дискретно-тонового изображения оказывается, что различные значения таких параметров, как количество подряд идущих пикселей одного цвета, а также расстояние до ближайшего встреченного пикселя такого же цвета, не являются равновероятными, то есть такие данные имеют статистическую избыточность.

3. Массив пикселей. Будем называть этот массив остаточным изображением. Это те пиксели исходного изображения, которые не были заменены в ходе кодирования гибридным алгоритмом некоторыми служебными данными. Как правило, статистическая избыточность в этом массиве невысока. Зато в этих данных присутствует некоторая пространственная избыточность. Часто в остаточном изображении можно увидеть группы подряд идущих пикселей по вертикали или горизонтали близких цветов. Такой тип пространственной избыточности характерен для остаточного изображения, так как гибридный алгоритм не может его устранить.

Каждый из результирующих наборов данных гибридного алгоритма обладает специфическим типом избыточности и поэтому сжимается по отдельности на втором этапе выполнения комбинированного алгоритма. Создано два комбинированных алгоритма, использующих гибридный алгоритм на первом этапе сжатия. При тестировании комбинированный алгоритм, использущий на втором этапе библиотеку `zlib` [3], продемонстрировал более высокую степень сжатия. В тестировании принимали участие реализации 14 алгоритмов, некоторые из них с различными настройками. Тестирование проводилось на двух наборах данных: изображениях с преобладанием текста и с преобладанием деловой графики. Комбинированный алгоритм, основанный на гибридном алгоритме и `zlib`, обеспечил наивысшую степень сжатия на обоих тестовых наборах данных, превзойдя по этому показателю следующий за ним `zlib` с уровнем сжатия 9 на 9,5 % при сжатии изображений с преобладанием деловой графики и на 4 % — изображений с преобладанием текста. При этом комбинированный алгоритм, использующий на втором этапе `zlib`, производит сжатие быстрее, чем `zlib` уровня 9, в обоих случаях.

ЛИТЕРАТУРА

1. *Сэломон Д.* Сжатие данных, изображений и звука. М.: Техносфера, 2006. 365 с.
2. *Дружинин Д. В.* Комбинированный алгоритм сжатия ключевых кадров экранного видео // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2011. № 3(16). С. 67–77.
3. zlib [Электронный ресурс]. `http://zlib.net`

УДК 519.212.2

ВЕРОЯТНОСТНЫЕ ХАРАКТЕРИСТИКИ ВЕСОВЫХ СПЕКТРОВ СЛУЧАЙНЫХ ЛИНЕЙНЫХ ПОДКОДОВ НАД GF(p)

А. М. Зубков, В. И. Круглов

Получены формулы для первых двух моментов элементов весового спектра равновероятно выбранного линейного подкода фиксированного линейного кода над конечным полем F_p в терминах его весового спектра, а также оценки для распределения минимального веса ненулевого кодового слова в выбранном подкоде. Выведены формулы для распределения веса суммы двух независимых случайных векторов над F_p с заданными весами, вычислены математическое ожидание и дисперсия этого распределения.

Ключевые слова: *линейные коды, случайные подкоды, весовой спектр, слово минимальноо веса.*

Пусть p — фиксированное простое число. Будем обозначать через $F_p^N = \{X = (x_1, \ldots, x_N) : x_1, \ldots, x_N \in F_p\}$ линейное N-мерное пространство над простым полем F_p. Любое k-мерное ($k < N$) подпространство $L \subset F_p^N$ будем называть k-мерным линейным кодом.

Весом вектора $X = (x_1, \ldots, x_N) \in F_p^N$ назовём число $\mathrm{w}(X) = \sum\limits_{k=1}^{N} I\{x_k \neq 0\}$ его ненулевых координат.

Через $\left(F_p^N\right)_s$ и $\left(F_p^N\right)_{\leqslant s}$ будем обозначать соответственно множество векторов фиксированного веса s и множество ненулевых векторов веса, не превосходящего s, в F_p^N :

$$\left(F_p^N\right)_s = \left\{X \in F_p^N : \mathrm{w}(X) = s\right\}, \quad \left(F_p^N\right)_{\leqslant s} = \left\{X \in F_p^N : 0 < \mathrm{w}(X) \leqslant s\right\};$$

тогда $F_p^N = \bigsqcup\limits_{s=0}^{N} \left(F_p^N\right)_s$.

Определение 1. Пусть $v_s(L) = |L \cap \left(F_p^N\right)_s|$ и $v_{\leqslant s}(L) = |L \cap \left(F_p^N\right)_{\leqslant s}|$ — количество соответственно векторов веса s и ненулевых векторов веса не больше s в линейном коде L; набор $\{v_s(L)\}_{s=0}^N$ называют *весовым спектром* кода L.

Предельные пуассоновские теоремы для случайных величин $v_s(L)$ и аналогичных им доказаны в [1, 2].

Зафиксируем некоторый k-мерный линейный код L и рассмотрим k^*-мерный случайный код L^*, выбранный случайно и равновероятно из множества всех k^*-мерных подкодов кода L. Пусть $\{v_s(L^*)\}_{s=0}^N$ — весовой спектр выбранного случайного кода L^*.

Теорема 1. Если $L \subset F_p^N$ — линейный k-мерный код в F_p^N с весовым спектром $\{v_s = v_s(L)\}_{s=0}^N$, а L^* — случайный равновероятный k^*-мерный подкод L, $1 \leqslant k^* < k$, то при $s = 1, \ldots, N$

$$\mathbf{E}v_s(L^*) = v_s(L)\frac{p^{k^*} - 1}{p^k - 1},$$

$$\mathbf{D}v_s(L^*) = v_s(L)\frac{(p^{k^*} - 1)(p^k - p^{k^*})(p-1)}{(p^k - 1)^2}\left(1 - \frac{v_s(L) - (p-1)}{p^k - p}\right)$$

и при $s, t \in \{1, \ldots, N\}$, $s \neq t$,

$$\mathrm{cov}(v_s(L^*), v_t(L^*)) = -v_s(L)v_t(L)\frac{(p^{k^*} - 1)(p^k - p^{k^*})(p-1)}{(p^k - 1)^2(p^k - p)}.$$

Если $L = F_p^N$, т. е. $1 \leqslant k^* < k = N$, то, согласно теореме 1,

$$\mathbf{E}v_s(L^*) = v_s(F_p^N)\frac{p^{k^*} - 1}{p^N - 1}, \quad \text{где} \quad v_s(F_p^N) = C_N^s(p-1)^s,$$

$$\mathbf{D}v_s(L^*) = v_s(F_p^N)\frac{(p^{k^*} - 1)(p^N - p^{k^*})(p-1)}{(p^N - 1)^2}\left(1 - \frac{v_s(F_p^N) - (p-1)}{p^N - p}\right).$$

Вероятностные характеристики элементов весового спектра случайно выбранного линейного кода L^*, содержащего $p^{k^*} - 1$ ненулевых векторов, заметно отличаются от аналогичных характеристик элементов весового спектра случайного множества M,

выбранного равновероятно из совокупности $(p^{k^*}-1)$-элементных подмножеств множества F_p^N. Математические ожидания элементов весового спектра совпадают:

$$\mathbf{E}v_s(M) = v_s(F_p^N)\frac{p^{k^*}-1}{p^N-1} = \mathbf{E}v_s(L^*),$$

а отношение дисперсий

$$\frac{\mathbf{D}v_s(M)}{\mathbf{D}v_s(L^*)} = \frac{1}{p-1}\left(1+\frac{p^{k^*}}{p^N-p^{k^*}}\right)\frac{1-\dfrac{p^{k^*}-2}{p^N-2}-v_s(F_p^N)\dfrac{p^N-p^{k^*}}{(p^N-1)(p^N-2)}}{1-\dfrac{v_s(F_p^N)-(p-1)}{p^N-p}}$$

заметно меньше 1 (более того, меньше $1/(p-1)$) при $p \geqslant 3$.

Теорема 2. Если выполнены условия теоремы 1, то

$$\mathbf{E}v_{\leqslant s}(L^*) = \frac{p^{k^*}-1}{p^k-1}\,v_{\leqslant s}(L),$$

$$\mathbf{D}v_{\leqslant s}(L^*) = \frac{(p^{k^*}-1)(p^k-p^{k^*})(p-1)}{(p^k-1)^2}\,\frac{p^k-1-v_{\leqslant s}(L)}{p^k-p}\,v_{\leqslant s}(L) \leqslant (p-1)\,\frac{p^k-p^{k^*}}{p^k-1}\,\mathbf{E}v_{\leqslant s}(L^*)$$

и для минимального веса $\mu(L^*) = \min\{\mathrm{w}(X) : X \in L^*\backslash\{0\}\}$ ненулевых векторов в L^* справедлива оценка

$$\frac{1}{1+\dfrac{p^k-p^{k^*}}{p^k-1}\,(p-1)(\mathbf{E}v_{\leqslant s}(L^*))^{-1}} \leqslant \mathbf{P}\{\mu(L^*) \leqslant s\} \leqslant \mathbf{E}v_{\leqslant s}(L^*).$$

Теорема 3. Если X и Y — независимые случайные векторы, причём вектор X имеет равномерное распределение на множестве $(F_p^N)_s$ всех векторов веса s, а вектор Y имеет равномерное распределение на множестве $(F_p^N)_t$ всех векторов веса t, то при $|s-t| \leqslant m \leqslant \min\{s+t, N\}$

$$\mathbf{P}\left\{\mathrm{w}(X+Y)=m\right\} = \sum_{j=\max\{0,s+t-N\}}^{s} \frac{C_s^j C_{N-s}^{t-j}}{C_N^t}\,C_j^{m-(s+t-2j)}\,\frac{(p-2)^{m-(s+t-2j)}}{(p-1)^j},$$

$$\mathbf{E}\mathrm{w}(X+Y) = s+t-\frac{p}{p-1}\,\frac{st}{N},$$

$$\mathbf{D}\mathrm{w}(X+Y) = \frac{st}{N}\left(\frac{p^2}{(p-1)^2}\,\frac{N}{N-1}\left(1-\frac{t}{N}\right)\left(1-\frac{s}{N}\right)+\frac{p-2}{(p-1)^2}\right).$$

Доказательства теорем 1–3 опубликованы в [3]; перечисленные результаты могут применяться при исследовании системы шифрования Мак-Элис [4, 5].

ЛИТЕРАТУРА

1. *Копытцев В. А., Михайлов В. Г.* Теоремы пуассоновского типа для числа специальных решений случайного линейного включения // Дискретная математика. 2010. Т. 22. Вып. 2. С. 3–21.
2. *Михайлов В. Г.* Предельные теоремы для числа решений системы случайных линейных уравнений, попавших в заданное множество // Дискретная математика. 2007. Т. 19. Вып. 1. С. 17–26.

3. *Зубков А. М., Круглов В. И.* Статистические характеристики весовых спектров случайных линейных кодов над GF(p) // Математические вопросы криптографии. 2014. Т. 5. Вып. 1. С. 27–38.
4. *Berson T.* Failure of the McEliece public-key cryptosystem under message-resend and related-message attack // LNCS. 1997. V. 1294. P. 213–220.
5. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory. Jet Propulsion Lab. DSN Progress Report 42–44, 1978.