Лабораторная работа № 3.

АЛГОРИТМ БЕРЛЕКЭМПА-МЕССИ ДЛЯ НАХОЖДЕНИЯ КОЭФФИЦИЕНТОВ ОБРАТНОЙ СВЯЗИ ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ.

Рассмотрим, как можно восстановить полином, задающий обратные связи, по $2L$ битам М-последовательности.

Докажем следующую теорему:

Теорема. Пусть $LC(\mathbf{z}) = L$. Рассмотрим регистр сдвига длины L с линейной обратной связью, порождающий последовательность $\mathbf{z}$ длины N, где N может быть и бесконечным. Тогда

- L последовательных состояний регистра линейно независимы;
- $L+1$ последовательных состояний регистра линейно зависимы;
- Если $N \geq 2L$ символов последовательности заданы, то полином, задающий обратные связи, однозначно определен.

Доказательство.

Пусть, $c_1,\ldots,c_L$ - коэффициенты полинома, задающего обратные связи. Символы последовательности могут быть записаны в виде

$$z_k = c_1 z_{k-1} + \ldots + c_{L-1} z_{k-L+1} + c_L z_{k-L}. \qquad (1)$$

Обозначим через $\mathbf{Z}$ следующую матрицу размера $L \times L$ из символов выходной последовательности

$$\mathbf{Z} = \begin{pmatrix} z_1 & z_2 & \ldots & \ldots & z_L \\ z_2 & z_3 & \ldots & \ldots & z_{L+1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ z_L & z_{L+1} & \ldots & \ldots & z_{2L-1} \end{pmatrix}.$$

Тогда (1) может быть переписано в матричной форме

$$\mathbf{Z}\begin{pmatrix} c_L \\ c_{L-1} \\ \ldots \\ c_1 \end{pmatrix} = \begin{pmatrix} z_{L+1} \\ z_{L+2} \\ \ldots \\ z_{2L} \end{pmatrix} \qquad (2)$$

Из (2) следует, что линейная комбинация из L строк матрицы $\mathbf{Z}$ (последовательных состояний регистра сдвига) равна $(L+1)$-му состоянию регистра, т.е. $L+1$ последовательных состояний линейно зависимы. Если L последовательных состояний линейно зависимы, то рекурсия (1) выполняется для $L-1$ элемента последовательности, а значит последовательность может быть получена на выходе регистра сдвига с линейной обратной связью длины меньше, чем L. Если по крайней мере $2L$ элементов последовательности известны, то матрица $\mathbf{Z}$ известна. Так как строки матрицы $\mathbf{Z}$ линейно независимы (в силу линейной независимости L последовательных состояний), то определитель матрицы $\mathbf{Z}$ не равен нулю и матрица обратима, что дает единственное решение $(c_1, c_2, ..., c_L)$ системы (2). Если гипотеза о линейной сложности L верна, то существует единственное решение этой системы уравнений, оно и является решением этой задачи.

Тот факт, что на практике сложность L не известна заранее, не намного усложняет задачу, так как можно по очереди проверять гипотезы $L = 1,2,....$ Решение системы из L уравнений имеет сложность не более L^3, поэтому общая сложность нахождения регистра не превышает L^4, т.е. остается в любом случае полиномиальной.

Пример 1. Рассмотрим последовательность

$$z_1, z_2, ... = 01011110001001101011111....$$

Найдем ее линейную сложность. Если бы последовательность состояла из одних нулей, то мы бы заключили, что $L = 0$. В случае последовательности из всех единиц, $L = 1$, $c_1 = 1$, а уравнение (1) имеет вид $z_i + c_1 z_{i-1} = 0$. Так как ни та, ни другая ситуация не имеют место, проверяем гипотезу о том, что $L = 2$. Система (3) имеет вид

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c_2 \\ c_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Ее единственное решение $c_1 = 0$, $c_2 = 1$. Посмотрим, порождает ли этот фильтр всю последовательность

$$c_1 z_2 + c_2 z_1 = c_1 1 + c_2 0 = 0 = z_3$$

$$c_1 z_3 + c_2 z_2 = c_1 0 + c_2 1 = 1 = z_4$$

$$c_1 z_4 + c_2 z_3 = c_1 1 + c_2 0 = 0 \neq z_5 = 1$$

На пятом символе получили несовпадение, следовательно, гипотеза не верна. Положим $L = 3$.

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}\begin{pmatrix} c_3 \\ c_2 \\ c_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

Решение $(c_1 \quad c_2 \quad c_3) = (0 \quad 1 \quad 1)$. Теперь

$$c_1 z_3 + c_2 z_2 + c_3 z_1 = c_1 0 + c_2 1 + c_3 0 = 1 = z_4$$

$$c_1 z_4 + c_2 z_3 + c_3 z_2 = c_1 1 + c_2 0 + c_3 1 = 1 = z_5$$

$$c_1 z_5 + c_2 z_4 + c_3 z_3 = c_1 1 + c_2 1 + c_3 0 = 1 = z_6$$

$$c_1 z_6 + c_2 z_5 + c_3 z_4 = c_1 1 + c_2 1 + c_3 1 = 0 \neq z_7 = 1$$

Еще одна попытка оказалась неудачной. Попробуем $L = 4$.

$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}\begin{pmatrix} c_4 \\ c_3 \\ c_2 \\ c_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

Решение имеет вид: $(c_1, c_2, c_3, c_4) = (0,0,1,1)$. Предоставляем читателю возможность самостоятельно проверить, что вся последовательность порождается этим фильтром.

Описываемый ниже алгоритм Берлекэмпа-Месси решает совместно обе задачи – определение линейной сложности и нахождение коэффициентов полинома со сложностью порядка L^2. Это упрощение возможно благодаря тому, что матрица коэффициентов имеет специфический вид: строки коэффициентов являются сдвигами предыдущих строк. Такие матрицы называют теплицевыми.

Необходимо найти регистр сдвига с обратной связью наименьшей длины L, генерирующий заданную последовательность $\mathbf{z} = (z_1, z_2, ..., z_n)$ при начальном состоянии $(z_1, z_2, ..., z_L)$, $L < n$. Процедура является рекуррентной. Для каждого

r, начиная с $r = 1$, строим регистр, генерирующий первые r элементов последовательности $(z_1, z_2, ..., z_n)$. Обозначим длину построенного регистра через L_r, а сам регистр с обратной связью опишем вектором коэффициентов $\mathbf{c}^{(r)} = (c_1^{(r)}, c_2^{(r)}, ..., c_{L_r}^{(r)})$. На r-й итерации вычисляем r-й выход предыдущего $(r-1)$-го регистра

$$\hat{z}_r = \sum_{j=1}^{r-1} c_j^{(r-1)} z_{r-j}.$$

На самом деле степень полинома $\mathbf{c}^{(r-1)}$ может быть меньше, чем $r-1$, но, чтобы упростить запись, мы игнорируем тот факт, что многие слагаемые в последней сумме тождественно равны нулю.

Истинный элемент последовательности z_r может не совпадать с $\hat{z}_r$. "Невязку" запишем в виде

$$\Delta_r = z_r + \hat{z}_r = z_r + \sum_{j=1}^{r-1} c_j^{(r-1)} z_{r-j} = \sum_{j=0}^{r-1} c_j^{(r-1)} z_{r-j},$$

где подразумевается, что $c_0^{(r-1)} = 1$. Если невязка нулевая, то итерация закончена. В противном случае, нужно модифицировать вектор, задающий регистр, чтобы сделать ее нулевой. Новый полином будем искать в виде ,

$$c^{(r)}(x) = c^{(r-1)}(x) + x^l c^{(m-1)}(x), \quad (3)$$

где $c^{(m-1)}(x)$ - это один из уже использовавшихся полиномов, а $m < r$ таково, что невязка на m-м шаге была ненулевой. Если к тому же положить $l = r - m$, то после такой модификации

$$\Delta_r^{'} = \sum_{j=0}^{r-1} c_j^{(r-1)} z_{r-j} + \sum_{j=0}^{r-1} c_j^{(m-1)} z_{r-j-l} = \Delta_r + \Delta_m = 1+1 = 0.$$

Осталась некоторая свобода в выборе m. Нужно выбрать его так, чтобы минимизировать длину получаемого регистра. Оказывается, что этому условию удовлетворяет выбор последнего такого m, при котором невязка была равна 1.

Алгоритм Берлекэмпа-Месси.

Вход –последовательность **z** длины n.

1. Инициализация: $r = 0$, $c(x) = 1$, $b(x) = 1$.
2. Полагаем $r \leftarrow r+1$. Вычисляем невязку $\Delta = z_r + \sum_{j=1}^{r-1} c_j z_{r-j} = \sum_{j=0}^{r-1} c_j z_{r-j}$
3. Если $\Delta = 0$, сдвиг: $b(x) = xb(x)$, переходим к 5 в противном случае выполняем 4.
4. Формируем новый полином $t(x) \leftarrow c(x) + xb(x)$. Сохраняем предыдущий полином: $b(x) = c(x)$. Меняем связи регистра $c(x) = t(x)$.

5. Если $r < n$, возвращаемся к 2. В противном случае работа закончена, результаты работы алгоритма – полином ЛРОС $c(x)$ и линейная сложность последовательности $\mathbf{z}$ равная $L = \deg c(x)$.

Пример 2. Применим алгоритм Берлекэмпа-Месси к последовательности из примера 4. Результаты промежуточных вычислений приведены в Таблице 1.

Таблица 1. Вычисление линейной сложности и ЛРОС для последовательности 0101111000100110101111…

r	z_r	Δ	**c**	**b**
0	-	-	1	1
1	0	0	1	x
2	1	1	$1+x^2$	1
3	0	0	$1+x^2$	x
4	1	0	$1+x^2$	x^2
5	1	1	$1+x^2+x^3$	$1+x^2$
6	1	0	$1+x^2+x^3$	$x+x^3$
7	1	1	$1+x^3+x^4$	$1+x^2+x^3$
8	0	0	$1+x^3+x^4$	$(1+x^2+x^3)x$
9	0	0	$1+x^3+x^4$	$(1+x^2+x^3)x^2$
10	…	…	…	…
Результат: $L=4$, $c(x)=1+x^3+x^4$				

ЗАДАНИЕ

1. По заданному отрезку псевдослучайной последовательности восстановить генератор.

ИСХОДНЫЕ ДАННЫЕ: Файл с отрезком псевдослучайной последовательности.

СОДЕРЖАНИЕ ОТЧЕТА: Отчет по лабораторной работе должен содержать

1. Описание алгоритма нахождения генератора ПСП.
2. Найденный полином.
3. Выводы по работе.