Math Background for AES

Math 4175

§4.6a. Finite Fields

In contrast to S-boxes in DES, which are apparently "random" substitutions, the AES S-box can be defined algebraically.

In order to explain this algebraic formulation, we need some background on Finite Fields.

Recall from section 1.3 that a (commutative) ring is a set S with two operations $+$ (addition) and $\cdot$ (multiplication) satisfying 10 properties:

§4.6a. (Commutative) Ring

1. For any $a, b \in S,\ a + b \in S$ (addition is closed)
2. For any $a, b \in S,\ a + b = b + a$ (addition is commutative)
3. For any $a, b, c \in S,\ (a + b) + c = a + (b + c)$ (associative)
4. For any $a \in S,\ a + 0 = a$ (0 is an additive identity)
5. For any $a \in S,\ a + (-a) = (-a) + a = 0$ (additive inverse)
6. For any $a, b \in S,\ ab \in S$ (multiplication is closed)
7. For any $a, b \in S,\ ab = ba$ (multiplication is commutative)
8. For any $a, b, c \in S,\ (ab)c = a(bc)$ (associative)
9. For any $a \in S,\ a1 = 1a = a$ (1 is a multiplicative identity)
10. For any $a, b, c \in S,\ (a + b)c = (ac) + (bc)$ and $a(b + c) = (ab) + (ac)$ (distributive)

§4.6a. Finite Field

Definition: A commutative ring S is called a field if satisfies one more additional property (called multiplicative inverse): for every non-zero element $a \in S$, there exists an element $b \in S$ such that $a \cdot b = 1$. In this case, we usually denoted it by F instead of S.

Examples of Fields:

1. $(\mathcal{Q}, +, \cdot)$
2. $(\mathcal{R}, +, \cdot)$
3. $(\mathbb{Z}_p, \oplus, \odot)$, where p is prime.

The following rings are NOT fields, why?

1. $(\mathbb{Z}, +, \cdot)$ *hint:* What is 2^{-1}?
2. $(\mathbb{Z}_n, \oplus, \odot)$ where n is composite.

§4.6a. Finite Field

Fields such as $\mathcal{Q}$ and $\mathcal{R}$ are infinite fields, whereas $\mathbb{Z}_p$ is a finite field.

There are finite fields which are not of the form $\mathbb{Z}_p$.

Indeed, there are finite fields with q elements if $q = p^n$ where p is a prime number and $n \geq 1$ is an integer.

On the other hand, it can be proved that if F is a finite field with q elements, then $q = p^n$ for some prime number p and positive integer n.

We are particularly interested in a field with $2^4 = 16$ and $2^8 = 256$ elements, because there are 16 possible binary nibbles and 256 possible binary bytes, where 1 nibble $=$ 4 bits and 1 byte $=$ 8 bits.

We will discuss on how to construct such a finite field.

§4.6a. Finite Field

- Let us start with a finite field $\mathbb{Z}_p$. Define $\mathbb{Z}_p[x]$ as the set of all polynomials in the indeterminate x with coefficients in $\mathbb{Z}_p$.
- For example, $f(x) = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$ and $g(x) = 4x^3 + 3x^2 + 2 \in \mathbb{Z}_5[x]$.
- As usual, we define the degree of f to be the highest exponent of f and denote it by deg(f). In the above example, deg(f) = deg(g) = 3.
- Since we are only interested in the case $p = 2$, we will restrict our attention to $\mathbb{Z}_2[x]$, though similar constructions hold for any prime number p.
- By defining the addition and multiplication of polynomials in the usual way (and reducing the coefficients modulo 2), we can see that $\mathbb{Z}_2[x]$ is a ring.
- For example if $f(x) = x^3 + x^2 + 1$ and $g(x) = x^2 + x + 1$ in $\mathbb{Z}_2[x]$, find $f(x) + g(x)$ and $f(x)g(x)$.

§4.6a. Finite Field

$$\begin{aligned} f(x) + g(x) &= (x^3 + x^2 + 1) + (x^2 + x + 1) \\ &= x^3 + 2x^2 + x + 2 \\ &= x^3 + x \end{aligned}$$

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

§4.6a. Finite Field

- Recall that given two integers $b \geq a$, one can find, by performing the long division, the quotient q and the reminder r such that $0 \leq r < b$ and $b = aq + r$.
- For example, $186 = (7)(26) + 4$.
- Similar to integers, if $\deg(g) \geq \deg(f)$, then by performing long division, one can find $q(x)$ and $r(x)$ such that either $r(x) = 0$ or $\deg(r) < \deg(f)$ and $g(x) = f(x)q(x) + r(x)$ (see next slide for an example).
- Just like integers, we say that $f(x)$ divides $g(x)$ in $\mathbb{Z}_2[x]$ (denoted by $f(x)|g(x)$ if $r(x) = 0$. In other words, $g(x) = f(x)q(x)$.

§4.6a. Finite Field

Example: Let $g(\mathbf{x}) = \mathbf{x}^5 + \mathbf{x}^3 + \mathbf{x}^2 + 1$ and $f(\mathbf{x}) = \mathbf{x}^3 + \mathbf{x}^2 + 1$ in $\mathbb{Z}_2[\mathbf{x}]$.

Find $q(\mathbf{x})$ and $r(\mathbf{x})$. (Remember that $-x^n = x^n$ in $\mathbb{Z}_2[x]$.)

$$
\begin{array}{r|llllll}
 & \mathbf{x}^2 & +\mathbf{x} & & & & \\
\hline
\mathbf{x}^3+\mathbf{x}^2+1 & \mathbf{x}^5 & +0\mathbf{x}^4 & +\mathbf{x}^3 & +\mathbf{x}^2 & +0\mathbf{x} & +1 \\
 & \mathbf{x}^5 & +\mathbf{x}^4 & +0\mathbf{x}^3 & +\mathbf{x}^2 & & \\
\cline{2-7}
 & & +\mathbf{x}^4 & +\mathbf{x}^3 & +0\mathbf{x}^2 & +0\mathbf{x} & +1 \\
 & & +\mathbf{x}^4 & +\mathbf{x}^3 & +0\mathbf{x}^2 & +\mathbf{x} & \\
\cline{3-7}
 & & & & & +\mathbf{x} & +1
\end{array}
$$

$q(\mathbf{x}) = \mathbf{x}^2 + \mathbf{x}$, $r(\mathbf{x}) = \mathbf{x} + 1$.

§4.6a. Finite Field

- Recall that an integer $p \in \mathbb{Z}$ $(p > 0)$ is called a prime number if there is no number greater than 1 that divides p (except of course p itself).
- Similarly a polynomial $f(x) \in \mathbb{Z}_2[x]$ is called irreducible if no other polynomial $h(x) \in \mathbb{Z}_2[x]$ with deg(h) > 0 that divides $f(x)$.
- Suppose that $f(x) \in \mathbb{Z}_p[x]$ with deg(f) $=$ n. Analogous to the construction of the ring $\mathbb{Z}_m$ (for example, $\mathbb{Z}_{26}$) from $\mathbb{Z}$ by defining the addition and multiplication modulo m, we can define a ring of polynomials "modulo $f(x)$" from $\mathbb{Z}_p[x]$, which is denoted by $\mathbb{Z}_p[x]/(f(x))$.
- Recall that $\mathbb{Z}_m$ has m elements $\{0, 1, \cdots, m-1\}$. Similarly $\mathbb{Z}_p[x]/(f(x))$ has p^n polynomials in $\mathbb{Z}_p[x]$ of degree at most $n-1$.
- Addition and multiplication in $\mathbb{Z}_p[x]/(f(x))$ are defined as in $\mathbb{Z}_p[x]$ followed by a reduction modulo $f(x)$, and so $\mathbb{Z}_p[x]/(f(x))$ is a ring.

§4.6a. Finite Field

Notice that $\mathbb{Z}_p$ is a field if p is a prime.

Fact: $\mathbb{Z}_p[x]/(f(x))$ is field if $f(x)$ is irreducible.

Example: Let us construct a field of $8 = 2^3$ elements starting with $\mathbb{Z}_2[x]$.

We need to find an irreducible polynomial of $f(x)$ degree 3. Notice that constant term cannot be zero, otherwise x divides $f(x)$.

There are four candidates:

$$
\begin{aligned}
f_1(x) &= x^3 + 1 \\
f_2(x) &= x^3 + x + 1 \\
f_3(x) &= x^3 + x^2 + 1 \\
f_4(x) &= x^3 + x^2 + x + 1
\end{aligned}
$$

§4.6a. Finite Field

Notice that $f_1(x)$ is reducilble, because $x^3 + 1 = (x + 1)(x^2 + x + 1)$.

Also $f_4(x)$ is reducible, because $x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1)$.

However, one can check that both $f_2(x)$ and $f_3(x)$ are irreducible, and hence we can use either of them.

For example, $\mathbb{Z}_2[x]/(x^3 + x + 1)$ is a field with 8 elements

$$\begin{aligned}&\{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}\\ &= \{000, 001, 010, 011, 100, 101, 110, 111\}\end{aligned}$$

Now the multiplication can be computed as follows:

$$\begin{aligned}(101) \cdot (111) &= (x^2 + 1)(x^2 + x + 1) = x^4 + x^3 + 2x^2 + x + 1\\ &= x^4 + x^3 + x + 1 = (x + 1)(x^3 + x + 1) + (x^2 + x)\\ &= x^2 + x = 110.\end{aligned}$$

§4.6a. Finite field

Since we are interested in a field of $16 = 2^4$ and $256 = 2^8$ elements, we need irreducible polynomials of degree 4 and 8 in $\mathbb{Z}_2[x]$.

There are exactly three irreducible polynomials of degree 4 in $\mathbb{Z}_2[x]$, which are:

$$x^4 + x + 1, \;\; x^4 + x^3 + 1, \;\; x^4 + x^3 + x^2 + x + 1.$$

Hence

$$F = \mathbb{Z}_2[x]/(x^4 + x + 1)$$

is a field with 16 elements.

There are 30 irreducible polynomials of degree 8 in $\mathbb{Z}_2[x]$. One can check that $x^8 + x^4 + x^3 + x + 1$ is one of them, and hence

$$F = \mathbb{Z}_2[x]/(x^8 + x^4 + x^3 + x + 1)$$

is a field with 256 elements.

§4.6a. Finite field

Notice that in the field $\mathbb{Z}_2[x]/(x^4 + x + 1)$, the 16 elements are represented by all 4-bits or by polynomials of degree at most 3 in $\mathbb{Z}_2[x]$.

For example, the 4-bit 1101 is equivalent to the polynomial $x^3 + x^2 + 1$.

Similarly, in the field $\mathbb{Z}_2[x]/(x^8 + x^4 + x^3 + x + 1)$, the 256 elements are represented either by all 8-bits or by polynomials of degree at most 7 in $\mathbb{Z}_2[x]$.

Recall that every non-zero element in a field has the multiplicative inverse. We need to know how to find the multiplicative inverses in the above fields, which is explained in the file inversepoly.pdf.