# 多项式 4

## 循环卷积

### 定义

$$c_k=\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}[i+j\bmod p=k]a_ib_j$$

### 性质

对序列 $A,B$ 做长度为 $n$ 的 $\text{FFT}$ 等价于求序列 $A,B$ 的循环卷积。

考虑单位根反演证明

$$ \begin{equation}\begin{split} c_k&=\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}[i+j\bmod p=k]a_ib_j\\ &=\frac 1n\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}\sum_{d=0}^{n-1}w_n^{d(i+j-k)}a_ib_j\\ &=\frac 1n\sum_{d=0}^{n-1}w_n^{-dk}\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}w_n^{di}a_iw_n^{dj}b_j\\ &=\frac 1n\sum_{d=0}^{n-1}w_n^{-dk}\left(\sum_{i=0}^{n-1}a_iw_n^{di}\right)\left(\sum_{j=0}^{n-1}b_jw_n^{dj}\right) \end{split}\end{equation} $$ 不难发现 $\left(\sum_{i=0}^{n-1}a_iw_n^{di}\right)\left(\sum_{j=0}^{n-1}b_jw_n^{dj}\right)$ 即为原来的 $\text{DFT}$ 过程$\frac 1n\sum_{d=0}^{n-1}w_n^{-dk}$ 即为原来的 $\text{IDFT}$证毕。

事实上普通的卷积计算相当于长度为 $2^n$ 的循环卷积计算，只是循环卷积长度大于 $C$ 序列的长度，所以循环卷积结果即为普通卷积结果。

### Bluestein's Algotithm

考虑 $\text{DFT}$ 过程，有

$$ \begin{equation}\begin{split} y_k&=\sum_{i=0}^{n-1}a_iw_n^{ki}\\ &=\sum_{i=0}^{n-1}a_iw_n^{{k+i\choose 2}-{k\choose 2}-{i\choose 2}}\\ &=w_n^{-{k\choose 2}}\sum_{i=0}^{n-1}\left(a_iw_n^{-{i\choose 2}}\right)w_n^{{k+i\choose 2}} \end{split}\end{equation} $$

其中 ${n\choose 2}$ 表示组合数。易知上式可以通过普通卷积求解$\text{IDFT}$ 过程类似。

值得一提的是，循环卷积的快速幂直接对 $\text{DFT}$ 的点值快速幂即可。

### 算法例题