KYBERNETIKA — TOM 7 (1971) ВЫПУСК 3

Преобразователи вероятности

Йозеф Штефка

В статье рассмотрены две новые схемы преобразователей вероятности:

а) схема, для которой существует простая формула для расчета погрешности установки вероятности появления импульсов выходной случайной последовательности при известных отклонениях от 1/2 вероятностей входной последовательности,

б) схема, которая при незначительном понижении частоты следования импульсов выходной случайной последовательности понижает погрешность установки ее статистических параметров почти также, как сумматор по модулю 2.

1. ВВЕДЕНИЕ

Преобразователем вероятности (далее ПВ) [1] называется устройство, которое преобразует входную двоичную случайную последовательность независимых величин „0“ и „1“ с вероятностями появления импульсов $P(0) = P(1) = 1/2$ в случайную последовательность того-же типа, вероятности появления импульсов A, B в которой равны $P(A) = p$, $P(B) = 1 - p$, где p — устанавливаемое значение вероятности. Это — добавочное устройство к генератору случайного процесса [2]. Возможности использования ПВ были в достаточной степени освещены в литературе [1, 2], и здесь поэтому этими вопросами заниматься не будем.

В этой статье рассмотрены некоторые схемы ПВ, работа которых основана на „множественном“ принципе: входную последовательность разбивают на равные отрезки по n импульсам в каждом, образуя последовательность n-значных комбинаций. Вводят два непересекающиеся множества $\mathbf{A}$ и $\mathbf{B}$, объединение которых содержит все возможные двоичные n-значные комбинации. ПВ генерирует на своем выходе импульс типа A тогда, когда n-значная комбинация входной последовательности принадлежит множеству $\mathbf{A}$, в обратном случае он генерирует импульс типа B. Если для вероятностей появления импульсов „0“ и „1“ входной последовательности справедливы равенства $P(0) = P(1) = 1/2$, и импульсы независимы, то вероятности появления всех n-местных комбинаций одинаковы, и равны $1/2^n$. Очевидно, что вероятности появления импульсов A и B на выходе ПВ в этом случае зависят только от числа элементов соответствующих множеств. Обозначим число элементов множества $\mathbf{A}$ символом $N(\mathbf{A})$. Тогда искомые вероятности определяются по формулам:

$$P(A) = \frac{N(\mathbf{A})}{2^n}, \quad P(B) = 1 - \frac{N(\mathbf{A})}{2^n}. \tag{1}$$

В реальном ПВ вероятности $P(A)$ и $P(B)$ отличаются от вероятностей, рассчитанных по этой формуле, потому что вероятности входных нулей и единиц могут быть зависимы или отличаться от $1/2$. Частота следования импульсов выходной последовательности равна $1/n$ частоты следования импульсов последовательности входной.

Конструкция ПВ должна обеспечивать возможность выбора вероятностей $P(A)$ и $P(B)$. Это означает, что множество $\mathbf{A}$, а, следовательно, и $\mathbf{B}$ должны быть такими, чтобы обеспечивали возможность выбора числа их элементов. В ПВ описанном в [1] n-значные комбинации элементов „0“ и „1“ на входе рассматриваются как числа, записанные в двоичной системе счисления. Множеству $\mathbf{A}$ потом принадлежат те числа N, для которых справедливо неравенство $N \leqq V$, где V — некоторое, заранее устанавливаемое число. Выходная вероятность $P(A)$ может быть выбрана произвольно в пределах от $1/2^n$ до 1 по ступеням $1/2^n$.

2. ОПРЕДЕЛЕНИЕ МНОЖЕСТВА A И РАСЧЕТ ВЕРОЯТНОСТИ $P(A)$

В этой работе использован другой способ. Из множества всех возможных n-значных комбинаций выбраны попарно непересекающиеся подмножества $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ таким образом, чтобы для числа элементов, содержащихся в i-том подмножестве, было справедливо равенство $N(\mathbf{A}_i) = 2^{n-i}$, где $i = 1, 2, \ldots, n$. Вероятность того, что n-значная комбинация X принадлежит подмножеству $\mathbf{A}_i$ будет равна:

$$\mathsf{P}\{X \in \mathbf{A}_i\} = \frac{2^{n-i}}{2^n} = 2^{-i}. \tag{2}$$

Подмножества непересекаются, поэтому для любого их объединения справедливо:

$$\mathsf{P}\{X \in \bigcup_{i \in I} \mathbf{A}_i\} = \sum_{i \in I} 2^{-i}, \tag{3}$$

где I — произвольное подмножество индексов $\{1, 2, \ldots, n\}$. Формула (3) показывает способ выбора множества $\mathbf{A}$ для реализации заданной вероятности $P(A)$. Если

$$P(A) = \sum_{i=1}^{n} b_i 2^{-i}, \tag{4}$$

где b_i — коэфициенты равные нулю или единице, то множество $\mathbf{A}$ необходимо выбрать так, чтобы

$$\mathbf{A} = \bigcup_{i \in I_0} \mathbf{A}_i \,, \tag{5}$$

где I_0 — множество тех индексов, для которых выполняется равенство $b_i = 1$. Вероятность $P(A)$ на выходе ПВ может быть, следовательно, выбрана произвольно в пределах от 0 до $1 - 1/2^n$ по ступеням $1/2^n$.

Каждое подмножество $\mathbf{A}_i$ можно описать некоторой логической функцией так, что функция принимает значение 1 во всех тех случаях, когда для n-значной комбинации X на входе справедливо $X \in \mathbf{A}_i$, и значение 0 тогда, когда $X \notin \mathbf{A}_i$. Поставим каждой n-значной комбинации $X = a_1 a_2 \dots a_n$ в соответствие элементарную конъюнкцию $x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$, где, как обычно:

$$x_i^{a_i} = \begin{cases} \bar{x}_i & \text{при} \quad a_i = 1 \,, \\ x_i & \text{при} \quad a_i = 1 \,. \end{cases}$$

Подмножеетву $\mathbf{A}_i$ будет соответствовать логическая функция:

$$f(\mathbf{A}_i) = \bigvee_{X \in \mathbf{A}_i} x_1^{a_1} x_2^{a_2} \dots x_n^{a_n} \,, \tag{6}$$

и множеству $\mathbf{A}$ по уравнению (5) функция:

$$f(\mathbf{A}) = \bigvee_{i \in I_0} f(\mathbf{A}_i) \,. \tag{7}$$

Подмножества $\mathbf{A}_i$ необходимо выбрать так, чтобы функции $f(\mathbf{A}_i)$ были, по возможности, простыми. К задаче можно подойти с другой стороны: выбрать простые функции $f(\mathbf{A}_i)$ такие, что

(а) функция $f(\mathbf{A}_i)$ содержит 2^{n-i} элементарных конъюнкций при $i = 1, 2, \dots, n$,
(б) произведение $f(\mathbf{A}_i) \,.\, f(\mathbf{A}_j) = 0$ для $i \neq j$ и все $i, j = 1, 2, \dots, n$.

Выбираем:

$$f(\mathbf{A}_i) = \bar{x}_{n-i+1} x_{n-i+2} \dots x_n \,. \tag{8}$$

Условие (а), очевидно, выполняется. Кроме того, для $i > j$ справедливо:

$$f(\mathbf{A}_i) f(\mathbf{A}_j) = \bar{x}_{n-i+1} x_{n-i+2} \dots x_{n-j+1} \dots x_n \bar{x}_{n-j+1} x_{n-j+2} \dots x_n = 0 \,,$$

потому что $x_{n-j+1} \bar{x}_{n-j+1} = 0$. Выполняется, следовательно, и условие (б).

Вероятности в формуле (2) были получены в предположении, что вероятности появлений „0“ и „1“ во входной последовательности равны в точности 1/2. На самом деле реальный генератор случайной последовательности генерирует последовательность с некоторым отклонением (ошибкой) в вероятностях. Пусть:

(9) $$P(0) = \tfrac{1}{2} - \varepsilon\,, \quad P(1) = \tfrac{1}{2} + \varepsilon\,,$$

и отдельные импульсы будем также, как и раньше, считать независимыми. Определим вероятность того, что n-значная комбинация X будет принадлежать подмножеству $\mathbf{A}_i$. Комбинация X принадлежит $\mathbf{A}_i$ тогда (8), когда i ее последних членов имеют вид:

$$0\underbrace{1\,1\,\ldots\,1}_{i-1}\,.$$

Справедливо, следовательно:

(10) $$\mathsf{P}\{X \in \mathbf{A}_i\} = (\tfrac{1}{2} - \varepsilon)(\tfrac{1}{2} + \varepsilon)^{i-1} = 2^{-i}(1 - 2\varepsilon)(1 + 2\varepsilon)^{i-1}\,,$$

откуда для расчета $P(A)$ следует формула:

(11) $$P(A) = P\{X \in \mathbf{A}\} = \sum_{i \in I_0} 2^{-i}(1 - 2\varepsilon)(1 + 2\varepsilon)^{i-1}\,.$$

Функция ПВ, естественно, не изменится, если вместо системы подмножеств $\{\mathbf{A}_i\}$ определенной уравнением (8) использовать систему подмножеств $\{\mathbf{B}_i\}$, где

(12) $$f(\mathbf{B}_i) = x_{n-i+1}\bar{x}_{n-i+2}\ldots\bar{x}_n\,.$$

Система подмножетсв $\{\mathbf{B}_i\}$ отличается от $\{\mathbf{A}_i\}$ только выбором обозначений, поэтому для нее справедливы все свойства, справедливые для подмножеств $\mathbf{A}_i$, и кроме того:

(13) $$\mathsf{P}\{X \in \mathbf{B}_i\} = 2^{-i}(1 + 2\varepsilon)(1 - 2\varepsilon)^{i-1}\,.$$

3. КОНСТРУКЦИЯ ПРЕОБРАЗОВАТЕЛЯ ВЕРОЯТНОСТИ

Перейдем к некоторым вопросам конструкции ПВ. Для его правильного функционирования необходимо обеспечить:

а) разбиение входной бинарной последовательности в последовательность n-значных комбинаций,

б) определение принадлежности каждой входной n-значной последовательности множествам $\mathbf{A}$ или $\mathbf{B}$,

в) выдачу импульса A на выходе ПВ в том случае, если входная комбинация принадлежит множеству $\mathbf{A}$, импульса B в обратном случае.

Подробную блочную схему ПВ здесь приводить не будем, потому что схема, опубликованная в [1] справедлива без изменений и для нашего случая, за исключением блока сравнения, который работает другим образом. На рис. 1 изображена упрощенная блочная схема ПВ. Схема содержит n-местный кольцевой распределитель Р, который переключает свои выходы синхронно с поступающими входными импульсами, и практически осуществляет разбиение входной последовательности на отрезки по n членам (n-значные комбинации), ключи $K_1, K_2, \ldots, K_n$, при помощи которых осуществляется выбор множества $\mathbf{A}$,

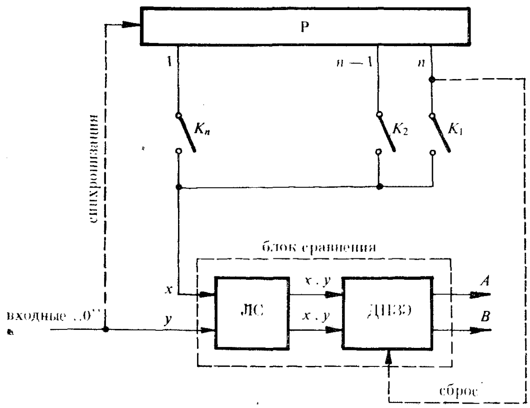

Рис. 1.

и, следовательно, вероятности $P(A)$, и блок сравнения, содержащий логическую схему ЛС и двухпозиционный запоминающий элемент ДПЗЭ (триггер, или другое родственное устройство).

Как следует из выражения (8), входная n-значная комбинация X принадлежит подмножеству $\mathbf{A}_i$ только тогда, когда в $n - i + 1$ разряде входной комбинации X появляется символ „0" и следующие $i - 1$ разряда комбинации нули больше не содержат. Выбор подмнождства $\mathbf{A}_i$ производится ключем K_i. Если ключ K_i замкнут, и $n - i + 1$ разряд входной комбинации X содержит символ „0", переводит логическая схема ЛС блока сравнения элемент ДПЗЭ в положение, которое соответствует выходу A. Если во всех следующих разрядах будут только символы „1", состояние ДПЗЭ больше менятся не будет, и после прихода — n-ого импульса комбинации X на выходе ПВ появится импульс A. В конце цикла ДПЗЭ приводится сбрасывающим импульсом в начальное положение. Если, наоборот, в некотором из последующих разрядов с номером $n - j + 1$, $j < i$ появится импульс „0", и соответствующий ключ K_j будет разомкнут, вернет логическая схема элемент ДПЗЭ в начальное положение, которое соответствует выходному импульсу B. На рис. 2 изображена схема блока сравнения, которая использует ДПЗЭ типа $J-K$ [3]. Логическая схема содержит, в этом случае, единственный элемент И+НЕ, потому что ДПЗЭ перенимает часть логических функций на себя.

Из описания работы сравнивающего влока следует, что ДПЗЭ будет после прихода n входных импульсов в положении, которое соответствует выходному импульсу A тогда и только тогда, когда эти импульсы образуют комбинацию, принадлежащую множеству $\boldsymbol{A}$.

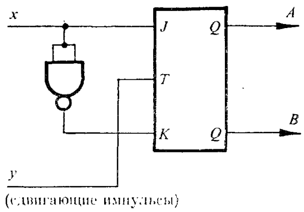

Рис. 2.

4. УМЕНЬШЕНИЕ ПОГРЕШНОСТИ УСТАНОВКИ ВЕРОЯТНОСТИ $P(A)$

Иногда отклонение вероятности появления импульсов входной последовательности от 1/2 (величина ε в формуле (9)) слишком велико, что приводит к большой ошибке в установке вероятности $P(A)$. В таких случаях, обычно, для уменьшения ε используют полусумматоры (сумматоры по модулю 2), установленные на входе ПВ (в установке GENAP-2 [2] они встроены в корпус генератора случайного процесса). Полусумматоры разбивают входную последовательность на отрезки по два или четыре импульса в каждом, и производят сложение по модулю 2 импульсов внутри каждого отрезка. Для вероятностей появления импульсов „0“ к „1“ в новой последовательности справедливо:

(14) $$P(0) = \tfrac{1}{2} + 2^{k-1}(-\varepsilon)^k\,, \quad P(1) = \tfrac{1}{2} - 2^{k-1}(-\varepsilon)^k\,,$$

где k-число импульсов, суммируемых в каждом отрезке, которое в нашем случае равно 2 или 4. При этом, конечно, частота поступления случайных импульсов на вход ПВ понизится в два или четыре раза, что существенно уменьшит максимально достижимую частоту выходной последовательности ПВ.

Рассмотрим другой способ уменьшения погрешности в установке вероятности $P(A)$, который основан на особом выборе множеств $\boldsymbol{A}$ и $\boldsymbol{B}$. Выше были введены две системы подмножеств $\{\boldsymbol{A}_i\}$ и $\{\boldsymbol{B}_i\}$. Обе эти системы — это системы попарно непересекающихся подмножеств. Если из множества подмножеств $\{\boldsymbol{A}_i\}$ устранить подмножество $\boldsymbol{A}_1$, и из $\{\boldsymbol{B}_i\}$ устранить $\boldsymbol{B}_1$, то система подмножеств, содержащая все оставшиеся подмножества систем $\{\boldsymbol{A}_i\}$ и $\{\boldsymbol{B}_i\}$, образует также систему попарно непересекающихся подмножеств. Построим новую систему $n - 1$ подмножеств $\mathbf{C}_i$:

$$\mathbf{C}_i = \mathbf{A}_i \cup \mathbf{B}_i\,, \quad i = 2, 3, \ldots, n\,.$$

Ясно, что при $i \neq j$ справедливо $\mathbf{C}_i \cap \mathbf{C}_j = \emptyset$. Из уравнений (10) и (13) следует, что вероятность того, что n-значная комбинация X принадлежит подмножеству $\mathbf{C}_i$ равна:

$$\text{(15)} \qquad \mathrm{P}\{X \in \mathbf{C}_i\} = 2^{-i}(1 - 4\varepsilon^2)\left[(1 + 2\varepsilon)^{i-2} + (1 - 2\varepsilon)^{i-2}\right].$$

Выражение в квадратных скобках содержит только четные степени ε. Это означает, что формула (15) не содержит первую степень ε, и так как $\varepsilon \ll 1$, то отклонение действительной вероятности от теоретического значения, определенного уравнением (1) будет меньше, чем в случаях, описываемых уравнениями (10) и (13).

Подмножество $\mathbf{C}_2$ определено следующей логической функцией:

$$\text{(16)} \qquad f(\mathbf{C}_2) = \bar{x}_{n-1}x_n \vee x_{n-1}\bar{x}_n = x_{n-1} + x_n \pmod 2\,.$$

Значит ошибка, которая соответствует этому подмножеству уменьшается также, как в случае использования полусумматора. Для остальных подмножеств

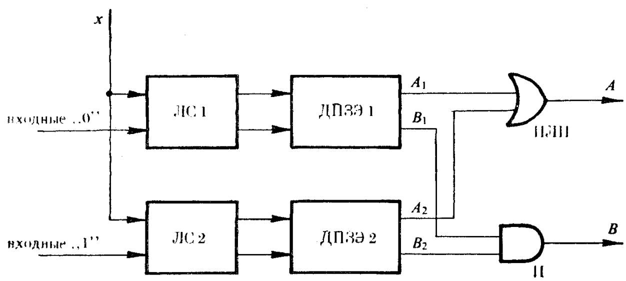

Рис. 3.

$\mathbf{C}_3, \ldots, \mathbf{C}_n$ ошибка уменьшается меньше. Если, однако, учесть, что отклонение от установливаемого значения вероятности больше для подмножеств, которым отвечают большие вероятности, то видим, что использование системы подмножеств $\{\mathbf{C}_i\}$ приводит к более равномерному распределению погрешностей на подмножествах $\mathbf{C}_i$, и, следовательно, к лучшему использованию добавочной позиции.

На рис. 3 изображена схема блока сравнения, которая производит сравнение входных n-значных комбинаций с подмножествами $\mathbf{C}_i$. Работа блока очевидна.

Ключ K_1 ПВ (см. рис. 1) не должен быть, в случае использования этого блока сравнения, замкнут, потому что в обратном случае бы на выходе ПВ был с вероятностью 1 импульс A. Вероятности, соответствующие остальным ключам удваиваются. ПВ допускает установку выходной вероятности $P(A)$ произвольно, в пределах от 0 до $1 - 1/2^{n-1}$ по ступеням $1/2^{n-1}$.

5. ЗАКЛЮЧЕНИЕ

Работа всех ПВ, рассмотренных в этой статье, основанна на одном и том-же принципе. Множество всех возможных реализаций входных n-значных комбинаций делят на два подмножества, и сигнал на выходе выбирают в зависимости от того, которому подмножеству принадлежит поступающая входная комбинация. С этой точки зрения работа ПВ с блоком сравнения по рис. 1 не отличается от ПВ, описанном в [1]. Как способ установки выходной вероятности $P(A)$, так и средняя ошибка ее установки в обоих случаях примерно одинаковы. Отличие в выборе множества $\boldsymbol{A}$ отразится только в способе расчета отклонения действительной вероятности $P(A)$ от установленного значения. Для ПВ [1] не существует простой формулы для расчета этого отклонения. Ошибку необходимо в каждом отдельном случае определять на основании всех элементов множества $\boldsymbol{A}$. Сложность расчета приводит к тому, что при использовании ПВ эту ошибку часто не определяют. Наоборот, для ПВ с блоком сравнения по рис. 1 расчет ошибки в установке выходной вероятности производится очень просто. В этом случае, на основании формулы (10) или (13), соответствует каждому ключу определенная ошибка, которая не зависит от того, если остальные ключи замкнуты или разомкнуты. Полная ошибка может быть определена путем суммирования ошибок, соответствующих замкнутым ключам.

По поводу схемы блока сравнения, изображенной на рис. 3 необходимо заметить, что ее работа не будет нарушена, если логические схемы ЛС1 и ЛС2 определить также, как в работе [1].

(Поступила в редакцию 18 ноября 1970 г.)

ЛИТЕРАТУРА

[1] J. Havel: Měnič pravděpodobnosti. Slaboproudý obzor *24* (1963), 2, 83—87.
[2] J. Havel, K. Janáč: Souprava pro generování náhodných procesů. Alfa, Bratislava 1968.
[3] J. Stach: Číslicové integrované obvody TESLA — klopný obvod MJA 111. Sdělovací technika *17* (1969), 6, 165.

Měniče pravděpodobnosti

Josef Štefka

Jsou uvedeny dvě modifikace měniče pravděpodobnosti, jejichž funkce se zakládá na „množinovém" principu. Vstupní posloupnost náhodných pulsů se dělí na skupiny po n členech. Množina všech možných n-místných skupin je rozčleněna do dvou podmnožin a signál na výstupu je volen podle toho, které podmnožině realizovaná skupina patří.

V práci je navrženo dělení množiny všech n-místných skupin do n navzájem disjunktních podmnožin $\mathbf{A}_i$, s počtem prvků $N(\mathbf{A}_i) = 2^{n-i}$ pro $i = 1, 2, \ldots, n$. Podmnožiny $\mathbf{A}_i$ jsou voleny tak, aby konstrukce měniče pravděpodobnosti byla co možná nejjednodušší. Potom, je-li nastavena výstupní pravděpodobnost

$$P(A) = \sum_{i \in I} 2^{-i},$$

je na výstupu měniče pravděpodobnosti posloupnost s pravděpodobností jednoho z pulsů:

$$P(A) = \sum_{i \in I} 2^{-i}(1 - 2\varepsilon)(1 + 2\varepsilon)^{i-1}.$$

Ve druhé části článku je zavedeno nové dělení množiny všech n-místných skupin do podmnožin $\mathbf{C}_i$, které jsou voleny tak, aby pravděpodobnost $P(A)$ neobsahovala první mocninu ε.

Ing. Josef Štefka, CSc., Ústav teorie informace a automatizace ČSAV (Институт теории информации и автоматики ЧСАН), Vyšehradská 49, Praha 2.