МЕТОД СЖАТИЯ НОРМ СИНДРОМОВ ДЛЯ КОРРЕКЦИИ КРАТНЫХ ОШИБОК

Липницкий В.А., Конопелько В.К., Курилович А.В.

БГУИР
220027, г.Минск ул. П.Бровки 6

БЧХ-коды относятся к разряду наиболее популярных в теории и практике помехоустойчивых кодов [1]. В [2,3,4] разработана теория норм синдромов для БЧХ-кодов и их модификаций, позволяющая предложить перестановочные методы коррекции ошибок названными кодами, не прибегая к решению уравнений в полях Галуа. Применение норм синдромов позволяет расширить спектр декодируемых ошибок по сравнению с традиционными методами. Норменный метод, в принципе, не зависит от роста d, но его реализация наталкивается на рост аппаратурной сложности, связанный с увеличением объема обрабатываемых норм синдромов.

В докладе предлагается подход к преодолению названной трудности, дается математическое обоснование и изложение модифицированного норменного метода коррекции кратных ошибок, основанного на сжатии множества норм Г-орбит корректируемой совокупности K путем отображения множества K на ошибки большей кратности со специальными свойствами синдромов.

В дальнейшем рассматривается произвольный двоичный примитивный в узком смысле БЧХ-код C с проверочной матрицей $\mathrm{H}=\left[\alpha^{i},\alpha^{3\cdot i},\ldots,\alpha^{(2\cdot t-1)\cdot i}\right]^{\mathrm{T}}$, $0\le i\le n-1$, где $n=2^{m}-1$, α - примитивный элемент поля Галуа $GF\left(2^{m}\right)$ [1]. В этом коде имеется C_n^{ω} векторов-ошибок весом ω. По значениям первой компоненты s_1 синдромов ошибки делятся на $n+1$ классов. Важную роль играют множества $\mathrm{M}_{0,\omega}$ и $\mathrm{M}_{1,\omega}$ всех векторов весом ω и с компонентой $s_1=0$ и $s_1=1$ соответственно.

Теорема 1. *Пусть $T_\omega=\left|M_{0,\omega}\right|$ – мощность множества векторов ошибок, с компонентой синдрома $s_1=0$ в БЧХ-коде С. Тогда $T_1=T_2=0;\ T_3=C_n^2/3;\ T_4=(C_n^3-T_3)/4$, а для $\omega>4$:* $T_\omega=\left[C_n^{\omega-1}-T_{\omega-1}-T_{\omega-2}(n-\omega+2)\right]/\omega$.

Пусть $\overline{1}=(1,0,\ldots,0)$ и $\tau:\overline{f}\to\overline{f}+\overline{1}=\overline{h}$ - отображение, связывающее множество $\mathrm{M}_{1,\omega}$ с $\mathrm{M}_{0,\omega+1}$ и $\mathrm{M}_{0,\omega-1}$. Через $(i_1,i_2,\ldots,i_\omega)$ обозначаем вектор-ошибку в коде C с единственными ненулевыми и равными 1 координатами на позициях $i_1,i_2,\ldots,i_\omega$.

Предложение 1. *Справедливы следующие равенство и включения:*
1) $\tau\left(\mathrm{M}_{1,1}\right)=\{0\}$; *2)* $\tau\left(\mathrm{M}_{1,2}\right)\subset\mathrm{M}_{0,3}$; *3)* $\tau\left(\mathrm{M}_{1,3}\right)\subset\mathrm{M}_{0,4}$; *4)пусть* $4\le\omega<n$ *и вектор* $\overline{f}=(1,i_2,\ldots,i_\omega)\in\mathrm{M}_{1,\omega}$, $1<i_2<\ldots<i_\omega$, *тогда* $\tau\left(\overline{f}\right)\in\mathrm{M}_{0,\omega-1}$; *если же* $\overline{f}=(i_1,i_2,\ldots,i_\omega)\in\mathrm{M}_{1,\omega}$, *где* $1<i_1<i_2<\ldots<i_\omega$, *то* $\tau\left(\overline{f}\right)\in\mathrm{M}_{1,\omega+1}$.

Согласно предложению 1 отображение τ делит $\mathrm{M}_{1,\omega}$ на два непересекающихся класса: $\mathrm{M}_{1,\omega}^{1}$ - состоящий из всех векторов $\overline{f}=(1,i_2,\ldots,i_\omega)\in\mathrm{M}_{1,\omega}$, и $\tilde{\mathrm{M}}_{1,\omega}=\mathrm{M}_{1,\omega}-\mathrm{M}_{1,\omega}^{1}$.

Полная Г-орбита ошибок весом $\omega\ge1$ с полным спектром синдромов и $s_1\ne0$ содержит единственный вектор $\overline{f}\in\mathrm{M}_{1,\omega}$. Пусть $\overline{f}\in\tilde{\mathrm{M}}_{1,\omega}$. Тогда $\tau\left(\overline{f}\right)=\overline{h}=(1,i_1,\ldots,i_\omega)\in\mathrm{M}_{0,\omega+1}$. Г-орбита $<\overline{h}>$ содержит несколько векторов с первой координатой, равной 1. О том, какие вектора $\overline{f}$ их порождают с помощью отображения τ, говорит следующее утверждение.

Предложение 2. *Пусть вектор $\overline{h}=(i_1,i_2,\ldots,i_\omega)$ порождает полную Г-орбиту и имеет $s_1=0$ в коде С. Тогда все векторы $\overline{f}_k$ весом $\omega-1$, получающиеся занулением первой координаты у вектора $\sigma^{i_k-1}\left(\overline{h}\right)$, $1\le k\le\omega$, попарно различны и, более того, порождают ω различных Г-орбит, но принадлежат $\mathrm{M}_{1,\omega-1}$.*

Множество $\mathrm{M}_{0,\omega-1}$ можно разделить на два непересекающихся подмножества: $\mathrm{M}^1_{0,\omega-1}=\left\{\overline{f}\in \mathrm{M}_{0,\omega} \mid \overline{f}=(1,i_2,\ldots,i_\omega)\right\}$ и $\tilde{\mathrm{M}}_{0,\omega}=\mathrm{M}_{0,\omega}-\mathrm{M}^1_{0,\omega}$. Тогда отмеченные предложением 1 включения можно уточнить следующим образом:

$$\tau\left(\mathrm{M}^1_{1,\omega}\right)\subseteq\tilde{\mathrm{M}}_{0,\omega-1};\ \tau\left(\tilde{\mathrm{M}}_{1,\omega}\right)\subseteq\mathrm{M}_{0,\omega+1}. \text{ (*)}$$

Теорема 2. *Отображение τ устанавливает взаимно однозначное соответствие между множествами $\mathrm{M}^1_{1,\omega}$ и $\tilde{\mathrm{M}}_{0,\omega-1}$, $\tilde{\mathrm{M}}_{1,\omega}$ и $\mathrm{M}^1_{0,\omega-1}$, включения (*) являются равенствами.*

Следствие 1. *Отображение τ устанавливает взаимно однозначное соответствие между множествами $\mathrm{M}_{1,2}$ и $\mathrm{M}_{0,3}$, $\mathrm{M}_{1,3}$ и $\mathrm{M}^1_{0,4}$.*

Следствие 2. *Пусть векторы из $\mathrm{M}_{0,\omega+1}$ порождают полные Г-орбиты. Тогда количество $\left|\Gamma\mathrm{M}_{0,\omega+1}\right|$ этих Г-орбит равно $\left|\tilde{\mathrm{M}}_{1,\omega}\right|/(\omega+1)=\left|\mathrm{M}_{0,\omega+1}\right|/n$; $\left|\Gamma\mathrm{M}_{0,3}\right|=\left|\mathrm{M}_{1,2}\right|/3$; $\left|\Gamma\mathrm{M}_{0,4}\right|=\left|\mathrm{M}_{1,3}\right|/4$.*

Установленные факты позволяют модифицировать метод норм синдромов [3] с целью сокращения хранимой в ПЗУ информации. Он заключается в погружении ошибок весом $\omega-1$ во множество ошибок весом ω и с первой компонентой синдрома $s_1=0$.

Пусть принятое сообщение содержит неизвестный вектор ошибок $\overline{e}$, принадлежащий корректируемой совокупности K, а его синдром $S(\overline{e})=(s_1,s_2,\ldots,s_t)$ имеет первую компоненту $s_1=\alpha^q\neq 0$, $0\le q<n$. Осуществим циклический сдвиг координат вектора $\overline{e}$ на $n-q$ разрядов. Фактически же мы от синдрома $S(\overline{e})$ перейдем к синдрому $S=\left(\alpha^{n-q}\cdot s_1,\alpha^{3\cdot(n-q)}\cdot s_2,\ldots,\alpha^{(2\cdot t-1)\cdot(n-q)}\cdot s_t\right)$. Здесь $\alpha^{n-q}\cdot s_1=1=\alpha^0$. Такой синдром имеет единственный вектор $\overline{f}\in<\overline{e}>$. При этом во многих важных случаях (например, при $\omega=2,3$ в силу предложения 1) первая координата вектора $\overline{f}$ равна нулю. Тогда у вектора $\overline{g}=\overline{f}+\overline{1}$ первая координата равна 1, а синдром $S(\overline{g})=S(\overline{f})+(1,1,\ldots,1)$ и первая компонента синдрома $s_1(\overline{g})=0$. Векторы $\overline{g}$ образуют подмножество $\mathrm{M}^1_{0,\omega}$ в множестве $\mathrm{M}_{0,\omega}$. Согласно следствию 2 из теоремы 2 количество Г-орбит, содержащих такие векторы $\overline{g}$, примерно в ω раз меньше, чем Г-орбит векторов $\overline{f}$ весом $\omega-1$. Эти орбиты объединяются в циклоклассы. Показатели компоненты норм Г-орбит каждого циклокласса образуют циклотомические классы по модулю n. Поэтому, зная один из показателей, остальные однозначно восстанавливаются по известной структуре циклотомических классов. Таким образом, в памяти хранятся значения одной из норм каждого циклокласса ошибок множества $\mathrm{M}_{0,\omega}$ - список Z. По вычисленному синдрому $S(\overline{g})$ вычисляем его норму $\overline{N}=\overline{N}\left(S(\overline{g})\right)$ или показатели компонент этой нормы. Норму сравниваем с хранящимся списком Z. Предположим, что $\overline{N}=\overline{N}(J)\in Z$, т.е. норма $\overline{N}$ совпадает с нормой Г-орбиты J ошибок из $\mathrm{M}_{0,\omega}$. Тогда $\overline{g}$ совпадает с одним из векторов этой Г-орбиты вида $(1,i_2,\ldots,i_\omega)$. Таблица их синдромов также должна храниться в памяти. Сравнив $S(\overline{g})$ с этими синдромами, мы тем самым идентифицируем вектор $\overline{g}$: он равен тому вектору $\overline{f}_k\in J$, для которого $S(\overline{f}_k)=S(\overline{g})$. Тогда $\overline{f}=\overline{f}_k+\overline{1}$ и искомый вектор ошибок $\overline{e}=\sigma^q\left(\overline{f}_k+\overline{1}\right)$. Если $\overline{N}\notin Z$, то вычисляем $\overline{N}^2$ и сравниваем его со списком и т.д. В конце концов, для некоторого k, $1\le k\le m$, величина $\overline{N}^{2^k}$ будет принадлежать списку норм Z. Следовательно, $\varphi^k(\overline{g})=\overline{f}_k\in J$. Тогда $\overline{g}=\varphi^{m-k}\left(\overline{f}_k\right)$, а искомый вектор $\overline{e}=\sigma^q\left(\varphi^{m-k}\left(\overline{f}_k\right)+\overline{1}\right)$.

Отметим, что возможны совпадения спектров норм различных циклоклассов множества $\mathrm{M}_{0,\omega}$. Если при этом спектры векторов из $\mathrm{M}^1_{0,\omega}$, принадлежащих таким классам, не пересекаются, то такая ситуация только уменьшает список Z и благоприятна для реализации. Следует также помнить, что

при конкретной реализации метода список Z будет содержать нормы Г-орбит из $\mathrm{M}_{0,3}, \mathrm{M}_{0,4}, \ldots, \mathrm{M}_{0,t}$, если код декодирует t - кратные ошибки, $t \geq 2$. Метод прост в реализации при коррекции ошибок весом $1 \div 3$, так как в этом случае нет необходимости учитывать ошибки, вес которых уменьшается под действием τ (за исключением одиночных, что легко учитывается). При этом векторы с компонентой синдрома $s_1 = 0$ имеют норму синдрома $\bar{N} = (\infty, \infty, N_3)$. Поэтому список Z в данном случае реально должен состоять из значений одного параметра N_3 или его показателя $\deg N_3$.

Для прямой реализации метода норм синдромов потребовалось бы заполнить $\frac{1}{n}\left[C_n^2 + n + C_n^3\right] = \frac{n^2+5}{6}$ норм Г-орбит ошибок весом $1 \div 3$ (если это число целое и примерно столько же, если дробное), имеющих 3 координаты, столько же синдромов образующих (по крайней мере по одной координате синдрома) и столько же образующих Г-орбит. Метод погружения $\mathrm{M}_{1,\omega\text{-}1}$ в $\mathrm{M}_{0,\omega}$ требует знания информации об $\frac{1}{n}\left[\frac{1}{3}C_n^2 + \frac{1}{4 \cdot n}\left(C_n^3 - \frac{1}{3}C_n^2\right)\right] = \frac{n^2+1}{24}$ Г-орбитах (если это число целое и немногим больше – если дробное). Если использовать циклотомические подстановки, то следует запомнить $\left(n^2+1\right)/(m \cdot 24)$ значений N_3 или $\deg N_3$, а реально меньше, так как возможны (как показывают примеры, см. [5]) совпадения значений N_3 для различных циклоклассов ошибок из $\mathrm{M}_{0,3}$ и $\mathrm{M}_{0,4}$. Это в $4 \cdot m$ раза меньше, чем $\left(n^2+1\right)/6$. При этом из каждого циклокласса следует запомнить по 3 или 4 вектора, имеющих первую, равную 1, координату, а также показатели одной из координат их синдромов.

Литература

1. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки: Пер. с англ. – М.: Связь, 1979.-744 с.
2. Конопелько В.К., Липницкий В.А. Перестановочный метод декодирования БЧХ-кодов и его возможности. 1-ая Международная конференция “Цифровая обработка сигналов и ее применение”, Москва, 30 июня - 3 июля 1998г. Доклады, т.II, с. 79-86.
3. Конопелько В.К., Липницкий В.А. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. – Мн.: БГУИР, 2000. – 242 с.
4. Липницкий В.А., Конопелько В.К. Перестановочный метод декодирования реверсивных кодов и его возможности. // 2-ая МНК “Цифровая обработка сигналов и её применения”, 21-24 сент. 1999г., М., Доклады, т. 1, с. 158-163.
5. Качановский Д.В., Конопелько В.К., Липницкий В.А. Декодирование БЧХ-кодов с помощью норм синдромов, циклических и циклотомических перестановок. // 2-ая МНК “Цифровая обработка сигналов и её применения”, 21-24 сент. 1999г., М., Доклады, т. 1, с. 146-150.

METHOD OF COMPRESSION OF SYNDROM NORMS FOR CORRECTION OF MULTIPLE ERRORS

Lipnitsky V., Konopelko V., Kurilovich A.

BCH-codes concern to the category of the most popular in the theory and practice of noise-resistant codes [1]. In [2] the theory of syndrom norms for BCH-codes and their modifications is developed, allowing to offer permutable methods of correction of errors the named codes, not resorting to the decision of the equations in Galois fields. Application of norms of syndromes allows to expand a spectrum of decoding errors in comparison with traditional methods, the method of norms, basically, does not depend on growth d, but its realization encounters growth of hardware complexity, connected with increase of volume of processable norms of syndromes.

In the report the approach to overcoming the named difficulty is offered, the mathematical substantiation and a statement of modified norms method of correction of the multiple errors is given, that is based on compression of the set of Γ-orbits normes of corrected set K by the way of a map of K on to errors of the greater frequency rate with special properties of syndromes.

Further the any binary primitive BCH-code C in narrow sense h [1] is considered. On values the first components s_1 of syndromes of a error are distributed on $n+1$ classes. The important role is played with sets $\mathrm{M}_{0,\omega}$ and $\mathrm{M}_{1,\omega}$ for all vectors of weight ω and with component $s_1 = 0$ and $s_1 = 1$ accordingly.

Theorem 1. *Let* $T_\omega = \left|M_{0,\omega}\right|$ *- capacity of set of vectors of errors, with component* of *syndrome* $s_1 = 0$ *in the BCH-code C. Then* $T_1 = T_2 = 0;\ T_3 = C_n^2/3\ T_n = (C_n^3 - T_3)/4$, *and for* $\omega > 4$*:* $T_\omega = \left[C_n^{\omega-1} - T_{\omega-1} - T_{\omega-2}(n-\omega+2)\right]/\omega$.

Let $\overline{1} = (1,0,\ldots,0)$ and $\tau : \overline{f} \to \overline{f} + \overline{1} = \overline{h}$ - The display connecting set $\mathrm{M}_{1,\omega}$ With $\mathrm{M}_{0,\omega+1}$ and $\mathrm{M}_{0,\omega-1}$. Each of sets $\mathrm{M}_{0,\omega}$ And $\mathrm{M}_{1,\omega}$ is possible to divide into two not crossed subsets: $\mathrm{M}^1_{i,\omega}$ and $\tilde{\mathrm{M}}_{i,\omega} = \mathrm{M}_{i,\omega} - \mathrm{M}^1_{i,\omega}$ for $i = 0,1$. Here $\mathrm{M}^1_{i,\omega}$ contains all vectors from $\mathrm{M}_{i,\omega}$ with nonzero first coordinate. Then the following inclusions are holds: $\tau\left(\mathrm{M}^1_{1,\omega}\right) \subseteq \tilde{\mathrm{M}}_{0,\omega-1}$; $\tau\left(\tilde{\mathrm{M}}_{1,\omega}\right) \subseteq \mathrm{M}_{0,\omega+1}$. (*)

Theorem 2. *The map* τ *establishes biunique conformity between sets* $\mathrm{M}^1_{1,\omega}$ *and* $\tilde{\mathrm{M}}_{0,\omega-1}$, $\tilde{\mathrm{M}}_{1,\omega}$ *and* $\mathrm{M}^1_{0,\omega-1}$, *inclusions (*) are equality.*

Consequence 1. *Let vectors from* $\mathrm{M}_{0,\omega+1}$ *derivate full Γ-orbits. Then number* $\left|\Gamma\mathrm{M}_{0,\omega+1}\right|$ of *these Γ-orbits is equally to* $\left|\tilde{\mathrm{M}}_{1,\omega}\right|/(\omega+1) = \left|\mathrm{M}_{0,\omega+1}\right|/n$; $\left|\Gamma\mathrm{M}_{0,3}\right| = \left|\mathrm{M}_{1,2}\right|/3$; $\left|\Gamma\mathrm{M}_{0,4}\right| = \left|\mathrm{M}_{1,3}\right|/4$.

Established facts allow to modify a method of syndrome norms [2] with the purpose of reduction of the information stored in the ROM. It consists in immersing errors in weight $\omega - 1$ in to the set of errors of weight ω and with the first component a syndrome $s_1 = 0$ (cyclic shift in set $\mathrm{M}_{1,\omega}$, and then τ operates). Thus in view of association Γ-orbit in to cycleclasses is a reduction approximately in $4 \cdot m$ time of set of processable norms of syndromes.

Literature

1. F.J. MacWilliams, N.J.A. Sloane. The theory of error-correcting codes. North-holland publishing company, 1977.-744 p.

2. Konopelko V.K., Lipnitsky V.A. The theory of syndrome norms and permutable decoding of noiseless codes. - Minsk.: BSUIR, 2000. – 242 p.