ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ

Сборник трудов
Института математики СО АН СССР

1966 г. Выпуск 25

ИСПОЛЬЗОВАНИЕ СТРУКТУРНОЙ ИЗБЫТОЧНОСТИ ДЛЯ ПОВЫШЕНИЯ НАДЕЖНОСТИ АВТОМАТОВ

Е.Н. Турута

В работе М.А.Гаврилова[1]предложен способ повышения надежности конечного автомата, основанный на идеях теории кодирования.

Мы укажем случай, когда можно вычислить вероятности пребывания автомата в различных состояниях и использовать эти данные для повышения его надежности,несколько видоизменяя метод синтеза надежной схемы, изложенный в [1] .

Будем рассматривать конечные автоматы с входным алфавитом $P=\{\rho_1,\dots,\rho_M\}$, выходным алфавитом $\Lambda=\{\lambda_1,\dots,\lambda_\ell\}$ и конечным множеством состояний $A=\{a_1,\dots,a_K\}$, задаваемые каноническими уравнениями:

$$a(t+1)=\varphi[a(t),\rho(t)], \qquad (1)$$

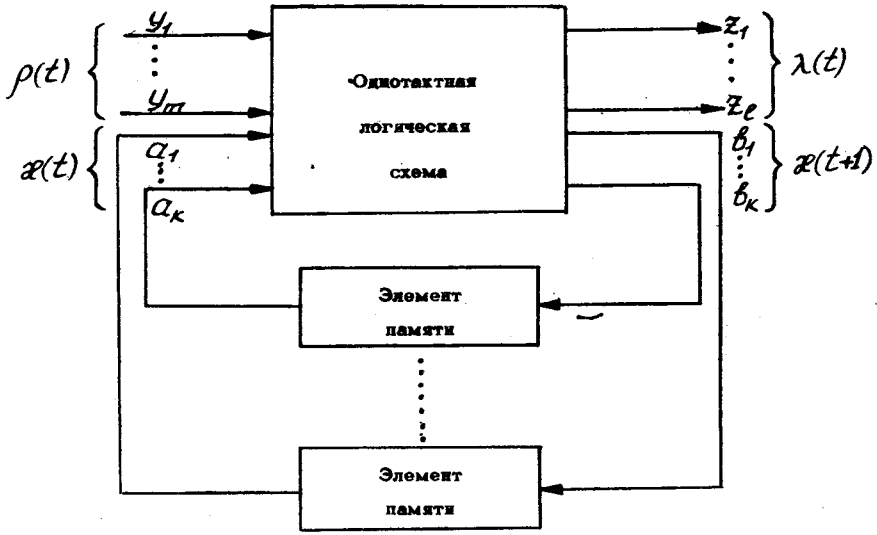
$$\lambda(t)=\varphi[a(t),\rho(t)]. \qquad (2)$$

При этом полагаем, что буквами алфавитов P , Λ и A являются двоичные последовательности:

$$\rho_\mu=(y_1,\dots,y_m);\quad \lambda_j=(z_1,\dots,z_e);\quad a_i=(\alpha_1,\dots,\alpha_k).$$

Как известно [2] , автомат может быть представлен в виде

схемы, показанной на рисунке:



Состояние автомата в каждый момент времени представляет собой комбинацию состояний его элементов памяти. Состояние $a_\nu(t+1)$, где $\nu = 1,\dots,k$, каждого элемента памяти в момент $t+1$ определяется значением поданного на его вход в момент t сигнала

$$b_\nu(t) = \eta[y_1(t),\dots,y_m(t);a_1(t),\dots,a_k(t)],$$

то есть $a_\nu(t+1) = b_\nu(t)$.

Будем считать, что как для логических элементов, так и для элементов памяти возможны два типа случайных неисправностей:

1) Элемент, который должен выдавать на выходе I, выдает 0.

2) Элемент, который должен выдавать на выходе 0, выдает I.

Назовем ошибкой в работе ν -го элемента памяти переход его в некотором такте в состояние $\bar{a}_\nu(t+1)$ вместо состояния $a_\nu(t+1) = \eta[y_1(t),\dots,y_m(t),a_1(t)\dots a_k(t)]$, где $\bar{a}_\nu(t+1)$ есть инверсия $a_\nu(t+1)$. Ошибка элемента памяти может быть как результатом искажения его входного сигнала $b_\nu(t)$ вслед-

ствие неисправностей каких-либо логических элементов, так и результатом неисправности самого элемента памяти.

Полагаем, что выполняются следующие условия:

1) Вероятность искажения входного сигнала $b_\nu(t)$ любого элемента памяти мала.

2) Ошибки различных элементов памяти независимы друг от друга.

3) Вероятности ρ ошибок одинаковы для всех элементов памяти и остаются постоянными с течением времени, причем $\rho < \frac{1}{2}$.

Пусть внутреннее состояние автомата в момент $t+1$, определяемое его функцией переходов, есть $x(t+1) = a_1,\dots,a_k$ и пусть в предыдущих тактах все элементы памяти работали без ошибок. Тогда переход автомата в момент $t+1$ в состояние $x(t+1)$ назовем правильным переходом, а переход его в результате ошибок элементов памяти в некоторое состояние $x'(t+1) = a'_1,\dots,a'_k$, где хотя бы одно $a'_\nu = \bar{a}_\nu$, - неправильным переходом. Неправильный переход в момент $t+1$ может повлечь за собой как искажение состояния выхода автомата, так и искажение входных сигналов элементов памяти в этот момент, что может привести к нарушению функционирования автомата во всех последующих тактах.

Для повышения вероятности правильного перехода в автомат вводится h дополнительных элементов памяти и K его состояний, называемых в дальнейшем основными, кодируются словами некоторого кода длины $n = k+h$ с k информационными и h избыточными символами [I]. Все двоичные последовательности $x = a_1,\dots,a_n$ длины n, не совпадающие ни с каким из кодовых слов x_i $(i = 1,\dots,K)$, назовем искаженными состояниями автомата, а отношение $R = \frac{n}{k}$ - коэффициентом избыточности.

Все множество Q искаженных состояний x разбивается на K непересекающихся подмножеств $S_1,\dots,S_K$, и каждому из основных состояний x_i сопоставляется одно из подмножеств S_i, причем подмножества, сопоставляемые различным состояниям, различны.

Всем состояниям $x^i \in S_i$ и некоторому входу ρ_ν сопоставляется один и тот же переход и одно и то же состояние выхода, определяемые основным состоянием x_i и входом ρ_ν, т.е.

$$\psi[x^i(t),\rho_\nu(t)] = \psi[x_i(t),\rho_\nu(t)] = x(t+1) \quad (3)$$

и

$$\varphi[x^i(t), \rho_\nu(t)] = \varphi[\mathfrak{x}_i(t), \rho_\nu(t)] = \lambda(t). \qquad (4)$$

Теперь переход автомата в любое из состояний $x^i \in S_i$ в результате ошибок элементов памяти эквивалентен переходу в состояние $\mathfrak{x}_i$ (при отсутствии ошибок) и так же, как и этот последний, будет называться правильным переходом. Неправильным переходом избыточного автомата является переход его в момент $t+1$ в некоторое основное состояние $\mathfrak{x}^r(t+1)$, не совпадающее с состоянием $\mathfrak{x}_i(t+1) = \varphi[x(t), \rho(t)]$, или в любое искаженное состояние x, не принадлежащее множеству S_i.

Пусть вероятность пребывания автомата в основном состоянии $\mathfrak{x}_i$ есть $P(\mathfrak{x}_i)$ (где $i = 1, \ldots, K$). Тогда, очевидно, вероятность правильного перехода определяется выражением:

$$Q = P(\mathfrak{x}_1) \sum_{v \in U_1} P(v/\mathfrak{x}_1) + \ldots + P(\mathfrak{x}_K) \sum_{v \in U_K} P(v/\mathfrak{x}_K), \qquad (5)$$

где U_i - множество, включающее основное состояние $\mathfrak{x}_i$ и подмножество S_i искаженных состояний,

$P(v/\mathfrak{x}_i)$- условная вероятность того, что автомат перейдет в состояние $v \in U_i$ при условии, что в случае отсутствия ошибок он должен был перейти в основное состояние $\mathfrak{x}_i$.

В силу предположения о независимости ошибок различных элементов памяти имеем:

$$P(v/\mathfrak{x}_i) = \rho^{r_i} q^{n - r_i},$$

где ρ - вероятность ошибки элементов памяти; $q = 1 - \rho$;

r_i - расстояние Хемминга между v и $\mathfrak{x}_i$.

Если распределение вероятностей $P(\mathfrak{x}_i)$ неизвестно, то принимают $P(\mathfrak{x}_1) = P(\mathfrak{x}_2) = \ldots = P(\mathfrak{x}_K)$. Тогда максимум величины Q достигается при таком разбиении множества $\mathfrak{X}$ на подмножества S_i, когда каждое искаженное состояние $x \in \mathfrak{X}$ сопоставляется тому основному состоянию $\mathfrak{x}_i$ (и включается в подмножество S_i), расстояние Хемминга от которого до данного x является наименьшим *). Этот способ разбиения применен для построения

*)Это следует из того, что данный способ разбиения эквивалентен декодированию по минимуму расстояния при передаче равновероятных сообщений по двоичному симметричному каналу с переходными вероятностями ρ и $1-\rho$. Такое декодирование, как известно [3], приводит к максимуму вероятности правильного декодирования.

структуры автомата, исправляющего заданное число α ошибок элементов памяти при переходе в любое основное состояние [I].

При этом все основные состояния размещаются на расстоянии не менее $d = 2\alpha + 1$ друг от друга, а каждое из множеств S_i содержит все искаженные состояния x, отстоящие от соответствующего $\mathfrak{x}_i$ на расстояние α или меньше. Вероятность правильного перехода в этом случае, очевидно, равна:

$$Q' = \sum_{i=0}^{\alpha} C_n^i \rho^i q^{n-i}. \qquad (6)$$

Однако в том случае, когда входная последовательность автомата представляет собой последовательность независимых испытаний с известным распределением вероятностей возможных исходов $P(\rho_1), \ldots, P(\rho_M)$, распределение вероятностей $P(\mathfrak{x}_i)$ может быть найдено.

Нетрудно показать, что в этом случае последовательность основных состояний автомата образует марковскую цепь. Если эта цепь является эргодической, то существуют предельные вероятности $P(\mathfrak{x}_i)$ пребывания автомата в состояниях $\mathfrak{x}_i (i = 1, \ldots, K)$, не зависящие от его начального состояния [4].

Разбиение множества $\mathfrak{X}$ на подмножества $S_i (i = 1, \ldots, K)$ соответствует принятию для каждого $x \in \mathfrak{X}$ решения о том, какое из K несовместных событий $\mathfrak{x}_1, \ldots, \mathfrak{x}_K$ явилось причиной появления данного x. Известно [5], что вероятность принять правильное решение будет максимальной в том случае, если в качестве причины появления данного x выбирается то из событий $\mathfrak{x}_i (i = 1, \ldots, K)$, для которого величина $P(\mathfrak{x}_i) P(x/\mathfrak{x}_i)$ максимальна (принцип максимума правдоподобия). Эти результаты теории статистических решений дают возможность для любых фиксированных значений вероятностей $P(\mathfrak{x}_i)$ осуществить такое разбиение множества $\mathfrak{X}$ на подмножества S_i, которое обеспечивает максимум величины Q. Это разбиение состоит в том, что каждому из основных состояний $\mathfrak{x}_i$ сопоставляется подмножество S_i тех искаженных состояний x, для которых величина $P(\mathfrak{x}_i) P(x/\mathfrak{x}_i)$ является наибольшей среди всех величин $P(\mathfrak{x}_j) P(x/\mathfrak{x}_j)$, где $j = 1, 2, \ldots, K$.

Пусть основные состояния $\mathfrak{x}_1, \ldots, \mathfrak{x}_K$ пронумерованы так, что $P(\mathfrak{x}_1) \geq P(\mathfrak{x}_2) \geq \ldots \geq P(\mathfrak{x}_K)$, и пусть произвольное искаженное состояние x отстоит от некоторых основных состояний $\mathfrak{x}_i$ и $\mathfrak{x}_j$ (где $i < j$) соответственно на расстояния r_i и

r_j , причем $r_i > r_j$. Тогда при разбиении по максимуму правдоподобия состояние x относится в подмножество S_i , если выполняется неравенство:

$$\frac{P(x_i)}{P(x_j)} > \frac{P(x/x_j)}{P(x/x_i)} = \frac{p^{r_j} q^{n-r_j}}{p^{r_i} q^{n-r_i}} = \frac{q^{r_i - r_j}}{p^{r_i - r_j}},$$

и в подмножество S_j - в противном случае, тогда как при разбиении по минимуму расстояния состояние x всегда включается в подмножество S_j . Так как минимальная разность $r_i - r_j = 1$, то, очевидно, что при выполнении неравенства

$$\max_{i,j} \frac{P(x_i)}{P(x_j)} > \frac{q}{p} \qquad (7)$$

(где $i, j = 1, \ldots, K$; $i < j$)

только разбиение по максимуму правдоподобия обеспечивает максимальную вероятность правильного перехода, в противном случае разбиение по максимуму правдоподобия совпадает с разбиением по минимуму расстояния.

В теории кодирования обычно рассматриваются способы построения кодов, обеспечивающих наименьшую вероятность ошибки при передаче равновероятных сообщений. Это обусловлено тем, что статистика источников сообщений в подавляющем большинстве случаев неизвестна. Кроме того, показано [6] , что результаты, полученные в предположении о равновероятности всех сообщений, вполне пригодны и для источников, статистическая структура которых является произвольной и неизвестной.

Если же известна статистика источника, то при заданном коде декодирование по максимуму апостериорной вероятности обеспечивает вероятность ошибки, меньшую, чем декодирование по минимуму расстояния. Однако практическое декодирующее устройство, учитывающее статистику источника, может оказаться слишком сложным, и тогда для уменьшения вероятности ошибки будет более выгодным увеличение избыточности кода, чем изготовление такого устройства [6] .

В отличие от системы связи, надежный автомат не требует ни кодирующего, ни декодирующего устройства. Поэтому за пре -

имущества, которые приносит применение декодирования, использующего априорные сведения о распределении вероятностей основных состояний, не приходится расплачиваться усложнением аппаратуры, тогда как увеличение избыточности кода (для снижения вероятности ошибки) означало бы увеличение числа элементов памяти автомата.

Следовательно, применение такого декодирования при построении надежной схемы всегда является выгодным.

Еще большего увеличения надежности можно было бы достичь, применяя коды, имеющие минимальную вероятность ошибки при декодировании по максимуму апостериорной вероятности. Поскольку способы построения таких кодов неизвестны, будем использовать известные (n,k) - коды, оптимальные [3] при декодировании по минимуму расстояния. Но даже в этом случае декодирование по максимуму апостериорной вероятности приводит к вероятности ошибки меньшей, чем наименьшая возможная вероятность ошибки для данных n и k при декодировании по минимуму расстояния.

Метод повышения надежности автомата при известном распределении вероятностей $P(x_i)$ проиллюстрируем на примере.

Пусть задана таблица переходов автомата (табл. I), имеющего $K = 4$ основных состояний, известно распределение вероятностей появления всех возможных состояний входа

$$P(\rho_1) = 0{,}01; \qquad P(\rho_2) = 0{,}9; \qquad P(\rho_3) = 0{,}09$$

и вероятность ошибки элемента памяти $p = 0{,}04$. Требуется построить автомат, имеющий максимальную вероятность правильного перехода при коэффициенте избыточности $R = 2{,}5$.

Максимальное количество элементов памяти, которое мы можем использовать, равно $n = k R = 5$ (так как $k = \log_2 K = 2$).

Построим матрицу переходных вероятностей, характеризующую последовательность основных состояний автомата (табл. 2 и 3).

Вероятности $P(x_i)$ пребывания автомата в состояниях x_i ($i = 1,2,3,4$) определим, решая систему уравнений:

$$P(x_1) + P(x_2) + P(x_3) + P(x_4) = 1,$$

$$0{,}01\, P(x_1) + 0{,}01\, P(x_2) = P(x_1);$$

$$0{,}09\, P(x_2) + 0{,}09\, P(x_4) = P(x_2);$$

$$0{,}99\, P(x_1) + 0{,}9\, P(x_2) + 0{,}99 P(x_3) + 0{,}9 P(x_4) = P(x_3);$$

$$0{,}01\, P(x_3) + 0{,}01\, P(x_4) = P(x_4).$$

Получим:

$P(x_1)=0{,}999\cdot10^{-5}; P(x_2)=0{,}989\cdot10^{-3}; P(x_3)=0{,}989; P(x_4)=0{,}999\cdot10^{-2}.$

Для $k = 2$ и $n = 5$ существует (5,2) - код с кодовым расстоянием $d = 3$. Закодируем основные состояния словами этого кода:

x_1 = IOIIO
x_2 = IIIOI
x_3 = 00000
x_4 = OIOII

Разобьем множество Q искаженных состояний на подмножества S_i по максимуму величины $P(x_i)\,P(x/x_i)$, вычисляя все величины $P(x_i)\,P(x/x_i)$ и сравнивая их для каждого искаженного состояния x. Полученное разбиение представлено в табл.4. Используя табл. 4, составим таблицу переходов-табл.5, по которой известными методами [7,8] можно синтезировать структуру избыточного автомата, имеющего максимальную для выбранного (n,k) - кода *) вероятность правильного перехода, определяемую выражением (5):

$$Q = P(x_1)\cdot q^5 + P(x_2)\cdot(q^5+2pq^4+2p^2q^3)+$$

$$+P(x_3)\cdot(q^5+5pq^4+10p^2q^3)+P(x_4)\cdot(q^5+2pq^4+7p^2q^3)\approx0{,}999.$$

Если бы разбиение множества Q проводилось по минимальному расстоянию, то, поскольку выбранный код исправляет одну ошибку ($\alpha = 1$), по формуле (6) найдем:

$$Q' = q^5+5pq^4 = 0{,}985.$$

Вероятности неправильного перехода в том и другом случае соответственно равны:

$$P = 1-Q = 10^{-3},$$

$$P' = 1-Q' = 1{,}5\cdot10^{-2},$$

*) Выбираем (n, k) - код, оптимальный [3] при декодировании по минимуму расстояния. Тогда декодирование по максимуму правдоподобия для этого кода приводит к вероятности ошибки меньшей, чем наименьшая возможная для данных n и k при декодировании по минимуму расстояния. Вопрос о построении кодов, оптимальных при декодировании по максимуму величины $P(x_i)\,P(x/x_i)$, не исследовался

и их отношение

$$\delta = \frac{P'}{P} = 15.$$

Таким образом, в данном случае разбиение по максимуму величины $P(x_i)\,P(x/x_i)$ дало возможность при той же самой избыточности снизить вероятность неправильного перехода в 15 раз.

Следует заметить, что состояния автомата могут различаться по их важности с точки зрения выполняемых автоматом функций (при этом вероятность пребывания автомата в наиболее важных состояниях может быть мала). Тогда ошибки в работе автомата, состоящие в переходе его в некоторое состояние x_j вместо состояния x_i, могут быть неравноценными для различных пар x_i, x_j $(i,j=1,\dots,K;\ i\neq j)$ с точки зрения вызываемых ими последствий.

Изложенный метод синтеза может быть видоизменен с учетом этого факта путем введения некоторого критерия, характеризующего величину потерь для всевозможных пар состояний x_i и x_j.

Таблица I

	ρ_1	ρ_2	ρ_3
x_1	①	3	3
x_2	I	3	②
x_3	4	③	③
x_4	④	3	2

Таблица 2

	x_1	x_2	x_3	x_4
x_1	$P(\rho_1)$	0	$P(\rho_2\vee\rho_3)$	0
x_2	$P(\rho_1)$	$P(\rho_3)$	$P(\rho_2)$	0
x_3	0	0	$P(\rho_2\vee\rho_3)$	$P(\rho_1)$
x_4	0	$P(\rho_3)$	$P(\rho_2)$	$P(\rho_1)$

Таблица 3

	x_1	x_2	x_3	x_4
x_1	0,0I	0	0,99	0
x_2	0,0I	0,09	0,9	0
x_3	0	0	0,99	0,0I
x_4	0	0,09	0,9	0,0I

Таблица 4

i	I	2	3	4
$\mathcal{X}_i$	IOIIO	IIIOI	00000	OIOII
S_i		IIIIO IIIOO IOIII IOIOI	0000I 000IO 00I00 0I000 I0000 000II 00I0I 0I00I 0I0I0 0II00 I000I II000 00II0 I00I0 I0I00	00III 0IIOI 0IIIO 0IIII I00II II00I II0I0 II0II IIIII

Таблица 5

		ρ_1	ρ_2	ρ_3
$\mathcal{X}_1$	IOIIO	①	3	3
$\mathcal{X}_2$	IIIOI	I	3	②
S_2	IIIIO . . . IOIOI	I . . . I	3 . . . 3	2 . . . 2
$\mathcal{X}_3$	00000	4	③	③
S_3	0000I . . . IOI00	4 . . . 4	3 . . . 3	3 . . . 3
$\mathcal{X}_4$	OIOII	④	3	2
S_4	00III . . . IIIII	4 . . . 4	3 . . . 3	2 . . . 2

ЛИТЕРАТУРА

1. М.А. Гаврилов. Структурная избыточность и надежность работы релейных устройств.–Труды I-го конгресса ИФАК, I960, т.3, стр.323-338.
2. С. Колдуэлл. Логический синтез релейных устройств. М.,ИЛ, I962.
3. У. Питерсон. Коды, исправляющие ошибки. М., "Мир", I964.
4. Б.В. Гнеденко. Курс теории вероятностей. М., Физматгиз, I96I.
5. В.Б. Давенпорт, В.Л. Рут. Введение в теорию случайных сигналов и шумов. М., ИЛ, I960.
6. П. Элайс. Кодирование в реальных системах связи.–Кибернетический сборник, М.,ИЛ.I962,вып.4,стр.7-32.
7. В.Г. Лазарев, Е.И. Пийль. Синтез асинхронных конечных автоматов. М., "Наука", I964.
8. Н.Е. Кобринский, Б.А. Трахтенброт. Введение в теорию конечных автоматов. М., Физматгиз, I962.

Институт проблем передачи информации АН СССР.

Поступила в редакцию
IO.IУ. I966 г.