УДК 004.021

Декодирование ранговых кодов с использованием дополнительной информации

И.Ю. Сысоев

Московский Физико-Технический Институт (государственный университет),

кафедра радиотехники и систем управления, igor.sisoev@gmail.com

***Аннотация* — В данной работе рассмотрена процедура декодирования ранговых кодов с использованием дополнительной информации. Процедура основана на использовании предыдущих результатов декодирования, а именно – базиса пространства ошибок. Предложен алгоритм определения принадлежности заданного вектора базису ошибок, алгоритм использования известных векторов базиса ошибок с l элементами и определено, что сложность вычисления алгоритма Евклида при использовании дополнительной информации пропорциональна $(d-l)^2$.**

***Ключевые слова* — ранговые коды, ключевое уравнение, сетевое кодирование, сложность вычислений, быстрые вычисления, декодер, оптимизация.**

I. Введение

Основным принципом сетевого кодирования [1] является передача суперпозиции частей целого пакета. Причём суперпозиция меняется от ретранслятора к ретранслятору. Данный способ приводит к распространению возникающих в канале ошибок, так как они также являются частью суперпозиции. На рисунке 1 показан пример передачи данных от двух источников информации к двум приёмникам информации. Источники информации обозначены номерами 3 и 10. Получатели информации обозначены номерами 6 и 11. Сплошной стрелкой показана передача частей пакета от источника, подключённого к узлу 3. Пакет от источника 3 передаётся по следующим маршрутам: 3-9-1-6, 3-9-1-4-6, 3-5-2-4-6, 3-5-7-6, 3-8-7-6. Пунктирной стрелкой показана передача частей пакета от источника, подключённого к узлу 10. Пакет от источника 10 передаётся частями по маршрутам: 10-3-9-1-6-11, 10-5-2-11, 10-8-7-11. При передаче пакета от источника 3 на графах 9-1, 8-7 и 7-6 возникли ошибки. При передаче пакета также использовались 8-7 и 7-6, поэтому возникшие ошибки распространились и на данные, передаваемые от узла 10 к узлу 11. В простом случае узел 6 осуществляет декодирование пакета и в процессе вычисляет базис пространства ошибок E_1, E_2, E_3, а узел 11 также декодирует полученный пакет и вычисляет независимо базис пространства ошибок E_1, E_2. Если бы узел 6 после декодирования сообщил результаты E_1, E_2, E_3 в буфер узла 11, то узел 11 смог бы за меньшее количество операций (траты энергии) декодировать полученный пакет. В данной статье рассматривается вопрос определения принадлежности данных в буфере пространству ошибок и снижение сложности декодирования в случае, когда информация о базисе ошибок частично известна декодеру.

II. Ранговые коды

Распространение ошибок в сетевом кодировании за счёт суперпозиции не позволяет использовать стандартные коды (Хэмминга, БЧХ и Рида-Соломона), поскольку в данных кодах используется метрика Хэмминга [2]. Оценка расстояния в метрике Хэмминга приводит к стремительному превышению кодового расстояния при постоянном смешивании частей пакета.

Лучшим вариантом помехоустойчивого кодирования будет использование ранговых кодов или кодов Габидулина [3]. В ранговых кодах, как и в кодах Рида-Соломона, элементами кодового расстояния являются элементы расширенного поля, и в качестве разницы между двумя векторами используется ранг разницы векторов.

$$d(A-B) = rg(A-B).$$

При такой метрике перемешивание частей пакета не будет приводить к увеличению кодового расстояния. Использование ранговых кодов в сетевом кодировании было предложено в 2008-м году [4].

Ранговый код можно задать проверочной матрицей

$$H_{(d-1\times n)} = \begin{Vmatrix} h_1 & h_2 & \cdots & h_n \\ h_1^{[1]} & h_2^{[1]} & \cdots & h_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ h_1^{[d-1]} & h_2^{[d-1]} & \cdots & h_n^{[d-1]} \end{Vmatrix},$$

где элементы проверочной матрицы $h_i \in GF(q^n)$.

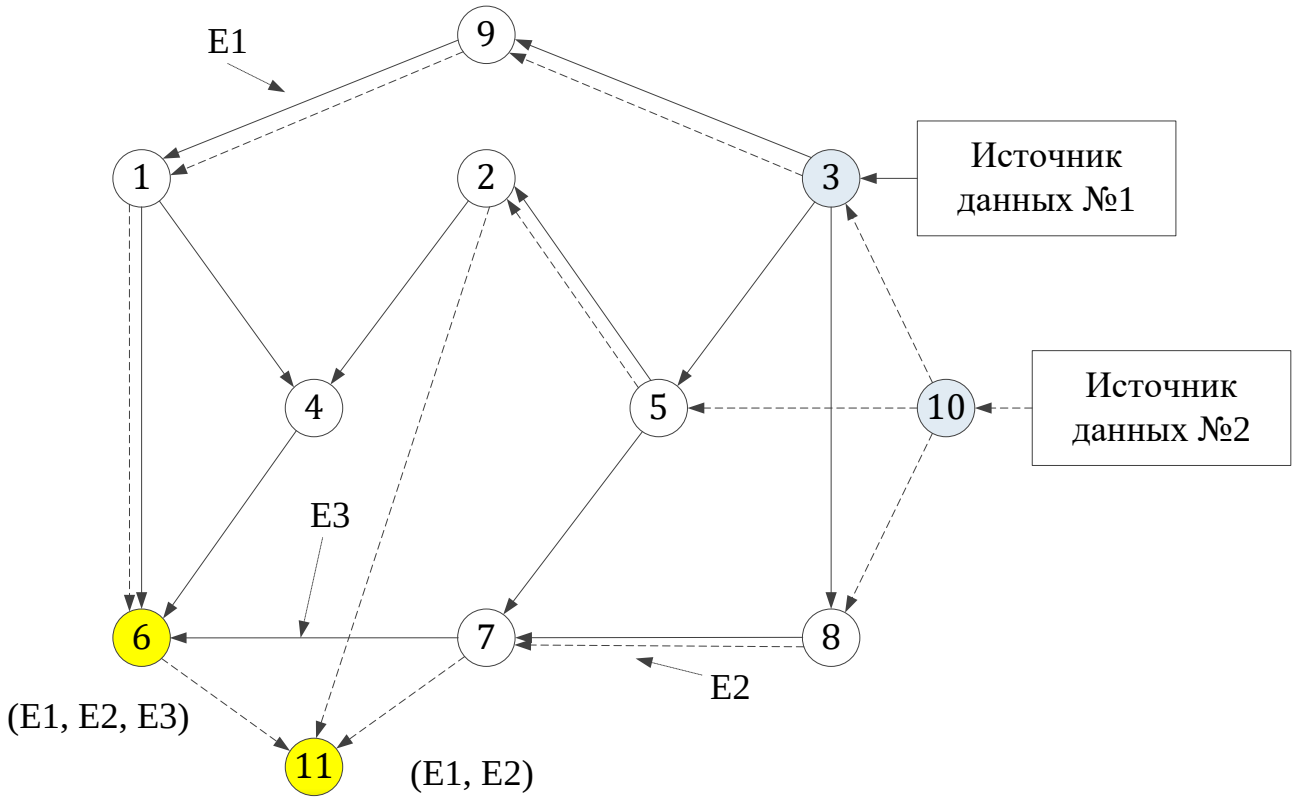

Рис. 1. Распространение ошибок в сетевом кодировании

III. Использование дополнительной информации

A. *Дополнительная информация при декодировании*

При декодировании одним из этапов является этап определения базиса ошибок.

$$e = EY = (E_1,..., E_l, E_{l+1},..., E_m)Y, \quad (1)$$

где $Y = (Y_{ij})$ - матрица ранга m с элементами из $GF(q)$.

B. *Случай вектора, принадлежащего базису ошибок*

Рассчитанный вектор синдрома можно представить в виде

$$s = eH^T = EYH^T, \quad (2)$$

где E – базис ошибок, Y – матрица локаторов ошибок.

Исходя из определения матрицы H, её ранг равняется $rg\,H = \min\{m, n\}$. Ранг матрицы s определяется как минимальный ранг матриц, входящих в уравнение **Ошибка! Источник ссылки не найден.**). Рассмотрим добавление к рассчитанному вектору синдрома вектора, определяемого уравнением

$$\breve{s} = \breve{E}\breve{Y}H^T, \quad (3)$$

где $\breve{E} = \left|\breve{E}_1\right|$, $\breve{Y} = |\ Y_{11}\quad Y_{12}\quad Y_{13}\quad \dots\quad Y_{1n}\ |$.

Для простоты вычислений в качестве $\breve{Y}$ выберем следующую матрицу

$$\breve{Y}_{n\times m} = \begin{Vmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{Vmatrix}. \quad (4)$$

Стоит заметить, что в качестве матрицы $\breve{Y}$ можно выбрать любую ненулевую матрицу, однако это приведёт к усложнению вычислений.

Рассмотрим случай, когда $\breve{E}_1$ является одним из базисных векторов пространства ошибок E. То есть вектор $\breve{E}_1$ выражается в виде

$$E' = E \times \breve{I} = E \times \begin{Vmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{Vmatrix}, \quad (5)$$

причём,

$$rg\breve{I} = 1. \quad (6)$$

В таком случае должно выполняться условие

$$rg\left(E^T \mid E'^T\right) = rgE^T \cdot rg\left(I \mid \breve{I}\right) = rgE. \quad (7)$$

Выполним сложение векторов s и $\breve{s}$ в случае, когда $\breve{E}_1$ является одним из базисных векторов пространства ошибок:

$$s+\breve{s}=EYH^T+\breve{E}\breve{Y}H^T \tag{8}$$

или

$$s+\breve{s}=(EY+\breve{E}\breve{Y})H^T. \tag{9}$$

Применяя условие (7), получаем

$$s+\breve{s}=(EY+E\breve{Y})H^T, \tag{10}$$

$$s+\breve{s}=E(Y+\breve{Y})H^T. \tag{11}$$

Исходя из формулы (11), можно сделать вывод:

$$rg(s+\breve{s})\le rgs=rgE. \tag{12}$$

Если $\breve{E}_1$ является суперпозицией нескольких базисных векторов пространства ошибок, то формула (11) преобразуется к виду

$$s+\breve{s}=E(Y+\sum_{i=1}^{m}\breve{Y}_i)H^T=E\hat{Y}H^T, \tag{13}$$

а оценка ранга суммы будет совпадать с выражением (12).

C. *Случай вектора, не принадлежащего базису ошибок*

Рассмотрим случай, когда вектор $\overline{E}$ нельзя выразить через суперпозицию базиса ошибок. В этом случае

$$rg\overline{E}=rg\left(E^T\mid\breve{E}\right)>rgE^T=rgE. \tag{14}$$

Оценим вектор

$$s+\bar{s}=(EY+\overline{E}\overline{Y})H^T. \tag{15}$$

Его ранг будет определяться по формуле

$$rg(s+\bar{s})=rg(EY+\overline{E}\overline{Y})\ge rgE. \tag{16}$$

Возникает проблема отделения случая, когда вектор $\breve{E}$ представляется в виде суперпозиции базисных векторов и $rg(s+\breve{s})=rgE$, и случая, когда вектор $\overline{E}$ нельзя представить в виде суперпозиции базисных векторов и $rg(s+\bar{s})=rgE$. Для отделения этих двух случаев необходимо выполнить вспомогательный расчёт вектора

$$s+\breve{s}=(EY+\breve{E}\hat{Y})H^T \tag{17}$$

и определить его ранг. Причем матрица $\hat{Y}$ должна равняться матрице, у которой все элементы равняются единичному в базовом конечном поле

$$\hat{Y}=\begin{Vmatrix}1 & 1 & \cdots & 1\\ 1 & 1 & \cdots & 1\\ \vdots & \vdots & \ddots & \vdots\\ 1 & 1 & \cdots & 1\end{Vmatrix}. \tag{18}$$

В этом случае если $\breve{E}$ не представляется в виде суперпозиции векторов (не входит в набор базисных векторов), то выполнится следующая система

$$\begin{cases}rg(s+\breve{s})=rgE,\\ rg(s+\hat{s})>rgE.\end{cases} \tag{19}$$

Если $\breve{E}$ представляется в виде суперпозиции векторов, то выполняется следующая система неравенств

$$\begin{cases}rg(s+\breve{s})\le rgE,\\ rg(s+\hat{s})\le rgE.\end{cases} \tag{20}$$

D. *Сложность определения принадлежности к базису ошибок*

Оценим сложность определения принадлежности вектора $\breve{E}_1$ к базису ошибок. Эта сложность будет соответствовать сложности вычисления системы

$$\begin{cases}rg(s+\breve{s})?rgE,\\ rg(s+\hat{s})?rgE,\end{cases} \tag{21}$$

сложность которой определяется по формуле

$$\Xi_{check}(n)=\Xi_{mult}(n)\cdot(d-1), \tag{22}$$

где Ξ_{mult} – сложность умножения элементов в расширенном поле $GF(q^n)$.

IV. Модификация алгоритма Евклида

После проведения процедуры проверки будет известен линейно-независимый набор векторов.

$$\breve{E}^T=\left|\breve{E}_1\quad\breve{E}_2\quad\cdots\quad\breve{E}_l\right|. \tag{23}$$

При декодировании ранговых кодов необходимо решить ключевое уравнение

$$F(z)=\Delta(z)\times S(z)\bmod z^{[d-1]}. \tag{24}$$

Одним из способов решения ключевого уравнения (24) является алгоритм Евклида. Результатом решения ключевого уравнения является многочлен $\Delta(z)$, корнем которого являются элементы базиса пространства ошибок, то есть

$$\Delta(z)=\prod_{i=1}^{m}(z^{[1]}-E_i^{[1]}). \tag{25}$$

Используя известную информацию (23), модифицируем $\Delta(z)$

$$\Delta(z) = \tilde{\Delta}(z) \times \breve{\Delta}(z), \quad (26)$$

где

$$\breve{\Delta}(z) = \prod_{i=1}^{l} (z^{[1]} - \breve{E}_i^{[1]}) \quad (27)$$

– многочлен, корнем которого являются известные векторы базиса ошибок, а

$$\tilde{\Delta}(z) = \prod_{i=1}^{l} (z^{[1]} - \tilde{E}_i^{[1]}), \quad (28)$$

– многочлен, корнем которого являются неизвестные векторы базиса ошибок

$$\tilde{E}^T = \left| \tilde{E}_1 \quad \tilde{E}_2 \quad \cdots \quad \tilde{E}_l \right|. \quad (29)$$

Таким образом, базис ошибок с использованием (23) и (29) можно выразить как

$$E^T = \left(\breve{E}^T \mid \tilde{E}^T \right). \quad (30)$$

Использование известной информации (24) позволяет модифицировать ключевое (26)

$$F(z) = \tilde{\Delta}(z) \times S(z) \bmod G(z), \quad (31)$$

где

$$G(z) = \left(\breve{\Delta}(z) \right)^{-1} \times z^{[d-1]}. \quad (32)$$

Известный вектор (23) позволяет снизить сложность декодирования. В работе [3] показан один из способов снижения сложности. Для известного базиса $\tilde{E}$ определяем минимальный многочлен

$$\Gamma_D(z) = M_{\{\breve{E}_1 \quad \breve{E}_2 \quad \cdots \quad \breve{E}_l\}}(z). \quad (33)$$

Модифицируем вектор синдрома

$$S_D(z) = \Gamma_D(z) \otimes S(z) \quad (34)$$

и решим модифицированное ключевое уравнение

$$\Omega(z) = \Gamma_F(z) \times S_D(z) \bmod z^{[d-1]}. \quad (35)$$

Сложность вычисления (34) определяется по формуле

$$\Xi_{S_D}(n) = l\Xi_q(n) + (d-1)l\Xi_{mult}(n), \quad (36)$$

где $\Xi_q(n)$ – сложность возведения в степень q.

Решить уравнение (35) можно с помощью алгоритма Евклида [5]. Выполнять алгоритм необходимо до тех пор, пока на очередной итерации степень текущего остатка не будет соответствовать неравенству

$$\deg F_i < \frac{d-1-l}{2} = \frac{d'-1}{2}, \quad (37)$$

где используется замена $d' = d - l$.

Сложность алгоритма Евклида будет равняться [4]

$$\Xi_{Euclid}(n) = \frac{3}{2}(d'-1) \cdot \left(d' + \frac{1}{2} \right) \cdot \Xi_{mult}(n). \quad (38)$$

После вычисления $\Gamma_F(z)$ вычислим корни данного многочлена, используя алгоритм, описанный в [4]. Сложность данной операции будет снижена в $\frac{m-l}{l}$ раз из-за того, что при решении системы требуется работа над матрицей $n \times l$ вместо $n \times m$.

Остальные действия выполняются так, как описано в [4].

V. Итоговая оценка сложности

Сравним итоговые сложности в режиме без дополнительной информации и в режиме с дополнительной информацией. Сравнение сложности с использованием дополнительной информации и без использования дополнительной информации показано в таблице 1. В таблице используется обозначение b – количество векторов в буфере ошибок. В частном случае размер буфера можно взять равным $\frac{d-1}{2}$. Анализируя таблицу 1, можно сделать вывод, что доминирующим слагаемым является слагаемое, пропорциональное d^2. Разница в сложности растёт пропорционально l^2 и понятно, что данная система эффективна при большом количестве «попаданий» векторов из буфера в базис ошибок.

Таблица 1

Сложность алгоритма Евклида в случае использования дополнительной информации

	Без использования дополнительной информации	С использованием дополнительной информации
Определение принадлежности вектора	–	$\Xi_{mult}(n) \cdot \cdot (d-1) \cdot b$ (см. (22))
Модификация многочлена синдрома	–	$l\Xi_q(n) + + (d-1)l \cdot \cdot \Xi_{mult}(n)$ (см. (36))
Решение ключевого уравнения	$\frac{3}{2}(d-1) \cdot \cdot \left(d + \frac{1}{2} \right) \cdot \cdot \Xi_{mult}(n)$	$\frac{3}{2}(d'-1) \cdot \cdot \left(d' + \frac{1}{2} \right) \cdot \cdot \Xi_{mult}(n)$ (см. (38))

VI. Заключение

В данной работе показано, что при использовании дополнительной информации возможно снизить сложность декодирования ранговых кодов. Процедура основана на использовании предыдущих результатов декодирования (или результатов от соседних узлов при сетевом кодировании), а именно – базиса пространства ошибок. Показан алгоритм определения принадлежности заданного вектора базису ошибок, а также определена сложность определения. Также предложена модификация алгоритма использования известных векторов базиса ошибок с l элементами и определено, что сложность вычисления алгоритма Евклида при использовании дополнительной информации пропорциональна $(d-l)^2$,а выигрыш пропорционален квадрату количества известных векторов базиса ошибок.

Литература

[1] R. Ahlswede E., N. Cai S.-Y. R. Li. and R. W. Yeung Network information flow // IEEE Trans. Inform. Theory. 2000. V. 46. PP. 1204–1216.

[2] Берлекэмп Э., Алгебраическая теория кодирования. 1971. М: Мир.

[3] Габидулин Э.М. Теория кодов с максимальным ранговым расстоянием / Проблемы передачи информации. Т. 21. Вып.1 – 1985. С. 3–14.

[4] D. Silva, F. R. Kschischang, R. Koetter, A rank-metric approach to error control in random network coding // IEEE Trans. Inform. Theory. 2008. V. 54 PP. 3951-3967.

[5] Silva D. Error control for Network Coding: Ph.D thesis. 2009. 194 p.

[6] Сысоев И.Ю. Аппаратная реализация кодека ранговых кодов // Всероссийская научно-техническая конференция «Пролемы разработки перспективных микро- и наноэлектронных систем», МЭС-2014. – 2014.

[7] Sysoev I.Y Euclidian algorithm for linearized polynomials // Algebraic and combinatorial coding theory, ACCT-2014. – 2014.

Rank codes with partially known error basis

I.Y. Sysoev

Moscow Institute of Physics and Technology, igor.sisoev@gmail.com

***Keywords* — rank codes, key equation, network coding, complexity, fast computing, decoder, optimization.**

Abstract

In this paper, decoding procedure with the use of additional information is proposed, i.e. partially known error basis. This information may be read from previous decoding result or got from neighbor node in network coding. Author developed the algorithm to check additional information in rank codes, that is, check whether the current error vector is contained in the error set for the received vector. The complexity of this operation is proportional to code distance *d*.

In the case when some elements of error basis are given, i.e. if the known error count equals *l*, the complexity of Euclidean algorithm is proportional to the square of *(d-l)*. The result may be used in the development of rang codec.

References

[1] R. Ahlswede E., N. Cai S.-Y. R. Li. and R. W. Yeung Network information flow // IEEE Trans. Inform. Theory. 2000. V. 46. PP. 1204–1216.

[2] Berlekjemp Je., Algebraicheskaja teorija kodirovanija. 1971. Moscow, Mir. (in Russian).

[3] Gabidulin Je.M. Teorija kodov s maksimal'nym rangovym rasstojaniem / Problemy peredachi informacii. Vol. 21. Vyp.1 – 1985. pp. 3–14. (in Russian).

[4] D. Silva, F. R. Kschischang, R. Koetter, A rank-metric approach to error control in random network coding // IEEE Trans. Inform. Theory. 2008. V. 54 PP. 3951-3967.

[5] Silva D. Error control for Network Coding: Ph.D thesis. 2009. 194 p.

[6] Sysoev I.Ju. Apparatnaja realizacija kodeka rangovyh kodov // Vserossijskaja nauchno-tehnicheskaja konferencija «Prolemy razrabotki perspektivnyh mikro- i nanojelektronnyh sistem», MES-2014. 2014. (in Russian).

[7] Sysoev I.Y Euclidian algorithm for linearized polynomials // Algebraic and combinatorial coding theory, ACCT-2014. 2014.