ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 38 2002 Вып. 4

УДК 621.391.15

© 2002 г. Б. С. Цыбаков, А. Р. Рубинов

# НЕКОТОРЫЕ КОНСТРУКЦИИ КОДОВ, ИЗБЕГАЮЩИХ КОНФЛИКТОВ

Даются конструкции кодов, избегающих конфликтов. Эти коды могут быть использованы как протокольные последовательности, обеспечивающие успешную передачу пакетов по каналу с конфликтами и без обратной связи. Указывается на связь между различными кодами, которые избегают конфликтов различного числа пользователей. Даются верхние границы для максимального размера кода и приводятся три конкретные кодовые конструкции.

## § 1. Введение

В статье рассматриваются коды, избегающие конфликтов. Кодовое слово длины $N$ такого кода приписывается пользователю как его протокольная последовательность. Каждый пользователь использует его протокольную последовательность для передачи информации по каналу с конфликтами и без обратной связи. Максимальное число пользователей канала может быть самое большее равным числу кодовых слов в коде. Время в канале разбито на интервалы одинаковой длины (окна). Каждый пользователь имеет точную информацию о моментах начала окон. Никакой другой синхронизации не предполагается. Пользователь может передавать свои пакеты в течение сеанса, имеющего длину $N$ окон. Предполагается, что любое окно может принадлежать самое большее $k$ сеансам. В течение своего сеанса каждый пользователь передает пакеты в соответствии со своей протокольной последовательностью. Если пользователь начинает свой сеанс в момент $T$ ($T$ – это начальный момент окна $T$) и его протокольная последовательность имеет символ 1 (символ 0) на первой позиции, то пользователь передает (соответственно, не передает) пакет в окне $T$. Аналогично, если символ 1 (символ 0) стоит на $i$-й позиции, то пользователь передает (не передает) пакет в окне $T+i-1$, $1 \le i \le N$. Если только один пользователь посылает пакет в окне, этот пакет считается успешно переданным. Если больше чем один пользователь передает пакет в окне, то в этом окне образуется конфликт, и ни один из пакетов не считается успешно переданным. Протокольные последовательности должны быть такими, чтобы они гарантировали успешную передачу по меньшей мере $r$ пакетов каждого пользователя в течение его сеанса. Множество таких протокольных последовательностей или слов называется кодом, избегающим конфликтов и имеющим параметры: $N$ – длина слова, $k$ – максимальное число сеансов, пересекающихся в окне, $r$ – минимальное число успешно переданных пакетов в сеансе.

Важные результаты по каналу с конфликтами и без обратной связи, а также по кодам, избегающим конфликтов, были опубликованы в работах [1–7]. Задачи, рассмотренные в этих работах и в настоящей статье, иллюстрирует рис. 1 в случае $k=2$. При $k=2$ точные формулировки задач, рассмотренных в настоящей статье, даются в §§ 2 и 3.


Рис. 1

Рис. 1,*а* показывает задачу, рассмотренную в [1–6]. В этой задаче какой-то рассматриваемый сеанс, для определенности называемый сигнальным кодовым словом, может наложиться в канале на два других сеанса, также для определенности называемыми шумовыми кодовыми словами, которые следуют один за другим без промежутка между ними. Наложение сигнального кодового слова на каждое из этих двух шумовых кодовых слов является частичным; в противном случае сигнальное кодовое слово полностью наложилось бы на одно из этих шумовых кодовых слов. Эти два шумовых кодовых слова называются одинаковыми в том смысле, что они являются сеансами одного и того же пользователя. Это означает, что сигнальное кодовое слово может наложиться на любой циклический сдвиг другого кодового слова. Эта задача мотивирована традиционным для теории информации рассмотрением передачи длинных информационных потоков.

Рис. 1,*б* иллюстрирует задачу, рассмотренную в [7]. В этой задаче каждое кодовое слово должно иметь длину $N = 2N' - 1$ и не менее чем $N' - 1$ нулей в конце. Это означает, что сигнальное кодовое слово длины $N'$, удлиненное с помощью нулевой последовательности длины $N' - 1$, может полностью наложиться на любой циклический сдвиг другого сигнального кодового слова, удлиненного таким же образом. Эта задача мотивирована передачей коротких сообщений, таких как в радиоканале, где происходит доступ новых пользователей. В случае $r = 1$ в [7] дано достаточное условие того, что код является избегающим конфликтов, а в случае $k = 2,\ r = 1$ в [7] найдены оптимальные коды и их размеры.

В этой статье мы рассматриваем задачи, иллюстрируемые рис. 1,*б,в*. Первая из этих задач рассматривается в § 2, а вторая – в § 3. Вторая задача похожа на задачу, иллюстрируемую рис. 1,*а*. Единственное отличие состоит в том, что шумовые кодовые слова не обязательно являются совпадающими. Отметим, что рис. 1,*в* иллюстрирует частный случай более общей задачи, в которой разрешается иметь некоторый пустой интервал между двумя шумовыми сеансами.

Несмотря на близость содержательных постановок, иллюстрируемых рис. 1, соответствующие комбинаторые задачи имеют значительное отличие.

В § 2 дается точная постановка задачи, иллюстрируемой рис. 1,*б*, связь между кодами с различными $k$, верхние границы для кода максимального размера, а также приводятся две кодовые конструкции в случае $k = 2,\ r \geq 1$. В § 3 рассматривается задача, иллюстрируемая рис. 1,*в*, и приводится конструкция кода, имеющего $k = 2, r = 1$.

## § 2. Коды со словами, удлиненными нулями

В этом параграфе рассматривается задача, которая иллюстрируется рис. 1,*б*. Сначала мы введем обозначения и дадим формулировку задачи.

**2.1. Обозначения и постановка задачи.** Обозначим через $\boldsymbol{v} = (v_1, \ldots, v_{N'})$ двоичное слово длины $N'$, а через $\boldsymbol{v}' = \boldsymbol{v}\mathbf{0}$ – удлиненное слово $\boldsymbol{v}$ длины $2N' - 1$, где здесь и далее $\mathbf{0}$ – это нулевое слово длины $N' - 1$. Пусть $w(\boldsymbol{v})$ – вес Хэмминга слова $\boldsymbol{v}$, т.е. обозначает число символов 1 в $\boldsymbol{v}$. Через $d(\boldsymbol{u}, \boldsymbol{v})$ обозначим расстояние Хэмминга между словами $\boldsymbol{u}$ и $\boldsymbol{v}$, где $\boldsymbol{u} = (u_1, \ldots, u_{N'})$ – двоичное слово длины $N'$, а через $\alpha(\boldsymbol{u}, \boldsymbol{v})$ обозначается число символов 1 в слове $\boldsymbol{u}$, которые *не покрываются* символами 1 слова $\boldsymbol{v}$, т.е. $\alpha(\boldsymbol{u}, \boldsymbol{v})$ – число позиций $i$ таких, что $u_i = 1,\ v_i = 0$. Обозначим через $\beta(\boldsymbol{u}, \boldsymbol{v})$ число символов 1 слова $\boldsymbol{u}$, которые покрываются символами 1 слова $\boldsymbol{v}$, т.е. $\beta(\boldsymbol{u}, \boldsymbol{v})$ – число позиций $i$ таких, что $u_i = 1, v_i = 1$.

Заметим, что $\alpha(\boldsymbol{u}, \boldsymbol{v}) + \beta(\boldsymbol{u}, \boldsymbol{v}) = w(\boldsymbol{u})$ при любых $\boldsymbol{u}$ и $\boldsymbol{v}$, а $d(\boldsymbol{u}, \boldsymbol{v}) = 2\alpha(\boldsymbol{u}, \boldsymbol{v})$, если $w(\boldsymbol{u}) = w(\boldsymbol{v})$.

Если все символы 1 слова $\boldsymbol{u}$ покрываются словом $\boldsymbol{v}$, то мы условимся говорить, что $\boldsymbol{u}$ есть *подслово* слова $\boldsymbol{v}$ (термин подслово используется только в разделе 2.3).

Обычный *циклический сдвиг* $\boldsymbol{v}$ на $i$ позиций вправо обозначается как $\boldsymbol{v}^{(i)}$, $i = 0, 1, \ldots, N'-1$, где $\boldsymbol{v}^{(0)} \equiv \boldsymbol{v}$. В дальнейшем также используется *параллельный сдвиг* (или просто *сдвиг*) слова $\boldsymbol{v}$ на $i$ позиций вправо, который определяется как $\underline{\boldsymbol{v}}^{(i)} \triangleq \boldsymbol{v}'^{(i)}$, $i = 0, 1, \ldots, N' - 1$, где $\underline{\boldsymbol{v}}^{(0)} \triangleq \boldsymbol{v}' \equiv \boldsymbol{v}'^{(0)}$.

При любых заданных $\boldsymbol{u}$ и $\boldsymbol{v}$ минимум $\alpha(\boldsymbol{u}', \underline{\boldsymbol{v}}^{(i)})$ по всем $i$ обозначается через $t(\boldsymbol{u}, \boldsymbol{v})$. Аналогично при любых заданных словах $\boldsymbol{u}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{k-1}$ и их сдвигах $\underline{\boldsymbol{v}}_1^{(i_1)}, \ldots, \underline{\boldsymbol{v}}_{k-1}^{(i_{k-1})}$, $i_j = 0, 1, \ldots, N' - 1$, $j = 1, \ldots, k - 1$, мы обозначим через $\alpha(\boldsymbol{u}', \underline{\boldsymbol{v}}_1^{(i_1)}, \ldots, \underline{\boldsymbol{v}}_{k-1}^{(i_{k-1})})$ число символов 1, которые не покрываются в слове $\boldsymbol{u}$ ни одним из этих $\underline{\boldsymbol{v}}_1^{(i_1)}, \ldots, \underline{\boldsymbol{v}}_{k-1}^{(i_{k-1})}$ сдвигов. Минимум $\alpha(\boldsymbol{u}', \underline{\boldsymbol{v}}_1^{i_1}, \ldots, \underline{\boldsymbol{v}}_{k-1}^{(i_{k-1})})$, взятый по всем $i_1, \ldots, i_{k-1}$, обозначается через $t(\boldsymbol{u}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{k-1})$.

При заданных целых числах $N \geq 3$, $k \geq 2$, $r \geq 1$ код $C$, состоящий из двоичных слов длины $N = 2N' - 1$, оканчивающихся $N' - 1$ нулями, называется $[N, k, r]$-кодом, если для любых $l$, $2 \leq l \leq k$, его различных слов $\boldsymbol{u}' = \boldsymbol{u}\mathbf{0}, \boldsymbol{v}_1' = \boldsymbol{v}_1\mathbf{0}, \ldots, \boldsymbol{v}_{l-1}' = \boldsymbol{v}_{l-1}\mathbf{0}$ выполняется неравенство $t(\boldsymbol{u}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{l-1}) \geq r$. Заметим, что в силу этого определения, если код $C$ является $[N, l, r]$-кодом и $|C| = l$, то он также является и $[N,k,r]$-кодом при любом $k > l$. Это замечание избавляет нас от того, чтобы в дальнейшем оговаривать случаи с $k > |C|$.

Задача, которая называется здесь $[N,k,r]$-*задачей*, состоит в отыскании $[N,k,r]$-кода с максимальным числом кодовых слов. Это максимальное число обозначается через $M[N,k,r]$, а число кодовых слов (т.е. *размер кода*) произвольного кода $C$ обозначается через $|C|$. Таким образом, $[N,k,r]$-код $C$ дает оптимальное решение $[N,k,r]$-задачи, если $|C| = M[N,k,r]$.

Также мы рассмотрим $[N,w,k,r]$-задачу, которая отличается от $[N,k,r]$-задачи тем, что рассматриваются $[N,k,r]$-коды со словами постоянного веса $w$. Такие коды называются $[N,w,k,r]$-кодами, и их максимальный размер обозначается через $M[N,w,k,r]$.

**2.2. Связь между $[N,w,k,r]$-кодами с различными $k$.** Пусть $C$ есть $[N,w,2,r^*]$-код с $r^* > w/2$. Это означает, что $\beta(\boldsymbol{u}', \underline{\boldsymbol{v}}^{(i)}) < w/2$ для любых различных кодовых слов $\boldsymbol{u}0, \boldsymbol{v}0$ и сдвигов на $i$, т.е. любой сдвиг одного кодового слова может покрыть только меньше чем половину символов 1 другого слова. Поэтому все символы 1 любого кодового слова не могут быть покрыты сдвигами любых двух других кодовых слов. Таким образом, код $C$ является $[N,w,3,1]$-кодом. В действительности число символов 1 одного кодового слова, покрываемых сдвигами двух других кодовых слов, может быть оценено сверху величиной $2(w-r^*)$. Следовательно, число непокрытых символов 1 оценивается снизу величиной $w - 2(w-r^*) = 2r^* - w$. Это означает, что $C$ есть $[N,w,3,r]$-код с $r = 2r^* - w$. Более того, это также означает, что оптимальное решение $[N,w,2,r^* = \lceil (r+w)/2 \rceil]$-задачи можно использовать как некоторое решение $[N,w,3,r]$-задачи и что $M[N,w,3,r] \geq M[N,w,2,\lceil (r+w)/2 \rceil]$. Здесь и далее $\lceil x \rceil$ – минимальное целое число, большее или равное $x$, а $\lfloor x \rfloor$ – целая часть числа $x$.

Аналогично неоптимальное решение $[N,w,k,r]$-задачи может быть получено из решения $[N,w,k^*,r^*]$-задачи с $k^* < k$ и $r^* > r$. Чтобы показать это, предположим, что $k^*-1$ есть делитель $k-1$, т.е. $k-1 = m(k^*-1)$, где $m > 1$ – некоторое целое число. Заметим, что условие $w - t(\boldsymbol{u}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{k-1}) \leq w - r$ слабее, чем условие $w - t(\boldsymbol{u}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{k^*-1}) \leq (w-r)/m$. Возьмем $r^* = \lceil (r + (m-1)w)/m \rceil$. Тогда $w - r^* \leq$ $\leq (w-r)/m$, и справедлива следующая

Теорема 1. *Пусть* $k-1 = m(k^*-1)$, $r^* = \lceil (r+(m-1)w)/m \rceil$, *где* $m > 1$ – *целое число. Тогда*

1. *Каждый* $[N,w,k^*,r^*]$-*код является* $[N,w,k,r]$-*кодом;*
2. $M[N,w,k,r] \geq M[N,w,k^*,r^*]$.

**2.3. Верхние границы для $M[N,w,2,r]$ и $M[N,3,r]$.** Пусть $C$ – $[N,w,2,r]$-код, $\boldsymbol{u}0$ и $\boldsymbol{v}0$ – слова кода $C$, $\widetilde{\boldsymbol{u}}0$ и $\widetilde{\boldsymbol{v}}0$ – подслова, соответственно, слов $\boldsymbol{u}0$ и $\boldsymbol{v}0$ с весом $w(\widetilde{\boldsymbol{u}}) = w(\widetilde{\boldsymbol{v}}) = w - r + 1$.

Если бы некоторый сдвиг $\underline{\boldsymbol{v}}^{(i)}$ переводил $\widetilde{\boldsymbol{v}}0$ в $\widetilde{\boldsymbol{u}}0$, то слово $\underline{\boldsymbol{v}}^{(i)}$ могло бы покрыть не меньше чем $w-r+1$ символов 1 в слове $\boldsymbol{u}0$, и это противоречило бы неравенству $t(\boldsymbol{u},\boldsymbol{v}) \geq r$. Т аким образом, подслова веса

$$w_0 \stackrel{\triangle}{=} w - r + 1,$$

которые содержатся в различных кодовых словах кода $C$, не совпадают при любых сдвигах. Подслова, которые не совпадают при любых сдвигах, называются *строго различными.*

Мы хотим найти для кода $C$ верхнюю границу для максимального числа попарно строго различных подслов веса $w_0$ кодовых слов кода $C$.

Для этого заметим, что два подслова являются строго различными тогда и только тогда, когда их сдвиги, которые переводят первую ненулевую позицию (т.е. первую позицию, на которой стоит символ 1) в первую позицию, являются различными. Рассмотрим множество всех различных слов длины $N'$ и веса $w_0$ с символом 1 на первой позиции. Число элементов в этом множестве равно $\begin{pmatrix} N'-1 \\ w_0-1 \end{pmatrix}$. (Здесь $\begin{pmatrix} a \\ b \end{pmatrix}$ – число сочетаний из $a$ элементов по $b$.)

Теперь мы найдем нижнюю границу для числа строго различных подслов веса $w_0$ произвольного исходного слова веса $w$. Множество различных подслов веса $w_0$ слова веса $w$ имеет размер $\begin{pmatrix} w \\ w_0 \end{pmatrix}$. Некоторые пары подслов в этом множестве могут быть не строго различными. Принимая это во внимание, выберем из рассматриваемого множества только те подслова, которые имеют 1 на первой ненулевой позиции исходного слова веса $w$. Число таких выбранных подслов равно $\begin{pmatrix} w-1 \\ w_0-1 \end{pmatrix}$, и все они попарно строго различные.

Таким образом, число строго различных подслов веса $w_0$ каждого кодового слова кода $C$ не меньше чем $\begin{pmatrix} w-1 \\ w_0-1 \end{pmatrix}$; эти подслова, строго различные для различных кодовых слов кода $C$, и число строго различных подслов веса $w_0$ равно $\begin{pmatrix} N'-1 \\ w_0-1 \end{pmatrix}$. Поэтому число слов кода $C$ не больше чем $\begin{pmatrix} N'-1 \\ w_0-1 \end{pmatrix} \Big/ \begin{pmatrix} w-1 \\ w_0-1 \end{pmatrix}$, т.е. справедлива следующая

Теорема 2. *Для максимального числа слов $[N, w, 2, r]$-кода справедлива следующая верхняя граница:*

$$M[N, w, 2, r] \leq \frac{\begin{pmatrix} N'-1 \\ w-r \end{pmatrix}}{\begin{pmatrix} w-1 \\ w-r \end{pmatrix}} = \frac{(N'-1)!(r-1)!}{(N'-w+r-1)!(w-1)!}, \qquad N = 2N'-1. \tag{1}$$

*При $r = 1$ граница* (1) *выполняется с равенством, т.е.* $M[N, w, 2, 1] = \begin{pmatrix} N'-1 \\ w-r \end{pmatrix}$, *и* $\max\limits_{w} M[N, w, r, 1] = \begin{pmatrix} N'-1 \\ \lfloor (N'-1)/2 \rfloor \end{pmatrix}$, *причем максимум достигается при* $w = \lfloor (N'-1)/2 \rfloor$.

Утверждение этой теоремы для случая $r = 1$ было получено в [7]. Заметим также, что граница (1) напоминает границу Джонсона [8] для кодов постоянного веса, хотя эти границы различны.

Наша цель – дать верхнюю границу для $M[N, 3, r]$. Для этого мы рассмотрим еще один тип кодов.

При заданных целых числах $N' \geq 2$, $k \geq 2$, $r \geq 1$ код $C$, состоящий из двоичных слов длины $N'$, называется $[N', k, r]_f$*-кодом* (здесь $f$ – первая буква английского слова fixed), если для любых $k$ его различных слов $\boldsymbol{u}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{k-1}$ выполняется неравенство $\alpha(\boldsymbol{u}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{k-1}) \geq r$. Максимум $|C|$ по всем $[N', k, r]_f$-кодам обозначается через $M_f[N', k, r]$. Как и ранее, если мы будем рассматривать код с заданным постоянным весом $w$, то включим символ $w$ в обозначение кода (например, раньше мы писали $[N', w, k, r]$, теперь будем писать $[N', w, k, r]_f$). Введенные здесь коды отличаются от $[N, k, r]$-кодов тем, что сравнение кодовых слов выполняется теперь без сдвигов. Заметим, что $[N', w, k, r]_f$-коды – это коды постоянного веса $w$ с расстоянием Хэмминга не меньшим чем $2r$.

Ясно, что каждый $[N,k,r]$-код после урезания $\mathbf{0}$ в конце кодовых слов превращается в $[N',k,r]_f$-код и выполняются следующие неравенства:

$$\begin{aligned} &M_f[N',w,k,r] \geq M[N,w,k,r], \\ &M_f[N',k,r] \geq M[N,k,r]. \end{aligned} \tag{2}$$

Интересно заметить, что фактически $[N',3,1]_f$-задача была поставлена Эрдешем как следующая нерешенная задача: для заданного множества найти максимальное семейство его подмножеств такое, что любое подмножество из этого семейства не может быть покрыто объединением двух других подмножеств из этого семейства.

Найдем теперь верхнюю границу для $M_f[N',3,r]$. С этой целью для каждых двух различных слов $\boldsymbol{u}$ и $\boldsymbol{v}$ $[N',3,r]_f$-кода $C$ определим слово $\boldsymbol{a}(\boldsymbol{u},\boldsymbol{v})$. Слово $\boldsymbol{a}(\boldsymbol{u},\boldsymbol{v})$ имеет символ 1 на позиции $i$, если хотя бы одно из слов $\boldsymbol{u}$ или $\boldsymbol{v}$ имеет символ 1 на этой позиции, $1 \leq i \leq N'$, и $\boldsymbol{a}(\boldsymbol{u},v)$ имеет символ 0 на позиции $i$ в остальных случаях. Множество всех таких слов $\boldsymbol{a}(\boldsymbol{u},\boldsymbol{v})$ для $\boldsymbol{u}$ и $\boldsymbol{v}$ из $C$ обозначается через $\dot{C}$. Заметим, что $\dot{C}$ – это $[N',2,r]_f$-код, и $|\dot{C}| = |C|(|C|-1)/2$. Это дает следующую теорему.

Теорема 3. *Для числа слов $M_f[N',3,r]$ справедливы следующие границы:*

$$M[N,3,r] \leq M_f[N',3,r] \leq \left\lfloor \sqrt{2M_f[N',2,r]} \right\rfloor + 1. \tag{3}$$

При $r=1$ неравенство (3) означает, что

$$M[N,3,1] \leq \left\lfloor \sqrt{2\binom{N'}{\lfloor N'/2 \rfloor}} \right\rfloor + 1.$$

**2.4. Первая конструкция $[N,2,r]$-кода.** Первая конструкция $[N,2,r]$-кодов, которая дается в этом разделе, является естественным обобщением конструкции Цыбакова – Вебера [8].

Пусть $N' = N_1' + N_2'$, код $C_1$ – это $[N_2',2,r]_f$-код, и слово $\boldsymbol{z}$ длины $N_1'$ является таким, что $\alpha(\boldsymbol{z}',\underline{\boldsymbol{z}}^{(i)}) \geq r$ при всех $i=1,\dots,N'-1$. Тогда код $C$, состоящий из всех слов $\boldsymbol{u}' = \boldsymbol{z}\boldsymbol{x}\mathbf{0}$, где $\boldsymbol{x} \in C_1$, есть $[N,2,r]$-код. В самом деле, неравенство $\alpha(\boldsymbol{u}',\underline{\boldsymbol{v}}^{(i)}) \geq r$ при $\boldsymbol{u}',\boldsymbol{v}' \in C$ выполняется в случае $i=0$, так как код $C_1$ является $[N_2',2,r]$-кодом; оно выполняется в случае $i=1,\dots,N'-1$ благодаря свойству слова $\boldsymbol{z}$.

В конструкции Цыбакова – Вебера [7] $r=1$, $N_1'=1$, и $\boldsymbol{z}$ – слово длины 1 с символом 1. Если $r>1$, можно взять $\boldsymbol{z}$ таким, что $\boldsymbol{z} = \boldsymbol{z}_0\boldsymbol{z}_r\boldsymbol{z}_{r-1}\dots\boldsymbol{z}_2$, где $\boldsymbol{z}_0$ – слово, состоящее из $r$ символов 1, а при $i>0$ $\boldsymbol{z}_i$ – слово длины $i$, имеющее лишь один символ 1, стоящий на позиции $i$. Например, $\boldsymbol{z}=1101$ при $r=2$ или $\boldsymbol{z}=11100101$ при $r=3$. Заметим, что длина использованного слова $\boldsymbol{z}$ равна $(r(r+3)-2)/2$.

Существуют более эффективные конструкции. Например, можно выбрать в качестве $\boldsymbol{z}$ псевдослучайную последовательность, в частности $m$-последовательность, с автокорреляционной функцией, равной $-1$ при всех ненулевых сдвигах (если заменить 0 и 1 на $\pm 1$) [1, 9, 10]. Главное свойство $(n+2)$-последовательности длины $L = 2^{n+2}-1$ состоит в том, что $d(\boldsymbol{z},\boldsymbol{z}^{(i)}) = 2^{n+1}$ и $\alpha(\boldsymbol{z},\boldsymbol{z}^{(i)}) = 2^n$, $i=1,\dots,L$. Ясно, что при этом $\alpha(\boldsymbol{z}',\underline{\boldsymbol{z}}^{(i)}) \geq 2^n$. Учитывая, что в интервале $[r,2r)$ находится единственное число вида $2^n$, можно получить следующие соотношения:

$$M_f[N'-8r,2,r] \leq M[N,2,r] \leq M_f[N',2,r], \tag{4}$$

где $M[\cdot]$ (и $M_f[\cdot]$) обозначает максимальный размер кода с параметрами, вписанными в $[\cdot]$. Второе неравенство в (4) является тривиальным. Для доказательства первого неравенства в (4) мы заметим, что для любого $r \geq 1$ существует $(n+2)$-последовательность длины $2^{n+2}-1$, где $4r-1 \leq 2^{n+2}-1 \leq 8r-5$. Следовательно, если взять произвольный $[N'-8r, 2, r]_f$-код и придать каждому его кодовому слову такую $(n+2)$-последовательность в качестве префикса, а также некоторое число нулей в конце для получения полной длины слова, равной $N$, то получим $[N, 2, r]$-код и первое неравенство в (4). Неравенства (4) связывают $[N, 2, r]$-задачу со стандартной задачей кодов, исправляющих ошибки.

Вместо $(n+2)$-последовательности можно использовать также другие псевдослучайные последовательности $z$, длина которых имеет вид $4m-1$, такие что $d(z, z^{(i)}) = 2m$ и $\alpha(z, z^{(i)}) = m$ при всех $i > 0$ (см., например, [11]).

Можно применить представленную первую конструкцию $[N, 2, r]$-кодов вместе с теоремой 1 к построению $[N, w, k, 1]$-кода. Теорема 1 утверждает, что можно взять $[N, w, k^*, r^*]$-код в качестве $[N, w, k, r]$-кода, если $k^* < k$ и $r^* > r$. Например, давайте построим код с $k = 4$ и $r = 1$. Возьмем $m = 3$ ($m$ – целое число, участвующее в теореме 1), $r^* = \lceil (1+2w)/3 \rceil$ и используем некоторый $[N, w, 2, \lceil (1+2w)/3 \rceil]$-код в качестве $[N, w, 4, 1]$-кода. Что касается $[N, w, 2, \lceil (1+2w)/3 \rceil]$-кода, он может быть построен с использованием $[N_2', \lfloor N_2'/2 \rfloor, 2, r]_f$-кода, который является кодом из классической теории кодирования, имеющим вес $w = \lfloor N_2'/2 \rfloor$, длину $N_2'$ и расстояние Хэмминга не меньше чем $2r$.

**2.5. Вторая конструкция $[N, 2, r]$-кода; код постоянного веса.** Здесь будет дана вторая конструкция $[N, 2, r]$-кодов. Для ее описания нам понадобятся еще два типа кодов.

Циклический код со словами постоянного веса $w$, длиной слов $N'$ и минимальным расстоянием Хэмминга $d = 2r$ называется $[N', w, r]_c$-*кодом*. Пусть $M_c[N', w, r]$ обозначает максимальный размер $[N', w, r]$-кода.

Далее используем циклически перестановочный код [12], который является двоичным блоковым кодом длины $N'$ таким, что каждое кодовое слово имеет $N'$ различных сдвигов, и такой, что кодовые слова циклически различны (т.е. ни одно кодовое слово не может быть получено циклическим сдвигом другого кодового слова). Циклически перестановочный код со словами постоянного веса $w$ и минимальным расстоянием Хэмминга $d = 2r$ называется $[N', w, r]_p$-*кодом*. Пусть $M_p[N', w, r]$ обозначает максимальный размер $[N', w, r]_p$-кода.

Заметим, что параллельный сдвиг $\underline{v}^{(i)}$ слова $v$ не покрывает больше символов 1 слова $u$, чем циклический сдвиг $v^{(i)}$. Следовательно, $M[N, w, 2, r] \geq M_p[N', w, r]$.

Пусть $C_2$ – это $[N', w, r]_c$-код с $r \leq w/2$. Для простоты предположим, что $N'$ и $w$ – взаимно простые числа. Тогда $N'$ различных циклических сдвигов $u^{(i)}$, $i = 0, \ldots, N-1$, кодового слова $u$ кода $C_2$ также являются словами кода $C_2$, и код $C_2$ распадается на такие классы циклических сдвигов. Без потери общности можно считать, что на первой позиции слова $u$ стоит символ 1. Выберем числа $i_1 = 0, i_2, \ldots, i_g$, где $g = \lfloor w/r \rfloor$, так чтобы сдвиг $u^{(i_j)}$ кодового слова $u$ переводил $((j-1)r+1)$-й символ 1 слова $u$ на первую позицию. Включим $g$ слов $u^{(i_j)}$ в код $C$ и сделаем то же самое для всех оставшихся классов циклических сдвигов.

Теперь мы можем привести утверждение, касающееся построенного кода $C$.

Теорема 4. *Код, полученный удлинением на* $\mathbf{0}$ (*т.е. дописыванием последовательности* $\mathbf{0}$ *длины* $N_1'$) *всех слов кода* $C$, *является* $[N, w, 2, r]$-*кодом.*

Доказательство. Если $u$ и $v$ – слова из построенного выше кода $C$ и эти слова получены из различных циклических классов, то $t(u, v) \geq r$, так как параллельный сдвиг одного слова может покрыть не более чем то же самое число символов 1 другого слова, которое может покрыть циклический сдвиг. Если $u$ и $v$ получены из одного и того же циклического класса и $i$ такое, что $u \neq v^{(i)}$, то $\alpha(u', \underline{v}^{(i)}) \geq r$ по той же самой причине. Наконец, если $i$ такое, что $\boldsymbol{u} = v^{(i)}$, то $\alpha(\boldsymbol{u}', \underline{v}^{(i)}) \geq r$, так как после параллельного сдвига $\underline{v}^{(i)}$ по меньшей мере $r$ символов 1 слова $\boldsymbol{v}$ выдвигаются из позиций $1, \ldots, N'$, где расположено слово $\boldsymbol{u}$. ▲

Построеннный код $C$ имеет $|C_2| \lfloor w/r \rfloor / N'$ слов. Следовательно,

$$M[N, w, 2, r] \geq M_c[N', w, r] \lfloor w/r \rfloor / N'. \tag{5}$$

## § 3. Обобщение $[N, k, r]$-задачи

В этом параграфе дается обобщение $[N, k, r]$-задачи.

**3.1. Постановка задачи.** Рассмотрим код $C$ с $|C|$ кодовыми словами длины $N$. Считается, что символы кодовых слов могут появляться в моменты времени $T = \ldots, -1, 0, 1, \ldots$ Кодовое слово длины $N$ может занимать интервал $T+1, \ldots, T+N$ с любым $T$. Если кодовое слово $\boldsymbol{u}$ занимает интервал $T+1, \ldots, T+N$, то будем говорить, что $\boldsymbol{u}$ передается в этом интервале. Этот интервал называется интервалом передачи слова $\boldsymbol{u}$. Мы будем считать, что каждый момент $T$ принадлежит не более чем $k$ интервалам передачи различных кодовых слов, т.е. в каждый момент $T$ передается самое большее $k$ различных кодовых слов. Одно и то же кодовое слово не может покрывать любой заданный момент $T$ более чем один раз, т.е. интервалы передачи одного и того же кодового слова не пересекаются.

Здесь рассматриваются $\{N, k, r\}$-коды, которые являются обобщением $[N, k, r]$-кодов. Код $C$ называется $\{N, k, r\}$-кодом, если каждое переданное кодовое слово имеет не менее $r$ позиций с символом 1 таких, что эти позиции появляются в моменты, когда другие передаваемые слова имеют позиции с символом 0. Связь между $\{N, k, r\}$- и $[N, k, r]$-кодами состоит в следующем. Код со словами длины $N = 2N' - 1$ и $N' - 1$ нулями в конце своих слов является $\{N, k, r\}$-кодом, если и только если этот код есть $[N, k, r]$-код.

Задача, которая называется $\{N, k, r\}$-задачей, состоит в отыскании $\{N, k, r\}$-кода с максимальным числом кодовых слов. Это максимальное число обозначается через $M\{N, k, r\}$. Заметим, что $\{N, k, r\}$-задача отличается от $[N, k, r]$-задачи отсутствием условия, что на конце кодовых слов должны стоять нулевые последовательности. В этой статье приводится одна конструкция $\{N, 2, 1\}$-кода и показывается, что эта конструкция дает коды, которые значительно лучше по размеру, чем оптимальные $[N, 2, 1]$-коды. Кодовые слова в нашей конструкции $\{N, 2, 1\}$-кода также имеют нулевую последовательность на конце, но длина этой последовательности меньше чем $N' - 1$.

**3.2. Конструкция $\{N, 2, 1\}$-кода.** Здесь дается конструкция $\{N, k, r\}$-кода с $k = 2$ и $r = 1$. Ниже $\{N, k, r\}$-код со словами постоянного веса $w$ обозначается как $\{N, w, k, r\}$-код.

Теперь мы опишем код $C$, который, как будет доказано, является $\{N, w, 2, 1\}$-кодом. Пусть $l$ и $w$ – положительные целые числа такие, что $l + w \leq N$. Пусть $S(N, w, l)$ – множество всех различных слов веса $w - 1$ и длины $N - l - 1$, которые не содержат последовательности $0 \ldots 01$ с $l$ нулями, идущими подряд, и одной единицей в конце. Определим $C$ как код, слова которого состоят из следующих трех частей. Первая часть – это символ 1 на первой позиции. Третья часть – это нулевая последовательность длины $l$, занимающая $l$ последних позиций. Вторая часть – это слово из $S(N, w, l)$, и каждое слово из $S(N, w, l)$ соответствует одному слову из $C$. Размер кода $C$ равен размеру множества $S(N, w, l)$.

Теорема 5. *Код $C$ является $\{N, w, 2, 1\}$-кодом.*

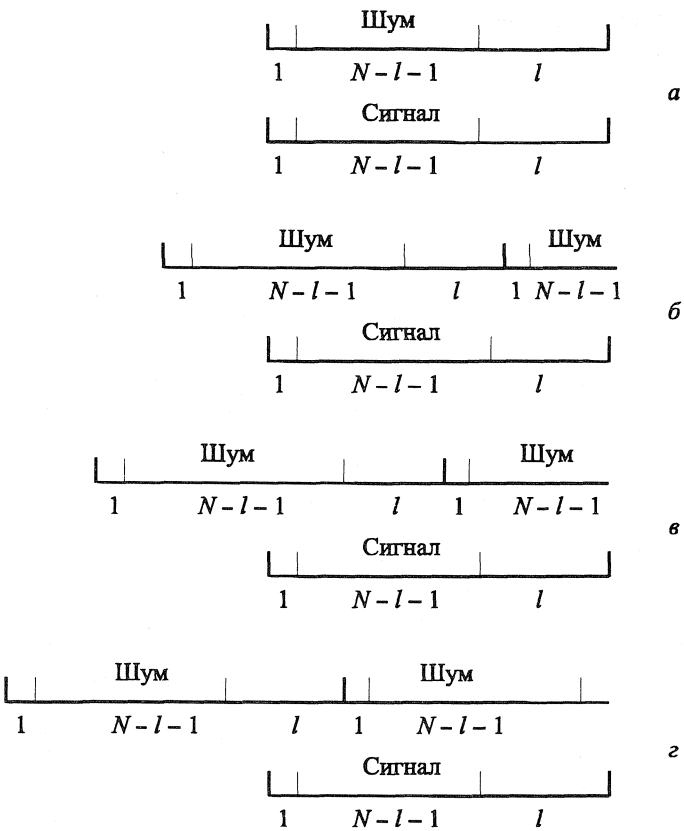


Рис. 2

Доказательство (рис. 2 является иллюстрацией доказательства). На рис. 2,*а* показаны два слова кода $C$. Одно кодовое слово называется сигналом, другое – шумом. Шум не сдвинут относительно сигнала. Так как вторые части слов различны и имеют одинаковый вес, то по крайней мере один символ 1 в сигнале не будет покрытым.

Теперь сдвинем шумовое слово влево. Наихудший случай для сигнала состоит в том, что другое шумовое кодовое слово присоединится к первому шумовому кодовому слову. Рассмотрим этот наихудший случай при различных типах сдвигов.

Для сдвига, показанного на рис. 2,*б*, шум имеет меньше чем $w$ символов 1, покрывающих первую и вторую части сигнала (вместе эти части имеют вес $w$).

Для сдвига, показанного на рис. 2,*в*, третья часть левого шума, которая является нулевой последовательностью длины $l$, покрывает некоторый интервал внутри второй части сигнала. Если этот интервал сигнала не является нулевой последовательностью, то ясно, что сигнал имеет по крайней мере один непокрытый символ 1. Если этот интервал сигнала является нулевой последовательностью, то согласно конструкции кода $C$ сигнал имеет только нули после этого интервала. Поэтому подобно случаю, показанному на рис. 2,*б*, левый шум, расположенный над первой и второй частями сигнала, имеет меньше чем $w$ символов 1, а сигнал – все $w$ символов 1.

Для сдвига, показанного на рис. 2,*г*, первая единица сигнала не является покрытой.

Если рассмотреть сдвиги шумовых слов вправо, то получатся те же самые случаи. ▲

Найдем теперь размер описанного кода $C$, имеющего слова с различными вторыми частями. Будем считать, что параметры $N$, $w$ и $l$ кода $C$ заданы. Размер кода $C$ обозначим через $V(N, w, l)$.

Лемма 1. *Размер $V(N, w, l)$ кода $C$ удовлетворяет рекуррентному соотношению*

$$V(N,w,l) = V(N-1,w,l) + V(N-1,w-1,l) - V(N-1-l,w-1,l),$$
$$V(N,N-l,l) = 1, \qquad V(N,w,l) = 0 \quad \textit{при} \quad l+w > N. \tag{6}$$

Доказательство. Рассмотрим последнюю позицию второй части кодового слова (ППВЧКС), т.е. позицию $N-l$ слова из кода $C$. Обозначим через $C(0)(C(1))$ множество слов кода $C$ с 0 (соответственно, 1) на ППВЧКС. Имеем $|C(0)| = V(N-1, w, l)$, так как когда опускается ППВЧКС, то получается просто код $C$ с параметрами $N-1, w, l$. Для множества $C(1)$ имеем $|C(1)| = V(N-1, w-1, l) - V(N-1-l, w-1, l)$. Последнее равенство справедливо по следующей причине. Когда опускается ППВЧКС, получаются слова кода $C$ с параметрами $N-1, w-1, l$. Однако множество $C(1)$ не содержит всех слов кода $C$ с параметрами $N-1, w-1, l$. Множество $C(1)$ не содержит слов с $l$ или большим числом нулей в конце второй части. Если опустить эти $l$ позиций, то получится код $C$ с параметрами $N-1-l, w-1, l$. Заметим, что код $C$ с параметрами $N, w, l$ был определен при $l+w \le N$. Следовательно, мы положим $V(N, w, l) = 0$ при $l + w > N$. ▲

Другой способ отыскания $V(N, w, l)$, который также используется далее, дается в следующей лемме.

Лемма 2. $V(N,w,l) = W(N-l-w, w-1, l-1)$, *где $W(x, y, z)$ удовлетворяет рекуррентному соотношению*

$$W(x,y,z) = W(x-0,y-1,z) + \dots + W(x-\min(x,z),y-1,z), \qquad y \ge 2,$$
$$W(x,1,z) = 1 + \min(x,z). \tag{7}$$

*При $x \le z$ соотношение* (7) *имеет решение*

$$W(x,y,z) = \binom{x+y}{y}. \tag{8}$$

Доказательство. Здесь потребуется использовать вектор расстояний [7]. *Вектор расстояний* $(v_1, \dots, v_{w-1})$, связанный с двоичной последовательностью веса $w \ge 2$, определяется как вектор длины $w-1$, в котором компонента $v_i$ показывает число нулей между $i$-м и $(i+1)$-м символами 1 в последовательности.

Рассмотрим двоичную последовательность на позициях $1, \dots, N-l$ кодовых слов кода $C$ с параметрами $N, w, l$. Рассмотрим вектор расстояний $(v_1, \dots, v_{w-1})$ этой последовательности. Пусть $W(x, y, z)$ обозначает число различных векторов расстояний, удовлетворяющих ограничению

$$v_1 + \dots + v_{y-1} \le x, \qquad 0 \le v_i \le z, \qquad 0 < i < y. \tag{9}$$

Соотношение (7) получается, если заметить, что $W(x-i, y-1, z)$ есть число векторов расстояний $(v_1 = i, v_2, \dots, v_{y-1})$, удовлетворяющих (9) при $0 \le i \le \min(x, z)$.

*Таблица 1*

| $w \backslash N$ | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 0 | 0 | 1 | 2 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 3 | 0 | 0 | 0 | 1 | 3 | 6 | 8 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 |
| 4 | 0 | 0 | 0 | 0 | 1 | 4 | 10 | 17 | 23 | 26 | 27 | 27 | 27 | 27 | 27 | 27 | 27 | 27 | 27 | 27 | 27 |
| 5 | 0 | 0 | 0 | 0 | 0 | 1 | 5 | 15 | 31 | 50 | 66 | 76 | 80 | 81 | 81 | 81 | 81 | 81 | 81 | 81 | 81 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 6 | 21 | 51 | 96 | 147 | 192 | 222 | 237 | 242 | 243 | 243 | 243 | 243 | 243 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 7 | 28 | 78 | 168 | 294 | 435 | 561 | 651 | 701 | 722 | 728 | 729 | 729 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 8 | 36 | 113 | 274 | 540 | 897 | 1290 | 1647 | 1913 | 2074 | 2151 | 2179 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 9 | 45 | 157 | 423 | 929 | 1711 | 2727 | 3834 | 4850 | 5634 | 6138 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 10 | 55 | 211 | 625 | 1507 | 3061 | 5365 | 8272 | 11411 | 14318 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 11 | 66 | 276 | 891 | 2343 | 5193 | 9933 | 16698 | 25048 |
| 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 12 | 78 | 353 | 1233 | 3510 | 8427 | 17469 | 31824 |
| 13 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 13 | 91 | 443 | 1664 | 5096 | 13170 | 29406 |
| 14 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 14 | 105 | 547 | 2198 | 7203 | 19930 |
| 15 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 15 | 120 | 666 | 2850 | 9948 |
| 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 16 | 136 | 801 | 3636 |
| 17 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 17 | 153 | 953 |
| 18 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 18 | 171 |
| 19 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 19 |

*Таблица 2*

| $w \backslash N$ | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 0 | 0 | 0 | 1 | 2 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 3 | 0 | 0 | 0 | 0 | 1 | 3 | 6 | 10 | 13 | 15 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 |
| 4 | 0 | 0 | 0 | 0 | 0 | 1 | 4 | 10 | 20 | 32 | 44 | 54 | 60 | 63 | 64 | 64 | 64 | 64 | 64 | 64 | 64 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 5 | 15 | 35 | 66 | 106 | 150 | 190 | 221 | 241 | 251 | 255 | 256 | 256 | 256 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 6 | 21 | 56 | 121 | 222 | 357 | 512 | 667 | 802 | 903 | 968 | 1003 | 1018 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 7 | 28 | 84 | 204 | 420 | 756 | 1212 | 1758 | 2338 | 2884 | 3340 | 3676 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 8 | 36 | 120 | 323 | 736 | 1464 | 2592 | 4146 | 6064 | 8192 | 10320 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 9 | 45 | 165 | 487 | 1215 | 2643 | 5115 | 8938 | 14266 | 20994 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 10 | 55 | 220 | 706 | 1912 | 4510 | 9460 | 17911 | 30962 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 11 | 66 | 286 | 991 | 2893 | 7348 | 16588 | 33793 |
| 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 12 | 78 | 364 | 1354 | 4236 | 11518 | 27820 |
| 13 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 13 | 91 | 455 | 1808 | 6032 | 17472 |
| 14 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 14 | 105 | 560 | 2367 | 8386 |
| 15 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 15 | 120 | 680 | 3046 |
| 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 16 | 136 | 816 |
| 17 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 17 | 154 |
| 18 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 18 |
| 19 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

*Таблица 3*

| $N$ | $M[(N+1)/2, 2, 1]$ | $\max\limits_{w,\ell} V(N, w, \ell)$ |
|---|---|---|
| 9 | 6 | 10 |
| 11 | 10 | 31 |
| 13 | 20 | 96 |
| 15 | 35 | 294 |
| 17 | 70 | 929 |
| 19 | 126 | 3061 |
| 21 | 256 | 9933 |
| 23 | 462 | 33793 |

Если $x \leq z$, то ситуация такая же, как в случае $M[N = x + y + 1, w = y + +1, 2, 1]$. Чтобы получить (8), мы использовали тождество $\binom{u}{v} = \binom{u-1}{v-1} + \ldots \ldots + \binom{v-1}{v-1}$. ▲

Отметим, что (9) в данном доказательстве в некотором смысле описывает структуру кода $C$. Он является множеством целочисленных точек многомерного куба, имеющего ограниченную сумму координат. Мощность этого усеченного куба (см. [13]) может быть использована для оценки числа этих целочисленных точек.

Дополнительно приведем еще одно рекуррентное соотношение для $V(N, w, l)$, а именно

$$V(N,w,l) = V(N-1,w,l-1) + (w-1)V(N-l-1,w-1,l-1) + \\ + \binom{w-1}{2} V(N-2l-1,w-2,l-1) + \ldots \\ \ldots + \binom{w-1}{i} V(N-i-1,w-i,l-1) + \ldots \tag{10}$$

Уравнения для $V(N, w, l)$, например (6), могут быть легко решены для заданного $l$ и различных $N$ и $w$. В табл. 1 дан размер кода $V(N, w, l)$ при $3 \leq N \leq 23$, $1 \leq \leq w \leq 19$, $l = 3$, в табл. 2 – размер кода $V(N, w, l)$ при $3 \leq N \leq 23$, $1 \leq w \leq 19$, $l = 4$. В табл. 3 дано сравнение размеров оптимального кода из [7] при $k = 2$, $r = 1$ и $V(N, w, l)$. Размер $V(N, w, l)$, данный в третьем столбце этой таблицы, есть максимум $V(N, w, l)$ по $w$ и $l$ при заданном $N$. Табл. 3 показывает, что $\max\limits_{w,l} V(N, w, l)$ существенно выше, чем размер оптимального кода из [7]. Сравнение оптимального кода из [7] с кодами из [1] проведено в [7]. Например, при $k = 2$, $r = 1$ в работе [1] даны коды с длинами 55, 78, 114 и 222, которые имеют размеры 11, 13, 19 и 37 соответственно.

Заметим в конце, что одно из множеств слов, которое было рассмотрено в этом разделе, изучалось Гильбертом [14] (см. также работу Гунбаса и Одлизко [15]). Однако здесь мы потребовали выполнения условия постоянного веса, которого не было в [14 и 15]. Для построения $\{N, 2, r\}$-кодов могут быть использованы коды, построенные в работах Левенштейна [11, 16, 17], которые обеспечивают заданное расстояние Хэмминга между любым кодовым словом и стыком любых двух кодовых слов.

## § 4. Заключение

В этой статье даются конструкции кодов, избегающих конфликтов. Две из них используют кодовые слова длины $N = 2N' - 1$ с $N' - 1$ нулевыми позициями на конце. Они гарантируют успешную передачу данного числа пакетов при конфликтах двух пользователей. Показано, как применить одну из этих конструкций для построения кода, избегающего конфликтов более чем двух пользователей. Третья конструкция дается для обобщенных кодов, которые не требуют $N' - 1$ нулевых позиций в конце кодовых слов. Также были получены некоторые границы для максимальных размеров кодов.

## СПИСОК ЛИТЕРАТУРЫ


1. *A N.Q., Györfi L., Massey J.* Constructions of Binary Constant-Weight Cyclic Codes and Cyclically Permutable Codes // IEEE Trans. Inform.Theory. 1992. V. 38. № 3. P. 940–949.
2. *Бассалыго Л.А., Пинскер М.С.* Ограниченный асинхронный множественный доступ // Пробл. передачи информ. 1983. Т. 19. № 4. С. 92–96.

3. *Györfi L., Vaida I.* Construction of Protocol Sequences for Multiple Access Collision Channel Without Feedback // IEEE Trans. Inform. Theory. 1993. V. 39. № 5. P. 1762–1765.
4. *Massey J.L., Mathys P.* The Collision Channel Without Feedback // IEEE Trans. Inform. Theory. 1985. V. 31. № 2. P. 192–204.
5. *Mathys P.* A Class of Codes for a $T$ Active Users Out of $N$ Multiple-Access Communication System // IEEE Trans. Inform. Theory. 1990. V. 36. № 6. P. 1206–1219.
6. *Цыбаков Б.С., Лиханов Н.Б.* Коммутация пакетов в канале без обратной связи // Пробл. передачи информ. 1983. Т. 19. № 2. С. 69–84.
7. *Tsybakov B.S., Weber J.H.* Conflict-Avoiding Codes // Proc. of the 17th Sympos. on Information Theory in the Benelux. Enschede. The Netherlands. May, 1996. P. 49–55.
8. *Johnson S.M.* A New Upper Bound for Error-Correcting Codes // IRE Trans. Inform. Theory. 1962. V. 8. № 3. P. 203–207.
9. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
10. *Simon M.K., Omura J.K., Scholtz R.A., Levit B.K.* Spread spectrum communications. V. 1. Rockville: Computer Science Press, 1985.
11. *Левенштейн В.И.* Об одном методе построения квазилинейных кодов, обеспечивающих синхронизацию при наличии ошибок // Пробл. передачи информ. 1971. Т. 7. № 3. С. 30–40.
12. *Gilbert E.N.* Cyclically Permutable Error-Correcting Codes // IEEE Trans. Inform. Theory. 1963. V. 9. № 2. P. 175–182.
13. *Хачиян Л.Г.* Задача вычисления объема многогранника перечислительно трудна // УМН. 1989. Т. 44. № 3. С. 179–180.
14. *Gilbert E.N.* Synchronization of Binary Messages // IRE Trans. Inform. Theory. 1960. V. 6. № 4. P. 470–477.
15. *Guibas L.J., Odlyzko A.M.* Maximal Prefix-Synchronized Codes // SIAM J. Appl. Math. 1978. V. 35. № 2. P. 401–418.
16. *Левенштейн В.И.* О максимальном числе слов в кодах без перекрытий // Пробл. передачи информ. 1970. Т. 6. № 4. С. 88–90.
17. *Левенштейн В.И.* Оценки для кодов, обеспечивающих исправление ошибок и синхронизацию // Пробл. передачи информ. 1969. Т. 5. № 2. С. 3–13.

Поступила в редакцию
14.08.2001

После переработки
18.06.2002