МАТЕМАТИКА

УДК 681.21

Кадиев И.П., Кадиев П.А.

ИНФОРМАЦИОННАЯ СПОСОБНОСТЬ СООБЩЕНИЙ ДИСКРЕТНЫХ ИСТОЧНИКОВ

Kadiev I.P., Kadiev P.A.

INFORMATION POSSIBILITY OF MESSAGES OF DISCRETE SYMBOLS

В статье предложен комбинаторный подход к определению информационной способности отдельных сообщений дискретных источников как количества информации при учете однородности структуры, наличия в них повторяющихся элементов алфавита.

Ключевые слова: *количество информации, перестановки, структура сообщения.*

In the article is offered a combinatory approach for determination of information possibility of individual messages of discrete sources as quantity of information in them when taken into account recurrent alphabetic symbols and structural uniformity allowing to estimate and to optimize information possibilities of the used messages.

Key words: *the amount of information, permutation, message structure.*

Структурная ветвь теории информации предполагает использование в качестве меры количества информации в сообщениях дискретных источников с объемом алфавита $\mathbf{m}$, состоящих из $\mathbf{n}$ символов, количество различных комбинаторных конфигураций или функции от их числа. Общее число этих конфигураций, равное $\mathbf{m^n}$, впервые было предложено для оценки информационных возможностей дискретных источников Р. Хартли [2] в качестве меры количества информации. Позже им же была предложена в качестве этой меры величина $\mathbf{I = nLog_b m}$, где выбор основания логарифма $\mathbf{b}$ определяет выбор единиц измерения количества информации, известной, как аддитивная мера.

В последствии, в рамках структурной ветви появились комбинаторные меры количества информации, которые предлагают в качестве меры число или функции от числа комбинаторных конфигураций различных типов. Чаще других в качестве этих конфигураций используются размещения $\mathbf{A_m^n}$, сочетания $\mathbf{C_m^n}$ или перестановки $\mathbf{P_n}$, которые можно составить из символов дискретного источника.

Общепринятым в комбинаторной теории информации является то, что во всех сообщениях, состоящих из равного числа символов алфавита, одного и того же дискретного источника содержится равное количество информации, что является одним из недостатков предлагаемых мер. Поэтому эти меры характеризуют информационные возможности источника в целом и не позволяют определить количество информации в отдельных, конкретных сообщениях.

Это обстоятельство является еще одним недостатком, присущим современной теории информации, наряду с отсутствием учета семантических и субъективных факторов, характерных для отдельных сообщений. Поэтому представляют интерес любые предложения, позволяющие учесть зависимость количества информации в сообщениях от тех или иных особенностей отдельных сообщений.

В данной статье предлагаются меры количества информации в дискретных сообщениях, учитывающие структурные особенности сообщений, в частности, степень их структурной однородности, которая характеризует повторяемость в сообщениях отдельных символов алфавита источника. Предлагаемые меры введены в рамках комбинаторной ветви теории информации, в которой количество информации рассматривается как функция от числа перестановок элементов сообщений.

Анализ особенностей некоторых комбинаторных конфигураций [1], состоящих из равного числа символов, позволяет сделать вывод, что их число является функцией степени однородности структуры сообщения. При этом, под структурой сообщения следует понимать состав элементов, образующих это сообщение, общее количество элементов в нем, число элементов различных типов.

В данной статье рассмотрены вопросы определения количества информации при использовании в качестве меры количества информации числа возможных перестановок, с учетом только тех из них, которые отличаются друг от друга структурой. Наличие среди вариантов перестановок, повторяющихся по структуре, имеет место, если в исходных блоках или массивах данных, подлежащих перестановке, имеются повторяющиеся символы алфавита источника информации. Например, в слове ***барабан*** имеются перестановка типа ***бааабрн,*** в которой перестановка между собой местами букв ***а*** или ***б,*** расположенных на различных позициях исходного слова, не меняет ее структуры, при этом будет получена та же по структуре перестановка.

При использовании в качестве количества информации в сообщениях, состоящих из **n** символов, числа перестановок - оно равно общему числу возможных перестановок - **n!.** Однако эта величина значительно меньше, если рассматривать только отличающиеся друг от друга структурой перестановки.

Известно **[1]**, что если среди **n** символов сообщения имеются **k** различных символов, каждый из которых повторяется соответственно $\mathbf{n_1}$, $\mathbf{n_2}$,

$n_3,., n_k$ раз, при этом $n = n_1+n_2+ n_3+\ldots +n_k$, то формула для определения числа перестановок с различной структурой имеет вид:

$$P(n_1, n_2, n_3,\ldots, n_k) = n! / (n_1! * n_2! * n_3! * \ldots * n_k!) \tag{1}$$

При учете повторяемости символов количество информации в сообщениях одинаковой длины, формируемых одним и тем же дискретным источником при наличии повторяющихся символов в сообщениях, оказывается различными. Например, в словах источника ***барабан*** и ***зеркало*** при **n=7** для первого слова число различимых перестановок определяется по формуле**:**

$$P_7(2, 3, 1, 1) = 7! /(2!\, 3!\, 1!1!) = 840,$$ для второго - $P_7 = 7! = 5040$.

В данном примере в слове с неповторяющимися символами число различимых перестановок в 6 раз больше, чем в слове с повторяющимися символами. С точки зрения комбинаторного подхода к определению количества информации в сообщениях дискретных источников, с использованием в качестве ее меры числа перестановок, в сообщениях, состоящих из равного числа символов, количество информации существенно различно и зависит от структуры исходных сообщений, их структурной однородности: наличия или отсутствия в них повторяющихся символов.

Таким образом, информационные способности сообщений, характеризующих количество информации в них, зависят от их структуры. При использовании логарифмической меры:

$$I_n = \mathrm{Log}_b P = \mathrm{Log}_b\, n! / (n_1! * n_2! * n_3! * \ldots * n_k!)$$

Для частных случаев, когда число различных символов в блоке из **n** символов равно **k** и все они повторяются равное число раз - **n/k,** формула (1) принимает вид:

$$P_n(n/k, n/k, ,\ldots, n/k) = n! / [(n/k) !]^k$$

Величина, обратная приведенной выше, характеризует частоту повторения сообщений в случайной последовательности с равномерным законом распределением.

Особый интерес вызывают приведенные результаты для последовательностей из двух символов, используемых в потоках данных, при хранении в устройствах памяти. При тех же условиях что и выше для двоичных последовательностей формула (1) имеет соответственно вид:

$$P(n_1, n_2) = n! / (n_1! * n_2!) \tag{2}$$

Естественно, что при использовании перестановок для оценки количества информации в сообщениях **I**, возникает вопрос, при каких соотношениях числа двоичных символов различных типов в последовательностях из **n** символов число перестановок $\mathbf{P_n}$, имеющих различные структуры, будет максимальным, что является условием максимума количество информации в таких последовательностях.

Анализ выражения (2) для двоичных последовательностей показывает, что оно максимально при равном числе в сообщениях двоичных символов каждого типа, т.е. при выполнении условия $\mathbf{n_1 = n_2 = n/2}$ и определяется из выражения вида:

$$\mathbf{max\ P\ (n/2,\ n/2) = n!\ /\ [\ (\ n/2)! * (\ n/2)!].} \quad (3)$$

В справедливости утверждения можно убедиться, представив формулу (3) в виде $\mathbf{P\ [(n/2) - j,\ (n/2 + j] = n!\ /\ [\ (\ n/2) - j\ ]! * [(n/2) + j]!}$,

или $\mathbf{I_n = Log_b P = Log_b n! - Log_b [(n/2) - j]! - Log_b P [(n/2) + j]!}$, (4)

Где **j** - число, показывающее превышение числа символов одного типа над другим.

Подставляя в **(4)** различные значения **j**, можно убедиться в справедливости отмеченного выше условия максимума числа структурно различимых перестановок при равенстве числа символов обоих типов в двоичной последовательности.

Полученные результаты согласуются и с результатами, полученными в статистической ветви теории информации, где доказано, что одним из условий максимума энтропии двоичных источников информации является равенство частот появления двоичных символов в последовательностях.

Можно обратить внимание и на то обстоятельство, что формула (4) соответствует числу комбинаторных конфигураций типа сочетаний из **n** элементов по **n/2:**

$$\mathbf{C_n^{n/2} = n!\ /\ (n/2)!\ (n/2)!.}$$

Это означает, что при определенных условиях имеет место равенство числа конфигураций разных типов: числа перестановок с различной структурой из **n** двоичных элементов, при равенстве в последовательностях числа элементов различных типов, и числа сочетаний из **n** по **n/2** - $\mathbf{C_n^{n/2}}$.

Следовательно, можно считать, что является справедливым следующее утверждение**: максимальное число структурно различных перестановок из двоичных последовательностей, состоящих из «n» элементов, при равенстве числа символов различных типов, равно числу сочетаний из этих последовательностей $\mathbf{C_n^{n/2}}$, во всех остальных соотношениях между количеством двоичных символов оно меньше этого числа.**

Полученные результаты подтверждают общность сущности природы подходов к измерению количества информации в комбинаторной и статистической ветвях теории информации. Условие максимума числа различимых перестановок может быть использовано при решении задач, связанных с повышением эффективности информационных процессов.

Выше были рассмотрены и проанализированы вопросы внутриблочных перестановок, образующих сообщения из **n** элементов. Они в основном предполагали перестановки элементов внутри отдельного информационного блока данных, состоящего из **n** элементов. На практике перестановки могут осуществляться и между блоками сообщений, каждый из которых состоит из **n** элементов, образующих информационные массивы сообщений, состоящих из **m** сообщений и **mxn** элементов.

При определении количества информации в виде числа перестановок в информационном массив **mxn,** можно рассматривать его как конфигурацию, состоящую из **m** строк и **n** столбцов, которые могут переставляться, как раздельно, так и одновременно. Если не учитывать то, что среди строк и столбцов элементов могут быть одинаковые по структуре, то при каждой из **m!** общем числе перестановок строк – сообщений может быть выполнено **(n-1)!** перестановок столбцов. Общее число таких перестановок в массиве будет равно **m!* (n-1)!.** Эта величина и характеризует комбинаторную меру количества информации в информационном **mxn** массиве, как общее число возможных перестановок элементов в массиве:

$$\mathbf{I = Log_b\, m! + Log_b\, (n-1)!.} \qquad (5)$$

При учете возможности наличия одинаковых строк и одинаковых столбцов это число значительно меньше. Оно будет зависеть от числа одинаковых строк и столбцов в массиве. Если информационный массив структурно не избыточен, то в нем не должно быть одинаковых сообщений, и общее число перестановок строк равно **m!.** Если в массиве нет и одинаковых столбцов, то для общего числа возможных перестановок справедливо выражение (5), приведенное выше. Для квадратных **n x n** массивов формула (5) принимает вид:

$$\mathbf{I = Log_b\, n! + Log_b\, (n-1)} \qquad (6)$$

Для массивов, элементами которых являются двоичные символы, количество информации, определяемое как количество перестановок строк и столбцов, для общего случая, предполагающего наличия повторяющихся строк и столбцов, приведенная выше формула **(5)** имеет вид:

$$\mathbf{P\,(m_1, m_2) = m! / (\, m_1! * m_2!)\,,\ P\,(n_1, n_2) = n! / (\, n_1! * n_2!)}$$
$$\mathbf{I_м} = \mathrm{Log_b}\mathbf{[m! / (\, m_1! * m_2!)] * [n! / (\, n_1! * n_2!)]} \qquad (7)$$

При равенстве числа двоичных символов разного типа, что обеспечивает максимум различимых перестановок и максимум количества информации в массиве, формула для определения количества информации принимает вид:

$$\mathbf{P = m! \, / \, [(m/2)!^2] * n! \, / [(n/2)!^2]} \quad (8)$$

$$\mathbf{I_м = Log_b\, m! \, / \, [(m/2)!^2] + Log_b\, n! \, / \, [(n/2)!^2] =}$$

$$\mathbf{Log_b\, m! - 2Log_b\,(m/2)! \; + Log_b\, n! - 2\, Log_b\,(n/2)!}$$

В заключение следует отметить, что в данной статье предложен комбинаторный подход к оценке количества информации в сообщениях с учетом их структурной однородности. При этом количество информации в сообщениях источника является не только функцией от объема его алфавита и числа элементов в нем, но зависит и от структуры самого сообщения. Это обстоятельство весьма важно при решении определенного класса задач, в частности, в криптографии при использовании методов перестановок для шифрования информации, число перестановок, в ряде случаев, рассматривается как число ключей шифрования, которые определяют такую характеристику шифра как стойкость.

Библиографический список:

1. Виленкин Н.Я. Комбинаторика. – М.: «Наука»,1969, 340с.
2. Хартли Р. Передача информации // Теория информации и ее приложения: сб. переводов под ред. А.А. Харкевича. - М.:Физматгиз,1959.- 328 с.

УДК: 528.2/.3

Мамедбеков С.Н.

ИССЛЕДОВАНИЕ ДИНАМИКИ ИЗМЕНЕНИЯ АБСЦИСС И ОРДИНАТ ТОЧЕК НА КРАЙНЕМ МЕРИДИАНЕ ШЕСТИГРАДУСНОЙ ЗОНЫ В ПРОЕКЦИИ ГАУССА-КРЮГЕРА

Mamedbekov S.N.

THE STUDY OF DYNAMICS OF CHANGE OF THE ABSCISSA AND ORDINATE OF THE POINT AT THE FAR MERIDIAN SIX DEGREE ZONE IN THE PROJECTION GAUSS-KRUGER

В данной работе рассматривается динамика изменения абсцисс и ординат точек на крайнем меридиане шестиградусной зоны в конформной проекции Гаусса-Крюгера. Выполнены вычисления и графическое представление результатов по классическим формулам конформной проекции.