Reeds-Sloane 算法

算法介绍

Reeds-Sloane 算法是 BM 算法的拓展，可以处理模任意正整数的递推式。

设环 $\mathbb{Z}/m\mathbb{Z}$ 上有一数列 $s_{0},s_{1},\cdots,s_{n-1}$，我们想要找到一个尽可能短的数列 $a_{0}=1,a_{1},\cdots,a_{l}$，使得 $\sum_{i=0}^{l}a_{i}s_{j-i}=0$ 对 $j=l,l+1,\cdots,n-1$ 成立。

不妨用多项式的语言来简单地定义一下递推式的长度：设 $a(x)=\sum_{i=0}^{l}a_{i}x^{i}$，$S(x)=\sum_{i=0}^{n-1}s_{i}x^{i}$，$a(x)S(x)\equiv b(x)\pmod{x^{n}}$，定义二元组 $A=(a(x),b(x))$，其长度 $L(A)=\max\{\deg(a(x)),\deg(b(x))+1\}$。当 $\deg(a(x))\le\deg(b(x))$ 时可能有些不好理解，这里可以当做是 a 后面补充了一些 0，以跳过开始若干不满足递推式的项。

中国剩余定理

设 $m=\prod p_{i}^{e_{i}}$，假设我们能够对每个 $p_{i}^{e_{i}}$ 求出递推式，那么对递推式的每一项做 crt 即可得到模 m 意义下的一个递推式，且显然长度不变。当然也容易证明不存在比这长度更短的递推式，否则对于递推式最长的那个质因子会产生矛盾。因此我们将问题归约到了模质数的幂。下面设模数为 p^{e}。

算法介绍

Reeds-Sloane 算法事实上解决了一个更加 general 的问题，即对每个 $\eta=0,1,\cdots,e-1$ 求出 $a(0)=p^{\eta}$ 时的最短递推式。算法的基本流程是对 s 的每个前缀依次处理。

首先定义几个记号，$a_{\eta}^{(k)}(x)$ 表示 $a(0)=p^{\eta}$ 时，$s_{0},\cdots,s_{k}$ 的递推式，$b_{\eta}^{(k)}(x)$ 是右边的余数，$A_{\eta}^{(k)}=(a_{\eta}^{(k)}(x),b_{\eta}^{(k)}(x))$，将 $\mathbb{Z}/p^{e}\mathbb{Z}$ 简记为 R，设 R 中可逆的元素为 R^{*}。

引理 1

设 $\mathscr{E}_{\eta}^{(k)}$ 表示所有满足 $a(x)S(x)\equiv b(x)\pmod{x^{k}}$，$a(0)=p^{\eta}$ 的二元组 $(a(x),b(x))$，$\mathscr{B}_{\eta}^{(k)}$ 表示所有满足 $a(x)S(x)\equiv b(x)+\theta p^{\eta}x^{k}\pmod{x^{k+1}}$ 的二元组 $(a(x),b(x))$，其中 $\theta\in R^{*}$。

设 $(a(x),b(x))\in\mathscr{E}_{\eta}^{(k)}$，$(c(x),d(x))\in\mathscr{B}_{u}^{(k-1)}$，且 $\eta+u<e$，那么 $L(a(x),b(x))+L(c(x),d(x))\ge k$。

证明：

$$ \begin{aligned} a(x)S(x)&\equiv b(x)\pmod{x^{k}}\\ c(x)S(x)&\equiv d(x)+\theta p^{u}x^{k-1}\pmod{x^{k}}\\ c(x)a(x)S(x)&\equiv a(x)d(x)+\theta p^{u}x^{k-1}a(x)\pmod{x^{k}}\\ c(x)b(x)-a(x)d(x)&\equiv\theta p^{u}x^{k-1}a(x)\pmod{x^{k}}

\end{aligned} $$

注意到等号右侧的最低次项是 x^{k-1}□系数为 $\theta p^{\eta+u}\not\equiv0$□因此 $$ \begin{aligned} \deg(c(x)b(x)-a(x)d(x))&\ge k-1\\ \max\{\deg(c(x)b(x)),\deg(a(x)d(x))\}&\ge k-1\\ \max\{\deg(c(x))+\deg(b(x))+1,\deg(a(x))+\deg(d(x))+1\}&\ge k\\ \max\{\deg(a(x)),\deg(b(x))+1\}+\max\{\deg(c(x)),\deg(d(x))+1\}&\ge k\\ L(a(x),b(x))+L(c(x),d(x))&\ge k\Box \end{aligned} $$

初始化

令 $a_{\eta}^{(0)}(x)=p^{\eta}$□$b_{\eta}^{(0)}=0$□$a_{\eta}^{(1)}(x)=p^{\eta}$□$b_{\eta}^{(1)}=p^{\eta}S_{0}$□$L(A_{\eta}^{(0)})=0$□定义 $S_{0}=\delta p^{\varepsilon}$□其中 $\delta\in R^{*}$□若 $\eta+\varepsilon<e$□$L(A_\eta^{(1)})=1$□否则 $L(A_\eta^{(1)})=0$□这两处的 L 显然是最小的。

另外我们定义 $\theta_{\eta k}$ 和 $u_{\eta k}$□满足 $S(x)a_{\eta}^{(k)}(x)\equiv b_{\eta}^{(k)}(x)+\theta_{\eta k}p^{u_{\eta k}}x^{k}\pmod{x^{k+1}}$□其中 $\theta_{\eta k}\in R^{*}$□$0\le u_{\eta k}\le e$□例如在初始化中，若 $\eta+\varepsilon<e$□那么可以令 $\theta_{\eta0}=\delta$□$u_{\eta0}=\eta+\varepsilon$□否则可以令 $\theta_{\eta0}=1$□$u_{\eta0}=e$□

递推计算

考虑对每个 η□计算 k 变化到 $k+1$ 时的答案。我们归纳地证明 $L(A_{\eta}^{(k)})$ 是最小的，以及 $L(A_{\eta}^{(k)})<L(A_{\eta}^{(k+1)})$ 时，存在一个 $0\le g<e$□使得$\eta+u_{gk}<e$□并且 $L(A_{\eta}^{(k+1)})=k+1-L(A_{g}^{(k)})$□

- 若 $u_{\eta k}=e$□那么令 $A_{\eta}^{(k+1)}=A_{\eta}^{(k)}$□显然 $\mathscr{E}_{\eta}^{(k+1)}$ 中的最短的元素要大于等于 $\mathscr{E}_{\eta}^{(k)}$ 中最短的元素，而我们又归纳假设 $A_{\eta}^{(k)}$ 是最短的元素，因此 $A_{\eta}^{(k+1)}$ 也是最短的元素。

- 若 $u_{\eta k}<e$□令 $g=e-1-u_{\eta k}$□并且记 $f(\eta,k)=g$□下面再分两种情况讨论：

  - 若 $L(A_{g}^{(k)})=0$□那么令 $A_{\eta}^{(k+1)}=A_{\eta}^{(k)}+(0,\theta_{\eta k}p^{u_{\eta k}}x^{k})$□显然有 $L(A_{\eta}^{(k+1)})=k+1$□

    由于 $L(A_{g}^{(k)})=0$□每个 $s_{0},\cdots,s_{k-1}$ 都是 p^{e-g} 的倍数，不妨设 $s_{i}=p^{e-g}s'_{i}(0\le i\le k-1)$□又由 θ_{gk} 和 u_{gk} 的定义有 $s_{k}p^{g}=\theta_{gk}p^{u_{gk}}$□从而有 $(p^{e-g}(s'_{0}+s'_{1}x+\cdots+s'_{k-1}x^{k-1})+\theta_{gk}p^{u_{gk}-g}x^{k})(p^{\eta}+\cdots)\equiv b_{\eta}^{(k)}(x)+\theta_{\eta k}p^{u_{\eta k}}x^{k}\pmod{x^{k+1}}$□

另外注意到 $b_{\eta}^{(k)}$ 是在 $\pmod{x^{k}}$ 意义下的，从而度数小于等于 $k-1$比较 x^{k} 的系数，有 $\alpha p^{e-g}+\theta_{gk}p^{u_{gk}+\eta-g}=\theta_{\eta k}p^{u_{\eta k}}$又由于 $e-g=u_{\eta k}+1$而 $\theta_{gk},\theta_{\eta k}\in R^{*}$因此 $u_{gk}+\eta-g\le u_{\eta k}$$u_{gk}+\eta\le e-1$另外有 $A_{\eta}^{(k+1)}\in\mathscr{E}_{\eta}^{(k+1)}$$A_{g}^{(k)}\in\mathscr{B}_{u_{gk}}^{(k)}$从而 $L(A_{\eta}^{(k+1)})+L(A_{g}^{(k)})\ge k+1$因此 $L(A_{\eta}^{(k+1)})$ 取到了最小值。

- 若 $L(A_{g}^{(k)})>0$那么一定存在唯一的一个 r 使得 $L(A_{g}^{(r)})<L(A_{g}^{(r+1)})=L(A_{g}^{(k)})$由归纳假设可知 $g+u_{hr}<e$又 $g=e-1-u_{\eta k}$从而 $u_{hr}\le u_{\eta k}$

  我们令 $a_{\eta}^{(k+1)}=a_{\eta}^{(k)}(x)-\theta_{\eta k}\theta_{hr}^{-1}p^{u_{\eta k}-u_{hr}}x^{k-r}a_{h}^{(r)}(x)$$b_{\eta}^{(k+1)}=b_{\eta}^{(k)}(x)-\theta_{\eta k}\theta_{hr}^{-1}p^{u_{\eta k}-u_{hr}}x^{k-r}b_{h}^{(r)}(x)$

  我们来验证 $a_{\eta}^{(k+1)}S(x)\equiv b_{\eta}^{(k+1)}(x)\pmod{x^{k+1}}$

  $$ \begin{aligned} a_{\eta}^{(k+1)}(x)S(x)&\equiv a_{\eta}^{(k)}(x)S(x)-\theta_{\eta k}\theta_{hr}^{-1}p^{u_{\eta k}-u_{hr}}x^{k-r}a_{h}^{(r)}(x)S(x)\\ &\equiv b_{\eta}^{(k)}(x)+\theta_{\eta k}p^{u_{\eta k}}x^{k}-\theta_{\eta k}\theta_{hr}^{-1}p^{u_{\eta k}-u_{hr}}x^{k-r}a_{h}^{(r)}(x)S(x)\\ &\equiv b_{\eta}^{(k)}(x)-\theta_{\eta k}\theta_{hr}^{-1}p^{u_{\eta k}-u_{hr}}x^{k-r}(-\theta_{hr}p^{u_{hr}}x^{r}+a_{h}^{(r)}(x)S(x))\\ &\equiv b_{\eta}^{(k)}(x)-\theta_{\eta k}\theta_{hr}^{-1}p^{u_{\eta k}-u_{hr}}x^{k-r}b_{h}^{(r)}(x)\\ &\equiv b_{\eta}^{(k+1)}(x)\pmod{x^{(k+1)}} \end{aligned} $$

  如果 $L(A_{\eta}^{(k)})=L(A_{\eta}^{(k+1)})$命题自然成立，下面假设 $L(A_{\eta}^{(k)})<L(A_{\eta}^{(k+1)})$

  根据归纳假设$L(A_{h}^{(r)})+L(A_{g}^{(r+1)})=r+1$我们来考虑 $L(A_{\eta}^{(k+1)})=(a_{\eta}^{(k+1)}(x),b_{\eta}^{(k+1)}(x))$ 的度数：

  $$ \begin{aligned} L(A_{\eta}^{(k+1)})&\le\max\{\deg a_{\eta}^{(k)}(x),\deg(\theta_{\eta k}\theta_{hr}^{-1}p^{u_{\eta k}-u_{hr}}x^{k-r}a_{h}^{(r)}(x)),\deg b_{\eta}^{(k)}(x),\deg(\theta_{\eta k}\theta_{hr}^{-1}p^{u_{\eta k}-u_{hr}}x^{k-r}b_{h}^{(r)}(x))\}\\ &\le\max\{\deg a_{\eta}^{(k)}(x),k-r+\deg a_{h}^{(r)}(x),\deg b_{\eta}^{(k)}(x),k-r+\deg

b_{h}^{(r)}(x)\}\\ &\le\max\{L(A_{\eta}^{(k)}),k-r+L(A_{h}^{(r)})\}\\ &=\max\{L(A_{\eta}^{(k)}),k+1-L(A_{g}^{(r+1)})\}\\ &=\max\{L(A_{\eta}^{(k)}),k+1-L(A_{g}^{(k)})\}\\ \end{aligned} $$

由于 $L(A_{\eta}^{(k)})<L(A_{\eta}^{(k+1)})$因此 $L(A_{\eta}^{(k+1)})\le k+1-L(A_{g}^{(k)})$考虑多项式 $q(x)=a_{\eta}^{(k)}(x)(a_{g}^{(k)}(x)S(x)-b_{g}^{(k)}(x))-a_{g}^{(k)}(x)(a_{\eta}^{(k)}(x)S(x)-b_{\eta}^{(k)}(x))=a_{g}^{(k)}(x)b_{\eta}^{(k)}(x)-a_{\eta}^{(k)}(x)b_{g}^{(k)}(x)$与引理 1 类似$\deg q(x)\le L(A_{\eta}^{(k)})+L(A_{g}^{(k)})-1\le k-1$但是注意到 $b_{\eta}^{(k)}(x)$ 和 $b_{g}^{(k)}(x)$ 中最低也只有 k 次项，因此 $q(x)=0$比较 x^{k} 项的系数可得 $p^{g+u_{\eta k}}\theta_{\eta k}-p^{\eta+u_{gk}}\theta_{gk}=0$因此 $g+u_{\eta k}=\eta+u_{gk}=e-1$与上一种情况类似$L(A_{\eta}^{(k+1)})\ge k+1-L(A_{g}^{(k)})$从而 $L(A_{\eta}^{(k+1)})=k+1-L(A_{g}^{(k)})$$\Box$

附注

两个实现时的数值分析与 BM 算法类似，从而有：对于一个由 k 阶矩阵转移而来的数列，至多需要 $2k$ 项即可由 RS 算法计算出递推式。

例题

暂时没有见到如此丧心病狂的出题人，不过应用场景与 BM 算法类似，可参考 BM 算法的例题。

参考文献

[1] Reeds J A, Sloane N J A. Shift register synthesis (modulo m)[J]. SIAM Journal on Computing, 1985, 14(3): 505-513.