信息安全数学基础

第六章 有限域

聂旭云
信息与软件工程学院
电子科技大学

信息安全数学基础

有限域的运算

聂旭云
信息与软件工程学院
电子科技大学

有限域上元素的表示

- 有限域上元素的三种表示方法：
  - 多项式表示法
  - 本原元表示法
  - 伴随矩阵表示法

多项式表示法

设p是素数，$q = p^n$。只要找到F_p上一个n次不可约多项式$f(x)$，就有

$$F_q = F_p[x]/\langle f(x)\rangle,$$

取$f(x)$的一个根α，根据定理6.2.3，$F_p(\alpha) \cong F_q$，且$1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$是$F_p[\alpha]$在$F_p$上的一组基。

因此，F_q中的元素可以表示成F_p上α的次数小于n的多项式，其上的加法为多项式的加法，而乘法为模多项式$f(\alpha)$的乘法。

多项式表示法（续）

例6.3.1 给出有限域$\mathbf{F}_9$的元素表示，并给出$\mathbf{F}_9$的乘法表。

解：F_9可以看成是F_3通过添加一个二次不可约多项式的根α得到的2次扩张。$f(x)=x^2+1$是F_3上一个不可约多项式，设α是$f(x)$的一个根，即$f(\alpha)=\alpha^2+1=0$，则$1,\alpha$是F_9在F_3上的一组基，从而，F_9中的元素可以表示成F_3上α的次数小于2的多项式，即

$$F_9=\{0,1,2,\alpha,1+\alpha,2+\alpha,2\alpha,1+2\alpha,2+2\alpha\}$$

多项式表示法（续）

*	**0**	**1**	**2**	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$
2	0	2	1	2α	$2+2\alpha$	$1+2\alpha$	α	$2+\alpha$	$1+\alpha$
α	0	α	2α	2	$2+\alpha$	$2+2\alpha$	1	$1+\alpha$	$1+2\alpha$
$1+\alpha$	0	$1+\alpha$	$2+2\alpha$	$2+\alpha$	2α	1	$1+2\alpha$	2	α
$2+\alpha$	0	$2+\alpha$	$1+2\alpha$	$2+2\alpha$	1	α	$1+\alpha$	2α	2
2α	0	2α	α	1	$1+2\alpha$	$1+\alpha$	2	$2+2\alpha$	$2+\alpha$
$1+2\alpha$	0	$1+2\alpha$	$2+\alpha$	$1+\alpha$	2	2α	$2+2\alpha$	α	1
$2+2\alpha$	0	$2+2\alpha$	$1+\alpha$	$1+2\alpha$	α	2	$2+\alpha$	1	2α

本原元表示法

- 设ξ是F_q中的本原元，则$F_q=\{0,\xi,\xi^2,\cdots,\xi^{q-1}\}$。在本原元表示下，乘法很容易实现，但加法需要结合$F_q$的多项式表示来计算。
- 例6.3.2 设$F_9=F_3(\xi)$，其中ξ是F_9中的本原元，且ξ是多项式x^2+x+2的根，则有$F_9=\{0,\xi,\xi^2,\cdots,\xi^8\}$。注意到，若$\alpha^2+1=0$，则$\xi=1+\alpha$是多项式$x^2+x+2$的根，可建立对应关系：$\xi=1+\alpha$，$\xi^2=2\alpha$，$\xi^3=1+2\alpha$，$\xi^4=2$，$\xi^5=2+2\alpha$，$\xi^6=\alpha$，$\xi^7=2+\alpha$，$\xi^8=1$，就可以很方便计算$F_9$中的加法。

伴随矩阵表示法

- 设$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$，定义$f(x)$的伴随矩阵为

$$A=\begin{bmatrix}0 & 0 & 0 & \cdots & 0 & -a_0\\ 1 & 0 & 0 & \cdots & 0 & -a_1\\ 0 & 1 & 0 & \cdots & 0 & -a_2\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1}\end{bmatrix}$$

- 经过计算有，$f(x)=|xI-A|=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$，即$f(x)$是$A$的特征多项式。因此，$f(A)=A^n+a_{n-1}A^{n-1}+\cdots+a_1A+a_0I=0$，其中$I$是单位矩阵。所以$A$可以看作是$f(x)$的根。

有限域运算实现举例

例6.3.3考察阶为16的有限域F_{2^4}。容易验证多项式$f(x)=x^4+x+1$在F_2上不可约。设α是$f(x)$的一个根。因此有限域F_{2^4}可以表示为α的所有F_2次数小于4的多项式集合，即

$$F_{2^4}=\{a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0|a_i\in\{0,1\}\}$$

为方便起见，多项式$a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0$可以用长度为4的向量$(a_3a_2a_1a_0)$表示，且

$$F_{2^4}=\{(a_3a_2a_1a_0)|a_i\in\{0,1\}\}$$

有限域运算实现举例（续）

域F_{2^4}中算术的一些例子：

（1）域中元素相加，即为对应分量的简单相加，例如

$$(1011)+(1001)=(0010);$$

（2）要将域中元素(1101)与(1001)相乘，将它们做多项式乘法，再模去$f(\alpha)$取其余式：

$$\begin{aligned}(\alpha^3+\alpha^2+1)(\alpha^3+1) &= \alpha^6+\alpha^5+\alpha^2+1\\ &\equiv \alpha^3+\alpha^2+\alpha+1(\mathrm{mod}\, f(\alpha))\end{aligned}$$

因此(1101) ×(1001）=(1111);

（3）F_{2^4}的乘法单位元是（0001）；

（4）（1011）的逆元是（0101），因为：

$$\begin{aligned}(\alpha^3+\alpha+1)(\alpha^2+1) &= \alpha^5+\alpha^2+\alpha+1\\ &\equiv 1(\mathrm{mod}\, f(x))\end{aligned}$$

即(1011) × (0101)=(0001)。

GF（2^8）中运算的快速实现

- 域F_2上的8次不可约多项式$f(x)=x^8+x^6+x^5+x+1$，α是$f(x)$的一个根
- 有限域F_{2^8}可以表示为α的所有F_2次数小于8的多项式集合，即

$$F_{2^8}=\{a_7\alpha^7+a_6\alpha^6+a_5\alpha^5+a_4\alpha^4+a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0 | a_i \in \{0,1\}\}$$

- 每一个元素都与一个字节的比特串$a_7a_6a_5a_4a_3a_2a_1a_0$对应
- 可将每个字节表示为一个16进制数，即每4比特表示一个16进制数，代表较高位的4比特的符号仍在左边。例如，01101011可表示为6B
- 也可以用0-255这256个十进制整数来表示域中的元素
- 加法定义为二进制多项式的加法，且其系数模2
- 乘法定义为多项式的乘积模一个次数为8的不可约多项式

乘法的两种方法

- 直接模多项式$f(x)$
  - 需要64次GF(2)上乘法以及模多项式运算
- 建立乘法表
  - 需要256×256字节（64K）的存储空间
- 建立指数对数表
  - 512个字节的存储，每次乘法仅需要查表3次和1次加法

指数对数表的建立

- 域GF(256)中的元素用0-255这256个十进制整数来表示

（1）将元素‘02’表示成为α，依次计算$\alpha^i \bmod(f(\alpha))$，$i=0,1,\cdots,254$，将所得结果转变为十进制数，设为$\beta_i$，$i=0,1,\cdots,254$；如下表所示：

（2）建表。第一行为$0,1,\cdots,254,255$，第二行元素依次为β_i，$i=0,1,\cdots,254$。

由于$\alpha^0 \equiv \alpha^{255} \bmod(f(\alpha))$，约定第 2 行，第 255 列元素为 0。

i	0	1	2	3	$\cdots$	253	254	255
α^i	1	2	4	8	$\cdots$	233	177	0

指数对数表的建立（续）

（3）按所建表的第二行元素的大小进行重排列，如下表所示：

255	0	1	197	…	72	230	104
0	1	2	3	…	253	254	255

（4）将（3）中表的第一行放在（2）中表的第三行，即

序号	0	1	2	3	…	253	254	255
$(02)^i$	1	2	4	8	…	233	177	0
$\log_{(02)} i$	255	0	1	197	…	72	230	104

指数对数表的使用

例6.3.4 取F_2上的8次不可约多项式$f(x)=x^8+x^6+x^5+x+1$，α是$f(x)$的一个根。试求F_{2^8}中元素$\alpha+1$和$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+1$的乘积，并计算$\alpha+1$的逆元。

解：$\alpha+1$对应于“03”，$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+1$对应于“253”。通过查指数对数表可得$03=(02)^{197}$，$253=(02)^{72}$，因此，

$$(03)\cdot(253)=(02)^{197+72(mod\ 255)}=(02)^{14}=100。$$

“100”对应于$\alpha^6+\alpha^5+\alpha^2$，即

$$(\alpha+1)(\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+1)\equiv(\alpha^6+\alpha^5+\alpha^2)(mod\ f(\alpha))$$

- 由$03=(02)^{197}$，而$255-197=58$，所以$(03)^{-1}=(02)^{58}=222$。“222”对应于

$$\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2+\alpha,$$

- 即$(\alpha+1)^{-1}\equiv(\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2+\alpha)\ mod(f(\alpha))$。

感 谢 聆 听!

xynie@uestc.edu.cn