21.11.06.

Ключевое уравнение

Пусть задан ряд по отрицательным степеням z (∞-й).

$$\frac{a_1}{z} + \frac{a_2}{z^2} + \ldots,$$

∃ Th в соотв. с кот. сформир. условия при кот. наши коэф. $a_1, a_2, \ldots$ можно построить ∞-ю ганкелеву м-цу ранга n.
Данный ряд должен быть выражен в виде правильной дроби, отношения полиномов

$$\frac{W(z)}{b(z)}$$

Степень полинома $b(z) = n$

Изначально примем что степень $W(z)$ на 1-цу < $b(z)$, хотя м/б и > на 1-цу.

$$\frac{a_1}{z} + \frac{a_2}{z_2} + \frac{a_3}{z^3} + \ldots = \frac{W(z)}{b(z)}$$

Выделим в левой части 2n членов по max кол-ву возможных ошибок в слове (n)

$$\frac{a_1}{z} + \frac{a_2}{z^2} + \ldots + \frac{a_{2n}}{z^{2n}} + \frac{a_{2n+1}}{z^{2n+1}} + \frac{a_{2n+2}}{z^{2n+2}} + \ldots = \frac{W(z)}{b(z)}$$

Вв. полином $A(z) = a_1 z^{2n-1} + a_2 z^{2n-2} + \ldots + a_{2n-1} z + a_{2n}$

$$\frac{A(z)}{z^{2n}} + Q(z) = \frac{W(z)}{b(z)}$$

$Q(z)$ – все остальные члены.

Определим произв-ие $b(z) \cdot A(z)$

$$b(z) \cdot A(z) = z^{2n}\left[W(z) + Q(z)b(z)\right]$$

Это все в поле F_{2^m}

Здесь $b(z) = b_0 z^n + b_1 z^{n-1} + \ldots + b_{n-1} z + b_n$

$$W(z) = W_0 z^{n-1} + W_1 z^{n-2} + \dots + W_{n-2} z + W_{n-1}$$

Заменим z на $\frac{1}{z}$

$$b\left(\frac{1}{z}\right) A\left(\frac{1}{z}\right) = \frac{1}{z^{2n}} \left[W\left(\frac{1}{z}\right) + Q\left(\frac{1}{z}\right) B\left(\frac{1}{z}\right) \right]$$

Умножим лев. и пр. части на z^{3n-1}, приведем к общему знам-лю элем-ы полиномов и получим для левой части.

инверсия коэф-ов!

$$z^{3n-1} \frac{\overleftarrow{b}(z)}{z^n} \cdot \frac{\overleftarrow{A}(z)}{z^{2n-1}} = \overleftarrow{b}(z) \overleftarrow{A}(z)$$

$$\overleftarrow{A}(z) = a_{2n} z^{2n-1} + a_{2n-1} z^{2n-2} + \dots + a_2 z + a_1$$

Аналогично преобр полиномы $b(z)$ и $W(z)$

Правая часть

$$z^{3n-1} \frac{1}{z^{2n}} \left[\frac{\overleftarrow{W}(z)}{z^{n-1}} + \overleftarrow{Q}(z) \cdot \frac{\overleftarrow{b}(z)}{z^n} \right] =$$

$$= z^{n-1} \overleftarrow{W}(z) + z^{n-1} \overleftarrow{Q}(z) \frac{\overleftarrow{b}(z)}{z^n}$$

$$Q(z) = \frac{a_{2n+1}}{z^{2n+1}} + \frac{a_{2n+2}}{z^{2n+2}} + \dots$$

$$\overleftarrow{Q}(z) = a_{2n+1} z^{2n+1} + a_{2n+2} z^{2n+2} + \dots = z^{2n+1} (a_{2n+1} + a_{2n+2} z + \dots)$$

Тогда прав. часть имеет вид

$$\overleftarrow{W}(z) + z^{2n} [a_{2n+1} + a_{2n+2} z + \dots] \overleftarrow{b}(z)$$

$$\overleftarrow{b}(z) \overleftarrow{A}(z) = \overleftarrow{W}(z) + z^{2n} b(z) [a_{2n+1} + a_{2n+2} z + \dots]$$

возьмем ур. по модулю z^{2n}

$$\boxed{\overleftarrow{b}(z) \overleftarrow{A}(z) = \overleftarrow{W}(z) \mod z^{2n}}$$

по модулю

Введем полином соотв-й синдрому

$$S(z) = S_1 + S_2 z + S_3 z^2 + \dots + S_{2n} z^{2n-1}, \quad n = \frac{m}{2}$$

n - max кол-во ошибок

Сравним $S(z)$ и $A(z)$ по структуре. Очевидно что в ур. $\overleftarrow{A}(z) = S(z)$, тогда $\sigma(z) = \overleftarrow{b}(z)$

Введем полином $\omega(z) = \overleftarrow{W}(z)$ и назовем его полиномом ошибок. тогда получим.

$$\sigma(z) = \omega(z) \bmod z^{2n}$$

Степень полинома $S(z) = 2n-1$, степень $\deg \sigma(z) = n$

Коэфф-ы $\omega(z)$ выражаются через коэфф. $\sigma(z)$ и $S(z)$

$\deg \omega(z) = n-1$

Данное ур. наз. ключевым ур. оно имеет полиномиальный вид, в кот. известен полином $S(z)$ и неизв-ы полином локатора $\sigma(z)$ и полином ошибок $\omega(z)$ поэтому для опред. величины и позиций ошибок необх. решение.

2 его способа

Примечание

Пусть кол-во ошибок не max и равно $\nu < n$, степень полинома $A(z)$ - неизм. А степень полин. $\sigma(z)$ будет ν.

Пусть $\deg W(z) = \nu - 1$

Тогда все рассужд-я ост-ся теми же, только ур. нужно умножать не на z^{3n-1}, а на $z^{2n+\nu-1}$, получим тоже самое?

$$\omega(z) = z\overleftarrow{W}(z)$$

Метод Сугиямы (Sugiyama)

Данный метод основан на нахождении НОД 2-х полиномов.

А. Алгоритм Евклида

Пусть $f(z)$ и $g(z)$ - 2 полинома, причем $\deg f(z) > \deg g(z)$, находим делим данные полиномы и находим неполное частное и остаток R. Продолжаем эти действия в соотв-ии со след-м порядком.

$$f(z) = g(z)\, q_1(z) + R_1(z)$$

$$g(z) = R_1(z)\, q_2(z) + R_2(z)$$

$$R_1(z) = R_2(z) \cdot q_3(z) + R_3(z)$$

$$R_2(z) = R_3(z) \cdot q_4(z) + R_4(z)$$

$$R_{k-3}(z) = R_{k-2}(z) \cdot q_{k-1}(z) + R_{k-1}(z)$$

$$R_{k-2}(z) = R_{k-1}(z) \cdot q_k(z) + R_k(z)$$

$$R_{k-1}(z) = R_k(z) \cdot q_{k+1}(z)$$

$R_k(z)$ — НОД

Т.к. $R_k(z)$ нацело делит $R_{k-1}(z)$, то он явл. НОД $f(z)$ и $g(z)$ - это и есть алгоритм Евклида.

Тогда можно записать:

$$R_k(z) = f(z)\, U(z) + g(z)\, V(z)$$

т.е. найдутся такие $U(z)$ и $V(z)$ что выполн. данное соотношение.

Данные ф-ции нах-ся итерационным методом.

$$U_i(z) = q_i(z)\, U_{i-1}(z) + U_{i-2}(z)$$

$$V_i(z) = q_i(z)\, V_{i-1}(z) + V_{i-2}(z)$$

Начальные условия имеют вид
$U_{-1} = 0$, $U_0 = 1$, $V_{-1} = 1$, $V_0 = 0$

8. Цепные дроби

Разложение НОЗ можно представить в виде полинома

$$h(z) = \frac{f(z)}{g(z)} \text{ – в виде цеп. дроби,}$$

$$h(z) = q_1(z) + \cfrac{1}{q_2(z) + \cfrac{1}{q_3(z) + \dots + \cfrac{1}{q_k(z) + \cfrac{1}{q_{k+1}(z)}}}}$$

$$h(z) = q_1(z) + \left(q_2(z) + \left(q_3(z) + \dots + \left(q_k(z) + q_{k+1}^{-1}(z)\right)^{-1}\right)^{-1} \dots\right)^{-1}$$

В записи через строку выделяются н.т. подходящие дроби h_i, которые образуются если ограничить q с заданным индексом

$$h_1 = q_1; \quad h_2 = q_1 + \frac{1}{q_2}; \quad h_3 = q_3 + \cfrac{1}{q_2 + \frac{1}{q_3}} \text{ и т.д.}$$

Учитывая нач. усл. для U и V, замечаем что $h_1 = q_1 = \frac{q_1}{1} = \frac{q_1 U_0 + U_{-1}}{q_1 V_0 + V_{-1}} = \frac{U_1}{V_1}$

$$h_2 = q_1 + \frac{1}{q_2} = \frac{q_1 q_2 + 1}{q_2} = \frac{q_2 U_1 + U_0}{q_2 V_1 + V_0} = \frac{U_2}{V_2}$$

и т.д.

По индукции можно доказать что

$$h_i = \frac{U_i}{V_i}$$

Далее рассматривая вид $h_i - h_{i-1}$ и устанавливая что $h_i - h_{i-1} = \frac{U_i V_{i-1} - U_{i-1} V_i}{V_i V_{i-1}} =$

$$= \frac{(-1)^i}{v_i v_{i-1}}$$

5. Матричное описание u_i и v_i

Рассмотрим систему итерационного соотношения u_i и v_i, и запишем её в виде

$$\begin{pmatrix} u_i \\ v_i \end{pmatrix} = \begin{pmatrix} u_{i-1} & u_{i-2} \\ v_{i-1} & v_{i-2} \end{pmatrix} \begin{pmatrix} q_i \\ 1 \end{pmatrix}$$

Заменим крайние векторы расширенными матрицами.

$$\begin{pmatrix} u_i & u_{i-1} \\ v_i & v_{i-1} \end{pmatrix} = \begin{pmatrix} u_{i-1} & u_{i-2} \\ v_{i-1} & v_{i-2} \end{pmatrix} \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}$$

М-цу в правой части можно записать аналогичным образом.

$$\begin{pmatrix} u_{i-1} & u_{i-2} \\ v_{i-1} & v_{i-2} \end{pmatrix} = \begin{pmatrix} u_{i-2} & u_{i-3} \\ v_{i-2} & v_{i-3} \end{pmatrix} \begin{pmatrix} q_{i-1} & 1 \\ 1 & 0 \end{pmatrix}$$

И. м. д. можно расписать м-цы во правой части $\Rightarrow$ справедливо выражение

$$\begin{pmatrix} u_i & u_{i-1} \\ v_i & v_{i-1} \end{pmatrix} = \prod_{j=1}^{i} \begin{pmatrix} q_j & 1 \\ 1 & 0 \end{pmatrix}$$

Назовем данные м-цы P_i

P_i можно определ. как левую и как правую ее часть. Определитель P_i = опред. м-цы в левой части, но из ур. Эйлера этот определитель = $u_i v_{i-1} - u_{i-1} v_i = (-1)^i = 1$ (F_{2m})

Найдем обратную м-цу P_i^{-1}

$$D_i^{-1} = \begin{pmatrix} v_{i-1} & -u_{i-1} \\ -v_i & u_i \end{pmatrix}$$

D. Матричное описание системы остатков.

Рассмотрим алгоритм Евклида. Очевидно что для 2-х последних строк справедливо выражение

$$\begin{pmatrix} R_{k-2} \\ R_{k-1} \end{pmatrix} = \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} R_{k-1} \\ R_k \end{pmatrix}$$

Запишем тоже самое для R_{k-3}, R_{k-2}

$$\begin{pmatrix} R_{k-3} \\ R_{k-2} \end{pmatrix} = \begin{pmatrix} q_{k-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} R_{k-2} \\ R_{k-1} \end{pmatrix}$$

Вместо столбца $\begin{pmatrix} R_{k-2} \\ R_{k-1} \end{pmatrix}$ можно поставить предыдущ. выраж. Если т.о. двигаться вверх, то придем к самой верхней строчке алгоритма.

$$\begin{pmatrix} f(z) \\ g(z) \end{pmatrix} = \prod_{j=1}^{k} \begin{pmatrix} q_j & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} R_{k-1} \\ R_k \end{pmatrix}$$

Очевидно что данную операцию можно было произвести с любой строки алгоритма и двигаться вверх. Поэтому остаток R_k может быть произвольным не обязательно НОД.

Очевидно что векторы связ-ся с помощью м-цы D_k. Найдем ее обратную м-цу по описанному ранее правилу.

И выразим остатки через нач. функции $f(z)$ и $g(z)$.

$$\begin{pmatrix} R_{k-1} \\ R_k \end{pmatrix} = \begin{pmatrix} v_{k-1} & -u_{k-1} \\ -v_k & u_k \end{pmatrix} \begin{pmatrix} f(z) \\ g(z) \end{pmatrix}$$

E. Нахождение $\sigma(z)$ и $w(z)$

Из вывод-го соотн.-ия => что $R_k = v_k f(z) + u_k g(z)$ (F_{2^m})

R_k может быть любым остатком, кон. их закончим.

Пусть $f(z) = z^{2t}$, а $g(z) = S(z)$, тогда $R_k = v_k z^{2t} + u_k S(z)$

пусть R_k такой остаток, что степень $\deg R_{k+1} > t$, $\deg R_k < t$.

Такой остаток наз. полуНОД.

При этом усл. возьмем получ-ое ур-я по модулю z^{2t}.

$R_k = u_k S(z) \bmod z^{2t}$

Запишем ключевое ур.

$$\boxed{w(z) = \sigma(z) S(z) \bmod z^{2t}}$$

Налицо сходство 2-х этих формул.

$w(z)$ также имеет степень ниже t

=> $w(z)$ полуНОД

$\deg \sigma(z)$ и u_k там не совпад.

$w(z) = \xi R_k(z)$ — ксч

$\sigma(z) = \xi u_k(z)$

R_k — это полуНОД при нахождении НОД ф-ции z^{2t} и $S(z)$

Начинаем искать НОД этих ф-ции и остан-ся когда находим полуНОД

$3^{10} + 45 + 45 \cdot 45 = 5^{15}$

При этом опред. все σ_i и интерпол-и методом находим $u_k(z) \Rightarrow \sigma(z)$.

Алгоритм Эвклида в F_{2^m} выполн. сложностью до поли. многоч-на $\Rightarrow$ здесь необх. выбрать ξ – масштабир. коэф. В больш. случ. его выбирают исходя из того условия что $\sigma_0 = 1$. После этого на ξ умнож. все коэф. $u(z)$.

22.11.06.

Структура произведения σS

Рассмотрим случай когда кол-во ошибок max $\Rightarrow$ полином $\sigma(z)$ имеет степень n и при этом $S(z)$ имеет степ $2n-1$

Перемн. в общ. виде 2 этих полин. можно предст-ть в виде Σ 3-х полиномов

$$\sigma(z) S(z) = R(z) + Q(z) + P'(z)$$ — не производная

$$R(z) = \sigma_0 S_1 + (\sigma_1 S_1 + \sigma_0 S_2) z + (\sigma_2 S_1 + \sigma_1 S_1 + \sigma_0 S_3) z^2 + \ldots + (\sigma_{n-1} S_1 + \sigma_{n-2} S_2 + \ldots + \sigma_1 S_{n-1} + \sigma_0 S_n) z^{n-1}$$

$$Q(z) = (\sigma_n S_1 + \sigma_{n-1} S_2 + \ldots + \sigma_1 S_n + \sigma_0 S_{n+1}) z^n + (\sigma_n S_2 + \sigma_{n-1} S_3 + \ldots + \sigma_1 S_{n+1} + \sigma_0 S_{n+2}) z^{n+1} + \ldots + (\sigma_n S_n + \sigma_{n-1} S_{n+1} + \ldots + \sigma_1 S_{2n-1} + \sigma_0 S_{2n}) z^{2n-1}$$

$$P'(z) = (\sigma_1 S_{2n} + \sigma_2 S_{2n-1} + \ldots + \sigma_n S_{n+1}) z^{2n} + (\sigma_2 S_{2n} + \sigma_3 S_{2n-1} + \ldots + \sigma_n S_{n+2}) z^{2n+1} + \ldots + (\sigma_{n-2} S_{2n} + \sigma_{n-1} S_{2n-1} + \sigma_n S_{2n-2}) z^{3n-1} + (\sigma_{n-1} S_{2n} + \sigma_n S_{2n-1}) z^{3n-2} + \sigma_n S_{2n} z^{3n-1}$$

Проанализируем данные полиномы