Ш. Р. Нурутдинов, С. В. Шалагин, Минимизация количества элементов однородной вычислительной структуры,
Исслед. по информ., 2000, выпуск 2, 117–124

МИНИМИЗАЦИЯ КОЛИЧЕСТВА ЭЛЕМЕНТОВ ОДНОРОДНОЙ ВЫЧИСЛИТЕЛЬНОЙ СТРУКТУРЫ

Ш.Р. Нурутдинов, С.В. Шалагин

Рассматривается задача минимизации количества процессорных элементов однородной вычислительной структуры (ОВС), реализующей конечный детерминированный автомат с памятью (КДА). В [1] предложен подход, основанный на теории конечных полей, позволяющий построить КДА в виде асинхронной сети - ОВС, составленной из однотипных элементов и сумматоров по модулю два.

Пусть $M=(X,Q,\delta)$ - КДА без выходов, определённый в поле Галуа, где $X\in GF(2^m)=G$ - множество входных сигналов, $Q\in GF(2^k)=F$ - множество состояний, δ - отображение $\delta: G\times F\to F$, или $\delta(x,q)=q'$, где $x\in G$, $q,q'\in F$. Отображение δ можно представить в виде многочлена от двух переменных над полем $GF(2^n)$, где $n=\max(m,k)$:

$$\delta(x,q)=\sum_{i,j=0}^{r}a_{ij}x^i q^j,\ \ x,q,q',a_{ij}\in GF(2^n),\ r=2^n-1. \qquad (1)$$

Таким образом, M может быть реализован как ОВС, описываемая многочленом вида (1). При реализации $\delta(x,q)$ требуется r^2 блоков [2].

Рассмотрим задачу минимизации количества элементов ОВС, реализующей многочлен вида (1). В работе предложен способ выбора кодирования элементов множества состояний КДА, при котором ОВС, реализующая его функцию перехода, содержит минимальное количество типовых элементов.

Представим δ в виде отображения $\delta': GF(2^p)\to GF(2^p)$, $p=m+k$. При этом

$$\delta'(z)=z',\ z,z'\in GF(2^p),\ z=(x,q)^T.$$

В результате δ' представляется в виде многочлена от одной переменной:

$$\delta'(z)=\sum_{i=0}^{s-1}a_i z^i,\ \ z,a_i\in GF(2^p),\ s=2^p. \qquad (2)$$

Для реализации многочлена вида (2) требуется s-1 блоков, каждый из которых вычисляет произведение $a_i z^i$, $i=\overline{1,s-1}$. При этом сложность вычисления слагаемых многочлена (2) меньше, чем для многочлена (1).

В работе вводится математический аппарат, основанный на теории

конечных полей, позволяющий построить реализацию произвольного конечного автомата типа $M=(X,Q,\delta)$ в виде ОВС с минимальным количеством элементов.

Рассмотрим отображение $\delta'(z)=z'$, где $z=(x,q)^T$, $z'=(x',q')^T$, которое проиллюстрировано на рис. 1.

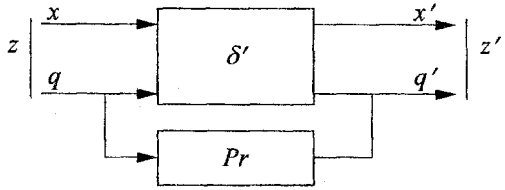

Рис. 1.

Из рис. 1 видно, что вектор z' содержит компоненту x', которая в дальнейших вычислениях не участвует и может принимать произвольные значения. Следовательно, отображению δ можно поставить в соответствие не одно отображение δ', а семейство отображений Δ вида δ'

$$\Delta:(x,q)^T\to(x',q')^T,\ \text{где}\ x\in X,\ q,q'\in Q\ \text{и}\ x'\in GF(2^m).$$

Семейство Δ содержит 2^m отображений вида δ', по одному для каждого x'. Во множестве Δ выделим такое отображение, для которого многочлен (2) имеет минимальную степень. Согласно [3], построим систему уравнений относительно коэффициентов многочлена (2)

$$A=C^{-1}Z', \tag{3}$$

где:

$A=(a_0,a_1,...,a_r)^T$, $Z'=(z'_0,z'_1,...,z'_r)^T$, $a_i,z_i\in GF(2^p)$, $r=2^p-1$, $p=m+k$,

C^{-1} - матрица над $GF(2^p)$:

$$C^{-1}=\begin{pmatrix}1&0&0&\cdots&0&0\\0&1&\xi^{r-1}&\cdots&\xi^{i(r-1)\bmod(r)}&\xi\\\vdots&\vdots&\vdots&\ddots&\vdots&\vdots\\0&1&\xi^2&\cdots&\xi^{2i\bmod(r)}&\xi^{r-2}\\0&1&\xi&\cdots&\xi^i&\xi^{r-1}\\1&1&1&\cdots&1&1\end{pmatrix},\quad 1\le i\le r-1. \tag{4}$$

Зададим элементы поля $GF(2^p)$ в виде многочленов от ξ, где ξ - примитивный элемент поля $GF(2^p)$, являющийся корнем примитивного многочлена $m(x)=x^p+x^{p-1}d_{p-1}+...+d_1+d_0$, $d_i\in GF(2)$. Тогда компоненты

вектора A будут иметь вид

$$a_i = a_{i0} + a_{i1}\xi + ... + a_{i(p-1)}\xi^{p-1},\ \ i = \overline{0,r},\ a_{ij} \in GF(2).$$

Компоненты вектора Z', в свою очередь, будут иметь вид

$$z'_i = t_{i0} + t_{i1}\xi + ... + t_{i(m-1)}\xi^{m-1} + \sigma_{i0}\xi^m + ... + \sigma_{i(k-1)}\xi^{p-1},\ \sigma_{ij} \in GF(2). \quad (5)$$

Вектору Z' соответствует матрица, содержащая коэффициенты многочленов (5):

$$\mathbf{Z} = \begin{pmatrix} t_{00} & t_{01} & \cdots & t_{0(m-1)} & \sigma_{00} & \cdots & \sigma_{0(k-1)} \\ t_{10} & t_{11} & \cdots & t_{1(m-1)} & \sigma_{10} & \cdots & \sigma_{1(k-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ t_{r0} & t_{r1} & \cdots & t_{r(m-1)} & \sigma_{r0} & \cdots & \sigma_{r(k-1)} \end{pmatrix}.$$

Каждый столбец матрицы $\mathbf{Z}$ содержит коэффициенты при соответствующих степенях элемента ξ. Запишем совокупность многочленов (5) в векторном виде:

$$\mathbf{Z}(\xi^0, \xi^1, ..., \xi^{p-1}) = \begin{pmatrix} t_{00} \\ t_{10} \\ \cdots \\ t_{r0} \end{pmatrix}\xi^0 + \begin{pmatrix} t_{01} \\ t_{11} \\ \cdots \\ t_{r1} \end{pmatrix}\xi^1 + ... + \begin{pmatrix} t_{0(m-1)} \\ t_{1(m-1)} \\ \cdots \\ t_{0(m-1)} \end{pmatrix}\xi^{m-1} +$$

$$+ \begin{pmatrix} \sigma_{00} \\ \sigma_{10} \\ \cdots \\ \sigma_{r0} \end{pmatrix}\xi^m + \begin{pmatrix} \sigma_{01} \\ \sigma_{11} \\ \cdots \\ \sigma_{r1} \end{pmatrix}\xi^{m+1} + ... + \begin{pmatrix} \sigma_{0(k-1)} \\ \sigma_{1(k-1)} \\ \cdots \\ \sigma_{r(k-1)} \end{pmatrix}\xi^{p-1}. \quad (6)$$

Введём следующие обозначения:

$$T_i = \begin{pmatrix} t_{0i} \\ t_{1i} \\ \cdots \\ t_{ri} \end{pmatrix},\ i = \overline{0, m-1}. \quad D_j = \begin{pmatrix} \sigma_{0j} \\ \sigma_{1j} \\ \cdots \\ \sigma_{rj} \end{pmatrix},\ j = \overline{0, k-1},\ m + k = p.$$

В результате (6) перепишется следующим образом

$$\mathbf{Z}(\xi^0, \xi^1, ..., \xi^{p-1}) = T_0\xi^0 + T_1\xi^1 + ... + T_{m-1}\xi^{m-1} + \\ + D_0\xi^m + D_1\xi^{m+1} + ... + D_{k-1}\xi^{p-1}. \quad (7)$$

Аналогично запишем компоненты вектора $\mathbf{A}$:

$$\mathbf{A}\ (\xi^0, \xi, ..., \xi^{p-1}) = A_0\xi^0 + A_1\xi + ... + A_{p-1}\xi^{p-1}, \quad (8)$$

где $A_i = (a_{i0}, a_{i1}, ..., a_{ir})^T$, $i = \overline{0, p-1}$.

Представим элементы матрицы C^{-1} в виде многочленов от ξ степени не выше p-1 с коэффициентами из $GF(2)$. Данные коэффициенты зависят

от примитивного многочлена, который имеет вид

$$m(x) = x^p + x^{p-1}d_{p-1} + ... + xd_1 + d_0,\ d_i \in GF(2),$$

корнем которого является элемент ξ. В качестве примера в табл. 1 представлены коэффициенты многочленов, соответствующих элементам поля $GF(2^3)$ для полиномов вида:

$$m_1(x) = x^3 + x + 1, \qquad m_2(x) = x^3 + x^2 + 1.$$

Таблица 1.

$m_1(x) = x^3 + x + 1$	$m_2(x) = x^3 + x^2 + 1$
$0 = (0\ \ 0\ \ 0) = 0$	$0 = (0\ \ 0\ \ 0) = 0$
$1 = (1\ \ 0\ \ 0) = 1$	$1 = (1\ \ 0\ \ 0) = 1$
$\xi = (0\ \ 1\ \ 0) = \xi$	$\xi = (0\ \ 1\ \ 0) = \xi$
$\xi^2 = (0\ \ 0\ \ 1) = \xi^2$	$\xi^2 = (0\ \ 0\ \ 1) = \xi^2$
$\xi^3 = (1\ \ 1\ \ 0) = 1 + \xi$	$\xi^3 = (1\ \ 0\ \ 1) = 1 + \xi^2$
$\xi^4 = (0\ \ 1\ \ 1) = \xi + \xi^2$	$\xi^4 = (1\ \ 1\ \ 1) = 1 + \xi + \xi^2$
$\xi^5 = (1\ \ 1\ \ 1) = 1 + \xi + \xi^2$	$\xi^5 = (1\ \ 1\ \ 0) = 1 + \xi$
$\xi^6 = (1\ \ 0\ \ 1) = 1 + \xi^2$	$\xi^6 = (0\ \ 1\ \ 1) = \xi + \xi^2$

Таким образом, матрице C^{-1} будет соответствовать выражение

$$C\ (\xi^0, \xi, ..., \xi^{p-1}) = C_0\xi^0 + C_1\xi + ... + C_{p-1}\xi^{p-1}. \qquad (9)$$

Приведём пример разложения (9) для поля $GF(2^2)$ с модулярным многочленом $m(x) = 1 + x + x^2$. Для $GF(2^2)$ имеем:

$$C^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & \xi^2 & \xi \\ 0 & 1 & \xi & \xi^2 \\ 1 & 1 & 1 & 1 \end{pmatrix}. \text{ При этом } \begin{cases} 0 = (0\ \ 0) = 0 \\ 1 = (1\ \ 0) = 1 \\ \xi = (0\ \ 1) = \xi \\ \xi^2 = (1\ \ 1) = 1 + \xi \end{cases}.$$

Тогда

$$C_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \quad C_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \qquad (10)$$

Окончательно $C\ (\xi^0, \xi^1) = C_0\xi^0 + C_1\xi^1$. Преобразуем (3), применяя формулы (7), (8) и (9). В результате получим:

$$A_0\xi^0 + A_1\xi^1 + ... + A_{p-1}\xi^{p-1} =$$
$$= (C_0\xi^0 + C_1\xi^1 + ... + C_{p-1}\xi^{p-1})(T_0\xi^0 + T_1\xi^1 + ... + T_{m-1}\xi^{m-1} + \quad (11)$$
$$+ D_0\xi^m + ... + D_{k-1}\xi^{p-1}).$$

Для того, чтобы в правой части (11) был многочлен степени, не превышающей $p-1$, необходимо все многочлены от ξ^i, $i > p-1$ заменить на представления в виде многочленов от ξ^j, $j \le p-1$. При этом коэффициенты многочленов будут либо единичной матрицей I, либо нулевой матрицей $\varnothing$. В результате преобразования правой части (11) получим

$$A_0\xi^0 + A_1\xi^1 + ... + A_{p-1}\xi^{p-1} =$$
$$= L_0[C_0, C_1, ..., C_{p-1}, T_0, T_1, ..., T_{m-1}, D_0, D_1, ..., D_{k-1}]\xi^0 +$$
$$+ L_1[C_0, C_1, ..., C_{p-1}, T_0, T_1, ..., T_{m-1}, D_0, D_1, ..., D_{k-1}]\xi^1 + ... \quad (12)$$
$$... + L_{p-1}[C_0, C_1, ..., C_{p-1}, T_0, T_1, ..., T_{m-1}, D_0, D_1, ..., D_{k-1}]\xi^{p-1}$$

где

$$L_1[C_0, C_1, ..., C_{p-1}, T_0, T_1, ..., T_{m-1}, D_0, D_1, ..., D_{k-1}] =$$
$$= \sum_{i=1}^{p-1}\sum_{j=0}^{m-1}\gamma_{ij}^{(1)}C_iT_j + \sum_{i=1}^{p-1}\sum_{j=0}^{k-1}\lambda_{ij}^{(1)}C_iD_j = \sum_{i=0}^{p-1}C_i(\sum_{j=0}^{m-1}\gamma_{ij}T_j + \sum_{j=0}^{k-1}\lambda_{ij}D_j).$$

Значения переменных $\gamma_{ij}, \lambda_{ij} \in GF(2)$ зависят от коэффициентов модулярного многочлена $m(x)$. Система (12) позволяет вычислять конкретные значения вектора $\mathbf{A}$ $(\xi^0, ..., \xi^{p-1})$, i-я компонента которого соответствует коэффициенту a_i в системе (3). Если a_i придать нулевые значения, то находим минимальную степень многочлена (3).

Опишем алгоритм, позволяющий минимизировать число элементов ОВС, состоящий из 8 шагов:

1. Кодирование элементов множеств X, Q элементами поля $GF(2^p)$.
2. Составление исходной таблицы соответствий $q = \delta(x, q)$, $q, x \in GF(2^p)$.
3. Построение C^{-1} согласно (4) и её разбиение на $C_0, C_1, ..., C_{p-1}$.
4. Построение матрицы $\mathbf{Z}$ (см. (6)).
5. Разбиение матрицы $\mathbf{Z}$ на T_i, D_i.
6. Построение избыточной системы уравнений (12).
7. Исключение противоречивых и подобных уравнений из системы.
8. Решение системы уравнений.

Разработана программа, реализующая данный алгоритм, в которой

для выполнения шага 7 алгоритма предложен диалоговый подход.

В процессе работы были выявлены следующие задачи, которые необходимо разрешить в дальнейшем:

1. Выявление классов КДА, для которых данная процедура минимизации работает наиболее эффективно.

2. Разработка специальных приёмов компактного хранения информации, так как при увеличении мощности множества входов X и множества состояний S наблюдается резкий рост размерности хранимых массивов промежуточных данных.

Рассмотрим пример использования алгоритма для КДА типа M, для которого

$$z=(x,q),\ z'=(x',q'),\ m(x)=1+x+x^2,\ z,z'\in GF(2^2)=\{0,\xi,\xi^2,1\},$$

с таблицей переходов

$q\setminus x$	x_0	x_1
q_0	0	1
q_1	1	0

(13)

Закодируем элементы входного алфавита X и множества внутренних состояний Q:

$$0\to(0,0),\ 1\to(1,0),\ \xi\to(0,1),\ \xi^2\to(1,1).$$

Затем составим исходную таблицу соответствий вида $z=(x,q)$. Разложение (9) для многочлена $m(x)$ имеет вид $C(\xi^0,\xi^1)=C_0\xi^0+C_1\xi^1$.

Вычисление C_0 и C_1 для $m(x)$ приведено ранее.

На основе (13) получим матрицы $\mathbf{Z}$, а также T_0 и D_0:

$$\mathbf{Z}=\begin{pmatrix}t_1&0\\t_2&1\\t_3&1\\t_4&0\end{pmatrix},\quad T_0=\begin{pmatrix}t_1\\t_2\\t_3\\t_4\end{pmatrix},\qquad D_0=\begin{pmatrix}0\\1\\1\\0\end{pmatrix},\quad \mathbf{Z}(\xi^0,\xi^1)=T_0\xi^0+D_0\xi^1.$$

Согласно (10), формула (11) расписывается в виде

$$A_0\xi^0+A_1\xi=(C_0\xi^0+C_1\xi)(T_0\xi^0+D_0\xi).$$

На основе (11) строим систему уравнений для вычисления коэффициентов $\{t_1,t_2,t_3,t_4\}$.

$$\begin{aligned}A_0&=C_0T_0+C_1D_0\\A_1&=C_1T_0+(C_0+C_1)D_0.\end{aligned}\qquad(14)$$

Приняв $A_0=0$ и $A_1=0$, получим:

$$C_0T_0 = C_1D_0$$
$$C_1T_0 = [C_0 + C_1]D_0.$$

В итоге коэффициенты многочлена $F(x) = \sum_{i=0}^{3} a_i z^i$ соответствуют компонентам вектора A в (3). При этом $A = (a_0, a_1, a_2, a_3)$, так как $a_i \in GF(2^2)$. Согласно (14), построим систему уравнений для коэффициентов, которая примет вид:

$$\begin{cases} t_1 + t_2 + t_3 + t_4 = 0, \\ t_2 + t_4 = 0, \\ t_3 + t_4 = 0, \\ t_2 + t_3 = 1, \\ t_3 + t_4 = 1. \end{cases}$$

В системе имеются противоречивые уравнения - третье и пятое. Одно из них (на выбор) может быть исключено. В программе, реализующей данный алгоритм, отбор уравнений производится в диалоговом режиме.

Система имеет два решения. Первое решение (в случае исключения третьего уравнения) - $\{t_1, t_2, t_3, t_4\} = \{0,0,1,1\}$. Второе решение (когда исключается пятое уравнение) - $\{t_1, t_2, t_3, t_4\} = \{0,1,0,1\}$.

Для первого решения, используя (5), строим новое отображение вида $z' = \{0, \xi^2, 1, \xi\}^T$, которое затем подставляем в (3). Из (3) получаем вектор коэффициентов искомого минимального многочлена $A = \{0,0,\xi^2,0\}$, что позволяет на основе (2) вычислить:

$$\delta'(x) = \xi^2 x^2, \; x \in GF(2^2).$$

Таким образом, КДА M может быть реализован единственным блоком ОВС, вычисляющим произведение квадратов x и ξ, тогда как реализация M в виде (1) - $\delta(x,q)$ - в общем случае требует $r^2 = 9$ блоков ОВС, а в виде (2) - $\delta'(z)$ - $s-1 = 15$ блоков.

Работа поддержана грантом РФФИ № 99-01-00163. "Энтропийно-сложностные свойства дискретных вычислительных моделей".

Литература

1. Нурутдинов Ш.Р., Столов Е.Л. Реализация автомата асинхронной сетью // Кибернетика. - Киев, 1988. - №6. - С. 108-109.

2. Нурутдинов Ш.Р. Обеспечение отказоустойчивости сетевой модели автомата // Исследования по прикладной математике. Вып. 16. - Казань: Изд-во Казанского ун-та, 1989. - С. 138-144.

3. Лидл Р., Ниддеррайтер Г. Конечные поля. - М.: Мир, 1988.