1　多項式の評価

$A(x)$ を $n-1$ 次の多項式 $A(x) = a_0+a_1x^1+a_2x^2+\cdots+a_{n-1}x^{n-1}$ とする．$A(x)$ の係数の列を $a_A = (a_0, \ldots, a_{n-1})$ で表す．ここで一般性を失うことなく n は偶数であると仮定してよい；そうでないなら $n' = n+1$ 次の $A'(x)$ ただし $a_{A'} = (a_0, a_1, \ldots, a_{n-1}, 0)$, つまり n 次の係数は 0, を考える．すると,

$$\begin{aligned} A(x) &= a_0 + a_2x^2 + \cdots + a_{n-2}x^{n-2} + a_1x^1 + a_3x^3 + \cdots + a_{n-1}x^{x-1} \\ &= \sum_{i=0}^{n/2-1} a_{2i}x^{2i} + x \cdot \sum_{i=0}^{n/2-1} a_{2i+1}x^{2i} \end{aligned}$$

と書ける．ここで係数列 $(a_0, a_2, \ldots, a_{n-2})$ を持つ $\frac{n}{2}$ 次の多項式 A_0 と $(a_1, a_3, \ldots, a_{n-1})$ の A_1 を導入すれば, 上式は

$$A(x) = A_0(x^2) + x \cdot A_1(x^2)$$

と書き換えられる．$n = 2^k$ であれば, 深さ $k = \log n$ 段の再帰的な評価をおこなえば $A(x)$ が求まることになる．

2　多項式の評価による文字列パタン照合

$\Sigma = \{\sigma_0, \ldots, \sigma_{N-1}\}$ を有限アルファベット, それぞれ文字 $\sigma_i \in \Sigma$ は数値 $(\sigma_i) = \mathrm{e}^{\iota\frac{2\pi}{N}i}$ で表すとする．ただし ι は虚数単位 $\iota^2 = -1$．このとき, 同じ文字どうしのノルム積（内積）は，$(\sigma_i)^\dagger \cdot (\sigma_i) = 1$ となる．

$t, p \in \Sigma^*$ はそれぞれ長さ n, m で, かつ $n \geq m$ を満たすとする．また $t^\dagger$ で t の文字ごとの複素共役をとったものを表すとする．この t, p それぞれの多項式による表現を

$$T(x) = \sum_{i=0}^{n-1} (t_i)^\dagger \cdot x^i, P(x) = \sum_{i=0}^{n-1} (p_i) \cdot w_p(i) \cdot x^{n-1-i},$$

ただし

$$w_p(i) = \begin{cases} 1 & 0 \leq i < m\,, \\ 0 & \text{それ以外} \end{cases}$$

と定義する．

たとえばパタン $p = p_0 \cdot p_1 \cdot p_2$ がテキスト $t = t_0 \cdots t_4 \cdot t_5 \cdot t_6 \cdots t_{n-1}$ の位置 4 に出現する, すなわち $0 \leq i < m$ について $p_i = t_{4+i}$ であるかどうかは, 多項式

$$\begin{aligned} &(t_4)^\dagger x^4 (p_0) x^{n-1} + (t_5)^\dagger x^5 (p_1) x^{n-2} + (t_6)^\dagger x^6 (p_2) x^{n-3} \\ &= x^{n+3} \sum_{i=0}^{2} (t_{i+4})^\dagger \cdot (p_i) = x^{n+3} \sum_{i=0}^{n-1} (t_{(i+4) \bmod n})^\dagger \cdot (p_i) \cdot w_p(i) \end{aligned}$$

が $|p|\cdot x^{n+3}$ に等しいかどうかで調べることができる．すなわち，

$$M(x) = T(x)\cdot P(x) = x^n \sum_{j=0}^{n-1} x^{j-1}\cdot \sum_{i=0}^{n-1} (t_{i+j})^{\dagger}\cdot w_p(i)\cdot (p_i)$$

の x^{n-1+j} の項の係数をすべて求めれば, p が位置 j に出現しているかどうか判定できることになる.

3　FFT による文字列検索

$x = \mathrm{e}^{-\iota\frac{2\pi}{n}y}$ とおくと，$T(x)$ は

$$\tilde{T}(y) = \sum_{i=0}^{n-1} t_i^{\dagger}\cdot \mathrm{e}^{-\iota\frac{2\pi}{n}yi}$$

と書ける．この右辺は $t_i^{\dagger}$ の離散フーリエ変換であり, n を 0 埋めで 2 のべきにすれば, FFT が使用できる．$p_i w_p(i)$ についても同様に $\tilde{P}(y)$ が得られる．これらの y の次数ごとの積を, y の関数 から x の関数に戻すために逆フーリエ変換を行えば, ここでは x のノルムは 1 であるので, 各 x についての $M(x)$ のノルムを取ることで各次数の係数を求めることができる.

したがって, 全体のアルゴリズムは以下のようになる.

入力: 有限アルファベット $\Sigma = \{\sigma_0, \ldots, \sigma_{N-1}\}$ 上のテキスト $t \in \Sigma^*$ と パターン $p \in \Sigma^*$.

1. $n = 2^{\lceil \log \max\{|t|,|p|\}\rceil}$ とする.
2. t の各文字 σ_i を $\mathrm{e}^{-\iota\frac{2\pi}{N}i}$ で置き換え, 長さ n に不足する部分は 0 で埋めた列 $t^{\dagger}$ と, p の各文字を $\mathrm{e}^{\iota\frac{2\pi}{N}i}$ で置き換え，長さ n に不足する部分は 0 で埋めた列を逆順にした列 p^R を作る.
3. $t^{\dagger}$ と p^R それぞれを高速フーリエ変換して列 $\tilde{T}, \tilde{P}$ を得る.
4. $\tilde{T}$ と $\tilde{P}$ の要素ごとの積からなる列 $\tilde{M}$ を求める．($\tilde{M}(i) = \tilde{T}(i)\cdot\tilde{P}(i)$)
5. $\tilde{M}$ を逆高速フーリエ変換し列 M を得る.
6. $|M(i)| = |p|$ となる位置 i を枚挙する．出現位置は $i+1$ である.

以上により $O(n\log n)$ 時間で終了する.