Solution:** The value of $m$ must be 8.

**Exercise 5: Polynomial Addition and Subtraction**

Polynomials essentially allow the same arithmetic operations as integers, however when polynomials are used the operations are performed modulo-$p(x)$, where $p(x)$ is an irreducible polynomial instead of a prime integer (e.g. 2 as in the case of the binary field). As with a prime number an irreducible polynomial is one which cannot be factored into products of two polynomials.

Ordinary polynomial addition is performed component-wise e.g. for two polynomials with a maximum degree of $k$:

$$f(x) = h(x) + g(x) \tag{2}$$

$$f(x) = \sum_{i=0}^{k} (h_i + g_i)x^i \tag{3}$$

In $\mathbb{F}_{p^m}$ we calculate $f(x)+g(x)$ as $f(x)+g(x) \mod p(x)$. This uses the usual component-wise addition as given in Equation (**??**), the only difference is that the coefficient sum is modulo $p$ i.e. $h_i + g_i \mod p$. As the degree of the resulting polynomial $f(x)$ cannot exceed the degree of the chosen prime polynomial, no further computations are needed.

**Example**

Lets consider a $w = 8$ bit architecture with the two polynomials $a(x) = x^7 + x^6 + x^2$ and $b(x) = x^7 + x^5 + x^3 + x^2$ with the binary representation of 11000100 and 10101100 respectively. In the following we use $\oplus$ to denote the XOR operation.

- Addition or subtraction: $11000100 \oplus 10101100 = 01101000$.

The result may be confirmed by adding the two polynomials directly:

$$f(x) = (x^7 + x^6 + x^2) + (x^7 + x^5 + x^3 + x^2) \tag{4}$$

$$= (1 \oplus 1)x^7 + x^6 + x^5 + x^3 + (1 \oplus 1)x^2 \tag{5}$$

$$= x^6 + x^5 + x^3 \tag{6}$$

Where $x^6 + x^5 + x^3$ has the expected binary representation 01101000.

(a) In $\mathbb{F}_{2^8}$ calculate $(x^5 + x) + (x^3 + x^2)$

**Solution:** $(x^5 + x) + (x^3 + x^2) = x^5 + x^3 + x^2 + x$

(b) In $\mathbb{F}_{2^8}$ calculate $(x^7 + x^3) + (x^7 + x + 1)$

**Solution:** $(x^7 + x^3) + (x^7 + x + 1) = x^3 + x + 1$

(c) In $\mathbb{F}_{2^8}$ calculate $(x^3 + x^2 + x + 1) + (x + 1)$

**Solution:** $(x^3 + x^2 + x + 1) + (x + 1) = x^3 + x^2$

(d) In $\mathbb{F}_{2^8}$ calculate $(x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1) + (x^4 + x^2 + 1)$

**Solution:** $(x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1) + (x^4 + x^2 + 1) = x^7 + x^6 + x^5 + x^3$

In the binary and binary extension field subtraction and addition are identical (based on the XOR).

**Subtraction** of two field elements can be defined in terms of addition, if $a, b \in \mathbb{F}$ then $a - b = a + (-b)$, where $-b$ is the unique field element in $\mathbb{F}$ such that $b + (-b) = 0$ ($-b$ is called the negative of $b$).

(e) In $\mathbb{F}_{2^8}$ calculate $(x^5 + x) - (x^3 + x^2)$

**Solution:** $(x^5 + x) - (x^3 + x^2) = x^5 + x^3 + x^2 + x$

(f) In $\mathbb{F}_{2^8}$ calculate $(x^7 + x^3) - (x^7 + x + 1)$

**Solution:** $(x^7 + x^3) - (x^7 + x + 1) = x^3 + x + 1$

(g) In $\mathbb{F}_{2^8}$ calculate $(x^3 + x^2 + x + 1) - (x + 1)$

**Solution:** $(x^3 + x^2 + x + 1) - (x + 1) = x^3 + x^2$

(h) In $\mathbb{F}_{2^8}$ calculate $(x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1) - (x^4 + x^2 + 1)$

**Solution:** $(x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1) - (x^4 + x^2 + 1) = x^7 + x^6 + x^5 + x^3$

**Exercise 6: Polynomial Multiplication**

For ordinary polynomial multiplication, the coefficients of $f(x) = h(x)g(x)$ are determined by convolution, the resulting polynomial $f(x)$ is of degree = deg(h)+deg(g):

$$f_i = \sum_{j=0}^{i} h_j g_{i-j} \tag{7}$$

The product $h(x)g(x)$ in $\mathbb{F}_{p^m}$ can be found by first multiplying $h(x)$ and $g(x)$ using ordinary polynomial multiplication. Then ensuring that the resulting polynomial $f(x)$ has degree $< m$ by reducing it modulo $p(x)$. The modulo operation can be implemented as polynomial long division and then taking the remainder. As for polynomial addition we must also ensure that all resulting coefficients are elements in $\mathbb{F}_p$ by reducing them modulo $p$.

In the following use the irreducible prime polynomial $p(x) = x^5 + x^2 + 1$

**Example**

$$\begin{aligned} f(x) &= (x^3 + x + 1) \cdot (x^2 + 1) && (8)\\ &= x^5 + (1 \oplus 1)x^3 + x^2 + x + 1 && (9)\\ &= x^5 + x^2 + x + 1 && (10) \end{aligned}$$

Since degree of $f(x)$ equal m, we perform the modulo operation using the irreducible polynomial $p(x)$

$$\begin{aligned} f(x) &= x^5 + x^2 + x + 1 \mod p(x) && (11)\\ f(x) &= x && (12) \end{aligned}$$

The result of the modulo operation can be calculated as the remaineder of polynomial long division with the irreducible polynomial:

$$\begin{array}{rl|llll} & & & & & 1 \\ \cline{3-6} x^5 + x^2 + 1 & & x^5 & +x^2 & +x & +1 \\ & & x^5 & +x^2 & & +1 \\ \cline{3-6} & & & & x & \end{array}$$

◁ qoutient

◁ remainder

(a) In $\mathbb{F}_{2^5}$ calculate $(x^4 + x) \cdot (x^3 + x^2)$

**Solution:** $f(x) = (x^4 + x) \cdot (x^3 + x^2) = x^7 + x^6 + x^4 + x^3$
Degree of $f(x) > 5$ so we must perform modulo i.e. long divsion with $p(x)$:

$$
\begin{array}{rl|llllll}
 & & & & & x^2 & +x & \triangleleft \text{ qoutient} \\
\hline
x^5 + x^2 + 1 & | & x^7 & +x^6 & +x^4 & +x^3 & & \\
 & & x^7 & & +x^4 & & +x^2 & \\
\hline
 & & & x^6 & & +x^3 & +x^2 & \\
 & & & x^6 & & +x^3 & & +x \\
\hline
 & & & & & x^2 & +x & \triangleleft \text{ remainder}
\end{array}
$$

Finally we therefore get:
$f(x) = (x^4 + x) \cdot (x^3 + x^2) \mod p(x) = x^7 + x^6 + x^4 + x^3 \mod p(x) = x^2 + x$

In Matlab this may be calculated as: `gf(18, 5)*gf(12, 5)`
The first parameter represents the field element i.g. 18 is the decimal value of $x^4 + x$ and 12 is the decimal value of $x^3 + x^2$. The second parameter represents the prime polynomial in Matlab decimal 5 represents the polynomial $x^5 + x^2 + 1$. For this calulation Matlab returns decimal value 6 which represents the polynomial $x^2 + x$, as we have shown above.

(b) In $\mathbb{F}_{2^5}$ calculate $(x^3) \cdot (x^2 + x^1 + 1)$

**Solution:** $(x^3) \cdot (x^2 + x^1 + 1) = x^4 + x^3 + x^2 + 1$

**Exercise 7: Polynomial Division**

Division can be implemented in terms of multiplication with the inverse element.

**Division** can be defined in terms of multiplication: if $a, b \in \mathbb{F}$ then $a/b = a \cdot (b^{-1})$, where $b^{-1}$ is the unique field element in $\mathbb{F}$ such that $b \cdot b^{-1} = 1$ ($b^{-1}$ is called the inverse of $b$).

The inverse of a polynomial may be found using the Extended Euclidean algorithm.

(a) In $\mathbb{F}_{2^5}$ calculate $(x^4 + x)/(x^3 + x^2)$ given $(x^3 + x^2)^{-1} = (x^2 + x + 1)$

**Solution:** $(x^4 + x)/(x^3 + x^2) = (x^4 + x) \cdot (x^3 + x^2)^{-1} = (x^4 + x) \cdot (x^2 + x + 1) = x^4 + 1$

(b) In $\mathbb{F}_{2^5}$ verify $(x^3 + x^2)^{-1} = (x^2 + x + 1)$

**Solution:** Is true if $(x^3 + x^2) \cdot (x^2 + x + 1) = 1$

$$
\begin{aligned}
(x^3 + x^2) \cdot (x^2 + x + 1) &= x^5 + (1 \oplus 1)x^4 + (1 \oplus 1)x^3 + x^2 && (13) \\
&= x^5 + x^2 && (14)
\end{aligned}
$$

Since degree of the resulting polynomial equal m, we perform the modulo operation using the choosen irreducible polynomial $p(x) = x^5 + x^2 + 1$

$$
\begin{aligned}
&= x^5 + x^2 \mod p(x) && (15) \\
&= 1 && (16)
\end{aligned}
$$