О мягком декодировании линейных кодов методом минимальных слов

Д. Н. Цымжитов

В работе рассмотрена модификация известного алгоритма ML-декодирования методом минимальных слов, имеющая явное ограничение на максимальное количество итераций в виде некоторого числа $t_{\max}$. В случае, если отведенного числа итераций недостаточно для получения оптимального решения, алгоритм объявляет об отказе. Предложена нижняя граница для константы $t_{\max}$, соблюдение которой гарантирует, что вероятность отказа декодера будет близка к нулю. Если n — длина кодового слова, то данная граница лежит в классе $O(\ln n)$ при $n \to \infty$. Полученная оценка является улучшением известной ранее линейной оценки.

Ключевые слова: мягкое декодирование, декодирование по максимуму правдоподобия, линейные коды, сложность декодирования, минимальные кодовые слова.

1. Введение

Известно, что метод декодирования по максимуму правдоподобия или просто ML-декодирование является самым сильным методом в том смысле, что при его использовании вероятность ошибки в принятой последовательности данных достигает минимума. Этот минимум зависит только от свойств канала связи и кода, характеризуя, таким образом, действительную эффективность последнего вне зависимости от какого-то конкретного алгоритма декодирования. Поэтому в теории помехоустойчивых кодов весьма распространена практика, при которой корректирующая эффективность кода оце-

нивается в предположении, что на приемном конце осуществляется ML-декодирование.

Декодирование по максимуму правдоподобия является важнейшей и наиболее сложной алгоритмической проблемой в теории кодирования. Известно, что, к примеру, для двоичного симметричного канала связи и произвольных линейных кодов эта проблема в общем случае является NP-полной [1]. Более того, она остается таковой даже в том случае, когда допускается сколь угодно долгая предобработка кода [2]. Тем не менее, к настоящему моменту разработано и изучено множество общих подходов к решению данной задачи, позволяющих уменьшить асимптотическую сложность декодирования по сравнению с переборным методом. Все эти алгоритмы имеют сложность, зависящую экспоненциально от длины кода, но в отличие от переборного метода — с меньшим показателем экспоненты. Кроме того, они вполне пригодны для практического применения в связке с кодами средней длины (до 200 символов в блоке).

К их числу, например, относится алгоритм декодирования по так называемым информационным совокупностям [3, 4, 5, 6, 7, 8], впервые рассматривавшийся в работе [3]. Другим примером решения задачи ML-декодирования является так называемый алгоритм «соседей нуля» (англ. *zero neighbors*), предложенный Левитиным и Хартманом [9]. Данный алгоритм относится к семейству градиентоподобных алгоритмов декодирования [4, 7, 10]. Еще одним представителем названного семейства является алгоритм ML-декодирования методом минимальных слов, изученный в работе [11]. В этой статье был впервые рассмотрен класс минимальных кодовых слов, характеризуемых тем свойством, что их носители не содержат носителей других нетривиальных кодовых слов. Изучению свойств минимальных кодовых слов и основанного на них метода декодирования целиком или частично посвящены работы [4, 7, 10, 12, 13, 14].

Алгоритм декодирования методом минимальных слов, равно как и другие градиентоподобные алгоритмы, является итеративным и состоит в постепенном приближении к оптимальному решению путем его последовательного уточнения. Известно, что данный алгоритм всегда сходится к наилучшему решению, если количество его итера-

ций никак не ограничено [11]. Однако, в заключительных замечаниях к статье [11] сам ее автор отмечает, что результаты проведенной им компьютерной симуляции свидетельствуют о крайне малом числе итераций, необходимых для завершения алгоритма. В статье [10] для случая двоичного симметричного канала связи приводится верхняя оценка общего числа итераций данного алгоритма, линейная по длине кодового слова. Насколько нам известно, других результатов, улучшающих эту оценку, получено не было.

В настоящей работе рассматривается модификация оригинального алгоритма декодирования методом минимальных слов, у которой имеется явное ограничение на максимальное количество итераций в виде некоторого числа $t_{\max}$. В случае, если отведенного числа итераций недостаточно для получения оптимального решения, алгоритм объявляет об отказе. Таким образом, он также является алгоритмом ML-декодирования. Предложена нижняя граница для константы $t_{\max}$, соблюдение которой гарантирует (при некоторых дополнительных предположениях об используемом коде), что вероятность отказа декодера будет близка к нулю. Если n — длина кодового слова, то данная граница лежит в классе $O(\ln n)$ при $n \to \infty$. В этом смысле полученная оценка является улучшением упомянутой выше линейной оценки.

Кроме этого, в качестве вспомогательной конструкции рассмотрена субоптимальная модификация оригинального алгоритма. Этот алгоритм отличается от первого тем, что вместо объявления об отказе возвращает лучшее решение, которое он успел построить за отведенное число итераций. Доказано, что при соблюдении той же границы для величины $t_{\max}$ вероятность ошибки декодирования с использованием данного алгоритма будет близка к минимальной. Отметим, что все эти результаты доказаны для модели двоичного канала с белым гауссовским шумом.

Автор выражает глубокую благодарность профессору Э. Э. Гасанову и к.ф.-м.н. П. А. Пантелееву за постановку задачи и помощь в работе.

2. Постановка проблемы и основные результаты

Постановка задачи

Более детальное изложение понятий и фактов, составляющих содержание этого раздела, можно найти в [15, гл. 1] или [16, гл. 1 и 11].

Пусть имеется двоичный канал с аддитивным белым гауссовским шумом. Напомним, что это дискретный канал связи без памяти с входным двоичным алфавитом $\mathbb{F}_2$ и выходным вещественным алфавитом $\mathbb{R}$. Его поведение определяется плотностью $p(r \mid a)$ условной вероятности того, что на выходе канала связи появится символ $r \in \mathbb{R}$, если на его вход был подан символ $a \in \mathbb{F}_2$. Она соответствует нормальному закону распределения и имеет вид

$$p(r \mid a) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{1}{2\sigma^2}\,(r-\tilde{a})^2\right), \quad \text{где } \tilde{a} = (-1)^a\sqrt{E}.$$

Величины $E > 0$ и $\sigma^2 > 0$ определяют соответственно энергию сигнала для одного передаваемого бита и дисперсию шума. Если данные передаются блоками длины n, то коль скоро канал связи не имеет памяти, для любых слов $\mathbf{r} \in \mathbb{R}^n$ и $\mathbf{a} \in \mathbb{F}_2^n$ будем иметь

$$p(\mathbf{r} \mid \mathbf{a}) = \prod_{j=1}^{n} p(r_j \mid a_j) = \frac{1}{(\sigma\sqrt{2\pi})^n} \exp\left(-\frac{1}{2\sigma^2}||\mathbf{r}-\tilde{\mathbf{a}}||^2\right),$$

где $\tilde{\mathbf{a}} = (\tilde{a}_1, \ldots, \tilde{a}_n)$ и $||\mathbf{r}-\tilde{\mathbf{a}}||$ — евклидово расстояние в $\mathbb{R}^n$ между векторами $\mathbf{r}$ и $\tilde{\mathbf{a}}$. Здесь $p(\mathbf{r} \mid \mathbf{a})$ обозначает плотность условной вероятности того, что на приемном конце будет принято слово $\mathbf{r} \in \mathbb{R}^n$, если было передано слово $\mathbf{a} \in \mathbb{F}_2^n$.

Будем считать, что для передачи данных используется линейный двоичный код $\mathcal{C}$ длины n. Если на приемном конце наблюдается некоторый вектор $\mathbf{r} \in \mathbb{R}^n$, то декодировать его — значит восстановить по нему тот кодовый вектор $\mathbf{c} \in \mathcal{C}$, который был подан на вход канала связи. Блоковая ошибка декодирования — это исход, при котором

декодер выдает некоторую кодовую последовательность, не совпадающую с той, что была передана на самом деле. Известно, что наиболее сильным методом декодирования, минимизирующим вероятность блоковой ошибки, является *декодирование по максимуму апостериорной вероятности* или просто *MAP-декодирование* (англ. *maximum a posteriori decoding*). Обозначим через $\mathrm{P}(\mathbf{c}\,|\,\mathbf{r})$ вероятность того, что был передан вектор $\mathbf{c} \in \mathcal{C}$, при условии, что на выходе канала связи принят вектор $\mathbf{r} \in \mathbb{R}^n$. Задача MAP-декодирования некоторой наблюдаемой $\mathbf{r} \in \mathbb{R}^n$ состоит в нахождении такого кодового вектора $\mathbf{c} \in \mathcal{C}$, который максимизировал бы апостериорную вероятность $\mathrm{P}(\mathbf{c}\,|\,\mathbf{r})$.

Далее мы будем предполагать, что источник в нашей системе связи распределен равномерно, то есть все кодовые слова $\mathbf{c} \in \mathcal{C}$ передаются с одинаковой вероятностью $\mathrm{P}(\mathbf{c}) = |\mathcal{C}|^{-1}$. Легко видеть, что в этом случае задача MAP-декодирования становится эквивалентной задаче *декодирования по максимуму правдоподобия* или просто *ML-декодирования* (англ. *maximum likelihood decoding*), которая состоит в максимизации величины $p(\mathbf{r}\,|\,\mathbf{c})$.

Фиксируем некоторую наблюдаемую $\mathbf{r} \in \mathbb{R}^n$. *Жестким решением* для $\mathbf{r}$ будем называть вектор $\hat{\mathbf{r}} = (\hat{r}_1, \ldots, \hat{r}_n) \in \mathbb{F}_2^n$, где

$$\hat{r}_j = \begin{cases} 0, & \text{если } r_j \geqslant 0, \\ 1, & \text{если } r_j < 0, \end{cases} \qquad j = 1, \ldots, n.$$

Попросту говоря, вектор $\hat{\mathbf{r}}$ представляет собой то решение, которое принимал бы декодер в случае, если бы для передачи данных не применялось кодирование. *Вектором правдоподобия* для наблюдаемой $\mathbf{r}$ будем называть вектор $\boldsymbol{\mu}(\mathbf{r}) = (|r_1|, \ldots, |r_n|) \in \mathbb{R}^n$. Его компоненты по сути являются мерой правдоподобия соответствующих компонент жесткого решения $\hat{\mathbf{r}}$.

Для произвольного $\boldsymbol{\mu} \in \mathbb{R}_+^n$ (где $\mathbb{R}_+$ — множество неотрицательных действительных чисел), определим функции

$$d_{\boldsymbol{\mu}}(\mathbf{a}, \mathbf{b}) = \sum_{j\colon a_j \neq b_j} \mu_j \quad \text{и} \quad w_{\boldsymbol{\mu}}(\mathbf{a}) = \sum_{j\colon a_j \neq 0} \mu_j, \quad \mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n,$$

называемые соответственно *взвешенным расстоянием Хэмминга* и *взвешенным весом Хэмминга*. Заметим, что взвешенное расстояние

не всегда является метрикой в строгом смысле. Хотя расстояние $d_{\boldsymbol{\mu}}$ симметрично и удовлетворяет неравенству треугольника, оно может оказаться вырожденным, если хотя бы одна из компонент вектора $\boldsymbol{\mu}$ равна нулю. Легко видеть, что

$$p(\mathbf{r}\,|\,\mathbf{a}) = p(\mathbf{r}\,|\,\hat{\mathbf{r}})e^{-Ld_{\boldsymbol{\mu}}(\hat{\mathbf{r}},\mathbf{a})}, \quad \text{где } \boldsymbol{\mu} = \boldsymbol{\mu}(\mathbf{r}),$$

(величину $L = \frac{2\sqrt{E}}{\sigma^2}$ называют *надежностью* гауссовского канала связи). Поэтому задача ML-декодирования эквивалентна задаче

$$d_{\boldsymbol{\mu}}(\hat{\mathbf{r}}, \mathbf{c}) \to \min, \quad \mathbf{c} \in \mathcal{C}, \tag{1}$$

которая в терминах вектора ошибки $\mathbf{e} = \hat{\mathbf{r}} - \mathbf{c}$ принимает вид

$$w_{\boldsymbol{\mu}}(\mathbf{e}) \to \min, \quad \mathbf{e} \in \hat{\mathbf{r}} + \mathcal{C}. \tag{2}$$

Здесь и далее мы пишем просто $\boldsymbol{\mu}$ вместо $\boldsymbol{\mu}(\mathbf{r})$, если из контекста понятно, о какой наблюдаемой идет речь.

Метод минимальных слов

Изложим вкратце суть интересующих нас результатов из [11] (в несколько измененной форме), опишем алгоритм минимальных слов и лежащую в его основе идею.

Ненулевой кодовый вектор $\mathbf{c} \in \mathcal{C}$ называется *минимальным*, если его носитель не содержит носителей других ненулевых кодовых векторов. Множество всех минимальных кодовых векторов обозначим как $\mathcal{M}(\mathcal{C})$. Согласно [11, теорема 2]:

> *вектор* $\mathbf{e} \in \hat{\mathbf{r}} + \mathcal{C}$ *является оптимальным решением задачи (2) тогда и только тогда, когда* $w_{\boldsymbol{\mu}}(\mathbf{e}) \leqslant w_{\boldsymbol{\mu}}(\mathbf{e} + \mathbf{c})$ *для любого* $\mathbf{c} \in \mathcal{M}(\mathcal{C})$.

Фиксируем наблюдаемую $\mathbf{r} \in \mathbb{R}^n$. Положив $\mathbf{e}_0 = \hat{\mathbf{r}}$, построим в смежном классе $\hat{\mathbf{r}} + \mathcal{C}$ последовательность векторов $\mathbf{e}_1, \mathbf{e}_2, \ldots$ таким образом, что $\mathbf{e}_{t+1} = \mathbf{e}_t + \mathbf{c}_{t+1}$ для всех $t \geqslant 0$, где $\mathbf{c}_{t+1}$ является оптимальным решением задачи

$$w_{\boldsymbol{\mu}}(\mathbf{e}_t + \mathbf{c}_{t+1}) \to \min, \quad \mathbf{c}_{t+1} \in \mathcal{M}(\mathcal{C}).$$

Вес $w_{\boldsymbol{\mu}}(\mathbf{e}_t)$ вектора $\mathbf{e}_t$ минимален в смежном классе $\hat{\mathbf{r}} + \mathcal{C}$ тогда и только тогда, когда $w_{\boldsymbol{\mu}}(\mathbf{e}_t) \leqslant w_{\boldsymbol{\mu}}(\mathbf{e}_t + \mathbf{c}_{t+1})$. Очевидно, существует наименьшее число $q \geqslant 0$, для которого $w_{\boldsymbol{\mu}}(\mathbf{e}_q) \leqslant w_{\boldsymbol{\mu}}(\mathbf{e}_q + \mathbf{c}_{q+1})$. При этом,

$$w_{\boldsymbol{\mu}}(\mathbf{e}_0) > w_{\boldsymbol{\mu}}(\mathbf{e}_1) > \ldots > w_{\boldsymbol{\mu}}(\mathbf{e}_q),$$

и вектор $\mathbf{e}_q$ является оптимальным решением задачи (2), а кодовый вектор $\mathbf{c} = \hat{\mathbf{r}} - \mathbf{e}_q$ — оптимальным решением задачи (1).

Итак, мы имеем итеративный алгоритм, который за конечное число шагов сходится к оптимальному решению задачи (1), и каждая итерация которого состоит в решении подзадачи вида

$$w_{\boldsymbol{\mu}}(\mathbf{e} + \mathbf{c}) \to \min, \quad \mathbf{c} \in \mathcal{M}(\mathcal{C}). \tag{3}$$

Обозначим его как $\mathsf{OptimalDecoder}$, а результат его выполнения для наблюдаемой $\mathbf{r}$ — как $\mathsf{OptimalDecoder}(\mathbf{r})$. Тогда (см. [11, теорема 4])

> *вектор* $\mathbf{c} = \mathsf{OptimalDecoder}(\mathbf{r})$ *является оптимальным решением задачи (1).*

Основные результаты

Рассмотрим модификацию описанного алгоритма, имеющую явное ограничение на максимальное количество итераций. Позволим новому алгоритму возвращать последний кодовый вектор из последовательности $\{\hat{\mathbf{r}} - \mathbf{e}_t\}_{t=1}^{q}$, который он успел построить за отведенное число итераций, в том случае, если тот является оптимальным решением. В противном случае новый алгоритм должен объявлять об отказе.

Алгоритм 1. (Оптимальный ограниченный алгоритм) Пусть дана процедура A, которая для любых параметров $\boldsymbol{\mu} \in \mathbb{R}_+^n$ и $\mathbf{e} \in \mathbb{F}_2^n$ выдает результат $\mathbf{c} = \mathsf{A}(\boldsymbol{\mu}, \mathbf{e})$, являющийся оптимальным решением задачи (3). Алгоритм имеет следующее описание.

- Параметры: число $t_{\max} \in \mathbb{N}$, вектор $\mathbf{r} \in \mathbb{R}^n$;
- Результат: вектор $\mathbf{c} \in \mathcal{C}$.

1) Инициализация: $\boldsymbol{\mu} \leftarrow \boldsymbol{\mu}(\mathbf{r})$; $\mathbf{e} \leftarrow \hat{\mathbf{r}}$; $\mathbf{c} \leftarrow \mathsf{A}(\boldsymbol{\mu}, \mathbf{e})$; $t \leftarrow 0$;

2) Пока $w_{\boldsymbol{\mu}}(\mathbf{e}) > w_{\boldsymbol{\mu}}(\mathbf{e}+\mathbf{c})$ и $t < t_{\max}$ выполнять: $\mathbf{e} \leftarrow \mathbf{e}+\mathbf{c}$; $\mathbf{c} \leftarrow \mathsf{A}(\boldsymbol{\mu}, \mathbf{e})$; $t \leftarrow t+1$;
3) Если $w_{\boldsymbol{\mu}}(\mathbf{e}) \leqslant w_{\boldsymbol{\mu}}(\mathbf{e}+\mathbf{c})$, то вернуть $\mathbf{c} \leftarrow \hat{\mathbf{r}} - \mathbf{e}$; иначе объявить об отказе.

Алгоритм 1 будем обозначать как $\mathsf{LimitedDecoder}_{\mathsf{A}}$, а результат его выполнения с параметрами $t_{\max}$ и $\mathbf{r}$ — как $\mathsf{LimitedDecoder}_{\mathsf{A}}(t_{\max}, \mathbf{r})$. Ясно, что данный алгоритм также является алгоритмом ML-декодирования. Пусть минимальное расстояние кода $\mathcal{C}$ равно d и $d \geqslant \delta n$ для некоторого δ, $0 < \delta < 1$. Обозначим

$$u(\delta) = \left\lceil \frac{1}{\delta} \right\rceil, \quad \alpha(\delta) = \frac{u(\delta)}{u(\delta)-1}.$$

Рассмотрим величину

$$\tau(L', \delta, \varepsilon, n) = \log_{\alpha(\delta)} \left(-n \frac{2\sqrt{L'}\left(1 - \ln\left(\frac{\sqrt{\pi}}{2}\left(1 - \sqrt[n]{1-\frac{\varepsilon}{2}}\right)\right)\right) + L'}{\ln(1-\frac{\varepsilon}{2})} \right),$$

где $\varepsilon \in (0,1)$ и $L' = \frac{2E}{\sigma^2} > 0$. Обозначим через $\mathcal{F}_{\text{opt}}$ событие отказа алгоритма $\mathsf{LimitedDecoder}_{\mathsf{A}}$.

Теорема 1. *Пусть $\varepsilon \in (0,1)$. Если максимальное число итераций $t_{\max}$ алгоритма $\mathsf{LimitedDecoder}_{\mathsf{A}}$ выбрано так, что $t_{\max} \geqslant \tau(L', \delta, \varepsilon, n)$, то справедлива оценка*

$$\mathrm{P}(\mathcal{F}_{\text{opt}}) < 2\mathrm{P}(\mathcal{E}_{\mathcal{C}}) + \varepsilon.$$

Теорема 2. *При фиксированных $L' > 0$ и $\delta, \varepsilon \in (0,1)$ верно соотношение*

$$\tau(L', \delta, \varepsilon, n) = O(\ln n) \quad \textit{при} \quad n \to \infty.$$

Пусть имеется последовательность кодов длины n, $n \to \infty$, имеющих скорость не менее $R > 0$ и относительное минимальное расстояние не менее $\delta > 0$. Пусть она реализует предсказание теоремы Шеннона, то есть вероятность блоковой ошибки с использованием ML-декодирования для этих кодов стремится к нулю при $n \to \infty$.

Тогда при любом $\varepsilon \in (0,1)$ применение к данной последовательности кодов алгоритма $\mathsf{LimitedDecoder}_{\mathsf{A}}$ с параметром $t_{\max} = \lceil \tau(L', \delta, \varepsilon, n) \rceil$ приведет к тому, что при $n \to \infty$ вероятность ошибки декодирования будет стремиться к нулю, а средняя скорость передачи данных будет стремиться к $(1-\varepsilon)R$. Первое верно по той причине, что даный алгоритм является алгоритмом ML-декодирования, а второе — в силу теоремы 1. При этом, согласно теореме 2 величина $t_{\max}$ будет расти не быстрее, чем $O(\ln n)$ при $n \to \infty$.

3. Ограниченный алгоритм декодирования

Общая оценка сходимости

Рассмотрим снова последовательность векторов $\hat{\mathbf{r}} = \mathbf{e}_0, \mathbf{e}_1, \ldots, \mathbf{e}_q$ в $\hat{\mathbf{r}} + \mathcal{C}$, где $\mathbf{e}_{t+1} = \mathbf{e}_t + \mathbf{c}_{t+1}$, и вектор $\mathbf{c}_{t+1}$ является оптимальным решением задачи

$$w_{\boldsymbol{\mu}}(\mathbf{e}_t + \mathbf{c}_{t+1}) \to \min, \quad \mathbf{c}_{t+1} \in \mathcal{M}(\mathcal{C}),$$

для всех $t \geqslant 0$. Пусть, как раньше,

$$w_{\boldsymbol{\mu}}(\mathbf{e}_0) > w_{\boldsymbol{\mu}}(\mathbf{e}_1) > \ldots > w_{\boldsymbol{\mu}}(\mathbf{e}_q),$$

и вектор $\mathbf{e}_q$ имеет наименьший вес в смежном классе $\hat{\mathbf{r}} + \mathcal{C}$, то есть является оптимальным решением задачи (2).

Предложение 3. *Для каждого t, $0 \leqslant t \leqslant q$, верно неравенство*

$$w_{\boldsymbol{\mu}}(\mathbf{e}_t) - w_{\boldsymbol{\mu}}(\mathbf{e}_q) \leqslant \alpha(\delta)^{-t}(w_{\boldsymbol{\mu}}(\mathbf{e}_0) - w_{\boldsymbol{\mu}}(\mathbf{e}_q)).$$

Доказательство. При $t = 0$ и $t = q$ справедливость данного неравенства очевидна. Пусть $1 \leqslant t < q$ и $\mathbf{c}' = \mathbf{e}_q - \mathbf{e}_{t-1}$. Тогда найдутся векторы $\mathbf{c}'_1, \ldots, \mathbf{c}'_p \in \mathcal{M}(\mathcal{C})$ с непересекающимися носителями, такие что

$$\mathbf{c}' = \mathbf{c}'_1 + \ldots + \mathbf{c}'_p.$$

Так как носители слагаемых не пересекаются, то во-первых,

$$p \leqslant \frac{n}{d} \leqslant \frac{1}{\delta} \leqslant u(\delta),$$

а во-вторых,

$$\sum_{s=1}^{p}\big(w_{\boldsymbol{\mu}}(\mathbf{e}_{t-1}+\mathbf{c}'_s)-w_{\boldsymbol{\mu}}(\mathbf{e}_{t-1})\big)=w_{\boldsymbol{\mu}}(\mathbf{e}_{t-1}+\mathbf{c}')-w_{\boldsymbol{\mu}}(\mathbf{e}_{t-1})<0.$$

А поскольку вес вектора $\mathbf{e}_q=\mathbf{e}_{t-1}+\mathbf{c}'$ минимален в $\hat{\mathbf{r}}+\mathcal{C}$, то

$$w_{\boldsymbol{\mu}}(\mathbf{e}_{t-1}+\mathbf{c}'_s)-w_{\boldsymbol{\mu}}(\mathbf{e}_{t-1})\leqslant 0\quad\text{для всех } s=1,\ldots,p.$$

Следовательно, найдется такое s_0, для которого

$$w_{\boldsymbol{\mu}}(\mathbf{e}_{t-1}+\mathbf{c}'_{s_0})-w_{\boldsymbol{\mu}}(\mathbf{e}_{t-1})\leqslant\frac{w_{\boldsymbol{\mu}}(\mathbf{e}_q)-w_{\boldsymbol{\mu}}(\mathbf{e}_{t-1})}{p}\leqslant\frac{w_{\boldsymbol{\mu}}(\mathbf{e}_q)-w_{\boldsymbol{\mu}}(\mathbf{e}_{t-1})}{u(\delta)}.$$

Вспоминая определение вектора $\mathbf{c}_t=\mathbf{e}_t-\mathbf{e}_{t-1}$, заключаем, что

$$w_{\boldsymbol{\mu}}(\mathbf{e}_t)\leqslant w_{\boldsymbol{\mu}}(\mathbf{e}_{t-1})+\frac{w_{\boldsymbol{\mu}}(\mathbf{e}_q)-w_{\boldsymbol{\mu}}(\mathbf{e}_{t-1})}{u(\delta)}$$

или, что то же самое,

$$w_{\boldsymbol{\mu}}(\mathbf{e}_t)\leqslant w_{\boldsymbol{\mu}}(\mathbf{e}_q)+\frac{u(\delta)-1}{u(\delta)}(w_{\boldsymbol{\mu}}(\mathbf{e}_{t-1})-w_{\boldsymbol{\mu}}(\mathbf{e}_q)).$$

Откуда, применяя индукцию, получаем неравенство

$$w_{\boldsymbol{\mu}}(\mathbf{e}_t)\leqslant w_{\boldsymbol{\mu}}(\mathbf{e}_q)+\left(\frac{u(\delta)-1}{u(\delta)}\right)^t(w_{\boldsymbol{\mu}}(\mathbf{e}_0)-w_{\boldsymbol{\mu}}(\mathbf{e}_q)).$$

Что и требовалось доказать.

Субоптимальный ограниченный алгоритм

Рассмотрим другую модификацию алгоритма OptimalDecoder, также имеющую явное ограничение на максимальное количество итераций. На этот раз позволим новому алгоритму возвращать последний кодовый вектор из последовательности $\{\hat{\mathbf{r}}-\mathbf{e}_t\}_{t=1}^{q}$, который он успел построить за отведенное число итераций, вне зависимости от того, является тот оптимальным решением или нет.

Алгоритм 2. (Субоптимальный ограниченный алгоритм) Пусть дана процедура A, которая для любых параметров $\boldsymbol{\mu}\in\mathbb{R}_+^n$ и $\mathbf{e}\in\mathbb{F}_2^n$ выдает результат $\mathbf{c}=\mathsf{A}(\boldsymbol{\mu},\mathbf{e})$, являющийся оптимальным решением задачи (3). Алгоритм имеет следующее описание.

- Параметры: число $t_{\max} \in \mathbb{N}$, вектор $\mathbf{r} \in \mathbb{R}^n$;
- Результат: вектор $\mathbf{c} \in \mathcal{C}$.

1) Инициализация: $\boldsymbol{\mu} \leftarrow \boldsymbol{\mu}(\mathbf{r})$; $\mathbf{e} \leftarrow \hat{\mathbf{r}}$; $\mathbf{c} \leftarrow \mathsf{A}(\boldsymbol{\mu}, \mathbf{e})$; $t \leftarrow 0$;
2) Пока $w_{\boldsymbol{\mu}}(\mathbf{e}) > w_{\boldsymbol{\mu}}(\mathbf{e}+\mathbf{c})$ и $t < t_{\max}$ выполнять:
   $\mathbf{e} \leftarrow \mathbf{e} + \mathbf{c}$; $\mathbf{c} \leftarrow \mathsf{A}(\boldsymbol{\mu}, \mathbf{e})$; $t \leftarrow t+1$;
3) Вернуть $\mathbf{c} \leftarrow \hat{\mathbf{r}} - \mathbf{e}$.

Алгоритм 2 будем обозначать как $\mathsf{LimitedDecoder}^*_{\mathsf{A}}$, а результат его выполнения с параметрами $t_{\max}$ и $\mathbf{r}$ — как $\mathsf{LimitedDecoder}^*_{\mathsf{A}}(t_{\max}, \mathbf{r})$. Выясним, какова нижняя оценка для максимального числа итераций $t_{\max}$, при котором вероятность блоковой ошибки декодирования для алгоритма $\mathsf{LimitedDecoder}^*_{\mathsf{A}}$ будет близка к минимальной. Обозначим как $\mathcal{E}_{\mathcal{C}}$ и $\mathcal{E}_{\text{sub}}$ события блоковой ошибки декодирования соответственно для оптимального декодера и для алгоритма $\mathsf{LimitedDecoder}^*_{\mathsf{A}}$.

Предложение 4. *Пусть* $0 < \varepsilon < 1$ *и* $\mathbf{r} \in \mathbb{R}^n$. *Если максимальное число итераций* $t_{\max}$ *алгоритма* $\mathsf{LimitedDecoder}^*_{\mathsf{A}}$ *выбрано так, что*

$$t_{\max} \geqslant \log_{\alpha(\delta)} \left(-\frac{L w_{\boldsymbol{\mu}}(\hat{\mathbf{r}})}{\ln(1-\varepsilon)} \right) \text{ при } w_{\boldsymbol{\mu}}(\hat{\mathbf{r}}) > 0,$$

то справедлива оценка $\mathrm{P}(\mathcal{E}_{\text{sub}} \,|\, \mathbf{r}) < \mathrm{P}(\mathcal{E}_{\mathcal{C}} \,|\, \mathbf{r}) + \varepsilon$.

Доказательство. Результатом работы алгоритма $\mathsf{LimitedDecoder}^*_{\mathsf{A}}$ с параметрами $t_{\max}$ и $\mathbf{r}$, подходящими под условия предложения, является кодовый вектор вида $\hat{\mathbf{r}} - \mathbf{e}_t$, где $0 \leqslant t \leqslant q$. Если $t = q$, то полученное решение оптимально и $\mathrm{P}(\mathcal{E}_{\text{sub}} \,|\, \mathbf{r}) = \mathrm{P}(\mathcal{E}_{\mathcal{C}} \,|\, \mathbf{r}) < \mathrm{P}(\mathcal{E}_{\mathcal{C}} \,|\, \mathbf{r}) + \varepsilon$. В частности, это верно при $w_{\boldsymbol{\mu}}(\hat{\mathbf{r}}) = 0$, когда $t = q = 0$.

Докажем нашу оценку для случая, когда $w_{\boldsymbol{\mu}}(\hat{\mathbf{r}}) > 0$ и $t < q$. Будем считать, что $\mathrm{P}(\mathcal{E}_{\mathcal{C}} \,|\, \mathbf{r}) + \varepsilon < 1$, так как в противном случае наше утверждение, очевидно, в доказательстве не нуждается. Положим $\mathbf{c}' = \hat{\mathbf{r}} - \mathbf{e}_q$ и $\mathbf{c} = \hat{\mathbf{r}} - \mathbf{e}_t$. Имеем

$$\begin{aligned}
\frac{1 - \mathrm{P}(\mathcal{E}_{\mathcal{C}} \,|\, \mathbf{r})}{1 - \mathrm{P}(\mathcal{E}_{\text{sub}} \,|\, \mathbf{r})} &= \frac{\mathrm{P}(\mathbf{c}' \,|\, \mathbf{r})}{\mathrm{P}(\mathbf{c} \,|\, \mathbf{r})} = \frac{p(\mathbf{r} \,|\, \mathbf{c}')}{p(\mathbf{r} \,|\, \mathbf{c})} = \\
&= \exp\{-L d_{\boldsymbol{\mu}}(\hat{\mathbf{r}}, \mathbf{c}') + L d_{\boldsymbol{\mu}}(\hat{\mathbf{r}}, \mathbf{c})\} = \exp\{L(w_{\boldsymbol{\mu}}(\mathbf{e}_t) - w_{\boldsymbol{\mu}}(\mathbf{e}_q))\} \leqslant \\
&\leqslant \exp\{\alpha^{-t} L(w_{\boldsymbol{\mu}}(\hat{\mathbf{r}}) - w_{\boldsymbol{\mu}}(\mathbf{e}_q))\} \leqslant \exp\{\alpha^{-t} L w_{\boldsymbol{\mu}}(\hat{\mathbf{r}})\}.
\end{aligned}$$

Здесь $\alpha = \alpha(\delta)$, а предпоследняя оценка следует из предложения 3. Преобразуя неравенства

$$1 \leqslant \frac{1 - \mathrm{P}(\mathcal{E}_{\mathcal{C}} \,|\, \mathbf{r})}{1 - \mathrm{P}(\mathcal{E}_{\mathrm{sub}} \,|\, \mathbf{r})} \leqslant \exp\{\alpha^{-t} L w_{\boldsymbol{\mu}}(\hat{\mathbf{r}})\},$$

получаем оценку

$$\mathrm{P}(\mathcal{E}_{\mathcal{C}} \,|\, \mathbf{r}) \leqslant \mathrm{P}(\mathcal{E}_{\mathrm{sub}} \,|\, \mathbf{r}) \leqslant 1 - \exp\{-\alpha^{-t} L w_{\boldsymbol{\mu}}(\hat{\mathbf{r}})\} \left(1 - \mathrm{P}(\mathcal{E}_{\mathcal{C}} \,|\, \mathbf{r})\right). \tag{4}$$

Разрешим относительно t неравенство

$$1 - \exp\{-\alpha^{-t} L w_{\boldsymbol{\mu}}(\hat{\mathbf{r}})\} \left(1 - \mathrm{P}(\mathcal{E}_{\mathcal{C}} \,|\, \mathbf{r})\right) - \mathrm{P}(\mathcal{E}_{\mathcal{C}} \,|\, \mathbf{r}) < \varepsilon. \tag{5}$$

Для этого приведем его к виду

$$\exp\{-\alpha^{-t} L w_{\boldsymbol{\mu}}(\hat{\mathbf{r}})\} > 1 - \frac{\varepsilon}{1 - \mathrm{P}(\mathcal{E}_{\mathcal{C}} \,|\, \mathbf{r})}.$$

Учитывая, что $\mathrm{P}(\mathcal{E}_{\mathcal{C}} \,|\, \mathbf{r}) + \varepsilon < 1$, заключаем, что обе части последнего неравенства положительны и, стало быть, оно равносильно неравенству

$$\alpha^{-t} < \frac{-\ln\left(1 - \frac{\varepsilon}{1 - \mathrm{P}(\mathcal{E}_{\mathcal{C}} \,|\, \mathbf{r})}\right)}{L w_{\boldsymbol{\mu}}(\hat{\mathbf{r}})}.$$

Поскольку $\alpha > 1$ и обе части нового неравенства, очевидно, также положительны, получаем окончательно

$$t > \log_{\alpha} \left(\frac{L w_{\boldsymbol{\mu}}(\hat{\mathbf{r}})}{-\ln\left(1 - \frac{\varepsilon}{1 - \mathrm{P}(\mathcal{E}_{\mathcal{C}} \,|\, \mathbf{r})}\right)} \right).$$

С другой стороны,

$$\log_{\alpha} \left(\frac{L w_{\boldsymbol{\mu}}(\hat{\mathbf{r}})}{-\ln\left(1 - \frac{\varepsilon}{1 - \mathrm{P}(\mathcal{E}_{\mathcal{C}} \,|\, \mathbf{r})}\right)} \right) < \log_{\alpha} \left(-\frac{L w_{\boldsymbol{\mu}}(\hat{\mathbf{r}})}{\ln(1 - \varepsilon)} \right).$$

Предположение $t < q$ означает, что решение $\mathbf{e}_t$ неоптимально, и алгоритм $\mathsf{LimitedDecoder}^{*}_{\mathsf{A}}$ завершил основной цикл, исчерпав весь запас итераций. Поэтому

$$t = t_{\max} \geqslant \log_{\alpha} \left(-\frac{L w_{\boldsymbol{\mu}}(\hat{\mathbf{r}})}{\ln(1 - \varepsilon)} \right),$$

и неравенство (5) выполняется. Данное заключение вкупе с неравенствами (4) окончательно доказывает наше утверждение.

Следствие 5. *Пусть* $0 < \varepsilon < 1$. *Если для каждого* $\mathbf{r} \in \mathbb{R}^n$ *параметр* $t_{\max}$ *алгоритма* $\mathsf{LimitedDecoder}^*_{\mathsf{A}}$ *выбирается так, что*

$$t_{\max} \geqslant \log_{\alpha(\delta)} \left(-\frac{L w_{\boldsymbol{\mu}}(\hat{\mathbf{r}})}{\ln(1-\varepsilon)} \right) \text{ при } w_{\boldsymbol{\mu}}(\hat{\mathbf{r}}) > 0,$$

то справедлива оценка $\mathrm{P}(\mathcal{E}_{\mathrm{sub}}) < \mathrm{P}(\mathcal{E}_{\mathcal{C}}) + \varepsilon$.

Доказательство. Согласно предложению 4 для любого вектора $\mathbf{r} \in \mathbb{R}^n$ верно неравенство $\mathrm{P}(\mathcal{E}_{\mathrm{sub}} \,|\, \mathbf{r}) < \mathrm{P}(\mathcal{E}_{\mathcal{C}} \,|\, \mathbf{r}) + \varepsilon$. Имеем

$$\mathrm{P}(\mathcal{E}_{\mathrm{sub}}) = \int_{\mathbb{R}^n} \mathrm{P}(\mathcal{E}_{\mathrm{sub}} \,|\, \mathbf{r}) p(\mathbf{r}) d\mathbf{r} < \\ < \int_{\mathbb{R}^n} \mathrm{P}(\mathcal{E}_{\mathcal{C}} \,|\, \mathbf{r}) p(\mathbf{r}) d\mathbf{r} + \varepsilon \int_{\mathbb{R}^n} p(\mathbf{r}) d\mathbf{r} = \mathrm{P}(\mathcal{E}_{\mathcal{C}}) + \varepsilon.$$

Как показывает следующее утверждение, в полученной оценке для максимального числа итераций алгоритма $\mathsf{LimitedDecoder}^*_{\mathsf{A}}$ можно избавиться от переменных $\boldsymbol{\mu}$ и $\hat{\mathbf{r}}$, зависящих от параметра $\mathbf{r}$.

Предложение 6. *Пусть* $0 < \varepsilon < 1$. *Если максимальное число итераций* $t_{\max}$ *алгоритма* $\mathsf{LimitedDecoder}^*_{\mathsf{A}}$ *выбрано так, что* $t_{\max} \geqslant \tau(L', \delta, \varepsilon, n)$, *то справедлива оценка*

$$\mathrm{P}(\mathcal{E}_{\mathrm{sub}}) < \mathrm{P}(\mathcal{E}_{\mathcal{C}}) + \varepsilon.$$

Доказательство. Фиксируем произвольное число $\beta > \sigma\sqrt{2} + \sqrt{E}$ и положим $U = \{\, \mathbf{v} \in \mathbb{R}^n \mid |v_j| \leqslant \beta, 1 \leqslant j \leqslant n \,\}$. Если

$$t_{\max} \geqslant \log_{\alpha(\delta)} \left(-\frac{L\beta n}{\ln(1-\frac{\varepsilon}{2})} \right), \tag{6}$$

то для любого $\mathbf{r} \in U$ будем иметь $w_{\boldsymbol{\mu}}(\hat{\mathbf{r}}) \leqslant \beta n$ и (по предложению 4)

$$\mathrm{P}(\mathcal{E}_{\mathrm{sub}} \,|\, \mathbf{r}) < \mathrm{P}(\mathcal{E}_{\mathcal{C}} \,|\, \mathbf{r}) + \varepsilon/2.$$

Следовательно,

$$\mathrm{P}(\mathcal{E}_{\mathrm{sub}}) = \int_U \mathrm{P}(\mathcal{E}_{\mathrm{sub}} \,|\, \mathbf{r}) p(\mathbf{r}) d\mathbf{r} + \mathrm{P}(\mathcal{E}_{\mathrm{sub}} \,|\, \overline{U}) \mathrm{P}(\overline{U}) <$$
$$< \int_{\mathbb{R}^n} \mathrm{P}(\mathcal{E}_{\mathcal{C}} \,|\, \mathbf{r}) p(\mathbf{r}) d\mathbf{r} + \frac{\varepsilon}{2} \int_{\mathbb{R}^n} p(\mathbf{r}) d\mathbf{r} + \mathrm{P}(\overline{U}) = \mathrm{P}(\mathcal{E}_{\mathcal{C}}) + \frac{\varepsilon}{2} + \mathrm{P}(\overline{U}),$$

где $\overline{U} = \mathbb{R}^n \backslash U$.

Для того, чтобы оценить сверху вероятность $\mathrm{P}(\overline{U})$, оценим снизу вероятность $\mathrm{P}(U)$. Имеем

$$\mathrm{P}(U) = \int_U p(\mathbf{r}) d\mathbf{r} = \frac{1}{|\mathcal{C}|} \sum_{\mathbf{c} \in \mathcal{C}} \int_U p(\mathbf{r} \,|\, \mathbf{c}) d\mathbf{r} =$$
$$= \frac{1}{|\mathcal{C}|} \sum_{\mathbf{c} \in \mathcal{C}} \int_U \frac{1}{(\sigma\sqrt{2\pi})^n} \exp\left(-\frac{1}{2\sigma^2} ||\mathbf{r} - \tilde{\mathbf{c}}||^2 \right) d\mathbf{r}.$$

Положим

$$U_{\mathbf{0}} = \{\, \mathbf{v} \in \mathbb{R}^n \mid |v_j| \leqslant \beta - \sqrt{E}, 1 \leqslant j \leqslant n \,\} \quad \text{и}$$
$$U_{\mathbf{c}} = \{\, \mathbf{v} \in \mathbb{R}^n \mid |v_j - \tilde{c}_j| \leqslant \beta - \sqrt{E}, 1 \leqslant j \leqslant n \,\} \quad \text{для всех } \mathbf{c} \in \mathcal{C}.$$

Тогда $U_{\mathbf{c}} \subset U$ для каждого $\mathbf{c} \in \mathcal{C}$ и

$$\mathrm{P}(U) > \frac{1}{|\mathcal{C}|} \sum_{\mathbf{c} \in \mathcal{C}} \int_{U_{\mathbf{c}}} \frac{1}{(\sigma\sqrt{2\pi})^n} \exp\left(-\frac{1}{2\sigma^2} ||\mathbf{r} - \tilde{\mathbf{c}}||^2 \right) d\mathbf{r} =$$
$$= \frac{1}{|\mathcal{C}|} \sum_{\mathbf{c} \in \mathcal{C}} \int_{U_{\mathbf{0}}} \frac{1}{(\sigma\sqrt{2\pi})^n} \exp\left(-\frac{1}{2\sigma^2} \mathbf{r}^2 \right) d\mathbf{r} =$$
$$= \int_{U_{\mathbf{0}}} \frac{1}{(\sigma\sqrt{2\pi})^n} \exp\left(-\frac{1}{2\sigma^2} \mathbf{r}^2 \right) d\mathbf{r} =$$
$$= \left(\int_{-\beta+\sqrt{E}}^{\beta-\sqrt{E}} \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{1}{2\sigma^2} x^2 \right) dx \right)^n = \left(\Phi\left(\frac{\beta - \sqrt{E}}{\sigma\sqrt{2}} \right) \right)^n,$$

где $\Phi(x)$ — функция Лапласа. Следовательно,

$$\mathrm{P}(\overline{U}) = 1 - \mathrm{P}(U) < 1 - \left(\Phi\left(\frac{\beta - \sqrt{E}}{\sigma\sqrt{2}} \right) \right)^n.$$

При $x > 1$ имеем

$$\Phi(x) = 1 - \frac{2}{\sqrt{\pi}} \int_x^{+\infty} e^{-t^2} dt > 1 - \frac{2}{\sqrt{\pi}} \int_x^{+\infty} e^{-t} dt = 1 - \frac{2}{\sqrt{\pi}} e^{-x},$$

откуда (поскольку $\beta > \sigma\sqrt{2} + \sqrt{E}$)

$$\mathrm{P}(\overline{U}) < 1 - \left(1 - \frac{2}{\sqrt{\pi}} \exp\left(-\frac{\beta - \sqrt{E}}{\sigma\sqrt{2}}\right)\right)^n.$$

Разрешив относительно β неравенство

$$1 - \left(1 - \frac{2}{\sqrt{\pi}} \exp\left(-\frac{\beta - \sqrt{E}}{\sigma\sqrt{2}}\right)\right)^n \leqslant \frac{\varepsilon}{2},$$

получаем

$$\beta \geqslant -\sigma\sqrt{2} \ln\left(\frac{\sqrt{\pi}}{2}\left(1 - \sqrt[n]{1 - \frac{\varepsilon}{2}}\right)\right) + \sqrt{E}. \tag{7}$$

Итак, если $\beta > \sigma\sqrt{2} + \sqrt{E}$, и при этом неравенства (6) и (7) выполняются, то $\mathrm{P}(\overline{U}) < \varepsilon/2$ и $\mathrm{P}(\mathcal{E}_{\mathrm{sub}}) < \mathrm{P}(\mathcal{E}_{\mathcal{C}}) + \varepsilon$. В частности, данное заключение будет справедливо, если

$$\beta = \sigma\sqrt{2}\left(1 - \ln\left(\frac{\sqrt{\pi}}{2}\left(1 - \sqrt[n]{1 - \frac{\varepsilon}{2}}\right)\right)\right) + \sqrt{E}$$

и

$$t_{\max} \geqslant \log_{\alpha(\delta)}\left(-\frac{L\beta n}{\ln(1 - \frac{\varepsilon}{2})}\right) = \tau(L', \delta, \varepsilon, n).$$

Предложение доказано.

Теперь мы можем перейти к доказательству основных результатов.

Доказательство теоремы 1. Ясно, что при равных значениях параметра $t_{\max}$ у алгоритмов $\mathsf{LimitedDecoder_A}$ и $\mathsf{LimitedDecoder^*_A}$ событие $\mathcal{F}_{\mathrm{opt}}$ состоит в том, что алгоритм $\mathsf{LimitedDecoder^*_A}$ выдает неоптимальное решение. Обозначим через $\mathcal{R}$ событие, при котором оптимальный

декодер и алгоритм $\mathsf{LimitedDecoder}^*_{\mathsf{A}}$ одновременно *не* ошибаются, то есть $\mathcal{R} = \overline{\mathcal{E}_{\mathcal{C}}} \cap \overline{\mathcal{E}_{\mathrm{sub}}}$. При этом событии алгоритм $\mathsf{LimitedDecoder}^*_{\mathsf{A}}$, очевидно, выдает оптимальное решение. Поэтому

$$\mathrm{P}(\mathcal{F}_{\mathrm{opt}}) \leqslant \mathrm{P}(\overline{\mathcal{R}}) = \mathrm{P}(\mathcal{E}_{\mathcal{C}} \cup \mathcal{E}_{\mathrm{sub}}) \leqslant \mathrm{P}(\mathcal{E}_{\mathcal{C}}) + \mathrm{P}(\mathcal{E}_{\mathrm{sub}}) < 2\mathrm{P}(\mathcal{E}_{\mathcal{C}}) + \varepsilon,$$

где последняя оценка следует из предложения 6.

Доказательство теоремы 2. Имеем (если обозначить $\alpha = \alpha(\delta)$)

$$\tau(L', \delta, \varepsilon, n) = \log_\alpha n + \log_\alpha \left(\frac{2\sqrt{L'}\left(1 - \ln\left(\frac{\sqrt{\pi}}{2}\left(1 - \sqrt[n]{1 - \frac{\varepsilon}{2}}\right)\right)\right) + L'}{-\ln(1 - \frac{\varepsilon}{2})} \right).$$

Очевидно, выражение, стоящее под логарифмом во втором слагаемом, есть $O\left(-\ln\left(1 - \beta^{1/n}\right)\right)$ при $n \to \infty$, где $\beta = 1 - \frac{\varepsilon}{2}$. Положим $\beta_0 = 1 - \frac{\varepsilon}{3}$, так что $\beta < \beta_0$ и $\ln \beta < \ln \beta_0 < 0$.

Поскольку $\beta^x = 1 + x \ln \beta + o(x)$ при $x \to 0$, то $1 + x \ln \beta_0 > \beta^x$ для всех достаточно малых $x > 0$. Следовательно, для всех достаточно больших n будем иметь

$$-\ln\left(1 - \beta^{1/n}\right) < -\ln\left(1 - \left(1 + \frac{1}{n}\ln\beta_0\right)\right) = \ln\left(\frac{n}{-\ln\beta_0}\right).$$

Поэтому $\tau(L', \delta, \varepsilon, n) = \log_\alpha n + O(\ln\ln n) = O(\ln n)$ при $n \to \infty$.

Список литературы

[1] Berlekamp E. R., McEliece R. J., Van Tilborg H. C. A. On the inherent intractability of certain coding problems // IEEE Trans. Inform. Theory. Vol. 24. 1978. P. 384–386.

[2] Bruck J., Naor M. The hardness of decoding linear codes with preprocessing // IEEE Trans. Inform. Theory. Vol. 36. 1990. P. 381–385.

[3] Prange E. The use of information sets in decoding cyclic codes // IRE Trans. Inform. Theory. Vol. 8. 1962. P. 5–9.

[4] Barg A. Minimum distance decoding algorithms for linear codes // in Proc. of the 12th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Lecture Notes in Computer Science. Vol. 1255. 1997. P. 1–14.

[5] Barg A., Krouk E., Van Tilborg H. C. A. On the complexity of minimum distance decoding of long linear codes // IEEE Trans. Inform. Theory. Vol. 45. 1999. P. 1392–1405.

[6] Coffey J. T., Goodman R. M. F. The complexity of information set decoding // IEEE Trans. Inform. Theory. Vol. 36. 1990. P. 1031–1037.

[7] Coffey J. T., Goodman R. M. F., Farrell P. G. New approaches to reduced-complexity decoding // Discr. Appl. Math. Vol. 33. 1991. P. 43–60.

[8] Крук Е. А. Граница для сложности декодирования линейных блоковых кодов // Пробл. передачи информ. Т. 25. 1989. С. 103–107.

[9] Levitin L. B., Hartmann C. R. P. A new approach to the general minimum distance decoding problem: the zero-neighbors algorithm // IEEE Trans. Inform. Theory. Vol. 31. 1985. P. 378–384.

[10] Ashikhmin A., Barg A. Minimal vectors in linear codes // IEEE Trans. Inform. Theory. Vol. 44. 1998. P. 2010–2017.

[11] Hwang T. Decoding linear block codes for minimizing word error rate // IEEE Trans. Inform. Theory. Vol. 25. 1979. P. 733–737.

[12] Borissov Y. Minimal/nonminimal codewords in the second order binary Reed-Muller codes: revisited // in Proc. of the 11th International Workshop on Algebraic and Combinatorial Coding Theory. Pamporovo, Bulgaria, 2008. P. 29–34.

[13] Borissov Y., Manev N., Nikova S. On the non-minimal codewords in binary Reed-Muller codes // Discr. Appl. Math. Vol. 128. 2003. P. 65–74.

[14] Борисов Ю. Ф., Манев Н. Л. Минимальные кодовые слова примитивных кодов БЧХ // Пробл. передачи информ. Т. 34. 1998. С. 37–46.

[15] Lin S., Costello D. J. Error Control Coding: Fundamentals and Applications. Englewood Cliffs, NJ: Prentice-Hall, 1983.

[16] Moon T. K. Error Correction Coding: Mathematical Methods and Algorithms. Hoboken, NJ: Wiley, 2005.