Finite fields

Application of discrete models

In this document, we continue discussing *field*s (see: Algebraic structures). Reminder: fields are a special case of rings, and their main feature is that all elements have a multiplicative inverse (or simply: division is always possible). The fields we have seen so far are the number fields: $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ (but $\mathbb{Z}$ is *not* a field), and also the field $\mathbb{Z}_p$ for any prime number p. In this document, we create new fields from existing ones.

1 Field extension

Definition 1.1. The field G is a **field extension** of the field F if $F \subseteq G$, and the corresponding operations ($+$ and $\cdot$) coincide in F.

Example. $\mathbb{R}$ is a field extension of $\mathbb{Q}$, and $\mathbb{C}$ is a field extension of both of them.

Definition 1.2. The field G is a **simple extension** of the field F if $\exists \theta \in G \setminus F$ such that G is the smallest field extension of F that contains θ. Notation: $G = F(\theta)$. Then G is called the **field generated by θ** (over F), and θ is the **primitive element** of the extension. (θ is spelled "theta".)

Example. $\mathbb{C}$ is a simple extension of $\mathbb{R}$, namely $\mathbb{C} = \mathbb{R}(i)$, because $i \in \mathbb{C} \setminus \mathbb{R}$, and $\mathbb{R}$ has no field extension smaller than $\mathbb{C}$ that contains i. This is because a field must be closed under addition and multiplication, so if it contains i, it must also contain $2i$, $-5i$, $i+1$, $2i-3/2$ etc., i.e. all numbers of the form $a+bi$, where $a, b \in \mathbb{R}$, but then we already have the entire $\mathbb{C}$.

Example. $\mathbb{R}$ is *not* a simple extension of $\mathbb{Q}$, because there is no θ for which $\mathbb{R} = \mathbb{Q}(\theta)$. (The reason lies in the cardinality of these sets: $\mathbb{Q}$ is countably infinite, while $\mathbb{R}$ is continuum, in other words $\mathbb{R}$ is "much bigger".)

Example. Now create a new field: $\mathbb{Q}(\sqrt{2})$, i.e. extend the rational field $\mathbb{Q}$ by $\sqrt{2}$ (as we know, $\sqrt{2} \notin \mathbb{Q}$). Besides all rational numbers, this field must contain $\sqrt{2}$, and all necessary numbers to make it closed under the operations, e.g. $2\sqrt{2}$, $1+\sqrt{2}$, $5/2+\sqrt{2}/3 \in \mathbb{Q}(\sqrt{2})$. It can be shown that $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. In this field, we can do arithmetic as follows:

- Addition and subtraction is trivial, just add/subtract the corresponding terms, for example:
$$(1+3\sqrt{2}) + (3-2\sqrt{2}) = 4+\sqrt{2}.$$
- Multiplication is also very easy, just use the fact that $\sqrt{2} \cdot \sqrt{2} = 2$, for example:
$$(1+\sqrt{2})(3+2\sqrt{2}) = 3+2\sqrt{2}+3\sqrt{2}+2\sqrt{2}^2 = 3+5\sqrt{2}+4 = 7+5\sqrt{2}.$$
- Multiplicative inverse (or division) can be calculated using *rationalization*, for example:
$$(5+2\sqrt{2})^{-1} = \frac{1}{5+2\sqrt{2}} = \frac{5-2\sqrt{2}}{(5+2\sqrt{2})(5-2\sqrt{2})} = \frac{5-2\sqrt{2}}{25-8} = \frac{5}{17} + \frac{-2}{17}\sqrt{2}.$$

Notice how similar arithmetic in $\mathbb{Q}(\sqrt{2})$ is to $\mathbb{C} = \mathbb{R}(i)$. This is not a coincidence, as both are simple field extensions. The difference is that the primitive element is $\sqrt{2}$ instead of i, and that the coefficients are in $\mathbb{Q}$ instead of $\mathbb{R}$.

Example. Consider another field extension: $\mathbb{Q}(\sqrt[3]{2})$. The main difference from $\mathbb{Q}(\sqrt{2})$ and $\mathbb{C} = \mathbb{R}(i)$ is that in this case, two coefficients (a and b) are no longer sufficient: if we multiply two numbers of the form $a + b\sqrt[3]{2}$, then the result will contain $\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{2}^2$, which cannot be written as $a + b\sqrt[3]{2}$. Therefore, we need *three* coefficients: $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 \mid a, b, c \in \mathbb{Q}\}$. Although multiplication of such elements will produce even higher powers of $\sqrt[3]{2}$, this is not a problem anymore, because $\sqrt[3]{2}^3 = 2$ and $\sqrt[3]{2}^4 = 2\sqrt[3]{2}$. For example:

$$\begin{aligned}(5 + \sqrt[3]{2}^2)(\sqrt[3]{2} - \sqrt[3]{2}^2) &= 5\sqrt[3]{2} - 5\sqrt[3]{2}^2 + \sqrt[3]{2}^3 - \sqrt[3]{2}^4 = \\ &= 5\sqrt[3]{2} - 5\sqrt[3]{2}^2 + 2 - 2\sqrt[3]{2} = \\ &= 2 + 3\sqrt[3]{2} - 5\sqrt[3]{2}^2.\end{aligned}$$

2 Structure of field extensions

Generally, the primitive element used for the field extension is not given in explicit form (e.g. $\sqrt{2}$), but by a rule that it must satisfy (e.g. $\theta^2 = 2$). The common way to describe such a rule is a polynomial (e.g. $x^2 - 2$) whose root is the primitive element.

Theorem 2.1. *Let $F(\theta)$ be a simple extension of the field F, where θ is a root of a polynomial $m \in F[x]$, which is **irreducible**, its degree is $n \geq 2$, and its leading coefficient is 1. Then all $\alpha \in F(\theta)$ elements can be written uniquely in the following form:*

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + \ldots + a_{n-1}\theta^{n-1},$$

where $a_0, a_1, \ldots, a_{n-1} \in F$; in other words, there is a unique polynomial $p_\alpha \in F[x]$ of degree $\leq n-1$ for which $\alpha = p_\alpha(\theta)$.

Definition 2.2. The above irreducible polynomial m is called the **minimal polynomial** of θ, and its degree, $n = \deg m$ is the **degree** of the field extension.

Example. $\mathbb{Q}(\sqrt{2})$ is a *quadratic* extension of $\mathbb{Q}$, where the minimal polynomial of $\sqrt{2}$ is $m = x^2 - 2$, and each $\alpha \in \mathbb{Q}(\sqrt{2})$ element can be written uniquely as $\alpha = a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$ (i.e. it can be represented by the linear polynomial $p_\alpha = a + bx$).

Example. $\mathbb{C} = \mathbb{R}(i)$ is a *quadratic* extension of $\mathbb{R}$, where the minimal polynomial of i is $m = x^2 + 1$, and each complex number $z \in \mathbb{C}$ can be written uniquely as $z = a + bi$ (where $a, b \in \mathbb{R}$).

Example. $\mathbb{Q}(\sqrt[3]{2})$ is a *cubic* extension of $\mathbb{Q}$, where the minimal polynomial of $\sqrt[3]{2}$ is $m = x^3 - 2$, and each $\alpha \in \mathbb{Q}(\sqrt[3]{2})$ element can be written uniquely as $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{2}^2$ (where $a, b, c \in \mathbb{Q}$), corresponding to the quadratic polynomial $p_\alpha = a + bx + cx^2$.

Field extensions can have more than one primitive elements. For example, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(2\sqrt{2}+1)$, i.e. not only $\sqrt{2}$, but also $\theta = 2\sqrt{2} + 1$ (minimal polynomial: $x^2 - 2x - 7$) can be used to write all elements of $\mathbb{Q}(\sqrt{2})$ in the form $a + b\theta$ (with different a and b, of course). For example, $\alpha = 4 + 3\sqrt{2}$ can be rewritten using $\theta = 2\sqrt{2} + 1$ as $\alpha = 5/2 + 3/2 \cdot \theta$. (But the number of coefficients is still two, i.e. the degree of the field extension is independent from the choice of the primitive element.)

How can we do arithmetic in an arbitrary field extension $F(\theta)$? Let θ be the root of the minimal polynomial $m \in F[x]$, whose degree is $n = \deg m$. Then, by the above theorem, the elements of $F(\theta)$ can be written in the form $\alpha = a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}$, i.e. they can be represented by a polynomial $p_\alpha = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$ of degree at most $n-1$. The arithmetic operations in the field are then performed using these representing polynomials as follows:

1. **Addition, subtraction:** simply add or subtract the representing polynomials.
2. **Multiplication:** if we just multiply the two polynomials, the product may exceed degree $n-1$, so we also need to take its remainder by the minimal polynomial m. For example, in $\mathbb{Q}(\sqrt{2})$:
$$\alpha = 1 + \sqrt{2} \quad \longrightarrow \quad p_\alpha = 1 + x,$$
$$\beta = 3 + 2\sqrt{2} \quad \longrightarrow \quad p_\beta = 3 + 2x,$$
$$p_{\alpha\beta} = p_\alpha p_\beta \bmod m = (1+x)(3+2x) \bmod (x^2-2) = (3 + 5x + 2x^2) \bmod (x^2-2) = 7 + 5x,$$
$$\longrightarrow \quad \alpha\beta \quad = \quad (1+\sqrt{2})(3+2\sqrt{2}) \quad = \quad 3 + 5\sqrt{2} + 2\sqrt{2}^2 \quad = \quad 7 + 5\sqrt{2}.$$
The remainder calculation by $x^2 - 2$ corresponds to simplifying the expression using $\sqrt{2}^2 = 2$. (Note: the calculation $p_\alpha p_\beta \bmod m$ is very similar to how we calculated with congruences, e.g. $3 \cdot 6 \equiv 8 \pmod{10}$, except that we do this with polynomials instead of integers.)
3. **Multiplicative inverse:** there are multiple ways to do this:
   (a) **Rationalization:** we have seen this for $\mathbb{Q}(\sqrt{2})$ above, and it works for all quadratic field extensions where the minimal polynomial is $x^2 - d$ (i.e. $\theta = \sqrt{d}$, e.g. $\sqrt{2}$ or $i = \sqrt{-1}$):
   $$(a+b\theta)^{-1} = \frac{1}{a+b\theta} = \frac{a-b\theta}{(a+b\theta)(a-b\theta)} = \frac{a-b\theta}{a^2-b^2d} = \frac{a}{a^2-b^2d} - \frac{b}{a^2-b^2d}\theta.$$
   (It can be extended to other field extensions too, but not in a trivial way.)
   (b) **System of linear equations:** write the representations of α and α^{-1} into $\alpha\alpha^{-1} = 1$, and solve this for the unknown coefficients of α^{-1}. For example, for $\alpha = 5 + 2\sqrt{2} \in \mathbb{Q}(\sqrt{2})$:
   $$\alpha\alpha^{-1} = 1,$$
   $$(5 + 2\sqrt{2})(u + v\sqrt{2}) = 1,$$
   $$5u + 5v\sqrt{2} + 2u\sqrt{2} + 4v = 1 + 0\sqrt{2},$$
   separating the rational and $\sqrt{2}$-terms (eliminating $\sqrt{2}$):
   $$5u + 4v = 1,$$
   $$2u + 5v = 0,$$
   and solving this gives $u = 5/17$ and $v = -2/17$, i.e. $\alpha^{-1} = 5/17 - 2/17 \cdot \sqrt{2}$.
   (c) **Extended Euclidean algorithm:** we know how to calculate the modular inverse of integers using the extended Euclidean algorithm (see: Congruences):
   $$7x \equiv 1 \pmod{10} \quad \longrightarrow \quad \mathrm{xgcd}(7, 10) = (1, 3, -2) \quad \longrightarrow \quad x = 3.$$
   The same works for polynomials too: e.g. in $\mathbb{Q}(\sqrt{2})$, the inverse of $\alpha = 5 + 2\sqrt{2}$ can be calculated by the extended Euclidean algorithm of $p_\alpha = 5 + 2x$ and $m = x^2 - 2$:
   $$\alpha\alpha^{-1} = 1 \quad \longrightarrow \quad p_\alpha p_{\alpha^{-1}} \bmod m = 1 \quad \longrightarrow$$
   $$\mathrm{xgcd}(p_\alpha, m) = \mathrm{xgcd}(5 + 2x,\ x^2 - 2) = (1,\ 5/17 - 2/17 \cdot x,\ 4/17)$$
   $$\longrightarrow \quad p_{\alpha^{-1}} = 5/17 - 2/17 \cdot x \quad \longrightarrow \quad \alpha^{-1} = 5/17 - 2/17 \cdot \sqrt{2}.$$
4. **Division:** multiply by the multiplicative inverse: $\alpha/\beta = \alpha\beta^{-1}$.

3 Finite fields

We can extend not only number fields, but also the fields $\mathbb{Z}_p$, for any prime number p (see: Congruences; Algebraic structures). Reminder: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-1}\}$, where all arithmetic is done modulo p, e.g. in $\mathbb{Z}_5$: $\overline{3} + \overline{4} = \overline{2}$, $\overline{1} - \overline{4} = \overline{2}$, $\overline{3} \cdot \overline{2} = \overline{1}$ and $\overline{3}^{-1} = \overline{2}$.

Example. Extend $\mathbb{Z}_5$ similarly to $\mathbb{Q}(\sqrt{2})$. Here "$\sqrt{2}$" is an "imaginary" value θ for which $\theta^2 = \overline{2} \in \mathbb{Z}_5$ (i.e. whose minimal polynomial is $m = x^2 - \overline{2} \in \mathbb{Z}_5[x]$). But first, we must check that θ is not already in $\mathbb{Z}_5$, because then it would not be an actual extension (just like $\mathbb{Q}(\sqrt{4})$ would not be one, because $\sqrt{4} = 2 \in \mathbb{Q}$). This is easy to check: $\overline{0}^2 = \overline{0}$, $\overline{1}^2 = \overline{1}$, $\overline{2}^2 = \overline{4}$, $\overline{3}^2 = \overline{4}$ and $\overline{4}^2 = \overline{1}$, i.e. no element of $\mathbb{Z}_5$ has the square $\overline{2}$, i.e. there is no "$\sqrt{2}$". The resulting field $\mathbb{Z}_5(\theta)$ has elements of the form $a + b\theta$ (where $a, b \in \mathbb{Z}_5$), e.g. $\overline{1} + \overline{3}\theta \in \mathbb{Z}_5(\theta)$, and arithmetic in it is very similar to $\mathbb{Q}(\sqrt{2})$:

$$(\overline{1} + \overline{3}\theta) - (\overline{4} + \theta) = (\overline{1} - \overline{4}) + (\overline{3} - \overline{1})\theta = \overline{2} + \overline{2}\theta,$$

$$(\overline{1} + \overline{3}\theta)(\overline{4} + \theta) = \overline{4} + \theta + \overline{4} \cdot \overline{3}\theta + \overline{3}\theta^2 = \overline{4} + \theta + \overline{2}\theta + \overline{3} \cdot \overline{2} = \overline{4} + \overline{3}\theta + \overline{1} = \overline{3}\theta,$$

$$(\overline{1} + \overline{3}\theta)^{-1} = \frac{\overline{1}}{\overline{1} + \overline{3}\theta} = \frac{\overline{1} - \overline{3}\theta}{(\overline{1} + \overline{3}\theta)(\overline{1} - \overline{3}\theta)} = \frac{\overline{1} - \overline{3}\theta}{\overline{1}^2 - \overline{3}^2 \cdot \overline{2}} = \frac{\overline{1}}{\overline{3}} - \frac{\overline{3}}{\overline{3}}\theta = \overline{2} - \theta = \overline{2} + \overline{4}\theta.$$

This field has finitely many elements ($5^2 = 25$, because both coefficients have 5 possible values):

$$\begin{array}{ccccc}
\overline{0}, & \overline{1}, & \overline{2}, & \overline{3}, & \overline{4}, \\
\theta, & \theta + \overline{1}, & \theta + \overline{2}, & \theta + \overline{3}, & \theta + \overline{4}, \\
\overline{2}\theta, & \overline{2}\theta + \overline{1}, & \overline{2}\theta + \overline{2}, & \overline{2}\theta + \overline{3}, & \overline{2}\theta + \overline{4}, \\
\overline{3}\theta, & \overline{3}\theta + \overline{1}, & \overline{3}\theta + \overline{2}, & \overline{3}\theta + \overline{3}, & \overline{3}\theta + \overline{4}, \\
\overline{4}\theta, & \overline{4}\theta + \overline{1}, & \overline{4}\theta + \overline{2}, & \overline{4}\theta + \overline{3}, & \overline{4}\theta + \overline{4}.
\end{array}$$

Definition 3.1. A field with finitely many elements is called a **finite field** (or **Galois field**).

In general, the above construction works as follows:

- Choose a base field $\mathbb{Z}_p$ (where p is a prime number).
- Choose an irreducible polynomial $m \in \mathbb{Z}_p[x]$ of degree $n \geq 2$, to be the minimal polynomial.
- The primitive element θ is a root of m. (Note: θ need not be an actual "existing" value, in the same way as the complex i is just an "imaginary" value whose square is -1.)
- The resulting field $\mathbb{Z}_p(\theta)$ has elements of the form $a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}$, where $a_i \in \mathbb{Z}_p$.
- Each coefficient a_i has p possible values, so the field has $pp \cdots p = p^n$ elements in total.

The significance of this construction is that *all* finite fields can be created in this way:

Theorem 3.2 (properties of finite fields)**.**

1. *The above construction works for any prime number p and any degree $n \geq 2$.*
2. *The finite field with p^n elements is unique up to isomorphism.*
3. *All finite fields have p^n elements, where p is a prime number and $n \geq 1$.*

Definition 3.3. The finite field with q elements is denoted by $\mathbb{F}_q$ (or $\mathrm{GF}(q)$, for Galois field).

So for each power of each prime number, there exists a unique finite field with that many elements:

- $\mathbb{F}_2 (= \mathbb{Z}_2)$, $\mathbb{F}_4$, $\mathbb{F}_8$, $\mathbb{F}_{16}$, ...,
- $\mathbb{F}_3 (= \mathbb{Z}_3)$, $\mathbb{F}_9$, $\mathbb{F}_{27}$, ...,
- $\mathbb{F}_5 (= \mathbb{Z}_5)$, $\mathbb{F}_{25}$, ...,
- ...;

and there are no other finite fields, e.g. there is no $\mathbb{F}_6$ or $\mathbb{F}_{10}$, because those are not prime powers.

Important: don't confuse $\mathbb{F}_m$ with $\mathbb{Z}_m$, because $\mathbb{F}_4 \neq \mathbb{Z}_4$, $\mathbb{F}_9 \neq \mathbb{Z}_9$ etc. (e.g. $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$, but $\mathbb{F}_4 = \{\overline{0}, \overline{1}, \theta, \theta + \overline{1}\}$), and most $\mathbb{Z}_m$'s are not even fields. Only for prime numbers are $\mathbb{F}_p = \mathbb{Z}_p$.

(The phrase "unique up to isomorphism" means that two finite fields with equal number of elements are always isomorphic, i.e. we can get one from the other by renaming the elements. For example, it can be shown that the set of logical values (T = "true", F = "false") with the operations "exclusive or" ($\oplus$) and "and" ($\wedge$), i.e. $(\{\mathrm{T}, \mathrm{F}\}, \oplus, \wedge)$ forms a field. This looks very different from $(\mathbb{Z}_2, +, \cdot)$, but they are still "essentially" the same (i.e. isomorphic), because we can get one from the other by renaming $\mathrm{F} \to \overline{0}$ and $\mathrm{T} \to \overline{1}$, e.g. $\mathrm{T} \oplus \mathrm{T} = \mathrm{F} \ \to\ \overline{1} + \overline{1} = \overline{0},\ \mathrm{F} \wedge \mathrm{T} = \mathrm{F} \ \to\ \overline{0} \cdot \overline{1} = \overline{0}$ etc.)

4 Field extensions in Sage

In Sage, the finite field $\mathbb{F}_q$ can be created by the notation `GF(q)`:

```
sage: GF(4)
Finite Field in z2 of size 2^2
sage: list(GF(4))       # list of all elements
[0, z2, z2 + 1, 1]
sage: g = GF(4).gen()   # primitive element (the above z2)
sage: g.minpoly()       # minimal polynomial
x^2 + x + 1
sage: GF(6)
[...]
ValueError: the order of a finite field must be a prime power
```

We can also specify a minimal polynomial, therefore choosing which θ primitive element is used to represent the elements. For example, for the above $\mathbb{F}_{25} = \mathbb{Z}_5(\theta)$ (where θ is called `g` in the code):

```
sage: F = GF(25, "g", modulus = x^2 - 2)
sage: g = F.gen()
sage: g^2
2
sage: 1/(1 + 3*g)
4*g + 2
```

Similarly to polynomials, we have a simplified syntax for creating both `F` and `g` simultaneously:

```
sage: F.<g> = GF(25, modulus = x^2 - 2)   # F = GF(...) and g = F.gen()
sage: g^2
2
sage: F.<g> = GF(25, modulus = x^2 - 3)   # another representation of GF(25)
sage: g^2
3
sage: (2*g)^2     # "above g" == "this 2*g"
2
sage: F.<g> = GF(25, modulus = x^2 - 4)   # it must be an irreducible polynomial
[...]
ValueError: finite field modulus must be irreducible but it is not
```

The elements can also be created from the list of coefficients, or from the representing polynomial:

```
sage: F.<g> = GF(27)      # cubic extension of Zmod(3) (any minimal polynomial)
sage: P.<x> = Zmod(3)[]   # representing polynomials
sage: F([1,1,2])
2*g^2 + g + 1
sage: F(2*x^2 + x + 1)
2*g^2 + g + 1
sage: P(2*g^2 + g + 1)
2*x^2 + x + 1
sage: P(2*g^2 + g + 1).list()
[1, 1, 2]
```

We can also create polynomial rings over finite fields, e.g. $\mathbb{F}_{25}[x]$ (which means that the coefficients of the polynomials are in $\mathbb{F}_{25}$, i.e. they are themselves represented by polynomials):

```
sage: F.<g> = GF(25, modulus = x^2 - 2)
sage: P.<x> = F[]
sage: P([1 + g, 3 + 2*g, 4*g, 2])
2*x^3 + 4*g*x^2 + (2*g + 3)*x + g + 1
sage: _.list()
[g + 1, 2*g + 3, 4*g, 2]
sage: (x-g)*(x-g-1)*(x-g-2)*(x-g-3)*(x-g-4)
x^5 + 4*x + 2*g
sage: _.roots()
[(g, 1), (g + 4, 1), (g + 3, 1), (g + 2, 1), (g + 1, 1)]
```

Not only finite fields, but also extensions of $\mathbb{Q}$ can be created, e.g. $\mathbb{Q}(\sqrt{2})$:

```
sage: F.<g> = NumberField(x^2 - 2)
sage: g^2
2
sage: 1/(5 + 2*g)
-2/17*g + 5/17
```

5 Advanced Encryption Standard (AES)

The **Advanced Encryption Standard (AES)** (originally called Rijndael) is one of the most popular cryptographic algorithms. It is used in a wide variety of places, including internet communication (e.g. HTTPS), disk encryption and the classified documents of the US government. Its popularity comes from not only its security, but also its high speed.

AES is a *symmetric-key* encryption, i.e. it uses the same key to encrypt and decrypt the message (as opposed to e.g. the RSA, which is *asymmetric*, see: Euler's totient and RSA).

The full algorithm of AES is not detailed here, as it is quite complicated, only some of its mathematically interesting parts. The full algorithm can be found in the specification: [3].

The message is split into 128-bit blocks, which are encrypted separately. Each such block has 16 bytes, which are written as a 4×4 matrix in column major order:

$$B = \begin{pmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{pmatrix}.$$

The bytes are represented as elements of the finite field $\mathbb{F}_{2^8} = \mathbb{F}_{256}$, where the primitive element $\theta \in \mathbb{F}_{256}$ is the root of the minimal polynomial $m = x^8 + x^4 + x^3 + x + \overline{1}$. The 8 bits are the coefficients of the representing polynomial, e.g. the byte [01001011] corresponds to $\theta^6 + \theta^3 + \theta + \overline{1} \in \mathbb{F}_{256}$.

One round of the encryption algorithm consists of four steps:

1. *SubBytes*: transforming each individual byte;
2. *ShiftRows*: shifting the rows cyclically;
3. *MixColumns*: multiplying the matrix by a constant matrix;
4. *AddRoundKey*: applying the key to the block.

The full algorithm runs these steps (with minor changes) 10-14 times (depending on the parameters). For decryption, the inverse steps are performed in reverse order. The four steps are detailed below.

5.1 AES: *SubBytes*

In this step, the bytes of the matrix are transformed independently from each other by an invertible function $S : \mathbb{F}_{256} \to \mathbb{F}_{256}$, without changing their place in the matrix (i.e. $\forall i : b'_i := S(b_i)$). This transformation is also called **Rijndael S-box** (S = substitution).

The transformation S works in two steps ($S(b) = S_2(S_1(b))$):

1. First, take the multiplicative inverse of the element in $\mathbb{F}_{256}$: $S_1(b) := b^{-1}$ – except for $b = 0$, which is not invertible, so let $S_1(0) := 0$.
2. The second step is an affine transformation, which is an exception in that it is not calculated in $\mathbb{F}_{256}$, but in another representation of the elements. It can be stated in two equivalent ways:
   (a) Using the polynomial representation of $b \in \mathbb{F}_{256}$ ($p_b = b_0 + b_1 x + \ldots + b_7 x^7 \in \mathbb{Z}_2[x]$):
   $$S_2(b) := \big(p_b \cdot (x^4 + x^3 + x^2 + x + 1)\big) \bmod (x^8 + 1) \quad + \quad (x^6 + x^5 + x + 1).$$
   (b) Using its coefficient vector ($v_b = (b_0, b_1, \ldots, b_7) \in \mathbb{Z}_2^8$), by a matrix multiplication ($\mathbb{Z}_2^{8\times 8}$):
   $$S_2(b) := \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$
   It is important to note again that for both representations, the bits (i.e. the polynomial coefficients or the vector components) are still in $\mathbb{Z}_2$, i.e. they are calculated modulo 2.

This S-box is the essence of AES: it is a *nonlinear* transformation (a linear transformation would be just a matrix multiplication), therefore it is very difficult to follow what happens with the bytes.

This transformation has only 256 possible values, so it is usually precalculated and stored in a table, to make encryption more efficient.

5.2 AES: *ShiftRows*

This step rearranges the bytes within the rows: the first row is unchanged, the second row is shifted left by one cyclically, the third row by two, and the fourth one by three, i.e.:

$$\begin{pmatrix} b_0 & b_4 & \underline{b_8} & \underline{\boldsymbol{b_{12}}} \\ b_1 & b_5 & \underline{b_9} & \underline{\boldsymbol{b_{13}}} \\ b_2 & b_6 & \underline{b_{10}} & \underline{\boldsymbol{b_{14}}} \\ b_3 & b_7 & \underline{b_{11}} & \underline{\boldsymbol{b_{15}}} \end{pmatrix} \longrightarrow \begin{pmatrix} b_0 & b_4 & \underline{b_8} & \underline{\boldsymbol{b_{12}}} \\ b_5 & \underline{b_9} & \underline{\boldsymbol{b_{13}}} & b_1 \\ \underline{b_{10}} & \underline{\boldsymbol{b_{14}}} & b_2 & b_6 \\ \underline{\boldsymbol{b_{15}}} & b_3 & b_7 & \underline{b_{11}} \end{pmatrix}$$

This ensures that the columns are mixed with each other, and not just independently manipulated.

5.3 AES: *MixColumns*

In this step, the 4×4 matrix is simply multiplied by a constant matrix (both are in $\mathbb{F}_{256}^{4\times4}$):

$$B' := \begin{pmatrix} \theta & \theta{+}1 & 1 & 1 \\ 1 & \theta & \theta{+}1 & 1 \\ 1 & 1 & \theta & \theta{+}1 \\ \theta{+}1 & 1 & 1 & \theta \end{pmatrix} B,$$

where $\theta \in \mathbb{F}_{256}$ is the primitive element defined above. The constants in the matrix were chosen to make multiplication faster (as bit sequences: $\overline{1} \to [00000001]$, $\theta \to [00000010]$, $\theta{+}\overline{1} \to [00000011]$).

The name of this step (*MixColumns*) indicates that this matrix multiplication is equivalent to multiplying each column vector of B independently by the same constant matrix.

This step ensures that the elements are not only rearranged and transformed separately, but they are also combined with each other (within the column).

5.4 AES: *AddRoundKey*

This step adds the current key to the block. The key is also a 128-bit sequence, which can be written in the same matrix form, so this step is just a matrix addition in $\mathbb{F}_{256}^{4\times4}$. Or equivalently, using bit sequences, it is a bitwise "exclusive or" (XOR) operation of the two 128-bit sequences.

The key is different in each round of the encryption (hence the name *RoundKey*), and it can be calculated from the master key, which is the input of the algorithm, and its length is between 128 and 256 bits (depending on the parameters). These calculations are omitted here.

The key is what makes the algorithm secure: anyone who knows it can easily decrypt the message, but for others, the encrypted text is just a meaningless sequence of bits. Without knowing the key, one has to check all of its possible values, which, even for the shortest 128-bit key, means $2^{128} = 340282366920938463463374607431768211456$ possibilities. This is practically impossible.

6 Author

This document was written by Uray M. János, partly using the following sources:

[1] https://en.wikipedia.org/wiki/Simple_extension

[2] Gonda János: Véges testek (2011) (Hungarian)

[3] US NIST (2001): Federal Information Processing Standards Publication: Advanced Encryption Standard (AES). https://doi.org/10.6028/NIST.FIPS.197-upd1

Errors and suggestions can be reported here: uray.janos@inf.elte.hu.