Advanced Mathematics

MiracleEEEE

December 9, 2017

Contents

1 多项式

1.1 多项式的定义

一个以 x 为变量的多项式定义在一个代数域 F，将函数 $A(x)$ 的表示为形式和：

$$A(x) = \sum_{i=0}^{n-1} a_j x^j$$

我们称 $a_0, a_1, \cdots, a_{n-1}$ 为如上多项式的系数，所有的系数都属于域 F。如果一个多项式 $A(x)$ 的最高次的非零系数是 a_k，那么称 $A(x)$ 的次数为 k，记入 $degree(A) = k$。任何一个大于一个多项式系数的次数的整数都是该多项式的次数界。

1.2 多项式的运算

1.2.1 多项式加法

我们在多项式上可以定义很多不同的运算。对于**多项式加法**，如果 $A(x)$ 和 $B(x)$ 是次数界为 n 的多项式，那么它们的和也是一个次数界为 n 的多项式 $C(x)$，对所有属于定义域的 x，都有 $C(x)=A(x)+B(x)$。也就是说，若 [898]

$$A(x)=\sum_{j=0}^{n-1}a_jx^j$$

和

$$B(x)=\sum_{j=0}^{n-1}b_jx^j$$

则

$$C(x)=\sum_{j=0}^{n-1}c_jx^j$$

其中对于 $j=0,1,\cdots,n-1$，$c_j=a_j+b_j$。例如，如果有多项式 $A(x)=6x^3+7x^2-10x+9$ 和 $B(x)=-2x^3+4x-5$，那么 $C(x)=4x^3+7x^2-6x+4$。

1.2.2 多项式乘法

两个次数界为 n 的多项式的乘积为一个次数界为 $2n-1$ 的多项式。

对于**多项式乘法**，如果 $A(x)$ 和 $B(x)$ 皆是次数界为 n 的多项式，则它们的**乘积** $C(x)$ 是一个次数界为 $2n-1$ 的多项式，对所有属于定义域的 x，都有 $C(x)=A(x)B(x)$。读者或许以前也学过多项式乘法，其方法是把 $A(x)$ 中的每一项与 $B(x)$ 中的每一项相乘，然后再合并同类项。例如，我们可以对两个多项式 $A(x)=6x^3+7x^2-10x+9$ 和 $B(x)=-2x^3+4x-5$ 进行如下的乘法：

$$\begin{array}{r}
6x^3+\ 7x^2-\ 10x+9\\
-2x^3\qquad\quad +\ 4x-\ 5\\
\hline
-30x^3-35x^2+50x-45\\
24x^4+28x^3-40x^2+36x\\
-12x^6-14x^5+20x^4-18x^3\\
\hline
-12x^6-14x^5+44x^4-20x^3-75x^2+86x-45
\end{array}$$

另外一种表示乘积 $C(x)$ 的方法是

$$C(x)=\sum_{j=0}^{2n-2}c_jx^j \tag{30.1}$$

其中

[899]

$$c_j=\sum_{k=0}^{j}a_kb_{j-k} \tag{30.2}$$

注意，$\text{degree}(C)=\text{degree}(A)+\text{degree}(B)$，意味着如果 A 是次数界为 n_a 的多项式，B 是次数界为 n_b 的多项式，那么 C 是次数界为 n_a+n_b-1 的多项式。因为一个次数界为 k 的多项式也是次数界为 $k+1$ 的多项式，所以通常称乘积多项式 C 是一个次数界为 n_a+n_b 的多项式。

对于两个 n 次多项式乘法，朴素的多项式乘法的时间复杂度为 $O(n^2)$。利用快速傅里叶变换算法可将时间复杂度优化到 $n\lg n$。

1.3 多项式的表示

1.3.1 系数表达

对一个次数界为 n 的多项式 $A(x)=\sum_{j=0}^{n-1}a_jx^j$ 而言，其系数表达是一个由系数组成的向量 $a=(a_0, a_1, \cdots, a_{n-1})$。

一般将向量作为列向量看待。

对于多项式在定点 x_0 的求值运算就是计算 $A(x_0)$ 的值。使用霍纳法则，可以在 $O(n)$ 的时间复杂度内完成求值运算。

900

$$A(x_0)=a_0+x_0(a_1+x_0(a_2+\cdots+x_0(a_{n-2}+x_0(a_{n-1}))\cdots))$$

由式子 (30.2) 推导出的系数向量 c 也称为输入向量 a 和 b 的卷积。表示成 $c=a\bigotimes b$。

1.3.2 点值表达

1. 点值表达的定义

一个次数界为 n 的多项式 $A(x)$ 的点值表达就是一个由 n 个点值对所组成的集合

$$\{(x_0,y_0),(x_1,y_1),\cdots,(x_{n-1},y_{n-1})\}$$

使得对 $k=0, 1, \cdots, n-1$，所有 x_k 各不相同，

$$y_k=A(x_k) \tag{30.3}$$

一个多项式可以有多种点值表达。

对一个用系数形式表达的多项式来说，在原则上计算其点值表达是简单易行的，因为我们所要做的就是选取 n 个不同 $x_0, x_1, \cdots, x_{n-1}$，然后对 $k=0, 1, \cdots, n-1$ 求出 $A(x_k)$。根据霍纳法则，求出这 n 个点值所需时间复杂度为 $\Theta(n^2)$。

如果选取复数单位根作为 x_k，就可以将其运行时间变为 $O(\lg n)$。对于一个点值表达的多项式，求它的在某个新点上的值得最简单的办法就是先把该多项式转换成系数表达，然后在新点处求值。

2. 插值运算

(a) 高斯消元

求值计算的逆(从一个多项式的点值表达确定其系数表达形式)称为插值。下面定理说明，当插值多项式的次数界等于已知的点值对的数目，插值才是明确的。

定理 30.1(插值多项式的唯一性) *对于任意 n 个点值对组成的集合 $\{(x_0, y_0), (x_1, y_1), \cdots, (x_{n-1}, y_{n-1})\}$，其中所有的 x_k 都不同；那么存在唯一的次数界为 n 的多项式 $A(x)$，满足 $y_k=A(x_k)$，$k=0, 1, \cdots, n-1$。* 901

证明 证明主要是根据某个矩阵存在逆矩阵。式(30.3)等价于矩阵方程

$$\begin{bmatrix}1 & x_0 & x_0^2 & \cdots & x_0^{n-1}\\ 1 & x_1 & x_1^2 & \cdots & x_1^{n-1}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 1 & x_{n-1} & x_{n-1}^2 & \cdots & x_{n-1}^{n-1}\end{bmatrix}\begin{bmatrix}a_0\\ a_1\\ \vdots\\ a_{n-1}\end{bmatrix}=\begin{bmatrix}y_0\\ y_1\\ \vdots\\ y_{n-1}\end{bmatrix} \tag{30.4}$$

左边的矩阵表示为 $V(x_0, x_1, \cdots, x_{n-1})$，称为范德蒙德矩阵，根据思考题 D-1，该矩阵的行列式值为

$$\prod_{0\leqslant j<k\leqslant n-1}(x_k-x_j)$$

因此，由定理 D.5，如果 x_k 皆不同，则该矩阵是可逆的(即非奇异的)。因此，给定点值表达，我们能够唯一确定系数 a_j：

$$a=V(x_0,x_1,\cdots,x_{n-1})^{-1}y$$ ■

我们可以利用高斯消元在 $O(n^3)$ 的时间内求出这些方程的解。

(b) 拉格朗日公式

一种更快的基于 n 个点的插值算法是基于如下拉格朗日公式：

$$A(x) = \sum_{k=0}^{n-1} y_k \frac{\prod_{j \neq k}(x - x_j)}{\prod_{j \neq k}(x_k - x_j)} \tag{30.5}$$

利用拉格朗日公式可以在 $O(n^2)$ 的时间复杂度内求出多项式 A 的所有系数。首先 $O(n^2)$ 求出

$$P(x) = \prod_j (x - x_j)$$

然后对于每个 k，分子部分等于 $\frac{P(x)}{x - x_k}$，分母部分可以 $O(n)$ 计算得到。

对于分子部分的计算：我们设 $A(x) = q(x)(x - x_k) + r$，$q(x)$ 为 $A(x)$ 除以 $(x - x_j)$ 的商，为一个 $n - 1$ 次多项式。考虑展开：

$$a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x^1 + a_0 x^0 = (x - x_k)(q_{n-2}x^{n-2} + q_{n-1}^x n - 1 + \cdots + q_1 x^1 + q_0 x^0)$$

将右边乘开，整理最后得到

$$\begin{aligned} &q_{n-2}x^{n-1} + q_{n-3}x^{n-2} + \cdots + q_0 x^1 = \\ &a_{n-1}x^{n-1} + (a_{n-2} + x_k q_{n-2})x^{n-2} + \cdots + (a_1 + x_k q_1)x^1 + (a_0 - r + x_k q_0)x^0 \end{aligned}$$

那么：

$$\begin{aligned} q_{n-2} &= a_{n-1} \\ q_{n-3} &= a_{n-2} + x_k q_{n-2} \\ &\cdots \\ q_0 &= a_1 + x_k q_1 \end{aligned}$$

$q(x)$ 的系数可以在 $O(n)$ 的时间内求出。总的时间复杂度为 $O(n^2)$。不过从数值稳定的角度来说，会受到较大浮点数误差的影响。

3. 点值表达下的加法乘法

(a) 加法

对许多多项式相关的操作，点值表达是很便利的。对于加法，如果 $C(x)=A(x)+B(x)$，则对任意点 x_k，满足 $C(x_k)=A(x_k)+B(x_k)$。更准确地说，如果已知 A 的点值表达 902

$$\{(x_0, y_0), (x_1, y_1), \cdots, (x_{n-1}, y_{n-1})\}$$

和 B 的点值表达

$$\{(x_0, y_0'), (x_1, y_1'), \cdots, (x_{n-1}, y_{n-1}')\}$$

（注意，A 和 B 在相同的 n 个位置求值），则 C 的点值表达是

$$\{(x_0, y_0 + y_0'), (x_1, y_1 + y_1'), \cdots, (x_{n-1}, y_{n-1} + y_{n-1}')\}$$

时间复杂度为 $O(n)$。

(b) 乘法

类似地，对于多项式乘法，点值表达也是方便的。如果 $C(x)=A(x)B(x)$，则对于任意点 x_k，$C(x_k)=A(x_k)B(x_k)$，并且对 A 的点值表达和 B 的点值表达进行逐点相乘，就可得到 C 的点值表达。不过，我们也必须面对这样一个问题，即 degree(C)＝degree(A)＋degree(B)；如果 A 和 B 次数界为 n，那么 C 的次数界为 $2n$。对于 A 和 B 每个多项式而言，一个标准点值表达是由 n 个点值对所组成。当我们把这些点值对相乘，就得到 C 的 n 个点值对，由于 C 的次数界为 $2n$，要插值获得唯一的多项式 C，我们需要 $2n$ 个点值对(参见练习 30.1-4)。因此，必须对 A 和 B 的点值表达进行“扩展”，使每个多项式都包含 $2n$ 个点值对。给定 A 的扩展点值表达

$$\{(x_0,y_0),(x_1,y_1),\cdots,(x_{2n-1},y_{2n-1})\}$$

和 B 的对应扩展点值表达：

$$\{(x_0,y_0'),(x_1,y_1'),\cdots,(x_{2n-1},y_{2n-1}')\}$$

则 C 的点值表达为

$$\{(x_0,y_0y_0'),(x_1,y_1y_1'),\cdots,(x_{2n-1},y_{2n-1}y_{2n-1}')\}$$

给定两个点值扩展形式的输入多项式，我们可以看到使其相乘而得到点值形式的结果需要 $\Theta(n)$ 时间，比采用系数形式表达的多项式相乘所需时间少得多。

2 复数

2.1 复数单位根

n 次单位复数根是满足 $\omega^n=1$ 的复数 w。n 次单位复数根恰好有 n 个：对于 $k=0,1,\cdots,n-1$，这些根是 $e^{2\pi ik/n}$。为了解释这个表达式，我们利用复数的指数形式的定义：

$$e^{iu}=\cos(u)+i\sin(u)$$

图 30-2 说明 n 个单位复数根均匀地分布在以复平面的原点为圆心的单位半径的圆周上。值

906

$$\omega_n=e^{2\pi i/n} \tag{30.6}$$

称为**主 n 次单位根**[⊖]，所有其他 n 次单位复数根都是 ω_n 的幂次。

n 个 n 次单位复数根 $\omega_n^0,\omega_n^1,\cdots,\omega_n^{n-1}$ 在乘法意义下形成一个群(参见 31.3 节)。该群与加法群($\mathbf{Z}_n$，＋)(整数模 n)具有相同的结构，因为 $\omega_n^n=\omega_n^0=1$意味着 $\omega_n^j\omega_n^k=\omega_n^{j+k}=\omega_n^{(j+k)\bmod n}$。类似地，$\omega_n^{-1}=\omega_n^{n-1}$。下面的引理给出了 n 次单位复数根的一些基本性质。

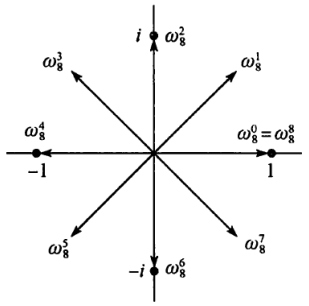

图 30-2 在复平面上 $\omega_8^0,\omega_8^1,\cdots,\omega_8^7$ 的值，其中 $\omega_8=e^{2\pi i/8}$ 是主 8 次单位根

2.1.1 复数单位根的运算性质

1. 消去引理

引理 30.3(消去引理) 对任何整数 $n\geqslant 0$，$k\geqslant 0$，以及 $d>0$，

$$\omega_{dn}^{dk}=\omega_n^k \tag{30.7}$$

证明 由式(30.6)可以直接推出引理，因为

907

$$\omega_{dn}^{dk}=(e^{2\pi i/dn})^{dk}=(e^{2\pi i/n})^k=\omega_n^k$$ ■

推论 30.4 对任意偶数 $n>0$，有

$$\omega_n^{n/2}=\omega_2=-1$$

2. 折半引理

引理 30.5(折半引理) 如果 $n>0$ 为偶数，那么 n 个 n 次单位复数根的平方的集合就是 $n/2$ 个 $n/2$ 次单位复数根的集合。

证明 根据消去引理，对任意非负整数 k，我们有 $(\omega_n^k)^2=\omega_{n/2}^k$。注意，如果对所有 n 次单位复数根进行平方，那么获得每个 $n/2$ 次单位根正好 2 次，因为

$$(\omega_n^{k+n/2})^2=\omega_n^{2k+n}=\omega_n^{2k}\omega_n^n=\omega_n^{2k}=(\omega_n^k)^2$$

因此，ω_n^k 与 $\omega_n^{k+n/2}$ 平方相同。我们也可以由推论 30.4 来证明该性质，因为 $\omega_n^{n/2}=-1$ 意味着 $\omega_n^{k+n/2}=-\omega_n^k$，所以 $(\omega_n^{k+n/2})^2=(\omega_n^k)^2$。■

这在 FFT 中是非常重要的。它保证了递归子问题的规模只是递归调用前的一半。

3. 求和引理

引理 30.6(求和引理) 对任意整数 $n\geqslant 1$ 和不能被 n 整除的非负整数 k，有

$$\sum_{j=0}^{n-1}(\omega_n^k)^j=0$$

908 **证明** 等式(A.5)既适用于实数，也适用于复数，因此有

$$\sum_{j=0}^{n-1}(\omega_n^k)^j=\frac{(\omega_n^k)^n-1}{\omega_n^k-1}=\frac{(\omega_n^n)^k-1}{\omega_n^k-1}=\frac{(1)^k-1}{\omega_n^k-1}=0$$

因为要求 k 不能被 n 整除，而且仅当 k 被 n 整除时 $\omega_n^k=1$ 成立，同时保证分母不为 0。■