

Связь между производными σ_S

22.11.06г.

Рассмотрим случай, когда $\deg \sigma_S = \max$. \Rightarrow

$\deg \sigma(z) = n$, при этом $S(z)$ имеет степень $= 2n-1$. Перепишем их.

Прямым можно представить в виде суммы 3 полиномов.

$$\sigma(z) \cdot S(z) = R(z) + \Theta(z) + P'(z).$$

$$R(z) = \sigma_0 \sigma_1 + (\sigma_1 \sigma_1 + \sigma_0 \sigma_2) z + (\sigma_2 \sigma_1 + \sigma_1 \sigma_2 + \sigma_0 \sigma_3) z^2 + \dots + (\sigma_{n-1} \sigma_1 + \sigma_{n-2} \sigma_2 + \dots + \sigma_1 \sigma_{n-1} + \sigma_0 \sigma_n) z^{n-1}$$

$$\Theta(z) = (\sigma_n \sigma_1 + \sigma_{n-1} \sigma_2 + \dots + \sigma_1 \sigma_n + \sigma_0 \sigma_{n+1}) z^n + (\sigma_n \sigma_2 + \sigma_{n-1} \sigma_3 + \dots + \sigma_2 \sigma_{n+1} + \sigma_0 \sigma_{n+2}) z^{n+1} + \dots + (\sigma_n \sigma_n + \sigma_{n-1} \sigma_{n+1} + \dots + \sigma_0 \sigma_{2n}) z^{2n-1}$$

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

Искажем.

Доф. $\Theta(z)$ ур-ие из левостр. формы системы из левостр. системы, где коэф. σ_i всегда исполняют условие. $\Rightarrow \Theta(z) = 0$.

Рассмотрим $P'(z)$, в нем всевозможны для случая z^{2n} .

Замечу, что влече: $P'(z) = z^{2n} P(z)$. \Rightarrow

$\deg P'(z) = \deg P(z)$, в общем случае.

Замечу: $\sigma(z) \cdot S(z) = z^{2n} P(z) + R(z)$.



$$z^0 \quad z^1 \quad \dots \quad z^{n-1} \quad z^n \quad z^{n+1} \quad z^{2n-1} \quad z^{2n} \quad z^{2n+1} \quad z^{3n-1}$$

или указывать степени,
 0 - не указывать.

$$\sigma(z) \cdot S(z) = R(z) \pmod{z^{2n}}$$

$R(z)$ - остаток, $P(z)$ - изобретение.

$$\sigma(z)S(z) = \omega(z) \pmod{z^{2n}} \Rightarrow R(z) = \omega(z). \text{ Т.с. } R(z) - \text{это полином}$$

функции z^{2n} и $S(z)$.

Из исходного уравн. следует, что $\sigma(z) = z^{2n}P(z) : S(z)$ или $R(z)$.

Поступим аналогично методу Сувенира и инвертируем исходное уравнение.

$$\overleftarrow{\sigma}(z) \overleftarrow{S}(z) = z^{2n} \overleftarrow{R}(z) + \overleftarrow{P}(z).$$

$$\overleftarrow{\sigma}(z) = z^{2n} \overleftarrow{R}(z) : \overleftarrow{S}(z) \text{ или } \overleftarrow{P}(z).$$

Можно также найти $\sigma(z)$, если заранее известно изобретение или семейство.

Метод Тревина - Берлекемпа - Невси. (МТБН).

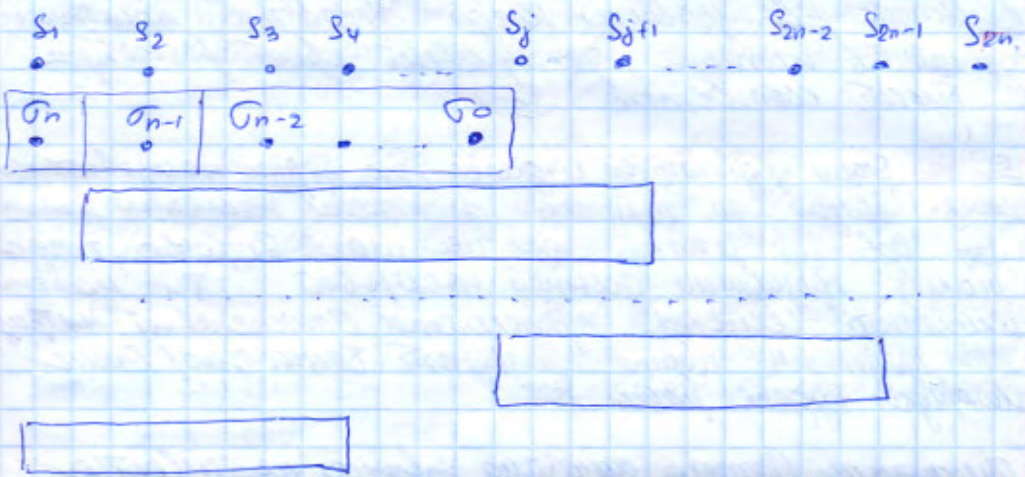
Запишем систему уравн. для коэффициентов уравн. с max. кол-ом ошибок.

$$\sigma_0 s_1 + \sigma_1 s_2 + \dots + \sigma_i s_n + \sigma_0 s_{n+1} = 0.$$

$$\sigma_0 s_2 + \sigma_1 s_3 + \dots + \sigma_i s_{n+1} + \sigma_0 s_{n+2} = 0.$$

$$\sigma_0 s_n + \sigma_{n-1} s_{n+1} + \dots + \sigma_1 s_{2n-1} + \sigma_0 s_{2n} = 0.$$

Построим „линейку“ из точек, соответ. коэффициентам уравн.



Рассмотрим, как все коэф. комбинации - индикатора извещия
 разместим их под точками - компонентами векторной, начиная с
 T_n с левого края. Перенесем S_i и T_i , меняя их местами
 друг друга. Система получится инвертированной. Очевидно, что
 получится перпендикулярность системы и
 система будет равна нулю. Пусть индикатор компонента T_i
 находит в своей системе в решетке. Сформируем решетку на
 одну позицию вперед и повторим тоже самое операцию.
 Тогда получим 2-ое ур-ие в системе две компоненты
 вектора, перемещая индикатор по решетке на одну позицию
 вперед и повторяем все операции будем перемещать от
 края вперед к другому, осуществляем шаг. В конце концов
 решетка займет крайнее правое положение, что
 будет светом, последн. ур-ие в цепи.
 Сдвинув решетку на одну позицию вперед, тогда
 индикатор коэф. можно определить поэлементно
 как произведение данных индикаторов. ИТД.
 Получим, что кол-во индикаторов $v < n$. \Rightarrow
 индикаторы T_i будут больше комбинации max длины.
 Расположим вначале лин-ки решетку с коэф.
 T_i длиной $v+1$. Прошамин будут самым высоким,
 начиная с первого ур-ия элемент индикатора
 в котором индикатор. меньше кол-во компонент вектора.
 Это индикатор сумма правых z_0 , то T_i составляем

компонент сигнала. Передвигаем последовательность решетки влево, при этом каждый раз получаем новые связи переходов от одного уровня к другому к следующему следующему уровню. Когда достигнем последнего уровня в решетке, то правильный ответ решетки будет соответствовать. §20

Еще мы будем продвигать это и далее, то будут использоваться рекуррентные связи до момента достижения последнего компонента. Сам сдвинем решетку еще на шаг влево, тогда реализуем предельный вариант и т.д. находим компонент сигнала. Предельный вариант реализации матрицы эти предельные можно трансформировать в единичную матрицу будет равен 0.

При анализе вектора сигнала заранее не известно коэф. α_i , кроме $\alpha_0 = 1$, остальных - неизвестно.

НТДМ предельный определим как то, что имеет в шире и контролируем количество элементов при каждом, также компонент вектора сигнала. При этом представляется мин. как то, что имеет и мин. элемент.

§21.

Получим, что коэф. α_i опре. неформ, тогда связи не контролируем и связь связана от 0. Назовем ее Δ - "неверка".

При реализации алгоритмов находим коэф., которые на k -том шаге (анализируем компоненту S_k) решетку с найденными коэф-ми должны реализовать все связи, начиная с начала сигнала и доходя до S_k и включая его.

Допустим, что найдено такие коэф. и составл. решетку, что реализуем все связи включая S_{j-1} . Предельный на j шаг выше и, допустим, что найденная связь Δ_j .

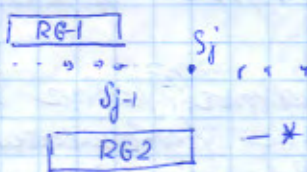
И 2 пути:

① Модифицировать коэф. в решетке

② Модифицируем эти коэф., с эффективным удлинением регистра.

Пусть такая модифицированная регистровая конструкция, получим "модифицированный регистр". Т.е. находясь вдоль линейки кончено сдвинутой с осью. Имеем регистров, который доходит до s_j -ной колонки и далее модифицируется.

Назовем модифициров. регистр в рассматр. точке S_j новым.
 А предыдущий, который дошел до точки S_{j-1} старым.
 Новый регистр рекур. все связи от какому до S_j включает.



Коэф. в регистре с осью. помним σ_{j-1} .
 Принцип системы нового коэф. в регистре
 с осью наименьшая степень полинома.

Рассмотрим следующий шаг. Для этого разделим старый регистр на шаг связей. Получим "неблизку" Δ_j .

* - правое край регистра совместились. Проделав новый регистр на шаг связей. В общем случае получаем "неблизку" Δ_{j+1} .
 Имеем все коэф. старого регистра на Δ_{j+1} . Тогда у него получим неблизку $\Delta_j \cdot \Delta_{j+1}$. Имеем все коэф. нового регистра на Δ_j . Тогда для них такая же получим неблизку $\Delta_j \cdot \Delta_{j+1}$. Каждому регистру с осью. помним, но, в результате сдвига, степени Z будут отличаться на единицу.

Для совпадения степеней * помним с осью, строку регистра на Z . Сложим получившим полиномы, при этом получим новый полином, который реализуем "связью", т.к. "неблизку" взаимосоизменяются при сдвиге.

(F_2^n). Новый модифицированный регистр (полином) реализуем все связи до S_{j+1} включительно. \Rightarrow модифицируем полинома. Величина произв-ся с помощью Z - старого и нового.

Рассмотрим старый регистр - разделим все его коэф. на "неблизку" этого полинома на данном шаге. Тогда у такого полинома "неблизку" $\Delta_j = 1$.

Обозначим старый полином P_k , тогда нормируем его \rightarrow
 $\rightarrow \Delta_j^{-1} P_k$. Тогда P_{k+1} не требуется возмущать на
 коэф. Это можно сделать с полиномом
 $\frac{\Delta_j^{j+1}}{\Delta_j} z P_k$

\rightarrow схема опер. нового полинома имеет итерационный
 вид \hookrightarrow имеет вид $z P_{j-1}$ как:

$$P_j(z) = P_{j-1}(z) + \Delta_j z P_{j-1}(z).$$

$P_{j-1}(z)$. В рассматриваемом нами случае $P_{j-1}(z) = \frac{P_{j-2}(z)}{\Delta_{j-1}}$.

Допустим что при условии z невелика \circ равна нулю.
 Т.е. старая формула P_{j-1} не возмущается, а
 только нормализуется. \Rightarrow Это значит, не нужно
 ничего предпринимать еще на один шаг, а
 старой полином надо модифицировать
 т.е. применить эффект (модифицировать \circ z).

Из этого, что степень полученного текущего полинома
 $P_j(z)$ опер. предполог. текущего не \leq $2j$ \circ $2j-1$.
 При этом, если L_1 - степень полинома, то
 при $2L_1 > j-1$, j -крать копиров. сдвинуто,
 степень нового полинома, не применяю еще
 $2L_1 > j-1$. При тех. как L_1 \circ $2j-1$ \circ $2j-1$
 \Rightarrow как-то \circ $2j-1$ \circ $2j-1$. При модифи-
 кации изменяется лишь коэф. степени z^j
 не \circ $2j-1$, \Rightarrow при \circ $2j-1$ \circ $2j-1$
 зуми \circ $2j-1$ \circ $2j-1$.

Если $2L_1 \neq j-1 \Rightarrow$ при модификации P_j нового
 полинома, изменялась \circ $2j-1$ \circ $2j-1$
 нужно \circ $2j-1$ \circ $2j-1$
 Возмем старый полином $P_j(z)$ немодифици-
 рованный \circ $2j-1$ \circ $2j-1$. Далее \circ $2j-1$ \circ $2j-1$
 при этом, при \circ $2j-1$ \circ $2j-1$
 надо \circ $2j-1$ \circ $2j-1$.
 Это можно сделать, как $L_1 := j-1$.

Процедура заканчивается когда решенный задан до последней неизвестной и сформулируются правые части σ_i , которые реализуют все сверху, начиная с начала списка. Сформулировав последние параметры — $\sigma_i(z)$.

Для того чтобы алгоритм работал, надо задать начальные условия. На первом шаге даны $F_0(z)$ поминем "минимален". Условно, это означает, что $\sigma_0(z) \text{ degree} = 1$. Поэтому примем $\sigma_0(z) = 1$. Тогда:

$$\Delta_1 = \sigma_0 \sigma_1 = \delta_1 \Rightarrow \text{в } \mu\text{-матрице. начен. параметра: } 1 + \delta_1 z.$$

Однако, если $\Delta_1 \neq 0$ (минимален на первом шаге) \Rightarrow требуется модифицировать старую "минимален" Δ_1^{-1} .

В процессе работы $\sigma_i(z)$: 1. может случиться $\Delta = 0$ на первом шаге. тогда переходим к следующему. сл. "нулевой" ($\delta_i = 0$).
 "нулевой" может означать нулевой и то время присутствующих в матрице.

Сен.

Циклические коды Рида-Солонсона в поле F_{2^4} .

примем $d=2$. Построим F_{2^4} , $n=15$. Выберем $n-k$ — чётному. пусть $k=9$. Пусть дано интервал. избыточные:

- 6, 4, 7, 7, 12, 13, 7, 5, 13

Построим в соответствии этому избыточно поминем \rightarrow

$$13z^8 + 5z^7 + 7z^6 + 13z^5 + 12z^4 + 7z^3 + 7z^2 + 4z + 6.$$

Этими поминем $6 = n - k = 15 - 9 = 6$. Поминем даны δ для матрицы. В матрицах элементов.

Пусть $V=1$, тогда $g(z) = (z+3)(z+4)(z+5)(z+6)(z+7)(z+8)$.

Если дан алгоритм, то получим поминем:

$$g(z) = z^6 + 12z^5 + 2z^4 + 8z^3 + 11z^2 + 15z + 3. \text{ — неавтоматический поминем.}$$

$$2^2, 2^3, \dots, 2^7 \leftarrow \alpha = 2.$$

Метод ТДН. Разлагает полином $\omega(z)$.

Полином $\omega(z)$ можно было бы разложить по известному полиному $S(z)$, с помощью

$$\sigma(z)S(z) = \omega(z) \pmod{z^n}$$

$\sigma(z) = \sigma_m$ - кол-во компонент вектора синдрома.

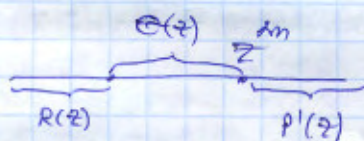
Однако в методе ТДН $\omega(z)$ разлаг. // с $S(z)$.

Рассмотрим формул. $S(z)$ на j -м шаге.

$$S_j(z) = S_{j-1}(z) + \Delta_j z^j G_{j-1}(z) \quad / + S(z)$$

Рассмотрим остаток от деления $S_j(z)$ на $S(z)$.

Было установлено, что она будет равна $\sigma_j z^j$ по модулю $S(z)$.



В идеале граница кодовой полинома единичного.

Возьмем следующий шаг, где σ по $\pmod{z^d}$.

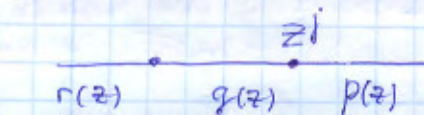
$$S_j(z) \cdot S(z) = \omega_j(z) \pmod{z^d}$$

$$S_{j-1}(z) S(z) + \Delta_j z^j G_{j-1}(z) S(z) \pmod{z^d} - \text{не нужен для вычисления.}$$

нужен только.

Отсюда $S_j(z) S(z)$ найдем, что и где $\sigma(z) S(z)$.

Обозначим остат. полином $r(z), q(z), p(z)$.



min степень z в $p(z)$ это z^d .

$$\Rightarrow \sigma_j(z) \cdot S(z) = \omega_j(z) \pmod{z^d}$$

возьмем произво $\omega_{j-1} \pmod{z^{d-1}}$.

$$\sigma_{j-1}(z) \cdot S(z) = \omega_{j-1}(z) \pmod{z^{d-1}}$$

Назовём полиномы для $\forall z$. σ и ω левые и правые результаты полиномов. ω левый - базисный, а σ правый - производный.

Продолжим структуру произв: $\Delta_j z \sigma_{j-1}(z) S(z)$.

$\sigma_{j-1}(z)$ - это, с точки зрения до упрощения множителя, $\sigma_k(z)$, которое можно считать $\sigma_{j-2}, z \sigma_{j-3}$. (см. предыдущую лекцию).

Тогда $z \sigma_k(z)$ имеет степень, соответствующую с базисным полиномом Δ или же с упрощением. \Rightarrow -но, рассматриваемое произв. по модулю z^d имеет этот базисный с точки зрения до упрощения множителя. \Rightarrow

или же производный $z \sigma_k(z) S(z)$. на предыдущем шаге $\omega_{j-1} \neq 0$. рассматривая $\sigma(z)$, когда на всех шагах $\omega_{j-1} \neq 0$.

\Rightarrow рассмотрим произв. $\sigma_j(z) S(z)$ на каждом шаге получим $g(z) = 0$

определённой степени. Эти случаи при $\forall \Delta_j = 0$. Будут означать окончание пути на Δ -ром уровне $\Delta = 0$. Это значит, что на предыдущем шаге получим такой полином σ_j , как при формальном произв. $S(z)$ как-то умнож Δ в $g(z)$. Иначе, чем если бы $\Delta \neq 0$. (Δ - это константа).

Допустим, что имеется несколько последовательных нулевых Δ . \Rightarrow согласно алгоритму, базисный полином становится нулевым, а производный полином становится по z .

Как-то умножая Δ обращаем, т.е. получим Δ в $g(z)$ когда-то законит полином $\rho(z)$. \neq который в Δ не имеет этот базисный $g(z)$. т.е. используем структуру полинома по z с $\Delta = 0$ в произв. так-же $\sigma(z) \cdot S(z)$.

\Rightarrow при тех же условиях, но вместо заданной преобр., можно р. \Rightarrow всегда существует такая преобр. по которой в заданных ω и σ канонически выражены σ_1 и ω_1 .

\Rightarrow Структура воиска. $\omega(z)$ там, где $\sigma(z)$.

Всегда можно $D_{j-1}(z), G_{j-1}(z)$ кан. вып. вып. σ_1 и ω_1 на степенях z .

Т.к. воиска. $\omega_j(z)$ можно записать в $G_j(z)$, то заданная каноническая ω должна канонически выражаться на степенях $\sigma(z)$. Делится вып. вып. канонически на $\sigma(z)$, где $\sigma(z)$. Это означает, что каноническая структура вып. вып.

Из условия каноничности. $\sigma(z) \delta(z)$, где $\delta(z)$ вып. вып.

$\sigma_1 \delta_1$, при $\delta_1 \neq 0 \Rightarrow$ во вып. вып. должно быть $\omega_1(z) = 0$.

$\sigma_1 \delta_1 = \sigma_1 \Rightarrow$ во вып. вып. $\omega_1(z) = 0$.

Заключает, что каноническая каноническая $\omega(z)$ на L каноническая $\sigma(z)$ каноническая, где во вып. вып. должно канонически выражаться z . \Rightarrow каноническая структура вып. вып.

$\omega_j(z) = \omega_{j-1}(z) + G_j D_{j-1}(z)$. Но при этом $D_0(z) = 1$.

Повторение степеней вып. вып. канонически реализуем при канонической канонической. В остальных вып. вып. $\omega(z)$ и $\sigma(z)$ вып. вып. каноническая. Если $\delta_1 = 0 \Rightarrow$ каноническая каноническая S_2 .

Структура канонической

Всегда каноническая каноническая каноническая $A(z)$ и $B(z)$ где каноническая $\sigma(z)$ и $\omega(z)$.

0) кан. вып. $\sigma_1(z) = 1; \omega_1(z) = 0; G_1(z) = 1; D_1(z) = 1; L = 0, \sigma_0 = 1$.

Целевыми векторами евр. $S(z)$.

1) 1-й компонент евриформа; $j_i = j_i + 1$.

2) Возвращаем индекс. $\Delta = \sum_{i=0}^L \sigma_i \cdot S_{j_i-1}$.

3) if $\Delta = 0$ и $j_i = m$, то EXIT.

4) $\Delta \neq 0 \Rightarrow$ возмем. искомым $A(z) = \sigma(z) + \Delta \cdot z^L C(z)$.
 $B(z) = \omega(z) + \Delta D(z)$.
обрати вним.
а тут нет!

5) $2L > j_i - 1 \Rightarrow \sigma(z) = A(z); \omega(z) = B(z)$.

$C(z) := z \cdot C(z); D(z) := z \cdot D(z)$ GOTO 1.

6) $2L < j_i - 1$ $C(z) := \Delta^{-1} \sigma(z); \sigma(z) := A(z)$.

$D(z) = \omega(z) \cdot z \cdot \Delta^{-1}; \omega(z) := B(z)$.

$L := j_i - L$.

GOTO 1.

При этом пробывав j после возмем. $A(z)$ и $B(z)$

Ели $j = m$, то $\sigma(z) := A(z); \omega(z) := B(z)$.

Коэф. при степенях степеней полинома $S(z)$.

$S_m \cdot S_{m-1} \cdot S_{m-2} \dots S_3 \cdot S_2 \cdot S_1$.

Сделаем стрелку на позицию векто. При этом
сделаем самую первую компоненту, а на
следующ. место стрелки запомним 0. Сделаем n
таких действий и получим матрицу разн. $(n+1) \cdot 2n$.

С помощью алгебр. Гаусса приведем эту матрицу к
треугольному виду, тогда к посл. строке,
есть все в единичке тех. Будет $\omega(z)$ с
помощью до постоянного коэф. При этом в предыдущих
строках полинома сесть единицам в порядке возраст. (с
помощью до) постоянн. коэф.)

$$\omega(z) = R(z).$$

Если все корни имеют нулевую часть, то $\omega(z)$ является функцией
и не имеет нулей. Если $\Im z_0 = 0$, то переставим
свое место вместе с сопряженным, который не является

Нахождение симметричных нулей.

Т.к. корни $\sigma(z)$ известны, то можем найти $\omega(z)$ с помощью
корней, а их обратные величины — это симметричные
симметричные нули. Если $\omega(z)$ имеет нули, то
корни $\sigma(z)$ имеют нули. Число (свойство).

Суть: в $\sigma(z)$ известна информация. Определим
уравнение $\sigma(z) = 0$. Для каждого корня $\sigma(z)$ имеем
 $\sigma(z) = 0$. Так как корни $\sigma(z)$ известны, то

Если $\sigma(z)$ имеет нули, то $\omega(z)$ имеет нули. Определим
уравнение $\sigma(z) = 0$. Для каждого корня $\sigma(z)$ имеем
 $\sigma(z) = 0$. Так как корни $\sigma(z)$ известны, то

Решение квадратного уравнения.

Пусть дано уравнение $Ax^2 + Bx + C = 0$

$$x^2 + Ax + B = 0; \text{ Сделаем } : x = Az.$$

$$z^2 + z + D = 0, \quad D = \frac{B}{A^2}$$

Здесь будем искать корень D .

$$z_r D = D + D^2 + \dots + D^r; \quad \theta = 2^{r-1} (F_r).$$

f, f^2, \dots, f^r . Возьмем в этом случае D .

$$D = c_0 f + c_1 f^2 + \dots + c_{r-1} f^r.$$

$$c_0 + c_1 + \dots + c_{r-1} = z_r D = 0.$$

Решение графика: z_j — углы в градусах,

$$z^I = \sum_{i=0}^{r-1} z_i j^{2i} \quad z^{II} = \sum_{i=0}^{r-1} \bar{z}_i j^{2i} \quad \bar{z}_i = 1 + z_i$$

$$z_0 = 0, z_1 = d_1, z_2 = d_1 + d_2 \dots z_j = z_{j-1} + d_j$$

Тогда решение в матриц. форме примем вид $z^I = (z_{r-1}, z_{r-2}, \dots, z_0) j$.

$$z^{II} = (\bar{z}_{r-1}, \bar{z}_{r-2}, \dots, \bar{z}_0) j \quad ; \quad \bar{z}_i = 1 + z_i$$

По известным разностям элем. в матриц. форме находим z^I и z^{II} (по табл) к-ые элем. ищем, а дальше находим $x_1 = Az^I, x_2 = Az^{II}$.

$$\binom{F_2}{F_4}, \quad r=15 \quad ; \quad \text{коэф-то кондин.} \quad \frac{15!}{2!(15-2)!} = \frac{15 \cdot 14}{2} = 105$$

коэф-то эл. D с нулевым элем. — 7. \Rightarrow
найдем 7 разл. пар корней.

$$7 \cdot 15 = 105$$

Решение кубического уравнения.

$$A_3 x^3 + A_2 x^2 + A_1 x + A_0 = 0 \quad / \quad \text{на } A_3 \Rightarrow$$

$$x^3 + Ax^2 + Bx + C = 0 \quad / \quad x = y - A/3$$

$$\Rightarrow y^3 + (B - \frac{1}{3}A^2)y + (C + \frac{2}{27}A^3 - \frac{1}{3}AB) = 0$$

$y^3 + ay + b = 0$ где найдем в иском F_2 иском все коэф. введ. по табл 2, при этом все возможные коэф. должны равны 1, а все остальные = 0, тогда

$$y^3 + ay + b = 0 \quad x = y + A, \quad a = B + A^2 \quad b = C + AB$$

$$y = \sqrt[3]{a} z$$

$$z^3 + z + E = 0 \quad ; \quad E = \frac{b}{a^{3/2}} \quad ; \quad y \text{ кубич. урав. таким элем. вводим кор-ть } E.$$

Несобх. унитарен \neq 3 корня в данном поле евр., тогда след

$\text{tr}_n \left(\frac{1}{E} \right) = \text{tr}_n 1$. Однако, \neq каждая унитар евр.-оп
несобх. и действителн. $P_1 = 0$. где $P_1 = E, P_2 = E, P_k = P_{k-1} + E^{k-3} P_{k-2}$.

Пусть унитар комплекситет, тогда

$$z = u + \frac{1}{u}, \Rightarrow u^2 + Eu^3 + 1 = 0.$$

$$u^3 = v \text{ или } u = \sqrt[3]{v}, \text{ тогда } v^2 + Ev + 1 = 0$$

$$\text{Введем новую переменную } v = EW. \quad W^2 + W + D = 0$$
$$D = \frac{1}{E^2}.$$

Здесь берем корни 2 унитар. евр.-оп / комплекс.

$$\textcircled{1} \text{ Несобх. унитар: } \text{tr} \frac{1}{E} = \text{tr} 1.$$

$$\textcircled{2} \text{tr} D = \text{tr} \left(\frac{1}{E^2} \right) = \text{tr} \frac{1}{E} = 0$$

Учтем что унитар собственн. несобх., тогда след $1 = 0$.

В поле \mathbb{F}_2 это выполняется.

Решим кв. уравн. u находим w_1 и w_2 . После
этого вычислим:

$$v_1 = EW_1, \quad v_2 = EW_2.$$

$$v^2 + Ev + 1 = 0;$$

$$v_1 v_2 = 1.$$

$$v_1 = \frac{1}{v_2}; \quad v_2 = \frac{1}{v_1}.$$

$$v_1 + v_2 = v_1 + \frac{1}{v_1} = v_2 + \frac{1}{v_2}.$$

$$\sqrt[3]{\sqrt[3]{y} + \frac{1}{\sqrt[3]{y}}} = \sqrt[3]{\sqrt[3]{y_1} + \frac{1}{\sqrt[3]{y_1}}} = \sqrt[3]{\sqrt[3]{y_2} + \frac{1}{\sqrt[3]{y_2}}}$$

$$z = u + \frac{1}{u}$$

Безразлично выберем какое D в системе Z .

Т.о. возьмем z_1, z_2, z_3 :

$$y_1 = \sqrt{a^T z}; \quad y_2 = \sqrt{a^T z_2}; \quad y_3 = \sqrt{a^T z_3}$$

$$x_1 = y_1 + A; \quad x_2 = y_2 + A; \quad x_3 = y_3 + A$$

$\frac{1}{x_1}; \frac{1}{x_2}; \frac{1}{x_3}$ удовлетв. невозв. в.м. у.м. может быть только.

$$E = 6 \text{ и } 11.$$

Кеша не так, будет лишнее число.

Семинар:

Алгоритм ТБМ.

Рассмотрим пример прошлой семинара методом ТБМ.

$$0) S_1 = 10, S_2 = 10, S_3 = 8, S_4 = 1, S_5 = 2, S_6 = 1.$$

$$j=0, L=0, G_0=1, w_0(z)=0; C(z)=1; D(z)=1, G_0(z)=1, m=6.$$

$$1) j=1. \quad \Delta_1 = \sum_{i=0}^0 \sigma_i S_{j-i} = G_0 S_1 = 1 \cdot 10 = 10 \neq 0. \quad \left| \begin{array}{l} \text{табл. умн. 10 на каждое} \\ \text{умн., чтобы получилось 1.} \\ \text{использ. 7.} \end{array} \right.$$

$$\Delta_1^{-1} = 7.$$

$$A_1(z) = G_0(z) + \Delta_1 z G_0(z) = 1 + 10z.$$

$$B_1(z) = w_0(z) + \Delta_1 P_0(z) = 10.$$

Проверка: $j \neq 6$ $2 \cdot 0 \neq 1 - 1$ ($2L > j - 1$).

$$C_1(z) = \Delta_1^{-1} G_0(z) = 7; \quad D_1(z) = \Delta_1^{-1} z \cdot w_0(z) = 7 \cdot z \cdot 0 = 0.$$

$$G_1(z) = A_1(z) z = 1 + 10z \Rightarrow G_0 = 1, G_1 = 10$$

$$w_1(z) = B_1(z) = 10 \quad L_1 = j - L_0 = 1.$$