快速傅里叶变换

By Yuekai Jia

【目的】

在$O(n\log_2 n)$的时间内，计算卷积$\boldsymbol{c}=\boldsymbol{a}\otimes\boldsymbol{b}$

$$c_i=\sum_{j=0}^{i}a_j\cdot b_{i-j}$$

【主要思想】

把$\boldsymbol{a}$看成一个n阶多项式$A(x)=a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1}$的系数。这个多项式可以用平面上$n$个点$\left\{\left(x_i,y_i^{[A]}\right)\middle|0\le i<n\right\}$唯一确定。其中$y_i^{[A]}=A(x_i)$。由此得到两个向量$\boldsymbol{x},\boldsymbol{y}^{[\boldsymbol{A}]}$。

再把$\boldsymbol{b}$也看成一个n阶多项式$B(x)$，通过求值得它的点值表示为$\left\{\left(x_i,y_i^{[B]}\right)\middle|0\le i<n\right\}$，其中$y_i^{[B]}=B(x_i)$。由此又得到一个向量$\boldsymbol{y}^{[\boldsymbol{B}]}$。

则两个多项式乘积$C(x)$的点值表示$\left\{\left(x_i,y_i^{[C]}\right)\middle|0\le i<n\right\}=\left\{\left(x_i,y_i^{[A]}y_i^{[B]}\right)\middle|0\le i<n\right\}$，其中$y_i^{[C]}=y_i^{[A]}y_i^{[B]}=C(x_i)$。把向量$\boldsymbol{y}^{[\boldsymbol{C}]}$称为$\boldsymbol{y}^{[\boldsymbol{A}]}$和$\boldsymbol{y}^{[\boldsymbol{B}]}$的点乘，记作$\boldsymbol{y}^{[\boldsymbol{C}]}=\boldsymbol{y}^{[\boldsymbol{A}]}\cdot\boldsymbol{y}^{[\boldsymbol{B}]}$。点乘显然可以$O(n)$求得。

再把点集$\left\{\left(x_i,y_i^{[C]}\right)\middle|0\le i<n\right\}$通过插值求出多项式$C(x)$的系数，即可得$\boldsymbol{a}$和$\boldsymbol{b}$的卷积$\boldsymbol{c}$。

对x_i取特定的值，即$x_i=\omega_i^{[n]}$，根据$\omega_i^{[n]}$的某些特殊性质，可以在$O(n\log_2 n)$的时间内用分治法进行快速傅里叶变换，对多项式进行求值和对点集进行插值。

【基本概念与定理】

- **单位复根：**

对于n，假设存在一个数$\omega^{[n]}$，记$\omega_k^{[n]} = \left(\omega^{[n]}\right)^k$，如果满足$\omega_n^{[n]} = 1$，且$\omega_k^{[n]}\ (1 \le k \le n)$互不相同，则称$\omega^{[n]}$为$n$的单位复根。

- **定理 1：**

如果$a \equiv b \pmod{n}$，有

$$\omega_a^{[n]} = \omega_b^{[n]} \tag{1}$$

- **证：**

a, b可以表示成

$$a = r + q_1 n, b = r + q_2 n\ (0 \le r < n, q_1, q_2 \in \mathbb{Z})$$

所以

$$\omega_a^{[n]} = \left(\omega^{[n]}\right)^{r+q_1 n} = \left(\omega^{[n]}\right)^r \cdot \left(\omega^{[n]}\right)^{q_1 n} = \omega_r^{[n]}$$

$$\omega_b^{[n]} = \left(\omega^{[n]}\right)^{r+q_2 n} = \left(\omega^{[n]}\right)^r \cdot \left(\omega^{[n]}\right)^{q_2 n} = \omega_r^{[n]}$$

$$\omega_a^{[n]} = \omega_b^{[n]}$$

- **定理 2(相消定理)：**

对于任何整数$d > 0$，有

$$\omega_{dk}^{[dn]} = \omega_k^{[n]} \tag{2}$$

- **证：**

$$\omega_{dk}^{[dn]} = \left(\omega^{[dn]}\right)^{dk} = \left(\omega_{dn}^{[dn]}\right)^{\frac{k}{n}} = 1^{\frac{k}{n}} = \left(\omega_n^{[n]}\right)^{\frac{k}{n}} = \omega_k^{[n]}$$

- **推论：**

对于任意偶数$n > 0$

$$\omega_{\frac{n}{2}}^{[n]} = \omega_1^{[2]}$$

而显然有$\omega_2^{[2]} = 1$，$\omega_1^{[2]} = -1$，所以

$$\omega_{\frac{n}{2}}^{[n]} = -1 \tag{3}$$

- **定理 3(折半定理)：**

  对于任意非负整数$k \in \left[0, \frac{n}{2}\right)$，有

$$\omega_{k+\frac{n}{2}}^{[n]} = -\omega_k^{[n]} \tag{4}$$

  - **证：**

$$\omega_{k+\frac{n}{2}}^{[n]} = \omega_k^{[n]} \cdot \omega_{\frac{n}{2}}^{[n]} = \omega_k^{[n]} \cdot -1 = -\omega_k^{[n]} \qquad \left(\text{根据式(3)}\right)$$

- **离散傅里叶变换(DFT)：**

  计算n阶多项式$A(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^n$在$x_k$处的值(求值)。

  令$x_k = \omega_k^{[n]}$，计算得

$$y_k = A\left(\omega_k^{[n]}\right) = \sum_{i=0}^{n-1} a_i \left(\omega_k^{[n]}\right)^i$$

  则称向量$\boldsymbol{y} = (y_0, y_1, \dots, y_{n-1})$为系数向量$\boldsymbol{a} = (a_0, a_1, \dots, a_{n-1})$的离散傅里叶变换，即$\boldsymbol{y} = \mathrm{DFT}_n(\boldsymbol{a})$。

  - **逆离散傅里叶变换($\mathbf{DFT^{-1}}$)：**

    根据值向量$\boldsymbol{y} = (y_0, y_1, \dots, y_{n-1})$，求出系数向量$\boldsymbol{a} = (a_0, a_1, \dots, a_{n-1})$(插值)，则称$\boldsymbol{a}$为$\boldsymbol{y}$的逆离散傅里叶变换，即$\boldsymbol{a} = \mathrm{DFT}_{\boldsymbol{n}}^{\boldsymbol{-1}}(\boldsymbol{y})$。

  - **卷积定理：**

    对于两个长度为n的向量$\boldsymbol{a}, \boldsymbol{b}$，它们的卷积$\boldsymbol{c} = \boldsymbol{a} \otimes \boldsymbol{b}$，则

$$\boldsymbol{c} = \mathrm{DFT}_{\boldsymbol{2n}}^{\boldsymbol{-1}}\left(\mathrm{DFT}_{\boldsymbol{2n}}(\boldsymbol{a}) \cdot \mathrm{DFT}_{\boldsymbol{2n}}(\boldsymbol{b})\right)$$

    其中n为2的幂次，不足的用0补。中间的乘号表示两个向量的点乘。

- **快速傅里叶变换(FFT)：**

  快速傅里叶变换使用分治法和单位复根的特殊性质，能在$O(n\log_2 n)$的时间内对$A(x)$求值，计算出$\mathrm{DFT}_n(\boldsymbol{a})$。

  - **算法：**

    令两个$\frac{n}{2}$阶的多项式

$$A^{[0]}(x) = a_0 + a_2x + a_4x^2 + \cdots + a_{n-2}x^{\frac{n}{2}-1}$$

$$A^{[1]}(x) = a_1 + a_3x + a_5x^2 + \cdots + a_{n-1}x^{\frac{n}{2}-1}$$

    则

$$A(x) = A^{[0]}(x^2) + xA^{[1]}(x^2)$$

    令

$$\boldsymbol{y}^{[0]} = \mathrm{DFT}_{\frac{n}{2}}(a_0, a_2, \dots, a_{n-2})$$

$$\boldsymbol{y}^{[1]} = \mathrm{DFT}_{\frac{n}{2}}(a_1, a_3, \dots, a_{n-1})$$

$$\boldsymbol{y} = \mathrm{DFT}_n(a_1, a_2, \dots, a_n)$$

则

$$y_k^{[0]} = A^{[0]}\left(\omega_k^{\left[\frac{n}{2}\right]}\right)$$

$$y_k^{[1]} = A^{[1]}\left(\omega_k^{\left[\frac{n}{2}\right]}\right)$$

根据定理 2(相消定理)，有$\omega_k^{\left[\frac{n}{2}\right]} = \omega_{2k}^{[n]}$，则

$$y_k^{[0]} = A^{[0]}\left(\omega_{2k}^{[n]}\right) = A^{[0]}\left(\left(\omega_k^{[n]}\right)^2\right)$$

$$y_k^{[1]} = A^{[1]}\left(\omega_{2k}^{[n]}\right) = A^{[1]}\left(\left(\omega_k^{[n]}\right)^2\right)$$

再根据定理 1 与定理 3(折半定理)，最后得

$$\begin{aligned}
y_k &= A\left(\omega_k^{[n]}\right) \\
&= A^{[0]}\left(\left(\omega_k^{[n]}\right)^2\right) + \omega_k^{[n]} A^{[1]}\left(\left(\omega_k^{[n]}\right)^2\right) \\
&= y_k^{[0]} + \omega_k^{[n]} y_k^{[1]} \\
y_{k+\frac{n}{2}} &= A\left(\omega_{k+\frac{n}{2}}^{[n]}\right) \\
&= A^{[0]}\left(\left(\omega_{k+\frac{n}{2}}^{[n]}\right)^2\right) + \omega_{k+\frac{n}{2}}^{[n]} A^{[1]}\left(\left(\omega_{k+\frac{n}{2}}^{[n]}\right)^2\right) \\
&= A^{[0]}\left(\omega_{2k+n}^{[n]}\right) + \omega_{k+\frac{n}{2}}^{[n]} A^{[1]}\left(\omega_{2k+n}^{[n]}\right) \\
&= A^{[0]}\left(\left(\omega_k^{[n]}\right)^2\right) - \omega_k^{[n]} A^{[1]}\left(\left(\omega_k^{[n]}\right)^2\right) \\
&= y_k^{[0]} - \omega_k^{[n]} y_k^{[1]}
\end{aligned}$$

- **逆快速傅里叶变换($\mathbf{FFT^{-1}}$)：**

逆快速傅里叶变换也用相似的方法，在$O(n\log_2 n)$的时间内对$\boldsymbol{y}$插值，计算出系数$\boldsymbol{a} = \mathrm{DFT}_n^{-1}(\boldsymbol{y})$。

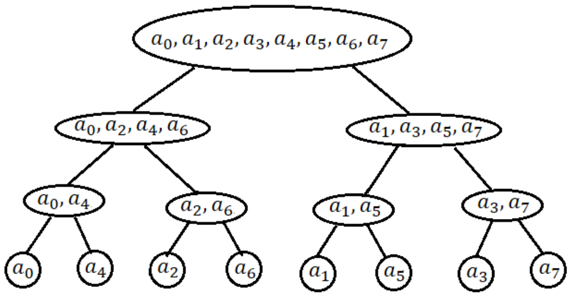
可以证明，

$$a_i = \frac{1}{n}\sum_{i=0}^{n-1} y_i \left(\omega_{-k}^{[n]}\right)^i$$

于是直接套用FFT即可，只需用$\omega_{-k}^{[n]}$替代$\omega_k^{[n]}$，最后答案除以n。

■ **非递归实现：**

如图，把序列的分割用一棵满二叉树表示，从底向上做，每次把两个区间的系数合并。



观察树的叶子节点上的数字，把它写成二进制，发现第i位的数的二进制正好是i的二进制数的逆序。

于是只需先预处理叶子节点是哪些系数，自底向上不断合并即可。

【实现】

具体实现时需要找出一个可以计算的满足单位复根性质的$\omega^{[n]}$，上述定理才能成立。对于$\omega^{[n]}$有如下两种形式：

● **复数：**

令

$$\omega^{[n]} = e^{\frac{2\pi i}{n}}, \omega_k^{[n]} = e^{\frac{2k\pi i}{n}}$$

即满足单位复根的性质。

■ **证：**

根据复数幂的定义

$$e^{ix} = \cos(x) + i\sin(x)$$

于是

$$\omega_n^{[n]} = \left(e^{\frac{2\pi i}{n}}\right)^n = e^{2\pi i} = \cos(2\pi) + i\sin(2\pi) = 1$$

且显然$\omega_k^{[n]}$互不相同。

● **原根(数论变换)：**

设质数$P = C \cdot 2^k + 1$ $\left(C, k\text{为常数，}2^k \geq n\right)$，$G$为$P$的一个原根，令

$$\omega^{[n]} = G^{\frac{P-1}{n}}, \omega_k^{[n]} = G^{\frac{(P-1)\cdot k}{n}} \pmod P$$

即满足单位复根的性质。

■ **证：**

根据原根的性质，有

$$\omega_n^{[n]} = \left(G^{\frac{P-1}{n}}\right)^n = G^{P-1} \equiv 1 \pmod{P}$$

且显然$\omega_k^{[n]}$互不相同。

【应用】

多项式乘法、高精度乘法、优化卷积式等。

【例题】

- **SPOJ**

  https://www.spoj.com/problems/MUL/

  https://www.spoj.com/problems/TMUL/

  https://www.spoj.com/problems/VFMUL/

  https://www.spoj.com/problems/TSUM/

- **BZOJ**

  http://www.lydsy.com/JudgeOnline/problem.php?id=2179 (VIP 专用)

  http://www.lydsy.com/JudgeOnline/problem.php?id=2194 (VIP 专用)

  http://www.lydsy.com/JudgeOnline/problem.php?id=2706