В дополнение о цифровых (t, m, s)-сетях над простыми полями

Как известно, цифровые (t, m, s)-сети $\{\boldsymbol{x}_n\}_{n\in[0..b^m)}$ над простыми полями $\mathbb{F}_b$ полностью задаются s генерирующими матрицами, принадлежащими $\mathbb{F}_b^{m\times m}$, с помощью которых выражаются координаты любой точки сети с номером n по следующей формуле:

$$x_n[i] = \sum_{j=0}^{m-1}\left(\sum_{k=0}^{m-1}\gamma_{jk}[i]\cdot(n)_{b,k}\right)\cdot b^{-1-j}$$

Здесь

- $x_n[i]$ обозначает i-ю координату точки $\boldsymbol{x}_n$;
- $(n)_{b,k}$ – k-й разряд в разложении n в b-ичной системе счисления;
- $\gamma_{jk}[i]$ – элементы i-й генерирующей матрицы $\Gamma[i]$;

Наряду со значениями t, m, s и b для любой цифровой (t, m, s)-сети значимым характеризующим параметром является *параметр линейной независимости* совокупности её генерирующих матриц.

ОПРЕДЕЛЕНИЕ 1.1:

Параметром линейной независимости совокупности генерирующих матриц $\mathcal{S} = \{\Gamma[i],\ i \in [1\,..\,s]\}$, задающих цифровую сеть над конечным полем $\mathbb{F}_b$, называется такое максимальное $d \in \mathbb{Z}_{\geq 0}$, что $\forall\, d_i \in \mathbb{Z}_{\geq 0} : d = \sum_{i=1}^{s} d_i$ система вектор-строк $\left\{\Gamma_j[i] : j \in [0\,..\,d_i), i \in [1\,..\,s]\right\}$ является линейно-независимой. Будем обозначать параметр линейной независимости как $\rho(\mathcal{S})$.

Главным свойством параметра линейной независимости является следующая теорема.

ТЕОРЕМА 1.1:

Цифровая сеть над конечным полем $\mathbb{F}_b$, задаваемая совокупностью генерирующих матриц $\mathcal{S}$, будет являться (t, m, s)-сетью, где $t = m - \rho(\mathcal{S})$.

Понятия изоморфных сетей и достраивающей сети

ОПРЕДЕЛЕНИЕ 2.1:

Будем называть цифровые сети $\{\boldsymbol{x}_n\}_{n\in[0..b^m)}$ и $\{\widetilde{\boldsymbol{x}}_n\}_{n\in[0..b^m)}$ над $\mathbb{F}_b$ *изоморфными*, если они совпадают с точностью до *перестановки* точек. То есть, если существует такое биективное отображение

$$f:\ [0\,..\,b^m) \leftrightarrow [0\,..\,b^m),$$

что

$$\boldsymbol{x}_n = \widetilde{\boldsymbol{x}}_{f(n)} \quad \forall\, n \in [0\,..\,b^m).$$

Рассмотрим подробнее введённое отношение изоморфизма. Координаты двух изоморфных сетей будут связаны уравнениями

$$x_n[i] = \tilde{x}_{f(n)}[i], \qquad \forall\, n \in [0\,..\,b^m), i \in [1\,..\,s],$$

которые эквивалентны

$$\sum_{j=0}^{m-1}\left(\sum_{k=0}^{m-1}\gamma_{jk}[i]\cdot(n)_{b,k}\right)\cdot b^{-1-j} = \sum_{j=0}^{m-1}\left(\sum_{k=0}^{m-1}\tilde{\gamma}_{jk}[i]\cdot\big(f(n)\big)_{b,k}\right)\cdot b^{-1-j}$$

$$\sum_{k=0}^{m-1}\gamma_{jk}[i]\cdot(n)_{b,k} = \sum_{k=0}^{m-1}\tilde{\gamma}_{jk}[i]\cdot\big(f(n)\big)_{b,k}, \quad \forall\, j \in [0\,..\,m)$$

Рассмотрев эти уравнения для $n = b^l$, где $l \in [0\,..\,m)$, получим выражение

$$\gamma_{jl}[i] = \sum_{k=0}^{m-1}\tilde{\gamma}_{jk}[i]\cdot\Big(f(b^l)\Big)_{b,k}, \qquad \forall i,j,\forall\, l \in [0\,..\,m),$$

которую можно альтернативно описать следующим способом:

$$\gamma_{jl}[i] = \tilde{\Gamma}_j[i]\cdot\Phi^l, \qquad \forall i,j,l,$$

где

- $\tilde{\Gamma}_j[i]$ – это j-я строка матрицы $\tilde{\Gamma}[i]$;
- $\Phi^l = \left[\Big(f(b^l)\Big)_{b,0}, \Big(f(b^l)\Big)_{b,1}, \dots, \Big(f(b^l)\Big)_{b,m-1}\right]^T$

Подытожим проведённые рассуждения утверждением.

УТВЕРЖДЕНИЕ 2.1:

Цифровые сети над полем $\mathbb{F}_b$ $\{\boldsymbol{x}_n\}_{n\in[0..b^m)}$ и $\{\widetilde{\boldsymbol{x}}_n\}_{n\in[0..b^m)}$ можно считать изоморфными, если существует такая матрица $\Phi \in \mathbb{F}_b^{m\times m}$, что

$$\Gamma[i] = \tilde{\Gamma}[i] \cdot \Phi, \qquad \forall\, i \in [1\,..\,s]$$

ОПРЕДЕЛЕНИЕ 2.2:

Будем называть сеть $\{\widetilde{\boldsymbol{x}}_n\}_{n\in[0..b^{m+p})}$ *достраивающей сетью* для сети $\{\boldsymbol{x}_n\}_{n\in[0..b^m)}$, если начальный участок $\{\widetilde{\boldsymbol{x}}_n\}_{n\in[0..b^m)}$ изоморфен $\{\boldsymbol{x}_n\}_{n\in[0..b^m)}$.

Проведём рассуждения, аналогичные описанным выше. Координаты достраивающей сети связаны с координатами достраиваемой уравнениями

$$x_n[i] = \tilde{x}_{f(n)}[i], \qquad \forall\, n \in [0\,..\,2^m), i \in [1\,..\,s],$$

где f – это биекция вида $f : [0\,..\,2^m) \leftrightarrow [0\,..\,2^m)$.

Эти уравнения эквивалентны

$$\sum_{j=0}^{m-1}\left(\sum_{k=0}^{m-1}\gamma_{jk}[i]\cdot(n)_{b,k}\right)\cdot b^{-1-j} = \sum_{j=0}^{m+p-1}\left(\sum_{k=0}^{m+p-1}\tilde{\gamma}_{jk}[i]\cdot\big(f(n)\big)_{b,k}\right)\cdot b^{-1-j}$$

Учитывая, что $f(n) \in [0\,..\,b^m)$, для любых i справедливо следующее:

$$\sum_{j=0}^{m-1}\left(\sum_{k=0}^{m-1}\gamma_{jk}[i]\cdot(n)_{b,k}\right)\cdot b^{-1-j} = \sum_{j=0}^{m+p-1}\left(\sum_{k=0}^{m-1}\tilde{\gamma}_{jk}[i]\cdot\big(f(n)\big)_{b,k}\right)\cdot b^{-1-j}$$

Исходя из данных уравнений, для любого $i \in [1\,..\,s]$ составим систему

$$\begin{cases}\displaystyle\sum_{k=0}^{m-1}\tilde{\gamma}_{jk}[i]\cdot\big(f(n)\big)_{b,k} = \sum_{k=0}^{m-1}\gamma_{jk}[i]\cdot(n)_{b,k}\,, & j \in [0\,..\,m)\\ \displaystyle\sum_{k=0}^{m-1}\tilde{\gamma}_{jk}[i]\cdot\big(f(n)\big)_{b,k} = 0, & j \in [m\,..\,m+p)\end{cases}$$

Рассмотрим отдельно уравнения системы каждого из двух видов:

1. Положим в уравнениях первого вида $n = b^l$, где $l \in [0\,..\,m)$:

$$\gamma_{jl}[i] = \sum_{k=0}^{m-1}\tilde{\gamma}_{jk}[i]\cdot\Big(f(b^l)\Big)_{b,k}, \qquad l \in [0\,..\,m)$$

Альтернативно получившийся результат можно записать как уравнение

$$\gamma_{jl}[i] = \left[\tilde{\gamma}_{j0}[i], \tilde{\gamma}_{j1}[i], \dots, \tilde{\gamma}_{j,m-1}[i]\right] \cdot \Phi^l,$$

которое, ввиду справедливости для $j, l \in [0\,..\,m)$, можно обобщить до

$$\Gamma[i] = \mathrm{reduce}\left(\tilde{\Gamma}[i], m\right) \cdot \Phi, \qquad i \in [1\,..\,s]$$

где

- $\mathrm{reduce}\left(\tilde{\Gamma}[i], m\right)$ – это верхний левый блок размера $m \times m$ матрицы $\tilde{\Gamma}[i] \in \mathbb{F}_b^{(m+p)\times(m+p)}$;
- Φ – матрица $[\Phi^0, \Phi^1, \dots, \Phi^{m-1}]$, каждый столбец которой равен $\Phi^l = \left[\left(f(b^l)\right)_{b,0}, \left(f(b^l)\right)_{b,1}, \dots, \left(f(b^l)\right)_{b,m-1}\right]^T$.

2. Уравнения второго типа выполняются для любых n, в частности и для $n = f^{-1}(b^l)$, $l \in [0\,..\,m)$, для которых справедливо

$$\sum_{k=0}^{m-1} \tilde{\gamma}_{jk}[i] \cdot (b^l)_{b,k} = \tilde{\gamma}_{jl}[i] = 0, \qquad \forall\, l \in [0\,..\,m)$$

Таким образом, необходимо, чтобы первые m элементов в строках матрицы $\tilde{\Gamma}[i]$ с номерами $j \in [m\,..\,m+p)$ были равны нулю.

Подытожим проведённые рассуждения утверждением.

УТВЕРЖДЕНИЕ 2.2:

Если сеть $\{\tilde{\boldsymbol{x}}_n\}_{n\in[0..b^{m+p})}$ является достраивающей для сети $\{\boldsymbol{x}_n\}_{n\in[0..b^m)}$, то

1. Генерирующие матрицы $\tilde{\Gamma}[i]$, $i \in [1\,..\,s]$, первой сети имеют вид:

$$\begin{bmatrix}
\tilde{\gamma}_{0,0}[i] & \tilde{\gamma}_{0,1}[i] & \cdots & \tilde{\gamma}_{0,m-1}[i] & \tilde{\gamma}_{0,m}[i] & \cdots & \tilde{\gamma}_{0,m+p-1}[i] \\
\tilde{\gamma}_{1,0}[i] & \tilde{\gamma}_{1,1}[i] & \cdots & \tilde{\gamma}_{1,m-1}[i] & \tilde{\gamma}_{1,m}[i] & \cdots & \tilde{\gamma}_{1,m+p-1}[i] \\
\vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\
\tilde{\gamma}_{m-1,0}[i] & \tilde{\gamma}_{m-1,1}[i] & \cdots & \tilde{\gamma}_{m-1,m-1}[i] & \tilde{\gamma}_{m-1,m}[i] & \cdots & \tilde{\gamma}_{m-1,m+p-1}[i] \\
0 & 0 & \cdots & 0 & \tilde{\gamma}_{m,m}[i] & \cdots & \tilde{\gamma}_{m,m+p-1}[i] \\
0 & 0 & \cdots & 0 & \tilde{\gamma}_{m+1,m}[i] & \cdots & \tilde{\gamma}_{m+1,m+p-1}[i] \\
\vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\
0 & 0 & \cdots & 0 & \tilde{\gamma}_{m+p-1,m}[i] & \cdots & \tilde{\gamma}_{m+p-1,m+p-1}[i]
\end{bmatrix}$$

2. Начальный участок $\{\tilde{\boldsymbol{x}}_n\}_{n\in[0..b^m)}$ достраивающей сети, является сетью с генерирующими матрицами равными левым верхним блокам размера m на m матриц $\tilde{\Gamma}[i]$.

Об алгоритме Нидеррайтера и сетях Нидеррайтера

Опишем *алгоритм Нидеррайтера*, служащий для построения генерирующих матриц цифровых (t, m, s)-сетей над конечными полями $\mathbb{F}_b$.

АЛГОРИТМ 1 (НИДЕРРАЙТЕРА):

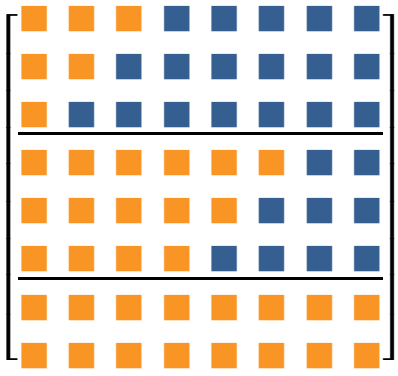
1. Выберем s многочленов $\pi[i]$ над полем $\mathbb{F}_b$;
2. Зададим поэлементно каждую генерирующую матрицу $\Gamma[i]$ элементами линейных рекуррентных последовательностей с *заданными* начальными значениями и с характеристическими многочленами $\pi^u[i]$ по следующему правилу:
   - Пусть $\{\alpha_l[i](u)\}$ – ЛРП с характеристическим многочленом $\pi^u[i]$. Тогда элементы $\gamma_{jk}[i]$ генерирующей матрицы $\Gamma[i]$ для любых j, $k \in [0\,..\,m)$ полагаются равными

$$\gamma_{jk}[i] = \alpha_{r_j[i]+k}[i]\big(u_j[i]\big),$$

где $u_j[i] \in \mathbb{Z}_{\geq 0}$, $r_j[i] \in [0\,..\deg \pi[i])$ такие, что

$$j = \big(u_j[i] - 1\big) \cdot \deg \pi[i] + r_j[i]$$

Довольно наглядно этот действие этого алгоритма можно изобразить графически. Для примера рассмотрим генерирующую матрицу $\Gamma[i]$ размера $m \times m$, где $m = 8$, ассоциированную с многочленом $\pi[i]$ степени 3:



На приведённом рисунке оранжевым цветом обозначены инициализирующие элементы ЛРП, а синим – элементы, вычисляемые рекуррентно.

Исследование свойств описанного алгоритма основывается на рассмотрении соотношений между формальными рядами Лорана от ω^{-1} над конечными полями. Прежде, чем перейти к дальнейшему рассмотрению алгоритма, уточним понятие формального ряда Лорана.

ОПРЕДЕЛЕНИЕ 3.2:

Формальным рядом Лорана от ω^{-1} называется выражение вида:

$$\sum_{l=w}^{+\infty} \alpha_l \cdot \omega^{-l}, \qquad \alpha_l \in \mathbb{F}_b, w \in \mathbb{Z}$$

Такие выражения называются формальными, поскольку они не представляют собой функцию от ω, а рассматриваются, как особенным образом записанные последовательности коэффициентов. Однако, в общем «невычисленном» виде формальные ряды Лорана являются обобщением как рациональных функций, так и многочленов над конечными полями. Относительно вводимых операций сложения и умножения, действующих аналогично таковым над многочленами, множество формальных рядов Лорана над $\mathbb{F}_b$ является *полем*, обозначаемым $\mathbb{F}_b\left((\omega^{-1})\right)$. Это множество включает в себя *поле* рациональных функций $\mathbb{F}_b(\omega)$, включающее в себя *кольцо* многочленов $\mathbb{F}_b[\omega]$.

ОПРЕДЕЛЕНИЕ 3.3:

Степенью формального ряда Лорана

$$\Lambda = \sum_{l=w}^{+\infty} \alpha_l \cdot \omega^{-l}, \qquad \alpha_l \in \mathbb{F}_b, w \in \mathbb{Z},$$

называется наибольшее целое число $\deg \Lambda$ такое, что

$$\Lambda = \sum_{l=-\deg \Lambda}^{+\infty} \alpha_l \cdot \omega^{-l}$$

Иными словами, степенью Λ называется такое целое число $\deg \Lambda$, что

$$\begin{cases} \alpha_l & = 0, \\ \alpha_{-\deg \Lambda} & \neq 0 \end{cases} \qquad \forall\, l < \deg \Lambda$$

Если формальный ряд Лорана Λ совпадает с многочленом π, то $\deg\Lambda = \deg\pi$. Степень произведения формальных рядов Лорана $\Lambda_1 \cdot \Lambda_2$ равняется сумме степеней множителей $\deg\Lambda_1 + \deg\Lambda_2$.

Если формальный ряд Лорана Λ совпадает с рациональной функцией $\rho = \pi/\tau$, где $\pi, \tau \in \mathbb{F}_b[\omega]$, то $\deg\Lambda = \deg\pi - \deg\tau$ (так как $\pi = \Lambda \cdot \tau$).

Формальные ряды Лорана являются замечательным инструментом для исследования свойств ЛРП по той причине, что любая ЛРП над полем $\mathbb{F}_b$ может быть задана, как последовательность коэффициентов формального ряда Лорана. Сформулируем строго это утверждение, с доказательством которого можно ознакомиться в Приложении А.

ТЕОРЕМА 3.1:

Пусть $\{\alpha_l\}$ – ЛРП над полем $\mathbb{F}_b$ с характеристическим многочленом μ вида

$$\mu(\omega) = \omega^m - \mu_{m-1}\omega^{m-1} - \mu_{m-2}\omega^{m-2} - \cdots - \mu_1\omega - \mu_0$$

Тогда существует единственный многочлен τ степени $d < m$ такой, что

$$\tau(\omega) = \tau_d\omega^d + \tau_{d-1}\omega^{d-1} + \tau_{d-2}\omega^{d-2} + \cdots + \tau_1\omega + \tau_0,$$

$$\frac{\omega\,\tau(\omega)}{\mu(\omega)} = \sum_{l=0}^{+\infty} \alpha_l \cdot \omega^{-l}$$

Притом начальные значения ЛРП и коэффициенты многочлена τ связаны следующей системой уравнений:

$$\begin{cases} 0 = \alpha_l, & l \in [0\,..\,m-1-d) \\ \tau_d = \alpha_{m-d-1} & \\ \tau_{d-1} = \alpha_{m-d} + \mu_{m-1}\alpha_{m-d-1} & \\ \tau_{d-2} = \alpha_{m-d+1} + \mu_{m-1}\alpha_{m-d} + \mu_{m-2}\alpha_{m-d-1} & \\ \vdots & \\ \tau_0 = \alpha_{m-1} + \mu_{m-1}\alpha_{m-2} + \mu_{m-2}\alpha_{m-3} + \cdots + \mu_{m-d}\alpha_{m-d-1} & \end{cases}$$

Описанных положений достаточно для того, чтобы сформулировать одну из важнейших теорем, описывающих алгоритм Нидеррайтера.

ТЕОРЕМА 3.2 (НИДЕРРАЙТЕРА):

Пусть $m \in \mathbb{Z}_{\geq 0}$, а также

1. Многочлены $\pi[i] \in \mathbb{F}_b[\omega]$, $i \in [1\,..\,s]$ попарно взаимно просты и удовлетворяют условию $\sum_{i=1}^{s}(\deg \pi[i] - 1) \leq m$;
2. Для любых $i \in [1\,..\,s]$ и $u \in [\,1\,..\,\lceil m/\deg \pi[i] \rceil\,]$ многочлены $\tau_u[i] \in \mathbb{F}_b[\omega]$, взаимно просты с $\pi[i]$.

Тогда с помощью коэффициентов формальных рядов Лорана вида:

$$\frac{\omega^{r+1}\,\tau_u[i](\omega)}{\pi^u[i](\omega)} = \sum_{l=w}^{+\infty} \alpha_l[i](u) \cdot \omega^{-l}, \qquad w \in \mathbb{Z}$$

возможно поэлементно задать генерирующие матрицы $\Gamma[i] \in \mathbb{F}_b^{m \times m}$ цифровой (t, m, s)-сети с $t = \sum_{i=1}^{s}(\deg \pi[i] - 1)$ следующим образом:

$$\gamma_{jk}[i] = \alpha_{r_j[i]+k}[i]\big(u_j[i]\big), \quad j, k \in [0\,..\,m),$$

где $u_j[i] \in \mathbb{Z}_{\geq 0}$, $r_j[i] \in [0\,..\,\deg \pi[i])$ определяются из равенства:

$$j = \big(u_j[i] - 1\big) \cdot \deg \pi[i] + r_j[i]$$

Суммируя предоставленные выше факты, отметим, что входными данными алгоритма Нидеррайтера можно считать:

1. s многочленов $\pi[i]$;
2. u^* многочленов $\tau_u[i]$, где

(3.1)

$$u^* \coloneqq \sum_{i=1}^{s} u^*[i] \coloneqq \sum_{i=1}^{s} \left\lceil \frac{m}{\deg \pi[i]} \right\rceil,$$

а для $i \in [1\,..\,s]$ степени $\deg \tau_u[i] < u \cdot \deg \pi[i]$, $u \in [1\,..\,u^*[i])$.

Сформулированная теорема описывает условия для входных данных алгоритма, удовлетворив которым, в результате получатся генерирующие матрицы цифровой сети со значением t, напрямую зависящим от входных данных. Это позволяет простым способом оценивать влияние задаваемых многочленов $\pi[i]$ на однородность сети, притом не только в s-мерном пространстве, но и в проекциях на подпространства, основанные на тех же осях. То есть, проекция любой (t, m, s)-сети, построенной по алгоритму

Нидеррайтера согласно Теореме 3.2, на пространство, задаваемое различными осями с номерами $i_1,\ i_2,\ \ldots,\ i_{s^*} \in [1\,..\,s]$, $s^* \le s$, будет являться (t^*, m, s^*)-сетью с

$$t^* = \sum_{i \in \{i_1, i_2, \ldots, i_{s^*}\}} (\deg \pi[i] - 1)$$

Ввиду этого свойства, к описанию подобных сетей, наряду с параметрами t, m и s удобно добавить s-мерный векторный параметр $\boldsymbol{e}$, каждый элемент которого

$$e[i] = \deg \pi[i],$$

а также рассматривать функцию

$$T(\boldsymbol{e}) = \sum_{i=1}^{s} (e[i] - 1),$$

оценивающую гарантированное значения параметра $t \le T(\boldsymbol{e})$.

Введём для таких сетей отдельное определение.

ОПРЕДЕЛЕНИЕ 3.4:

$(t, m, \boldsymbol{e}, s)$-*сетью Нидеррайтера над полем* $\mathbb{F}_b$ будем называть цифровую (t, m, s)-сеть над полем $\mathbb{F}_b$, генерирующие матрицы которой могут быть заданы с помощью алгоритма Нидеррайтера на входных данных вида (3.1), удовлетворяющих Теореме 3.2, где векторный параметр $\boldsymbol{e} = [e[1], \ldots e[s]]$ состоит из элементов $e[i] = \deg \pi[i]$.

Достраивающие сети Нидеррайтера

Основной нашей задачей является изучение достраивающих сетей в рамках семейства $(t, m, \boldsymbol{e}, s)$-сетей Нидеррайтера. Главным образом таких, у которых различные параметры $\boldsymbol{e}$. Как следует из Утверждения 2.2, необходимым условием существования достраивающей сети является существование изоморфной сети определённого вида. Для сетей Нидеррайтера этот факт имеет особенное значение. Чтобы его выразить, сформулируем важное следствие из Теоремы 3.2.

СЛЕДСТВИЕ ИЗ ТЕОРЕМЫ 3.2:

Пусть $\{\boldsymbol{x}_n\}_{n\in[0..b^m)}$ – $(t, m, \boldsymbol{e}, s)$-сеть Нидеррайтера, с генерирующими матрицами $\Gamma[i] \in \mathbb{F}_b^{m\times m}$ построенная при помощи:

1. Попарно взаимно простых многочленов $\pi[i]$, $i \in [1\,..\,s]$, вектор степеней которых удовлетворяет условию $T(\boldsymbol{e}) \le m$;
2. Многочленов $\tau_u[i]$, которые взаимно просты с $\pi[i]$, а также имеют степень меньшую $u \cdot e[i]$ для любых i и для $u \in \left[1\,..\,u^*[i]\right]$, где $u^*[i] = \lceil m/e[i] \rceil$.

Тогда любой её начальный участок вида $\{\boldsymbol{x}_n\}_{n\in[0..b^{\widetilde{m}})}$, $\widetilde{m} \in [T(\boldsymbol{e})\,..\,m]$, будет являться $(t, \widetilde{m}, \boldsymbol{e}, s)$-сетью Нидеррайтера, которую можно построить при помощи:

1. Тех же многочленов $\pi[i]$;
2. Многочленов $\tau_u[i]$ с $u \in \left[1\,..\,\tilde{u}^*[i]\right]$, где $\tilde{u}^*[i] = \lceil \widetilde{m}/e[i] \rceil \le u^*[i]$.

При этом генерирующие матрицы $\tilde{\Gamma}[i]$ $(t, \widetilde{m}, \boldsymbol{e}, s)$-сети будут совпадать с левыми верхними блоками размера $\widetilde{m} \times \widetilde{m}$ соответствующих генерирующих матриц $\Gamma[i]$ $(t, m, \boldsymbol{e}, s)$-сети или, иными словами:

$$\tilde{\Gamma}[i] = \mathrm{reduce}(\Gamma[i], \widetilde{m}), \qquad \forall\, i \in [1\,..\,s], \widetilde{m} \in [T(\boldsymbol{e})\,..\,m]$$

Таким образом, если достраивающая сеть Нидеррайтера задаётся многочленами $\pi[i]$, то и содержащаяся в ней сеть изоморфная достраиваемой может быть задана с помощью тех же многочленов.

Важным при рассмотрении сетей Нидеррайтера является вопрос об уникальности генерирующих матриц относительно различных многочленов их задающих. Рассмотрим этот вопрос для одной из разновидностей сетей Нидеррайтера, часто применяющейся на практике. Речь идёт о сетях, для построения которых в качестве многочленов $\pi[i]$ берутся *различные приведённые неприводимые* многочлены. Значительное преимущество такого решения не в последнюю очередь состоит в том, что при выборе s таких многочленов с наименьшими возможными степенями будет установлена минимальная допустимая по теореме Нидеррайтера оценка $T(\boldsymbol{e})$ параметра сети t. В этом нетрудно убедиться, попытавшись выбрать s попарно взаимно простых многочленов так, чтобы $T(\boldsymbol{e})$ принимало как можно меньшие значения.

Также сети Нидеррайтера, задаваемые приведёнными неприводимыми многочленами обладают некоторыми более выразительными свойствами, чем сети Нидеррайтера общего вида.

УТВЕРЖДЕНИЕ 4.1:

Пусть $\tilde{\Gamma} \in \mathbb{F}_b^{m\times m}$ – генерирующая матрица сети Нидеррайтера, заданная при помощи приведённого неприводимого многочлена $\tilde{\pi}$ степени $\deg\tilde{\pi} < m$ и многочленов $\tilde{\tau}_u$ взаимно простых с $\tilde{\pi}$.

Пусть $\Gamma \in \mathbb{F}_b^{m\times m}$ – генерирующая матрица сети Нидеррайтера, заданная при помощи приведённого неприводимого многочлена π степени $\deg\pi < m$ и многочленов τ_u взаимно простых с π.

Если $\Gamma = \tilde{\Gamma}$, то $\pi = \tilde{\pi}$

ДОКАЗАТЕЛЬСТВО:

Пусть $e \coloneqq \deg\pi,\ \tilde{e} \coloneqq \deg\tilde{\pi}$, а также, для определённости, $e \le \tilde{e}$.

Пусть $\Gamma = \tilde{\Gamma}$. Тогда $\Gamma_j = \tilde{\Gamma}_j$ для $j \in [0\,..\,e)$.

Согласно алгоритму, указанные строки заполняются элементами ЛРП $\{\alpha_l(u_j)\}$ с характеристическим многочленом π и $\{\tilde{\alpha}_l(\tilde{u}_j)\}$ с характеристическим многочленом $\tilde{\pi}$ соответственно по правилу:

$$\gamma_{jk} = \alpha_{r_j+k}(u_j),$$

$$\tilde{\gamma}_{jk} = \tilde{\alpha}_{\tilde{r}_j+k}(\tilde{u}_j),$$

где

- $u_j \in \mathbb{Z}_{\geq 1}$, $r_j \in [0\,..\,e)$ такие, что $j = (u_j - 1) \cdot e + r_j$;
- $\tilde{u}_j \in \mathbb{Z}_{\geq 1}$, $\tilde{r}_j \in [0\,..\,\tilde{e})$ такие, что $j = (\tilde{u}_j - 1) \cdot \tilde{e} + \tilde{r}_j$.

Для рассматриваемых j очевидно, $u_j = \tilde{u}_j = 1$ и $r_j = \tilde{r}_j = j$.

Следовательно, $\alpha_{j+k}(1) = \tilde{\alpha}_{j+k}(1)$, для $j \in [0\,..\,e)$, $k \in [0\,..\,m)$.

Для краткости введём сокращения $\alpha_l \coloneqq \alpha_l(1)$, $\tilde{\alpha}_l \coloneqq \tilde{\alpha}_l(1)$.

Получается, первые $m + e - 1$ элементов ЛРП $\{\alpha_l\}$ и $\{\tilde{\alpha}_l\}$ совпадают, что эквивалентно можно записать с помощью формальных рядов Лорана:

$$\frac{\omega\,\tau_1(\omega)}{\pi(\omega)} - \frac{\omega\,\tilde{\tau}_1(\omega)}{\tilde{\pi}(\omega)} = \sum_{l=0}^{+\infty} \alpha_l \cdot \omega^{-l} - \sum_{l=0}^{+\infty} \tilde{\alpha}_l \cdot \omega^{-l} =$$

$$= \sum_{l=m+e-1}^{+\infty} (\alpha_l - \tilde{\alpha}_l) \cdot \omega^{-l} =$$

$$= \Lambda$$

Умножим обе части уравнения на $\omega^{-1}\,\pi(\omega)\,\tilde{\pi}(\omega)$:

$$\tilde{\pi}(\omega)\,\tau_1(\omega) - \pi(\omega)\,\tilde{\tau}_1(\omega) = \omega^{-1}\,\pi(\omega)\,\tilde{\pi}(\omega) \cdot \Lambda$$

В левой части получившегося уравнения находится многочлен, а в правой – формальный ряд Лорана, степень которого равна

$$\deg \Lambda - 1 + \deg \pi + \deg \tilde{\pi} \leq (-m - e + 1) - 1 + e + \tilde{e} = -m + \tilde{e}$$

Исходя из определения (t, m, s)-сети и Теоремы 3.2,

$$m > \tilde{e} \quad \Leftrightarrow \quad 0 > -m + \tilde{e} \geq \deg(\omega^{-1}\,\pi(\omega)\,\tilde{\pi}(\omega) \cdot \Lambda)$$

Следовательно, ряд Λ является таким, что $\omega^{-1}\,\pi(\omega)\,\tilde{\pi}(\omega) \cdot \Lambda = 0$.

Таким образом,

$$\tilde{\pi}(\omega)\,\tau(\omega) = \pi(\omega)\,\tilde{\tau}(\omega)$$

Рассмотрим это равенство по модулю π:

$$\tilde{\pi}\,\tau \equiv 0 (\mathrm{mod}\,\pi),$$

что верно только в том случае, если

$$\tilde{\pi} \equiv 0 (\mathrm{mod}\,\pi),$$

так как τ и π взаимно просты. Ввиду неприводимости $\tilde{\pi}$ и π, предполагаемой по условию, последнее равенство эквивалентно равенству $\tilde{\pi} = \pi$.

Данное утверждение является важным, потому что с его помощью легко показать, что задать сеть, совпадающую с $(t, m, \boldsymbol{e}, s)$-сетью Нидеррайтера, построенной при помощи приведённых неприводимых многочленов $\pi[i]$ возможно *только* с помощью *идентичного* набора из тех же многочленов $\pi[i]$, а, следовательно, и с тем же параметром $\boldsymbol{e}$. Проблема доказанного утверждения заключается в его частном характере. Чтобы оно выполнялось, оказалось необходимым наложить на многочлены $\pi[i]$ не только требования к неприводимости, но и ограничения на степени $\deg \pi[i] < m$.

Приложения

Приложение А.

Доказательство Теоремы 3.1:

Рассмотрим формальный ряд Лорана вида:

$$\frac{\omega\,\tau(\omega)}{\mu(\omega)} = \Lambda_w := \sum_{l=-w}^{+\infty} \alpha_l \cdot \omega^{-l}, \qquad w \in \mathbb{Z}_{\geq 0}$$

Предварительно рассмотрим произведение многочлена μ и формального степенного ряда Λ_w:

$$\mu(\omega)\,\Lambda_w = \mu(\omega) \sum_{l=-w}^{+\infty} \alpha_l \cdot \omega^{-l}, \qquad w \in \mathbb{Z}_{\geq 0},$$

где $\mu(\omega) = \omega^m - \mu_{m-1}\omega^{m-1} - \mu_{m-2}\omega^{m-2} \ldots - \mu_0$.

$$\begin{aligned}
&\mu(\omega) \sum_{l=-w}^{+\infty} \alpha_l \cdot \omega^{-l} = \\
&= (\omega^m - \mu_{m-1}\omega^{m-1} - \cdots - \mu_0)(\alpha_{-w}\omega^w + \alpha_{1-w}\omega^{w-1} + \alpha_{2-w}\omega^{w-2} + \cdots) = \\
&= \alpha_{-w}\omega^{m+w} + (\alpha_{1-w} - \mu_{m-1}\alpha_{-w}\quad)\omega^{m+w-1} + \\
&\qquad + (\alpha_{2-w} - \mu_{m-1}\alpha_{1-w} - \mu_{m-2}\alpha_{-w})\omega^{m+w-2} + \\
&\qquad + \cdots + \\
&\qquad + (\alpha_0 - \mu_{m-1}\alpha_{-1} - \cdots - \mu_{m-w}\alpha_{-w}\quad)\omega^m + \\
&\qquad + (\alpha_1 - \mu_{m-1}\alpha_0 - \cdots - \mu_{m-w}\alpha_{1-w} - \mu_{m-w-1}\alpha_{-w})\omega^{m-1} + \\
&\qquad + \cdots + \\
&\qquad + (\alpha_{m-w}\quad - \mu_{m-1}\alpha_{m-1-w} - \cdots - \mu_1\alpha_{1-w} - \mu_0\alpha_{-w}\ )\omega^w + \\
&\qquad + (\alpha_{m+1-w} - \mu_{m-1}\alpha_{m-w}\quad - \cdots - \mu_1\alpha_{2-w} - \mu_0\alpha_{1-w})\omega^{w-1} + \\
&\qquad + \cdots
\end{aligned}$$

Эквивалентно полученное выражение можно записать в сокращённом виде:

$$\sum_{l=0}^{+\infty}\left(\alpha_{l-w}-\sum_{k=1}^{\min\{l,m\}}\mu_{m-k}\alpha_{l-k-w}\right)\omega^{m+w-l}$$

Рассмотрим теперь уравнение эквивалентное изначально заданному:

$$\omega\,\tau(\omega)=\mu(\omega)\sum_{l=-w}^{+\infty}\alpha_l\cdot\omega^{-l},$$

где $\tau(\omega)=\tau_d\omega^d+\tau_{d-1}\omega^{d-1}+\tau_{d-2}\omega^{d-2}+\cdots+\tau_0$

$$\tau_d\omega^{d+1}+\cdots+\tau_0\omega=\sum_{l=0}^{+\infty}\left(\alpha_{l-w}-\sum_{k=1}^{\min\{l,w\}}\mu_{m-k}\alpha_{l-k-w}\right)\omega^{m+w-l}$$

Очевидно, все слагаемые правой части, отвечающие степеням ω большим $d+1$ и меньшим 1, равны нулю, поэтому разумно положить $w=d+1-m$. Этот шаг является допустимым именно потому, что при всех значениях w больших выбранного, соответствующие коэффициенты при степенях ω рекуррентно занулятся, равно как и отвечающие им коэффициенты α_l.

Действительно, предположим, что $w+m>d+1$. Тогда

$$\alpha_{-w}\omega^{m+w}=0\ \Leftrightarrow\ \alpha_{-w}=0$$

В таком случае формальный ряд Лорана $\Lambda_w(\omega)$ можно выразить, как

$$\sum_{l=-w}^{+\infty}\alpha_l\cdot\omega^{-l}=\alpha_{-w}\omega^w+\sum_{l=1-w}^{+\infty}\alpha_l\cdot\omega^{-l}=0+\Lambda_{w-1}=\Lambda_{w-1}$$

Продолжая аналогичным образом, легко показать, что уравнение:

$$\omega\,\tau(\omega)=\mu(\omega)\,\Lambda_w(\omega)$$

сведётся к уравнению:

$$\omega\,\tau(\omega)=\mu(\omega)\,\Lambda_{d+1-m}(\omega)$$

В развёрнутом виде его можно записать как

$$\tau_d\omega^{d+1}+\cdots+\tau_0\omega=\sum_{l=0}^{+\infty}\left(\mu_m\alpha_{l+m-d-1}-\sum_{k=1}^{\min\{l,d+1-m\}}\mu_{m-k}\alpha_{l-k+m-d-1}\right)\omega^{d+1-l}$$

Без потери общности предположим, что $d+1>m$.

$$\tau_d\omega^{d+1}+\cdots+\tau_0\omega=$$
$$=\ \alpha_{m-d-1}\omega^{d+1}+$$
$$+(\alpha_{m-d}-\mu_{m-1}\alpha_{m-d-1})\omega^{d}+$$
$$+\ (\alpha_{m-d+1}-\mu_{m-1}\alpha_{m-d}-\mu_{m-2}\alpha_{m-d-1})\omega^{d-1}+$$
$$+\cdots+$$
$$+\ (\alpha_0-\mu_{m-1}\alpha_{-1}-\cdots-\mu_{2m-d-1}\alpha_{m-d-1})\omega^{m}+$$
$$+\ (\alpha_1-\mu_{m-1}\alpha_0\ -\cdots-\mu_{2m-d-1}\alpha_{m-d}-\mu_{2m-d-2}\alpha_{m-d-1})\omega^{m-1}+$$
$$+\cdots+$$
$$+\ (\alpha_{m-1}-\mu_{m-1}\alpha_{m-2}-\cdots-\mu_1\alpha_0-\mu_0\alpha_{-1})\omega+$$
$$+\ (\alpha_m\ -\mu_{m-1}\alpha_{m-1}-\cdots-\mu_1\alpha_1-\mu_0\alpha_0\ )\omega^0+$$
$$+\cdots$$

Описанное выше равенство эквивалентно системе равенств:

$$\begin{cases}\tau_d\ =\alpha_{m-d-1}\\ \tau_{d-1}\ =\alpha_{m-d}\ -\mu_{m-1}\alpha_{m-d-1}\\ \tau_{d-2}\ =\alpha_{m-d+1}-\mu_{m-1}\alpha_{m-d}\ -\mu_{m-2}\alpha_{m-d-1}\\ \dots\\ \tau_{d-m}=\alpha_{2m-d}-\mu_{m-1}\alpha_{2m-d-1}-\cdots-\mu_0\alpha_{m-d-1}\\ \dots\\ \tau_0\ =\alpha_{m-1}\ -\mu_{m-1}\alpha_{m-2}\ -\cdots-\mu_0\alpha_{-1}\\ 0\ =\alpha_{m+k}\ -\mu_{m-1}\alpha_{m+k-1}\ -\cdots-\mu_0\alpha_k,\qquad k\in\mathbb{Z}_{\geq 0}\end{cases}$$

С помощью данной системы возможно полностью восстановить значения α_l:

$$\begin{cases}\alpha_{m-d-1}=\tau_d\\ \alpha_{m-d}\ =\mu_{m-1}\alpha_{m-d-1}\ +\tau_{d-1}\\ \alpha_{m-d+1}=\mu_{m-1}\alpha_{m-d}\ +\mu_{m-2}\alpha_{m-d-1}+\ \tau_{d-2}\\ \dots\\ \alpha_{2m-d}\ =\mu_{m-1}\alpha_{2m-d-1}+\cdots+\mu_0\alpha_{m-d-1}+\tau_{d-m}\\ \dots\\ \alpha_{m-1}\ =\mu_{m-1}\alpha_{m-2}\ +\cdots+\mu_0\alpha_{-1}+\tau_0\\ \alpha_{m+k}\ =\mu_{m-1}\alpha_{m+k-1}\ +\cdots+\mu_0\alpha_k,\qquad k\in\mathbb{Z}_{\geq 0}\end{cases}$$

Эти значения образуют бесконечный набор $(\alpha_l)_{l\in\mathbb{Z}_{\geq m-d-1}}$, где $\alpha_l\in\mathbb{F}_b$, в котором можно выделить линейную рекуррентную последовательность $\{\alpha_l\}_{l\in\mathbb{Z}_{\geq 0}}$ с m начальными значениями, задающимися в зависимости от многочлена $\tau(\omega)$.

Получающиеся для определённого μ и различных τ наборы возможно разбить на b^m классов эквивалентности, полагая, что наборы (α_l) и $(\tilde{\alpha}_l)$ называются эквивалентными, если их порождаемые ими последовательности $\{\alpha_l\}_{l\in\mathbb{Z}_{\geq 0}}$ и $\{\tilde{\alpha}_l\}_{l\in\mathbb{Z}_{\geq 0}}$совпадают.

Описанное отношение эквивалентности выполняется, если совпадают начальные m членов этих последовательностей.

В каждом классе эквивалентности найдётся набор, заданный многочленом τ таким, что $\deg\tau \leq m-1$.

Действительно, предположим, что $\deg\tau = d = m-1$. Тогда

$$\begin{cases} \alpha_0 = \tau_{m-1} \\ \alpha_1 = \mu_{m-1}\alpha_0 + \tau_{m-2} \\ \alpha_2 = \mu_{m-1}\alpha_1 + \mu_{m-2}\alpha_0 + \ \tau_{m-3} \\ \dots \\ \alpha_{m-1} = \mu_{m-1}\alpha_{m-2} + \cdots + \mu_1\alpha_0 + \tau_0 \\ \alpha_m \ \ = \mu_{m-1}\alpha_{m-1} + \cdots + \mu_1\alpha_1 + \mu_0\alpha_k, \quad k \in \mathbb{Z}_{\geq 0} \end{cases}$$

Заметим, что первые m уравнений этой системы образуют СЛАУ относительно m неизвестных $\alpha_0, \alpha_1, \dots, \alpha_{m-1}$:

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ \mu_{m-1} & 1 & 0 & \cdots & 0 & 0 \\ \mu_{m-2} & \mu_{m-1} & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mu_1 & \mu_2 & \mu_3 & \cdots & 1 & 0 \\ \mu_0 & \mu_1 & \mu_2 & \cdots & \mu_{m-1} & 1 \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{m-2} \\ \alpha_{m-1} \end{bmatrix} = \begin{bmatrix} \tau_{m-1} \\ \tau_{m-2} \\ \tau_{m-3} \\ \vdots \\ \tau_1 \\ \tau_0 \end{bmatrix}$$

Матрица системы для любого ненулевого приведённого многочлена μ является невырожденной, следовательно, задаваемый ею линейный оператор будет взаимно-однозначно действовать на $\mathbb{F}_b$.

Следовательно, различным многочленам τ степени $\deg\tau \leq m-1$ (коих существует b^m) будут отвечать различные инициализирующие значения соответствующих линейных рекуррентных последовательностей $\{\alpha_l\}_{l\in\mathbb{Z}_{\geq 0}}$.