УДК 621.391

DOI: 10.18664/ikszt.v0i2.69000

ЖУЧЕНКО А.С., к.т.н., доцент,
ПАНЧЕНКО Н.Г., к.е.н., доцент,
ПАНЧЕНКО С.В., д.т.н., профессор,
ШТОМПЕЛЬ Н.А., к.т.н., доцент (УкрГУЖТ)

Метод декодирования линейных блоковых кодов на основе популяционных процедур поисковой оптимизации

Обоснована необходимость повышения эффективности декодирования линейных блоковых кодов, применяемых в современных телекоммуникационных системах. Рассмотрены варианты представления задачи декодирования линейных блоковых кодов в зависимости от используемой модели канала связи. Показано, что данная задача является задачей дискретной оптимизации, размерность которой можно уменьшить путем использования наиболее надежного базиса на основе информации о надежности элементов принятого вектора. Предложен метод декодирования линейных блоковых кодов, в основе которого лежит совместное использование наиболее надежного базиса и популяционных процедур поисковой оптимизации.

Ключевые слова: *декодирование, блоковые коды, целевая функция, популяционные процедуры.*

Постановка проблемы и анализ литературы

Классические методы декодирования линейных блоковых кодов основаны на решении алгебраических уравнений и обеспечивают получение жестких решений. Данные методы декодирования обладают невысокой корректирующей способностью, поэтому не удовлетворяют требованиям современных телекоммуникационных систем [1 – 3]. В [4] предложен метод неалгебраического декодирования линейных блоковых кодов по упорядоченным статистикам, который основан на создании списка кодовых слов на множестве наиболее надежных позиций. Недостатком данного метода является относительно высокая вычислительная сложность, что позволяет его использовать только для кодов небольшой длины. Таким образом, актуальной задачей является обеспечение заданной достоверности передачи информации в телекоммуникационных системах путем разработки метода декодирования линейных блоковых кодов с приемлемой вычислительной сложностью.

Цель статьи

Повышение эффективности декодирования линейных блоковых кодов для обеспечения заданной достоверности передачи информации в телекоммуникационных системах.

Основная часть

Пусть проверочная матрица линейного блокового (N, K) кода равна

$$H = \begin{pmatrix} h_{1,1} & h_{1,2} & \dots & h_{1,N} \\ h_{2,1} & h_{2,2} & \dots & h_{2,N} \\ \dots & \dots & \dots & \dots \\ h_{N-K,1} & h_{N-K,2} & \dots & h_{N-K,N} \end{pmatrix}, \quad (1)$$

где $h_{i,j}$ – элемент конечного поля $GF(q)$.

Рассмотрим частный случай двоичного линейного блокового кода C', тогда составляющие матрицы (1) являются элементами поля $GF(2)$.

Двоичный вектор $c' = (c'_1, c'_2, ..., c'_N)$ является кодовым словом данного кода, только если $c'H^T = 0$, что в развернутом виде соответствует

$$\sum_{j=1}^{N} h_{i,j} c'_i \equiv 0 \pmod 2, \; i = 1, 2, ..., N-K. \quad (2)$$

Известно [3], что для двоичных кодов задача жесткого декодирования «по ближайшему соседу» в двоичном симметричном канале заключается в следующем:

- по заданному двоичному принятому вектору $r' = (r'_1, r'_2, ..., r'_N)$ найти кодовое слово $c' \in C'$, которое минимизирует евклидово расстояние $\sum_{j=1}^{N} (r'_j - c'_j)^2$, т.е. фактически расстояние Хэмминга.

Применим отображение элементов конечного поля $GF(2)$ в символы поля действительных чисел R вида $c_j \to (-1)^{c'_j}$, что соответствует отображению двоичного кода C' в биполярный код C (т.е. осуществим отображение вида $C' \to C$).

При этом вектор $c = (c_1, c_2, ..., c_N)$ с элементами $c_j \in \{1, -1\}$ по аналогии с (2) является кодовым словом биполярного кода C, только если

$$\prod_{j=1}^{N} c_j^{h_{i,j}} = 1, \quad i = 1, 2, ..., N-K. \qquad (3)$$

Тогда задача мягкого декодирования «по ближайшему соседу» в двоичном канале с аддитивным белым гауссовским шумом заключается в следующем:

- по заданному принятому вектору $r = (r_1, r_2, ..., r_N)$ с элементами $r_j \in R$ найти кодовое слово $c \in C$, которое минимизирует евклидово расстояние $\sum_{j=1}^{N}(r_j - c_j)^2$.

Следует отметить, что при замене принятого вектора r на вектор правдоподобия $\phi = (\phi_1, \phi_2, ..., \phi_N)$, где $\phi_j = \log(\frac{P(r_j \mid 1)}{P(r_j \mid 0)})$, декодирование «по ближайшему соседу» соответствует декодированию максимального правдоподобия для любого дискретного канала без памяти.

Кодовое слово биполярного кода $c \in C$ минимизирует $\sum_{j=1}^{N}(r_j - c_j)^2$, только если максимизирует $\sum_{j=1}^{N} r_j c_j$, т.к. $\sum_{j=1}^{N} {c_j}^2 = N$ для всех $c \in C$ и $\sum_{j=1}^{N} {r_j}^2 = const$ для любого принятого вектора r, т.е.

$$\sum_{j=1}^{N}(r_j - c_j)^2 = \sum_{j=1}^{N} r_j^2 - 2\sum_{j=1}^{N} r_j c_j + \sum_{j=1}^{N} c_j^2 = \\ = \sum_{j=1}^{N} r_j^2 - 2\sum_{j=1}^{N} r_j c_j + N = \sum_{j=1}^{N} r_j c_j. \qquad (4)$$

Тогда с учетом (4) задача мягкого декодирования линейных блоковых кодов в поле действительных чисел R^N может быть представлена следующим образом:

- по заданному принятому вектору r найти кодовое слово $c \in C$, которое максимизирует $\sum_{j=1}^{N} r_j c_j$.

Для дальнейшего уменьшения сложности задачи мягкого декодирования линейных блоковых кодов необходимо уменьшить размерность данной задачи, т.е. представить ее в эквивалентной форме для размерности R^K. Это можно осуществить, учитывая, что только K из N элементов кодового слова линейного блокового кода являются независимыми, а остальные $N-K$ элементов можно определить с учетом алгебраической структуры кода на основе проверочной или порождающей матриц. Существует несколько вариантов уменьшения размерности рассматриваемой задачи с R^N до R^K, т.к. выбрать K независимых элементов в кодовом слове можно несколькими способами (можно выбрать разные наборы K независимых элементов в кодовом слове). Показано [4], что «хорошим» набором является набор из элементов, соответствующих K «наиболее надежным» независимым позициям в принятом векторе r. При этом элемент r_i является более надежным, чем элемент r_j, если $|r_i| > |r_j|$. Необходимо отметить, что «наиболее надежные» символы определяются заново для каждого принятого вектора r. Для упрощения обозначений, и без потери общности, будем предполагать, что $r_1, r_2, ..., r_K$ является набором наиболее надежных независимых позиций принятого вектора r, на основании которых определяется биполярный вектор $\tilde{c} = (c_1, c_2, ..., c_K)$ – информационная часть биполярного кодового слова. Тогда зависимые символы кодового слова $c_{K+1}, c_{K+2}, ..., c_N$ с учетом (3) вычисляются по независимым кодовым символам $c_1, c_2, ..., c_K$ следующим образом:

$$c_i = \pi_i(c_1, c_2, ..., c_K) = \prod_{j=1}^{N} c_j^{p_{i,j}}, \quad i = K+1, K+2, ..., N, \qquad (5)$$

где $p_{i,j} \in \{0, 1\}$ определяются из $N-K$ проверочных произведений (3) на основании K наиболее надежных независимых позиций в принятом векторе r.

Тогда согласно (4) и (5) можно записать

$$\sum_{j=1}^{N} r_j c_j = r_1 c_1 + r_2 c_2 + \ldots + r_K c_K +$$
$$+ r_{K+1}\pi_{K+1}(c_1, c_2, \ldots, c_K) + \ldots + r_N \pi_N(c_1, c_2, \ldots, c_K). \quad (6)$$

Обозначим функцию (6) как $f_r(\tilde{c})$, тогда задача мягкого декодирования линейного блокового кода размерности R^K состоит в следующем:

- по заданному принятому вектору r найти вектор $\tilde{c} = (c_1, c_2, \ldots, c_K)$, который максимизирует функцию $f_r(\tilde{c})$.

Тогда, если некоторый вектор $\tilde{c} = (c_1, c_2, \ldots, c_K)$ обеспечивает получение максимального значения функции $f_r(\tilde{c})$ по сравнению с остальными векторами из R^K, то кодовое слово, генерируемое данным вектором в соответствии с (3) является ближайшим кодовым словом к принятому вектору r, т.е. принимается в качестве переданного кодового слова.

Из рассмотренного выше следует, что задача мягкого декодирования линейного блокового кода может быть представлена в виде задачи дискретной оптимизации. При этом глобальное решение данной задачи достигается при замене вектора r вектором ϕ, элементами которого являются метрики максимального правдоподобия, и соответствует декодированию по максимуму правдоподобия, которое является оптимальным для любого дискретного канала без памяти. Однако, вычислительная сложность нахождения глобального решения является чрезмерно высокой для длинных линейных блоковых кодов, поэтому часто достаточно получить локальное (субоптимальное) решение данной задачи с использованием некоторых процедур, которое возможно будет глобальным максимумом.

В [5 – 8] обоснована целесообразность применения процедур стохастической оптимизации при декодировании кодов с малой плотностью проверок на четность, поэтому рассмотрим возможность совместного использования данных процедур и декодирования по упорядоченным статистикам.

Основные этапы предлагаемого метода мягкого декодирования линейных блоковых кодов представлены ниже.

Этап 1. Пусть $c_j = \mathrm{sign}(r_j)$, где $c_j = +1$, если $r_j \geq 0$, и $c_j = -1$ – в противном случае; для $j = 1, 2, \ldots, N$. В результате получаем вектор $c = (c_1, c_2, \ldots, c_N)$.

Этап 2. Если проверочное условие (3) выполняется для всех $i = 1, 2, \ldots, N-K$, то вектор c является биполярным кодовым словом и процесс декодирования завершается.

Этап 3. Нахождение наиболее надежного базиса (определение наиболее надежных позиций в принятом векторе r), который вычисляется с помощью двух перестановок порождающей матрицы линейного блокового кода G, соответствующей проверочной матрице H.

На данном этапе осуществляются следующие шаги.

Шаг 1. Размещение элементов принятого вектора r_j в порядке уменьшения их надежности $|r_j|$, что определяет перестановку столбцов π_1 матрицы G.

Шаг 2. Упорядочивание столбцов матрицы G в соответствии с перестановкой π_1, т.е. получение матрицы $G' = \pi_1(G)$.

Шаг 3. Формирование матрицы G'' таким образом, чтобы ее первые K столбцов были первыми K независимыми столбцами матрицы G', что определяет перестановку столбцов π_2 матрицы G'.

Шаг 4. Упорядочивание столбцов матрицы G' в соответствии с перестановкой π_2, т.е. получение матрицы $G'' = \pi_2(G')$, которая в систематической форме задает наиболее надежный базис G_s.

Этап 4. Поиск с использованием популяционных процедур поисковой оптимизации вектора $\tilde{c} = (c_1, c_2, \ldots, c_K)$, который обеспечивает максимальное значение функции $f_r(\tilde{c})$.

На данном этапе осуществляются следующие шаги.

Шаг 1. Инициализация популяции. В области поиска некоторым образом создается заданное число начальных приближений к искомому решению задачи. Например, путем формирования вектора $\tilde{c} = (c_1, c_2, \ldots, c_K)$, состоящего из K «наиболее надежных» независимых позиций в принятом векторе r, и заданного числа случайных биполярных векторов длиной K.

Шаг 2. Миграция агентов популяции. С помощью некоторого набора миграционных операторов, специфичных для каждой из популяционных процедур, агенты перемещаются в области поиска таким образом, чтобы в конченом итоге приблизиться к искомому экстремуму целевой функции $f_r(\tilde{c})$.

Шаг 3. Окончание поиска. Если число итераций меньше максимального числа итераций $L_{\max}$, то возвращаемся к шагу 2, в противном случае – текущий вектор $\tilde{c} = (c_1, c_2, ..., c_K)$ является наиболее вероятной информационной частью кодового слова c_s, сформированного с использованием надежного базиса G_s.

Этап 5. Формирование оценки переданного кодового слова с помощью обратного отображения $\hat{c} = \pi_1^{-1}[\pi_2^{-1}(c_s)]$ и процесс декодирования завершается.

Таким образом, в процессе декодирования, согласно с предложенным методом, сначала осуществляется жесткое решение на основании принятого вектора r, в результате которого формируется биполярный вектор c. Если проверочное условие выполняется для каждого элемента полученного биполярного вектора, то принимается решение, что данный вектор является переданным кодовым словом и процесс декодирования завершается. В противном случае осуществляется формирование наиболее надежного базиса G_s и поиск биполярного вектора $\tilde{c} = (c_1, c_2, ..., c_K)$ с использованием популяционных процедур поисковой оптимизации до достижения максимального числа итераций $L_{\max}$. Поиск завершается определением информационной части кодового слова c_s, которая обеспечивает максимальное значение целевой функции (6). Процесс декодирования завершается обратным отображением вектора c_s в наиболее вероятное переданное кодовое слово.

Выводы

Рассмотрены варианты представления задачи декодирования линейных блоковых кодов в зависимости от используемой модели канала связи. Показано, что данная задача является задачей дискретной оптимизации, размерность которой можно уменьшить путем использования наиболее надежного базиса на основе информации о надежности элементов принятого вектора. Предложен метод декодирования линейных блоковых кодов, в основе которого лежит совместное использование наиболее надежного базиса и популяционных процедур поисковой оптимизации.

Литература

1. Штомпель, Н. А. Методы мягкого декодирования кодов с малой плотностью проверок на четность [Текст] / Н. А. Штомпель // Вісник Національного технічного університету «Харківський політехнічний інститут»: збірник наукових праць. – 2013. – № 27 (1000). – С. 163 – 168.
2. Штомпель, Н. А. Вычислительная сложность методов декодирования кодов с малой плотностью проверок на четность [Текст] / Н. А. Штомпель // Системи обробки інформації: збірник наукових праць. – Харків: ХУПС ім. І. Кожедуба, 2013. – Вип. 6 (113). – С. 177 – 180.
3. Приходько, С. И. Декодирование двоичных блоковых кодов на основе методов стохастической оптимизации [Текст] / С. И. Приходько, Н. А. Штомпель // Матеріали X ювілейної міжнародної науково-практичної конференції «Проблеми економіки та управління на залізничному транспорті» (м. Одеса, 30 червня – 1 липня 2015 р.). – Київ: ДЕТУТ, 2015. – С. 126.
4. Fossorier, M. P. C. Soft-decision decoding of linear block codes based on ordered statistics / M. P. C. Fossorier, S. Lin // , IEEE Transactions on Information Theory. – 1995. – Vol. 41, № 5. – September. – P. 1379 – 1396.
5. Асауленко, И. А. Метод итеративного декодирования линейных блоковых кодов на основе стохастической оптимизации [Текст] / И.А. Асауленко, С.И. Приходько, Н.А. Штомпель // Матеріали стендових доповідей та виступів учасників 28-ої міжнародної науково-практичної конференції «Інформаційно-керуючі системи на залізничному транспорті» (м. Харків, 24 – 25 вересня 2015 р.). – Інформаційно-керуючі системи на залізничному транспорті: науково-технічний журнал. Додаток. – Харків: УкрДУЗТ, 2015. – Вип. 4 (113). – С. 27 – 28.
6. Асауленко, І. О. Метод декодування кодів з малою щільністю перевірок на парність на основі стохастичної оптимізації [Текст] / І. О. Асауленко, С. І. Приходько, М. А. Штомпель // Інформаційно-керуючі системи на залізничному транспорті: науково-технічний журнал. – Харків: УкрДУЗТ, 2015. – Вип. 5 (114). – С. 61 – 65.
7. Асауленко, І. О. Дослідження характеристик методу декодування кодів з малою щільністю перевірок на парність на основі стохастичної оптимізації [Текст] / І. О. Асауленко, О. С. Жученко, С. І. Приходько, М. А. Штомпель // Інформаційно-керуючі системи на залізничному транспорті: науково-технічний журнал. – Харків: УкрДУЗТ, 2016. – Вип. 1 (116). – С. 33 – 40.
8. Асауленко, І. О. Декодування кодів з малою щільністю перевірок на парність на основі природних обчислень [Текст] / І. О. Асауленко, М. А. Штомпель // Міжрегіональна науково-практична конференція молодих учених «ТАК»: телекомунікації, автоматика, комп'ютерного-інтегровані технології (м. Красноармійськ, 16 – 17 листопада 2015 р.). – Збірка доповідей – Красноармійськ: ДВНЗ «ДонНТУ», 2015. –С. 9 – 11.

Жученко О.С., Панченко Н.Г., Панченко С.В., Штомпель М.А. Метод декодування лінійних блокових кодів на основі популяційних процедур пошукової оптимізації

Обґрунтовано необхідність підвищення ефективності декодування лінійних блокових кодів, що застосовуються в сучасних телекомунікаційних системах. Розглянуто варіанти представлення задачі декодування лінійних блокових кодів залежно від моделі каналу зв'язку. Показано, що дана задача є задачею дискретної оптимізації, розмірність якої можна зменшити шляхом використання найбільш надійного базису на основі інформації про надійність елементів прийнятого вектору. Запропоновано метод декодування лінійних блокових кодів, в основі якого лежить спільне використання найбільш надійного базису і популяційних процедур пошукової оптимізації.

Ключові слова: декодування, блокові коди, цільова функція, популяційні процедури.

Жученко Олександр Сергійович, *кандидат технічних наук, доцент, доцент кафедри транспортного зв'язку, Український державний університет залізничного транспорту, Харків, Україна. E-mail: tz@kart.edu.ua.*

Панченко Наталія Георгіївна, *кандидат економічних наук, доцент, доцент кафедри вищої математики, Український державний університет залізничного транспорту, Харків, Україна. E-mail: math@kart.edu.ua.*

Панченко Сергій Володимирович, *доктор технічних наук, професор, ректор, Український державний університет залізничного транспорту, Харків, Україна. E-mail: tz@kart.edu.ua.*

Штомпель Микола Анатолійович, *кандидат технічних наук, доцент, доцент кафедри транспортного зв'язку, Український державний університет залізничного транспорту, Харків, Україна. E-mail: tz@kart.edu.ua.*

Zhuchenko O., Panchenko N., Panchenko S., Shtompel M. Decoding method of linear block codes based on population procedures of search optimization.

It is shown that the classical methods of decoding linear block codes are based on the solution of algebraic equations and provide hard decisions. Thus, these decoding methods have low correction ability so do not satisfy the requirements of modern telecommunications systems. It is shown that the lack of non-algebraic decoding methods of linear block codes for ordered statistics is relatively high computational complexity, which makes it suitable only for short length codes. The necessity to improve the efficiency of decoding linear block codes used in modern telecommunications systems has been grounded. The variants of representing the problem of linear block codes decoding depending on the communication channel model have been considered. It is shown that this problem is a problem of discrete optimization, the dimension of which can be reduced by using the most reliable basis based on information about the reliability of the elements of received vector. The objective function which is advisable to used in the decoding of linear block codes is presented. Decoding method of linear block codes based on the joint use of the most reliable basis, objective function and population procedures of search optimization has been proposed.

Key words: decoding, block codes, objective function, population procedures.

Zhuchenko O.S., *docent of "Transport connection" department, Candidate of Techn. Sciences, docent, Ukrainian State University of Railway Transport, Kharkiv, Ukraine.*

Panchenko N.G., *docent of "Higher Mathematics" department, Candidate of Econ. Sciences, docent, Ukrainian State University of Railway Transport, Kharkiv, Ukraine.*

Panchenko S.V., *rector, Doctor of Techn. Sciences, professor, Ukrainian State University of Railway Transport, Kharkiv, Ukraine.*

Shtompel M.A., *docent of "Transport connection" department, Candidate of Techn. Sciences, docent, Ukrainian State University of Railway Transport, Kharkiv, Ukraine.*

Рецензент д.т.н., профессор Алёшин Г.В. (УкрГУЖТ)

Поступила 01.03.2016 г.