РЕАЛИЗАЦИИ СИГНАТУРНЫХ АНАЛИЗАТОРОВ НА ОДНОМ СДВИГОВОМ РЕГИСТРЕ

Барашко А.С.
Кафедра ПМиИ, ДонГТУ
math@iamm.ac.donetsk.ua

Abstract

Anatoliy S. Barashko. Realizations of the signature analyzers on sole shift register. *Notionof the modelling of onechannel signature analyzer (SA) by multichannel SA, which can be realize on sole shift register, is defined. The different criterions of the possibility of suchmodelling are obtained.*

Большинство реализаций как одноканальных, так и многоканальных сигнатурных анализаторов (СА) базируется на одном сдвиговом регистре (СР). Это объясняется, прежде всего, простотой таких конструкций и наличием в распоряжении конструктора микросхем, реализующих сдвиговые регистры в чистом виде. Поэтому представляет интерес нахождение условий возможности реализации СА на одном СР. Неопределяемые в данной статье понятия заимствованы из [1].

В соответствии с [2] сигнатурным анализатором назовем линейную последовательностную машину (ЛПМ) [1] без выходов $C = (A,B)$, где A - квадратная, B - прямоугольная бинарные матрицы. Для $p \geq 1$ символом E_p обозначим векторное пространство бинарных векторов-столбцов размерности p, в котором в качестве сложения используется операция суммирования по модулю 2, а умножение векторов осуществляется только на 0 и 1. СА $C = (A,B)$, где A и B - бинарные $r \times r$- и $r \times m$-матрицы соответственно, можно рассматривать как конечный инициальный автомат без выходов $C=(E_r, E_m, \delta, \mathbf{0})$, в котором E_r множество состояний, E_m - входной алфавит, δ - функция переходов, определяемая A и B, $\mathbf{0}$ - начальное состояние ($\mathbf{0} \in E_r$ и все компоненты вектора $\mathbf{0}$ являются нулями). Как обычно, будем использовать расширение функции δ на последовательности $u \in E_m^*$, где E_m^* - множество всех входных последовательностей конечной длины, включая пустую последовательность e длины 0. Известно, что ошибки в последовательности $u \in E_m^*$ можно задавать последовательностью $v \in E_m^*$, имеющей единицы в тех позициях, в которых претерпели изменения компоненты символов из u. Множество необнаружимых СА C ошибок задается выражением $V_C = \{v \in E_m^* \mid \delta(\mathbf{0},v) = \mathbf{0}\}$. Пусть СА C_1 и C_2 имеют одинаковый входной алфавит. Будем говорить, что C_1 обнаруживает ошибки, которые обнаруживает C_2, если $V_{C_1} \subseteq V_{C_2}$ (обозначение $C_1 \leq C_2$). Если $C_1 \leq C_2$ и $C_2 \leq C_1$, то СА C_1 и C_2 называются эквивалентными (обозначение $C_1 \cong C_2$).

В инициальном автомате $C = (E_r, E_m, \delta, \mathbf{0})$, определяющем СА C, можно рассматривать только те состояния, которые достижимы из начального состояния $\mathbf{0}$. Положим $S = \{s \in E_r \mid \exists_{u \in E_m^*} (\delta(\mathbf{0},u) = s)\}$ СА C называется неизбыточным, если $S_C = E_r$. Для СА $C_1 = (A_1, B_1)$ и $C_2 = (A_2, B_2)$ с одинаковым входным алфавитом E_m СА C_2 является гомоморфным образом C_1, если существует такая сюръекция $f: S_{C_1} \to S_{C_2}$, что $f(\mathbf{0}) = \mathbf{0}$ и $f(A_1 s \oplus B_1 x) = A_2 f(s) \oplus B_2 x$ для всех $s \in S_{C_1}, x \in E_m$. СА C_2 есть гомоморфный образ C_1 тогда и только тогда, когда $C_1 \leq C_2$. Если C_1 - неизбыточный СА,

Пусть $f(x) = x^r + \alpha_{r-1} x^{r-1} + ... + \alpha_1 x + \alpha_0$ - полином с коэффициентами 0,1. Транспонированной сопровождающей матрицей (ТСМ) полинома $f(x)$ называется матрица

$$M_{f(x)} = \begin{bmatrix} 0 & 0 & 0 & ... & 0 & \alpha_0 \\ 1 & 0 & 0 & ... & 0 & \alpha_1 \\ 0 & 1 & 0 & ... & 0 & \alpha_2 \\ ... & ... & ... & ... & 0 & ... \\ 0 & 0 & 0 & ... & 1 & \alpha_{r-1} \end{bmatrix}$$

Определение 1. СА $C = (A,B) = (E_r, E_m, \delta, 0)$ реализуем на одном СР, если существует такой СА $\hat{C} = (\hat{A}, \hat{B}) = (E_{\hat{r}}, E_m, \hat{\delta}, 0)$, что $C \equiv \hat{C}$ и $\hat{A}$ является (ТСМ) некоторого полинома степени $\hat{r} \le r$.

Используя утверждение 21.4 главы 5 монографии [1], можно установить следующий критерий возможности реализации неизбыточного СА на одном СР.

Утверждение 1. *Пусть $C = (A,B)$ - неизбыточный СА и $d_1(x), d_2(x), ..., d_k(x)$ - элементарные делители матрицы A. СА C реализуем на одном СР тогда и только тогда, когда $\forall_{1 \le i,j \le k} (i \ne j \Rightarrow d_i(x), d_j(x)$ - взаимно просты).*

Так как характеристический полином $\varphi_A(x)$ матрицы A равен произведению всех элементарных делителей этой матрицы , а минимальный полином $m_A(x)$ этой матрицы равен произведению ее старших элементарных делителей, то из утверждения 1 получаем .

Следствие 1. *Неизбыточный СА $C = (A,B)$ реализуем на одном СР тогда и только тогда, когда $\varphi_A(x) = m_A(x)$.*

Конструируя m-канальные СА некоторые авторы, скажем [3], фактически строят m-канальный аналог одноканального СА. Напомним соответствующее понятие из [2]. Пусть $U \subseteq E_1^*$. Для $m \ge 1$ через $U(m)$ обозначим множество последовательностей из U, длина которых кратна числу m, т.е. $U(m) = \{u \in U \mid \exists_k (|u| = km)\}$, где $|u|$ - длина последовательности u. Если $u \in U(m)$ и $u = x(0)...x(m-1)x(m)...x(2m-1)...x((k-1)m)...x(km-1)$, то символом обозначим последовательность $y(0)...y(k-1)$, где

$$y(t) = \begin{bmatrix} x(tm) \\ x(tm+1) \\ ... \\ x((t+1)m-1) \end{bmatrix} \quad \text{для всех } 0 \le t \le k-1,$$

и положим $\overline{U}(m) = \{\overline{u} \in U(m)\}$. Если $C = (A,B) = (E_r, E_1, \delta, 0)$ - одноканальный СА, то для $m \ge 1$ m-канальным аналогом СА C называется СА $C = (A,B) = (E_r, E_m, \overline{\delta}, 0)$, который удовлетворяет условию $\forall_{u \in E_1^*} (\delta(0,u) = \overline{\delta}((0,\overline{u}))$. В случае, когда одноканальный СА неизбыточный, критерий того, что m-канальный СА является m-канальным аналогом данного одноканального СА, устанавливает следующее утверждение.

Утверждение 2. *Пусть СА $C = (A,B) = (E_r, E_m, \delta, 0)$ - одноканальный неизбыточный СА. Для $m \ge 1$ СА $\overline{C} = (\overline{A}, \overline{B}) = (E_r, E_m, \overline{\delta}, 0)$ является m-канальным аналогом СА C тогда и только тогда, когда $\overline{A} = A^m$ и $\overline{B} = [A^{m-1}B, ..., AB, B]$.*

Для $m \ge 1$ слабым m-канальным аналогом одноканального СА C называется такой m-канальный СА C_1, который эквивалентен некоторому m-канальному аналогу СА C. Можно показать, что СА C_1 является слабым m-канальным аналогом одноканального СА

C тогда и только тогда, когда $V_{C_1} = \overline{V_C(m)}$. Возникает вопрос, в каком случае m-канальный аналог может быть реализован на одном СР. Ниже исследуется этот вопрос в более общей постановке.

Определение 2. Одноканальный СА $C = (E_r, E_1, \delta, 0)$ назовем m-моделируемым на одном СР, если существует такой его слабый m-канальный аналог $\hat{C} = (E_{\hat{r}}, E_m, \hat{\delta}, 0)$, который реализуем на одном СР и $\hat{r} \le r$.

На основании соответствующих определений, следствия 1 и утверждения 2 можно доказать следующее утверждение.

Утверждение 3. *Неизбыточный одноканальный СА $C = (A,B)$ m-моделируем на одном СР тогда и только тогда, когда $\varphi_{A^m}(x) = m_{A^m}(x)$.*

На практике наибольшее распространение среди одноканальных получили СА, основанные на сдвиговых регистрах с линейной обратной связью (СРЛОС), которые задаются примитивными полиномами. В терминологии монографии [1] полином называется примитивным, если он принадлежит максимальному показателю. Если СРЛОС, состоящий из r разрядов, задан примитивным полиномом, то при первоначальном занесении на СР произвольного кода, отличного от нулевого, в течение $2^r - 1$ тактов СР пройдет все $2^r - 1$ ненулевых состояний при условии подачи на его вход только нулевых сигналов. СА $C = (A,B)$ назовем примитивным, если характеристический полином $\varphi_A(x)$ матрицы A примитивен.

Любой полином $f(x)$ степени $r \ge 1$ имеет единственное разложение $f(x) = [p_1(x)]^{e_1} \ldots [p_k(x)]^{e_k}$,где $p_1(x), \ldots, p_k(x)$ - различные неприводимые, отличные от константы, полиномы. Полином $f(x)$ назовем полупростым, если $e_1 = \ldots = e_k = 1$ (простым принято [4] называть неприводимый нормированный полином). Если характеристический полином $\varphi_A(x)$ матрицы A полупростой, то он совпадает с минимальным полиномом $m_A(x)$ этой матрицы.

В доказательстве последующих результатов используются понятия внутренней сети (ВС) и множества циклов ВС, определенных в [1].

Лемма 1. *Если характеристический полином $\varphi_A(x)$ бинарной $r \times r$-матрицы A примитивный, то для любого натурального числа $m \ne 0$ множество циклов ВС, характеризуемой матрицей A , определяется выражением $\Sigma = \{1[1] + N[T]\}$, где $N =$ н.о.д.$(2^r - 1, m)$ и $T = (2^r - 1)/N$.*

Используя лемму 1, можно доказать следующий результат.

Утверждение 4. *Пусть $C = (A,B)$ - одноканальный неизбыточный примитивный СА и m - произвольное целое положительное число. СА C - m-моделируем на одном СР тогда и только тогда, когда $\varphi_{A^m}(x)$ - полупростой полином.*

Следствие 2. *Пусть $C = (A,B) = (E_r, E_1, \delta, 0)$ -одноканальный неизбыточный примитивный СА и m - такое целое положительное число ,что $2^r - 1$ и m взаимно просты. Тогда СА C - m-моделируем на одном СР.*

Непосредственно из следствия 2 получаем.

Следствие 3. *Пусть r - такое целое положительное число, что $2^r - 1$ просто, и $C = (E_r, E_m, \delta, 0)$ - одноканальный неизбыточный примитивный СА. Тогда для любого целого положительного числа $m < 2^r - 1$ СА C - m-моделируем на одном СР.*

Пример. Рассмотрим неизбыточный одноканальный СА $C = (A,B)$, основанный на СРЛОС, который задан примитивным полиномом $\varphi_A(x) = x^4 + x + 1$. При этом

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \text{ и } B = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Так как при m = 2,4,7,8,11,13,14 числа 15 и m взаимно просты, то согласно следствию 2 C - m-моделируем на одном СР. Чтобы определить возможность m-моделирования для других m, необходимо найти полином $\varphi_{A^m}(x)$ и выяснить, является ли он полупростым. Так, для $m = 3$ $\varphi_{A^3}(x) = x^4 + x^3 + x^2 + x + 1$ - неприводим и, значит, полупрост. Поэтому в соответствии с утверждением 4 C - 3-моделируем на одном 4-х разрядном СР. При $m = 5$ $\varphi_{A^5}(x) = (x^2 + x + 1)^2$ не является полупростым и согласно утверждению 4 СА C не будет 5-моделируемым на одном СР.

Следующий результат о моделировании одноканального СА многоканальным на одном СР базируется на некоторых свойствах специфических ВС.

Лемма 2. *Пусть множество циклов ВС, характеризуемой r× r-матрицей A, определяется выражением* $\Sigma = \{1[1]+((2^r -1)/T)[T]\}$. *Тогда множество элементарных делителей* $d_1(x),...,d_w(x)$ *матрицы A обладает следующими свойствами:*

1) Для всех $1 \le i \le w$ $d_i(x)$ *-неприводимый полином.*

2) $\deg d_1(x) = ... = \deg d_w(x) = h$, *где* $\deg d_i(x)$ *- степень полинома* $d_i(x)$ *и h-такое наименьшее положительное число, что* $2^r - 1$ *делится на T.*

3) $r = wh$.

Утверждение 5. *Пусть r - простое число и* $C = (A,B) = (E_r, E_m, \delta, 0)$ *- одноканальный неизбыточный примитивный СА. Тогда для любого целого положительного числа* $m < 2^r - 1$ *СА C - m-моделируем на одном СР.*

В следствии 1 сформулирован критерий возможности реализации неизбыточного СА на одном СР. Согласно этому критерию для неизбыточного СА $C = (A,B)$ с матрицей A порядка r и $\varphi_A(x) \neq m_A(x)$ не существует СА, который был бы эквивалентен C и физическая реализация которого была бы выполнена на СРЛОС с r разрядами. В то же время для любого полинома $f(x)$ СА $C_1 = (A_1, B_1)$, у которого $A_1 = M_{f(x)}$, реализуем на СР с $\deg f(x)$ разрядами. Если $f(x) = \varphi_A(x)$, то при любом выборе матрицы B_1 C_1 не эквивалентно C. Если же $f(x) = m_A(x)$, то можно найти такую матрицу B_1, что $C \le C_1$, т.е. C_1 будет гомоморфным образом СА C.

Пусть $C = (A,B)$ - неизбыточный СА с входным алфавитом E_m и $d_1(x),...,d_w(x)$ - элементарные делители $r \times r$ -матрицы A. Естественной нормальной формой [1] матрицы A является матрица

$$A^* = \begin{bmatrix} M_{d_1(x)} & & & \\ & M_{d_2(x)} & & \\ & & \ddots & \\ & & & M_{d_w(x)} \end{bmatrix}.$$

Без потери общности можно считать, что в списке элементарных делителей вначале перечислены старшие элементарные делители, число которых равно $k \le w$. Для

канонической реализации $C^* = (A^*, B^*)$ СА C положим $B^* = \begin{bmatrix} B_1^* \\ \dots \\ B_w^* \end{bmatrix}$, где матрица B_i^* ($1 \le i \le w$) соответствует элементарному блоку $M_{d_i(x)}$ матрицы A^*, причем если $M_{d_i(x)}$ - $r_i \times r_i$-матрица, то B_i^* - $r_i \times m$-матрица. Известно [2],что $C \equiv C^*$, и, следовательно, C^* - также неизбыточный СА. Полагая для $1 \le i \le w$ $C_i^* = (M_{d_i(x)}, B_i^*)$, СА C можно представить в виде прямой суммы [2] СА $C_1^*, \dots, C_w^*$, т.е. $C^* = C_1^* + \dots + C_w^*$. Поэтому $V_C = V_{C^*} = \bigcap_{1 \le i \le w} V_{C_i^*}$.

Введем в рассмотрение матрицы $\hat{A}$ и $\hat{B}$, определив их следующим образом:

$$\hat{A} = \begin{bmatrix} M_{d_1(x)} & & & \\ & M_{d_2(x)} & & \\ & & \ddots & \\ & & & M_{d_k(x)} \end{bmatrix}, \quad \hat{B} = \begin{bmatrix} B_1^* \\ B_2^* \\ \vdots \\ B_k^* \end{bmatrix}.$$

Для СА $\hat{C} = (\hat{A}, \hat{B})$ $\hat{C} = C_1^* + \dots + C_k^*$, $V_{\hat{C}} = \bigcap_{1 \le i \le k} V_{C_i^*}$ и, поскольку $V_{C^*} \subseteq V_{\hat{C}}$, $C^* \le \hat{C}$. Можно также показать, что $\hat{C}$ - неизбыточный СА. Так как $m_A(x) = d_1(x) \dots d_k(x)$ и множества элементарных делителей матриц $M_{m_A(x)}$ и $\hat{A}$ совпадают, то $M_{m_A(x)}$ подобна $\hat{A}$. Если $\hat{A}$ - $r \times r$-матрица, то существует такая неособенная $r \times r$-матрица P, что $M_{m_A(x)} = P \hat{A} P^{-1}$. СА $\overline{C} = (M_{m_A(x)}, \overline{B})$, где $\overline{B} = P \hat{B}$, реализуем на одном СР и $\overline{C} \equiv \hat{C}$. Таким образом, доказано следующее утверждение.

Утверждение 6. *Пусть $C = (A,B)$ - неизбыточный СА с входным алфавитом E_m и $m_A(x)$ - минимальный полином матрицы A. Тогда $C \le \overline{C} = (M_{m_A(x)}, \overline{B})$ для некоторой матрицы $\overline{B}$ и СА $\overline{C}$ реализуем на одном СР. Если $\varphi_A(x) = m_A(x)$, то $C \equiv \overline{C}$.*

Литература

1. Гилл А. Линейные последовательностные машины. - М.:Наука, 1974. - 287 с.
2. Барашко А.С. К теории сигнатурных анализаторов // Кибернетика.- 1990. - № 2. - С.18 - 22.
3. Ярмолик В.Н. Применение сигнатурного анализа для контроля и диагностики сетевых дискретных структур // Автоматика и вычислительная техника. - 1985. - № 4. - С.73 - 79.
4. Блейхут Р. Теория и практика кодов, контролирующих ошибки. - М.:Мир, 1986. - 576 с.