Доклады Академии наук СССР
1972. Том 207, № 6

УДК 51:621.391

КИБЕРНЕТИКА И ТЕОРИЯ РЕГУЛИРОВАНИЯ

Г. Л. ХОДАК

О СРЕДНЕЙ ЗАДЕРЖКЕ ДЕКОДИРОВАНИЯ ДЕШИФРУЕМЫХ КОДОВ

(Представлено академиком С. Л. Соболевым 28 III 1972)

Рассматривается дешифруемое конечноавтоматное кодирование марковских источников произвольного конечного порядка. Вводится понятие средней задержки декодирования и доказывается, что она конечна, если вероятности всех слов положительны, а кодирующий автомат сильно связный. При побуквенном кодировании бернуллиевских источников положительности вероятностей всех слоев не требуется. Отсюда следует, что мера множества неоднозначно декодируемых последовательностей равна нулю. Это является решением одной из задач, поставленных Э. М. Гилбертом и Э. Ф. Муром в [1]. Ранее Ал. М. Марковым было показано, что мощность указанного множества может быть равна континууму [2].

Необходимые обозначения: если $\mathfrak{A}$ — некоторый алфавит, то $a_1 \dots a_k$ $(a_1, \dots, a_k \in \mathfrak{A};\ 0 \leqslant k < \infty)$ — слово в алфавите $\mathfrak{A}$, λ — пустое слово, $\mathfrak{A}^*$ — множество всех слов в алфавите $\mathfrak{A}$, включая пустое, $|A|$ — число букв в слове A, $\mathfrak{A}^\infty$ — множество всех последовательностей вида $\{a_i\}_{i=1}^\infty$, $a_1, a_2, \dots$ $\dots, \in \mathfrak{A}$. Если $A_1 = a_1 \dots a_k \in \mathfrak{A}^*$ и $A_2 = a_1 a_2' \dots \in \mathfrak{A}^* \cup \mathfrak{A}^\infty$, то $A_1 A_2 = a_1 \dots a_k a_1' a_2' \dots \in \mathfrak{A}^* \cup \mathfrak{A}^\infty$. Если $A \in \mathfrak{A}^*$ и n — натуральное число, то $A^n = A \dots A$ (n раз) и $A^\infty = AA \dots \in \mathfrak{A}^\infty$. Слово $A_1 \in \mathfrak{A}^*$ является префиксом $A_2 \in \mathfrak{A}^* \cup \mathfrak{A}^\infty$, что записывается $A_1 \prec A_2$, если $\exists A_3 \in \mathfrak{A}^* \cup \mathfrak{A}^\infty$ $(A_2 = A_1 A_3)$. Если $A \in \mathfrak{A}^*$ и $V \subset \mathfrak{A}^* \cup \mathfrak{A}^\infty$, то $AV = \bigcup_{A_1 \in V} (AA_1)$ и $A \prec V$ равносильно $\forall A_1 \in V$ $(A \prec A_1)$. Если V — некоторое множество, то $\|V\|$ — его мощность. Обозначим через $\sigma(\mathfrak{A})$ σ-алгебру подмножеств $\mathfrak{A}^\infty$, порожденную всеми множествами вида $A\mathfrak{A}^\infty$ $(A \in \mathfrak{A}^*)$.

Источник сообщений последовательно порождает буквы конечного входного алфавита $\mathfrak{A}$. Вероятностная структура источника задается мерой p, определенной на $\sigma(\mathfrak{A})$. Вероятность слова $A \in \mathfrak{A}^*$ есть $p(A) = p(A\mathfrak{A}^\infty)$. Тип источника (бернуллиевский, марковский и т. д.) определяется типом меры. Назовем источник (меру) положительным, если $\forall A \in \mathfrak{A}^*$ $(p(A) > 0)$. Положительность бернуллиевского источника равносильна положительности вероятностей всех букв.

Кодирование осуществляется конечным автоматом $\{\mathfrak{A}, \mathfrak{B}, S, s_0, \alpha, \beta\}$, где $\mathfrak{B}$ — выходной алфавит, S — конечное множество состояний, s_0 — начальное состояние, α: $\mathfrak{A} \times S \to \mathfrak{B}^*$, β: $\mathfrak{A} \times S \to S$. Положим $M = \max_{a \in \mathfrak{A},\ s \in S} |\alpha(a, s)|$. Заключительное состояние автомата при подаче на вход слова $A \in \mathfrak{A}^*$ обозначим через $t(A)$; формально оно определяется рекуррентными соотношениями $t(\lambda) = s_0$, $\forall A \in \mathfrak{A}^* | \forall a \in \mathfrak{A}\ (t(Aa) = \beta(a, t(A)))$.

Кодирующий автомат называется сильно связным если $\forall A_1 \in \mathfrak{A}^*$ $\exists A_2 \in \mathfrak{A}^* (t(A_1 A_2) = s_0)$ *. Кодирование есть отображение φ: $\mathfrak{A}^* \cup \mathfrak{A}^\infty \to$

* При рассмотрении кодирующих автоматов, не ограничивая общности, можно считать, что $\forall s \in S$ $\exists A \in \mathfrak{A}^*$ $(t(A) = s)$. При этом условии данное определение эквивалентно определению сильной связности в работе [3].

$\to \mathfrak{B}^* \cup \mathfrak{B}^\infty$, которое для автоматов определяется следующим образом: $\varphi(a_1a_2 \ldots a_i \ldots) = a(a_1, t(\lambda))a(a_2, t(a_1)) \ldots a(a_i, t(a_1 \ldots a_{i-1})) \ldots$

Кодирование является побуквенным, если $\|S\| = 1$. Конечноавтоматное кодирование называется дешифруемым, если $\forall A_1, A_2 \in \mathfrak{A}^*$ $A_1 = A_2 \Rightarrow$ $\Rightarrow \varphi(A_1) \neq \varphi(A_2) \vee t(A_1) \neq t(A_2)$ ([4]). Обозначим через E множество неоднозначно декодируемых последовательностей. По определению, $E = \{A \in \mathfrak{A}^\infty \mid \|\varphi^{-1} \times (\varphi(A))\| \geqslant 2\}$.

Естественно считать, что слово $A_1 \in \mathfrak{A}^*$ декодируется по $\varphi(A_1A_2)$ при некотором $A_2 \in \mathfrak{A}^*$, если $A_1 \prec \varphi^{-1}(\varphi(A_1A_2\mathfrak{A}^\infty))$ (см. ([1])). Такое слово A_2 назовем декодирующим для A_1. Задержка декодирования слова A_1 зависит от того, какая последовательность будет выработана источником после него, т. е. является функцией $\eta(A_1, A)$, определенной для $A \in A_1\mathfrak{A}^\infty$. Значение $\eta(A_1, A)$ равно длине самого короткого декодирующего для A_1 слова A_2, для которого $A_1A_2 \prec A$. Если такого слова A_2 не существует, то $\eta(A_1, A) = \infty$. Дадим формальное определение. Для $A_1 \in \mathfrak{A}^*$, $A \in A_1\mathfrak{A}^\infty$ положим $V(A_1, A) = \{A_2 \in \mathfrak{A}^* \mid A_1A_2 \prec A \& A_1 \prec \varphi^{-1}(\varphi(A_1A_2\mathfrak{A}^\infty))\}$,

$$\eta(A_1, A) = \begin{cases} \min\limits_{A_2 \in V(A_1, A)} |A_2|, & \text{если } V(A_1, A) \neq \phi; \\ +\infty, & \text{если } V(A_1, A) = \phi. \end{cases}$$

Достаточно просто доказываются следующие утверждения.

Лемма 1. *При конечноавтоматном кодировании множество E измеримо относительно $\sigma(\mathfrak{A})$.*

Лемма 2. *При любом $A_1 \in \mathfrak{A}^*$ функция $\eta(A_1, A)$ измерима относительно $\sigma(\mathfrak{A})$.*

Пусть p_A — условная вероятностная мера при данном множестве $A\mathfrak{A}^\infty$. Если $p(A) > 0$, то $\forall V \in \sigma(\mathfrak{A})$ $p_A(V) = p(V \cap A\mathfrak{A}^\infty) / p(A)$. Средней задержкой декодирования $N(A_1)$ слова $A_1 \in \mathfrak{A}^*$ назовем усреднение $\eta(A_1, A)$ относительно меры p_{A_1}, т. е. $N(A_1) = \int\limits_{A_1\mathfrak{A}^\infty} \eta(A_1, A)\, dp_{A_1}$ (интеграл имеет смысл, так как $\eta(A_1, A) \geqslant 0$). Средней задержкой декодирования назовем $N = \sup\limits_{A \in \mathfrak{A}^*, p(A) > 0} N(A)$.

В настоящей работе доказываются следующие утверждения.

Теорема 1. *Если источник является марковским произвольного конечного порядка и положительным, а дешифруемое кодирование осуществляется сильно связным конечным автоматом, то $N < \infty$.*

Следствие 1. *Если выполнены условия теоремы, то $p(E) = 0$.*

Следствие 2. *Если кодирование является дешифруемым и побуквенным, а источник бернуллиевским (необязательно положительным), то $N < \infty$ и $p(E) = 0$.*

Замечание. Если на $\sigma(\mathfrak{B})$ задана положительная марковская (произвольного конечного порядка) мера q, то аналогично доказывается, что при дешифруемом кодировании, осуществляемом сильно связанным конечным автоматом, $\varphi(E) \in \sigma(\mathfrak{B})$ и $q(\varphi(E)) = 0$. При побуквенном кодировании и бернуллиевской мере положительность не требуется.

При нарушении хотя бы одного условия утверждения теоремы 1 и следствий могут не выполняться Это показывают примеры кодирующих автоматов, представленные на рис. 1. Вершины графов здесь обозначают состояния автоматов, двойной кружок — начальное состояние, стрелка с написанными на ней символами, скажем x, y, означает, что автомат переходит из одного состояния в другое (по стрелке) при подаче на вход буквы x и выдает при этом слово y. Легко проверить, что эти автоматы осуществляют дешифруемое кодирование. Для автомата I не выполнено условие сильной связности и $E = \mathfrak{A}^\infty$, $p(E) = 1$, $N = \infty$ при любом источнике. Бернуллиевский источник с вероятностями букв $p(a) = p(b) = 1/2$, $p(c) = 0$ не является положительным. При кодировании его автоматом II $N = \infty$ и

$p(E) = 1$. Для автомата II можно подобрать положительную немарковскую меру, при которой $N = \infty$ и $p(E) = 1$ (за недостатком места пример не приводится). Если кодирование не дешифруемо, то найдутся $A_1, A_2 \in \mathfrak{A}^*$, для которых $\varphi(A_1) = \varphi(A_2)$, $t(A_1) = t(A_2)$, $A_1 \neq A_2$. Тогда при любом положительном источнике $\eta(A_1, A) \equiv \infty$, $N(A_1) = N = \infty$ и $p(E) \geqslant p(A_1) > 0$.

В работе ([1]) рассматривалось побуквенное кодирование бернуллиевских источников и была поставлена следующая задача: если дана кодовая система, однозначно дешифруемая, но не обладающая свойством конечной

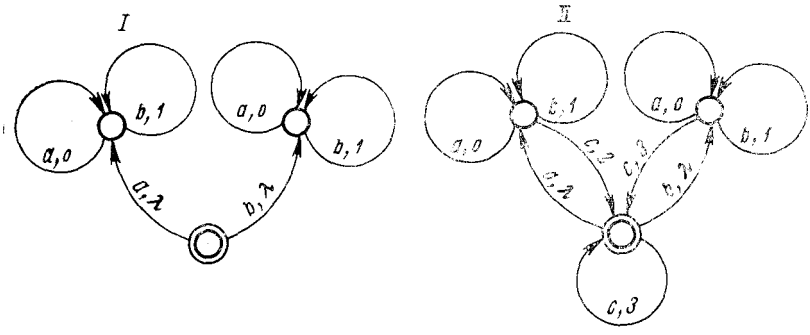

Рис. 1

задержки, то образует ли всегда множество предполагаемых сообщений с бесконечной задержкой... множество меры нуль?

Побуквенное кодирование эквивалентно кодированию автоматом с одним состоянием. В этом случае $t(A) \equiv s_0$ и автомат сильно связный, $\varphi(a_1a_2a_3\ldots) = \varphi(a_1)\varphi(a_2)\varphi(a_3)\ldots$, а условие дешифруемости конечноавтоматного кодирования принимает вид $\forall A_1, A_2 \in \mathfrak{A}^* \quad A_1 \neq A_2 \Rightarrow \varphi(A_1) \neq \varphi(A_2)$, т. е. совпадает с условием дешифруемости в ([1]). Множество предполагаемых сообщений с бесконечной задержкой в наших обозначениях есть $\varphi(E)$. Естественно интересоваться мерой его полного прообраза, т. е. $p(\varphi^{-1}(\varphi(E)))$. Но легко видеть, что $\varphi^{-1}(\varphi(E)) = E$. Ответ на поставленную задачу дается следствием 2. Если же интересоваться мерой $q(\varphi(E))$, где q — мера на $\sigma(\mathfrak{B})$, то ответ дается в замечании.

Основной в настоящей работе является

Лемма 3 (о существовании декодирующих слов). *Если кодирование дешифруемо и автомат сильно связный, то для любого $A \in \mathfrak{A}^*$ найдется декодирующее слово $f(A)$, т. е. $A \prec \varphi^{-1}(\varphi(Af(A)\mathfrak{A}^\infty))$.*

Доказательство. В качестве $f(\lambda)$ берем λ. Фиксируем произвольно непустое $A \in \mathfrak{A}$. По условию сильной связности, найдется $A_1 \in \mathfrak{A}^*$, для которого $t(AA_1) = s_0$. Пусть $L = M \cdot \|S\|$. В качестве $f(A)$ возьмем $A_1(AA_1)^L$. Предположим, что $f(A)$ не является декодирующим словом для A. Тогда найдется $A_2 \in \mathfrak{A}^*$, для которого $A \overline{\prec} A_2$ * и $\varphi(Af(A)) = \varphi((AA_1)^{L+1}) \prec \varphi(A_2)$. Из равенства $t(AA_1) = s_0$ следует, что при любом k $t((AA_1)^k) = s_0$ и $\varphi((AA_1)^{L+1}) \prec \varphi((AA_1)^kA_2)$. В силу последнего соотношения при любом $k = 0, 1, \ldots$ найдется $\bar{A}_k$ — минимальный по числу букв префикс слова $(AA_1)^kA_2$, для которого $\varphi((AA_1)^L) \prec \varphi(\bar{A}_k)$. Имеют место неравенства

$$|\varphi((AA_1)^L)| \leqslant |\varphi(\bar{A}_k)| < |\varphi((AA_1)^L)| + M, \quad k = 0, 1, \ldots$$

При $k \leqslant L$ $(AA_1)^k \prec \bar{A}_k$ и поэтому все слова $\bar{A}_k$ с $k \leqslant L$ попарно различны (используем $A \overline{\prec} A_2$, $A \neq \lambda$). При $k \leqslant L$ также имеем $\varphi(\bar{A}_k) \prec \varphi((AA_1)^{L+1})$. Из дешифруемости следует, что число различных слов $\bar{A}_k$, $k \leqslant L$, у которых $|\varphi(\bar{A}_k)|$ совпадают, не превышает $\|S\|$, а число различных слов $\bar{A}_k$, $k \leqslant L$, не превышает $M \cdot \|S\| = L$. Но все слова $\bar{A}_k$, $k = 0, \ldots, L$, различны, их число равно $L + 1$. Полученное противоречие доказывает лемму

* Здесь и ниже $A \overline{\prec} A_2$ означает, что соотношение $A \prec A_2$ не выполняется.

Далее $f(A)$ будет обозначать декодирующее для $A \in \mathfrak{A}^*$ слово.

Для $A \in \mathfrak{A}^*$ определим множества $W(A) = \{(B, s) \in \mathfrak{B}^* \times S \mid \exists A_1 \in \mathfrak{A}^* \; A \overline{<} A_1 \;\&\; \varphi(A_1) = \varphi(A)B \;\&\; t(A_1) = s \;\&\; |B| < M\}$. При всевозможных словах A число различных множеств $W(A)$ конечно.

Лемма 4. *Если слова $A_1, A_2, A_3 \in \mathfrak{A}^*$ таковы, что $W(A_1) \subset W(A_2)$, $t(A_1) = t(A_2)$ и A_3 является декодирующим для A_2, то A_3 является декодирующим и для A_1.*

Доказательство легко получается методом от противного.

Лемма 5 (об универсальном декодирующем слове). *Если кодирование дешифруемо и автомат сильно связный, то существует слово $U \in \mathfrak{A}^*$, которое является декодирующим для всех $A \in \mathfrak{A}^*$.*

Доказательство. Найдутся натуральное k и слова $A_1, \ldots, A_k$ такие, что $\forall A \in \mathfrak{A}^* \; \exists i \in \{1, \ldots, k\} \quad W(A) \subset W(A_i) \;\&\; t(A) = t(A_i)$.

Определим слово U рекуррентными соотношениями: $U_0 = \lambda$, $U_i = U_{i-1} f(A_i U_{i-1})$, $i = 1, \ldots, k$, $U = U_k$. Имеем $\forall i \in \{1, \ldots, k\}$ $A_i < A_i U_{i-1} < \varphi^{-1}(\varphi(A_i U_{i-1} f(A_i U_{i-1}) \mathfrak{A}^\infty)) \supset \varphi^{-1}(\varphi(A_i U \mathfrak{A}^\infty))$. В силу леммы 4 и выбора слов $A_1, \ldots, A_k$ лемма доказана

Пусть U — универсальное декодирующее слово. Для положительных источников определим $\mathfrak{P} = \inf\limits_{A \in \mathfrak{A}^*} \dfrac{p(AU)}{p(A)}$.

Очевидна

Лемма 6. *Если источник является марковским произвольного конечного порядка и положительным, то $\mathfrak{P} > 0$.*

Доказательство теоремы 1. Достаточно стандартным способом получается оценка $\forall A \in \mathfrak{A}^* \; N(A) \geqslant |U| / \mathfrak{P}^2$, что и доказывает теорему.

Следствие 1 получается в силу оценки

$$p(E) \leqslant \sum_{A_1 \in \mathfrak{A}^*} p(\{A \in A_1 \mathfrak{A}^\infty \mid \eta(A_1, A) = \infty\}) = 0.$$

Следствие 2 получается сужением кодирования на подалфавит из букв с положительными вероятностями.

Новосибирский государственный университет

Поступило 15 III 1972

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] E. N. Gilbert, E. F. Moore, Bell Syst. Techn. J., 38, 4, 933 (1959). Кибернетич. сборн., ИЛ, в. 3, 1961. [2] А. А. Марков, Проблемы кибернетики, 8, 1962, стр. 169. [3] E. F. Moore, Gedanken — Experiments on Sequential Machines, Automata Studies, 1956, p. 129. Сборн. Автоматы, ИЛ, 1956. [4] В. И. Левенштейн, Об обращении конечных автоматов, ДАН, 147, № 6, 1300 (1962).