Преимущество данного подхода к определению степени нелинейности заключается в том, что он полостью определяется свойствами только операции сложения. Вместе с тем в случае циклических групп, в отличие от элементарных абелевых групп, вопрос о способе выбора операции умножения представляется не таким однозначным. Если естественным образом рассматривать циклические группы примарного порядка как аддитивные группы колец вычетов с имеющимися в них операциями умножения, то определение степени нелинейности через степень многочлена является неудобным, так как не всякая функция F может быть задана многочленом (или набором многочленов координатных функций). Полиномиальные функции над кольцом вычетов, то есть функции, которые могут быть заданы многочленом над этим кольцом, составляют относительно малую долю функций [2, 3]. Следует отметить, что для полиномиальных функций над кольцом $\mathbb{Z}_{p^n}$ степень нелинейности функции совпадает с минимальной степенью многочлена, задающего эту функцию.

Теорема 3. Если $F : G^m \to G$ — полиномиальная функция над кольцом $G = \mathbb{Z}_{p^n}$, $p > 2$, $n \geqslant 1$, $m \geqslant 1$, и $P(x_1, \dots x_n) \in \mathbb{Z}_{p^n}[x_1, \dots x_n]$ — многочлен минимальной степени, задающий эту функцию, то степень нелинейности совпадает со степенью многочлена $P(x_1, \dots x_n)$:

$$\mathrm{dl}\, F = \deg P.$$

Из определения степени нелинейности с очевидностью вытекает

Теорема 4. Если G и H — циклические p-группы примарного порядка и R — подгруппа в G, то для степеней нелинейности функции $F : G \to H$ и её ограничения на подгруппу R, $F|_R : R \to H$, выполнено неравенство $\mathrm{dl}\,(F|_R) \leqslant \mathrm{dl}\, F$.

Подробное изложение представленных результатов можно найти в [4].

ЛИТЕРАТУРА

1. *Черемушкин А. В.* Аддитивный подход к определению степени нелинейности дискретной функции // Прикладная дискретная математика. 2010. № 2(8). С. 22–33.
2. *Keller G. and Olson F.* Counting polynomial functions (mod p^n) // Duke Math. J. 1968. V. 35. P. 835–838.
3. *Chen Z.* On polynomial functions from $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \mathbb{Z}_{n_r}$ to $\mathbb{Z}_m$ // Discrete Math. 1996. V. 162. P. 67–76.
4. *Черемушкин А. В.* Аддитивный подход к определению степени нелинейности дискретной функции на циклической группе примарного порядка // Прикладная дискретная математика. 2013. № 2(20). С. 26–38.

УДК 621.391: 519.728

ЭКОНОМНОЕ ПРЕДСТАВЛЕНИЕ НЕДООПРЕДЕЛЁННЫХ ДАННЫХ И ДИЗЪЮНКТИВНЫЕ КОДЫ[1]

Л. А. Шоломов

Предложены экономные представления недоопределённых данных, позволяющие полностью восстанавливать исходные данные. Установлена их связь с дизъюнктивными кодами, получены оценки длины представлений.

Ключевые слова: *представление недоопределённых данных, дизъюнктивный код, свободная от покрытий матрица.*

[1]Работа поддержана ОНИТ РАН по программе фундаментальных исследований.

Задан алфавит $A_0 = \{a_0, a_1, \ldots, a_{m-1}\}$ *основных символов*. Каждому непустому $T \subseteq M = \{0, 1, \ldots, m-1\}$ поставлен в соответствие *недоопределённый символ* a_T. Его *доопределением* считается всякий основной символ a_i, $i \in T$. Символ a_M, доопределимый любым a_i, называется *неопределённым* и обозначается $*$. Выделена система $\mathcal{T}$ некоторых непустых подмножеств T множества M и с ней связан *недоопределённый алфавит* $A = A_{\mathcal{T}} = \{a_T : T \in \mathcal{T}\}$. Подробнее о недоопределённых данных см. в [1].

Задавшись натуральным числом s, припишем каждому $a_i \in A_0$ набор $\lambda_i = (\lambda_i(1), \ldots, \lambda_i(s)) \in \{0,1\}^s$ — *код символа* a_i, а каждому $a_T \in A$ — набор $\lambda_T = (\lambda_T(1), \ldots, \lambda_T(s)) \in \{0, 1, *\}^s$. Обозначим через Λ и $\tilde{\Lambda}$ матрицы со столбцами λ_i, $i \in M$, и λ_T, $T \in \mathcal{T}$, соответственно. Скажем, что пара $(\Lambda, \tilde{\Lambda})$ задаёт для алфавита A *двоичное представление* (размерности s), если при всех i и T столбец λ_i доопределяет λ_T тогда и только тогда, когда $i \in T$. В случае, когда $\tilde{\Lambda}$ — матрица в двухбуквенном алфавите $\{0, *\}$, представление будем называть *строго двоичным*.

Будем говорить, что *множество столбцов* T матрицы Λ (i) *покрывает*, (ii) *инверсно покрывает*, (iii) *дважды покрывает* столбец λ_j, если (i) дизъюнкция столбцов λ_i, $i \in T$, покрывает λ_j, (ii) дизъюнкция инверсий столбцов λ_i, $i \in T$, покрывает инверсию столбца λ_j, (iii) множество столбцов T покрывает и инверсно покрывает λ_j. Матрица Λ *свободна от* $\mathcal{T}$*-покрытий* (*двойных* $\mathcal{T}$*-покрытий*), если для любого $T \in \mathcal{T}$ множество столбцов T не покрывает (не покрывает дважды) ни одного λ_j, $j \notin T$.

Теорема 1. Двоичное (строго двоичное) представление $(\Lambda, \tilde{\Lambda})$ с матрицей кодирования Λ существует для алфавита $A = A_{\mathcal{T}}$ тогда и только тогда, когда она свободна от двойных $\mathcal{T}$-покрытий ($\mathcal{T}$-покрытий).

По матрице Λ из теоремы можно эффективно (полиномиально) строить (строгие) представления недоопределённых последовательностей и восстанавливать по ним исходные последовательности, не используя $\tilde{\Lambda}$.

Скажем, что система $\mathcal{Z}$ подмножеств множества M образует *конъюнктивный базис* (*обобщённый конъюнктивный базис*) системы $\mathcal{T}$, если каждое множество $T \in \mathcal{T}$ может быть получено как пересечение некоторых множеств (множеств либо их дополнений) из $\mathcal{Z}$. Строке v, $v = 1, \ldots, s$, матрицы Λ сопоставим множество $Z_v \subseteq M$, образованное номерами единичных разрядов строки. Положим $\mathcal{Z} = \{Z_1, \ldots, Z_s\}$, $\mathcal{Z}' = \{\bar{Z}_1, \ldots, \bar{Z}_s\}$, где чёрточка означает дополнение. Для построения матриц, свободных от покрытий (либо двойных покрытий), может быть использован следующий факт.

Теорема 2. Матрица Λ свободна от $\mathcal{T}$-покрытий (двойных $\mathcal{T}$-покрытий) тогда и только тогда, когда соответствующая ей система $\mathcal{Z}'$ (система $\mathcal{Z}$) образует конъюнктивный базис (обобщённый конъюнктивный базис) системы $\mathcal{T}$.

Пусть $s(A)$ и $s_0(A)$ означают наименьшую размерность соответственно двоичных и строго двоичных представлений алфавита A. Недоопределённые данные, с которыми имеют дело в приложениях, обычно помимо неопределённого символа $*$ используют лишь символы, имеющие небольшое число доопределений. Обозначим через $s(m, n, t)$ максимумальную из размерностей $s(A)$ алфавитов A, для которых $|A_0| = m$, $|A| = n$ и каждый символ $a_T \in A$ имеет не более t доопределений либо является неопределённым. Аналогичную величину при использовании $s_0(A)$ обозначим $s_0(m, n, t)$.

Теорема 3. Справедливы оценки

$$s(m, n, t) \leqslant s_0(m, n, t) \leqslant e(t+1)\ln(mn) + 1.$$

Используя очевидное соотношение $n \leqslant m^t$, получаем границу вида $\mathrm{O}(t^2 \ln m)$. При малых t эта величина существенно меньше длины m естественного задания недоопределённых символов a_T посредством характеристического набора множества T.

Теорема 4. При выполнении условия $t = \mathrm{o}(\log n / \log\log n)$ имеют место оценки

$$s(m,n,t) \gtrsim \frac{(t-1)\log n}{2(2\log(t-1)+c)}, \quad s_0(m,n,t) \gtrsim \frac{(t+1)\log n}{2(2\log t + c)},$$

где $\log x = \log_2 x$, $c = \log(3e/4) < 1{,}027$.

При естественном условии $m \leqslant n$ верхние и нижние оценки теорем 3 и 4 различаются по порядку в $\log t$ раз.

В случае, когда система $\mathcal{T}$ состоит из всех t-элементных подмножеств множества M, $\mathcal{T}$-дизъюнктивную матрицу называют *t-дизъюнктивной*. Множество её столбцов образует *t-дизъюнктивный код*. Дизъюнктивные (superimposed) коды, введённые в [2], находят широкое применение в информатике. Эффективные методы построения t-дизъюнктивных кодов, развитые в [2, 3] и других работах, могут быть использованы для эффективного представления недоопределённых данных.

Более подробное изложение представленных результатов можно найти в [4].

ЛИТЕРАТУРА

1. *Шоломов Л. А.* Элементы теории недоопределенной информации // Прикладная дискретная математика. Приложение. 2009. № 2. С. 18–42.
2. *Kautz W. H. and Singleton R. C.* Nonrandom binary superimposed codes // IEEE Trans. Inform. Theory. 1964. V. 10. No. 4. P. 363–377.
3. *Kumar R., Rajagopalan S., and Sahai A.* Coding construction for blacklisting problems without computational assumptions // CRYPTO-99. LNCS. 1999. V. 1666. P. 609–623.
4. *Шоломов Л. А.* Двоичные представления недоопределённых данных и дизъюнктивные коды // Прикладная дискретная математика. 2013. № 1(19). С. 17–33.