

Исследование корректирующих свойств кодов, лежащих на границе Варшамова–Гилберта, для системы неортогонального множественного доступа¹

Иванов Ф. И., Роллов Д. В.

*Институт проблем передачи информации, Российская академия наук, Москва, Россия
Национальный исследовательский университет “Высшая школа экономики”, Москва, Россия*

Поступила в редколлегию 15.02.2020

Аннотация—В данной работе рассмотрен класс многопользовательских слотированных векторных дизъюнктивных каналов. Для данного канала получена нижняя оценка на его пропускную способность. Кроме того, в работе была предложена сигнально-кодовая конструкция для разрешения коллизий, возникающих на этапе передачи, в предположении, что код, входящий в конструкцию, лежит на границе Варшамова–Гилберта.

КЛЮЧЕВЫЕ СЛОВА: система неортогонального множественного доступа, перемеженные коды Рида-Соломона, граница Варшамова–Гилберта

1. ВВЕДЕНИЕ

На сегодняшний день одной из наиболее быстрорастущих и перспективных технологий являются беспроводные сети, которые позволяют объединять различные виды устройств в группы, а затем предоставляют возможность для обмена информацией между этими устройствами. Важнейшей особенностью беспроводных сетей является стремительный рост числа активных пользователей, что обусловлено динамичным развитием таких концепций, как блокчейн, интернет вещей, умный дом. Вследствие этого, обоюдное влияние пользователей друг на друга становится достаточно ощутимым.

В связи с этим необходимо, чтобы большое число пользователей или устройств могли беспрепятственно ввести некоординированную передачу в беспроводных сетях. Из всего числа пользователей следует выделить некоторую совокупность из U пользователей, в которой каждый будет передавать короткие пакеты бит длины L на базовую станцию, например, в качестве таких “пользователей” можно рассматривать различные измерительные устройства, всевозможные датчики. Предполагается, что единственной задачей базовой станции является восстановление списка сообщений без какой-либо идентификации пользователя. Небольшая длина передаваемых сообщений, а также некоординированный способ передачи данных оказывают сильное влияние на различные методы построения сигнально-кодовых конструкций.

Важно отметить, что практически все широко известные и использующиеся на практике сигнально-кодовые конструкции, использующиеся в классических многопользовательских каналах, например системы на основе разделения скоростей [1] или чередования [2], предполагают координирование передачи между пользователями. Вместе с тем параметры таких схем, как разделяющая последовательность, кодовые скорости зависят от числа пользователей в системе.

¹ Работа выполнена при финансовой поддержке РФФИ грант 18-37-00319 мол_a

В данной работе рассматривается конструкция кодов для многопользовательского векторного дизъюнктивного канала, который был предложен в [3]. Данный канал является обобщением А-канала [4]–[7]

Данная работа состоит из двух частей:

1. Вначале будет описана модель передачи и модель многопользовательского канала, а затем проведена оценка его пропускной способности.
2. Далее будет рассмотрена сигнально-кодовая конструкция, разрешающая коллизии при передаче, при условии, что параметры данной конструкции лежат на границе Варшавова–Гилберта.

2. ВЕКТОРНЫЙ ДИЗЪЮНКТИВНЫЙ КАНАЛ

2.1. Описание канала

Векторный дизъюнктивный канал состоит из $Q > 1$ независимых подканалов/частот, которые в дальнейшем будут именоваться как элементарные подканалы. В свою очередь, весь канал разделён на S слотов, каждый из которых состоит из L элементарных подканалов.

В произвольный момент времени τ каждый пользователь выбирает произвольный j -ый слот, где $j \in [1; S]$ и передаёт в нём блок, состоящий из L бит. Ясно, что максимальное число пользователей, которые могут осуществить передачу данных ортогонально в вышеупомянутых условиях, равно $S = \frac{Q}{L}$.

2.2. Модель коллизии

В пункте А, в котором была описана модель векторного дизъюнктивного канала не был учтён тот факт, что при передаче данных возможны коллизии в некотором фиксированном слоте. В данном случае коллизия имеет место быть, когда некоторое число пользователей выбирают один и тот же слот в один и тот же момент времени τ . Из вышесказанных рассуждений можно сделать вывод, что вероятность данного события вычисляется как:

$$P_s = 1 - \left(1 - \frac{1}{S}\right)^{U-1}.$$

В работе рассматривается бесшумный канал. Следовательно, в данном случае $U - 1$ пользователей выступают в качестве шума для заданного пользователя, иными словами, они являются возможными источниками коллизии.

Обозначим через символ κ кратность коллизии. Другими словами, это число активных пользователей, выбравших один и тот же j -ый слот, в котором осуществляется передача данных заданным пользователем. Ясно, что кратность коллизии лежит в пределах $\kappa \in [0; U - 1]$. Можно посчитать вероятность события $\kappa = t$. Воспользуемся функцией вероятности биномиального распределения:

$$P(\kappa = t) = \binom{U-1}{t} \left(\frac{1}{S}\right)^t \left(1 - \frac{1}{S}\right)^{U-t-1}.$$

Также очевидно, что

$$P_s = \sum_{t=1}^{U-1} P(\kappa = t), \kappa \geq 1.$$

Важно отметить, что передача данных несколькими пользователями в один и тот же векторный дизъюнктивный канал не всегда будет являться причиной возникновения коллизии

для заданного пользователя. К примеру, пусть некоторый заданный пользователь передаёт вектор $(1, 1, \dots, 1)$. Данный вектор будет принят корректно без каких-либо искажений вне зависимости от того, что будут передавать другие пользователи в этом же элементарном подканале.

Приведём пример случая, когда два случайных пользователя α и β выбрали один и тот же векторный дизъюнктивный канал в некоторый момент времени t :

Пусть пользователь α передаёт двоичный вектор длины L : $X_{\alpha,t} = (x_{\alpha,t}^{(1)}, x_{\alpha,t}^{(2)}, \dots, x_{\alpha,t}^{(L)})$, в то время как пользователь β : $X_{\beta,t} = (x_{\beta,t}^{(1)}, x_{\beta,t}^{(2)}, \dots, x_{\beta,t}^{(L)})$. Тогда в общем слоте на приёмник придёт соответственно: $X_{\alpha,t} \vee X_{\beta,t}$. Следовательно, при возникновении коллизии не происходит искажения вектора $X_{\alpha,t}$, если он покрывает вектор $X_{\beta,t}$, то есть если $\text{supp}(X_{\beta,t}) \subset \text{supp}(X_{\alpha,t})$, где $\text{supp}(X_{\alpha,t})$ – носитель $X_{\alpha,t}$, то есть $\text{supp}(X_{\alpha,t}) = \{i : X_{\alpha,t}^i = 1\}$.

Более детальное рассмотрение зависимости между вектором и вероятностью его искажения во время наступления коллизии будет представлено в следующем пункте.

2.3. Анализ свойств канала

Вначале рассмотрим пример канала при $L = 3$ со всеми возможными переходами, который изображён на рисунке 1.

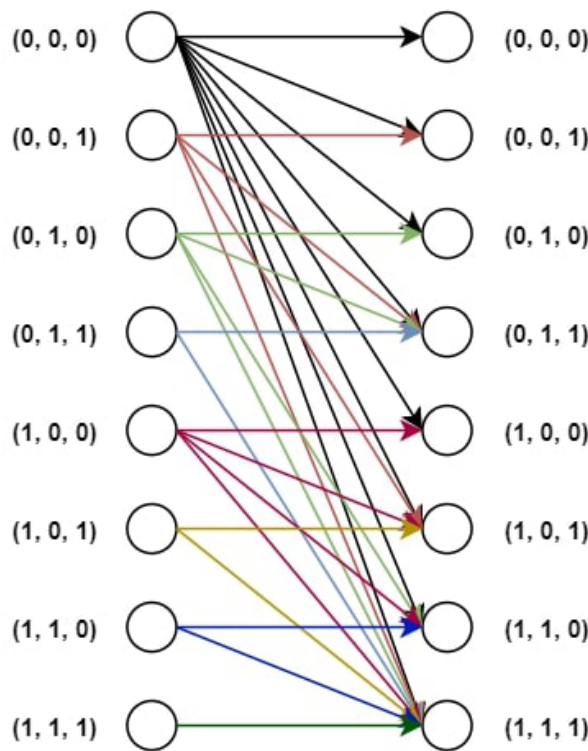


Рис. 1. Возможные переходы при $L = 3$.

Из рисунка видно, что для входного вектора с весом w существует 2^{L-w} возможных переходов в выходные векторы. Следовательно, общее число переходов, а также вероятность этих

переходов зависит только от w . Ввиду того, что канал является дизъюнктивным, вес выходного вектора больше или равен весу входного, причём равенство достигается в том и только том случае, если выходной вектор совпал со входным. Таким образом, вместо рассмотренной выше модели канала можно рассмотреть канал, входами и выходами которого будут веса Хэмминга двоичных векторов длины L .

Из вышесказанного можно сделать вывод, что входы канала перестали быть равновероятными. Следовательно, распределение на входе канала можно вычислить следующим образом:

$$P_{in}(w) = \binom{L}{w} 2^{-L}.$$

Ясно, что кратность коллизии не влияет на входное распределение, но от неё зависит выходное распределение. Допустим, что кратность коллизии $\kappa = t$. Тогда если некоторый входной вектор X имеет вес $w < L$, то выходной вектор X' будет иметь вес $w' > w$ только в том случае, если как минимум один из t пользователей, использующий тот же слот для передачи, что и выбранный пользователь, передаёт 1 на любую из позиций множества $[L] \setminus \{i : X_i = 1\}$, где $[L] = \{1, 2, \dots, L\}$. Вероятность $p(t)$, что хотя бы один из пользователей передаст 1 на любую из позиций $\kappa \in [L]$ равна:

$$p(t) = 1 - (1 - p)^t,$$

где p – вероятность 1 во входном слоте, а $1 - p$ – вероятность 0. В данной работе предполагается, что $p = 1 - p = \frac{1}{2}$, следовательно формула будет иметь вид:

$$p(t) = 1 - 2^{-t}.$$

Следующий шаг – вычисление условной вероятности $P(w'|w, t)$ того, что выходной вектор будет иметь вес w' , при условии того, что вектор данного пользователя имел вес w и произошла коллизия кратности t . Ясно, что при $w > w'$ значение условной вероятности будет равно 0. Учитывая, что при каждом значении w вероятность “успеха” постоянна, а число $(L - w)$ (так как рассматриваются значения $w' > w$) – есть количество независимых случайных экспериментов, можно вновь воспользоваться функцией вероятности биномиального распределения:

$$P(w'|w, t) = \begin{cases} 0, & w' < w \\ \binom{L-w}{w'-w} p(t)^{w'-w} (1 - p(t))^{L-w'}, & w' \geq w \end{cases}.$$

Распределение вероятностей выходов канала будет иметь следующий вид:

$$P_{out}(w'|t) = \sum_{i=0}^{w'} P(w'|i, t) P_{in}(i).$$

2.4. Оценка пропускной способности канала

Итак, рассмотрев модель канала, оценим снизу его пропускную способность.

Пусть \mathcal{X} – случайная величина, определённая на входном алфавите канала, а \mathcal{Y} – случайная величина, определённая на выходном алфавите канала. Выражение для пропускной способности \mathcal{C} имеет следующий вид:

$$\mathcal{C} = \sup_{p_{in}(\mathcal{X})} I(\mathcal{X}; \mathcal{Y}),$$

где $I(\mathcal{X}; \mathcal{Y})$ – взаимная информация между \mathcal{X} и \mathcal{Y} . В данном случае супремум берётся по всем возможным распределениям $p_{in}(\mathcal{X})$ случайной величины \mathcal{X} .

Итак, если $\kappa = t$, то пропускная способность $\mathcal{C}(t)$ может быть оценена снизу как:

$$\begin{aligned} \mathcal{C}(t) \geq \sum_{w=0}^L P_{in}(w) \sum_{w'=w}^L P(w'|w, t) \log_2 P(w'|w, t) - \\ - \sum_{w''=0}^L P_{out}(w''|t) \log_2 P_{out}(w''|t). \end{aligned} \quad (1)$$

Пропускная способность многопользовательского канала может быть оценена снизу как математическое ожидание случайной величины $\mathcal{C}(t)$:

$$\mathcal{C} \geq C^* = \sum_{t=0}^{U-1} P(\kappa = t) \mathcal{C}(t). \quad (2)$$

В данном случае величина C^* – доля информации, переданная корректно при одном использовании канала. Следовательно, величина “скорости передачи информации” (в битах) может быть выражена с помощью формулы: $T = C^*L$. Значение T демонстрирует долю корректно переданных из L бит, которые передаёт пользователь через канал. На рис. 2 представлена зависимость количества пользователей U от скорости передачи информации T , при $U_{max} = 500$, $Q = 1024$ и $S \in \{32, 64, 128, 256, 512, 1024\}$.

Из рис. 2 можно сделать несколько выводов:

1. Для некоторых диапазонов числа активных пользователей при меньшем S достигаются относительно большие значения скорости передачи информации T .
2. Для того, чтобы увеличить величину T при небольшом числе пользователей, стоит уменьшить значение S .
3. Чтобы увеличить число активных пользователей, необходимо увеличение независимых каналов.

Важно рассмотреть также суммарную относительную скорость передачи. Данная метрика используется для анализа качества многопользовательской системы передачи информации. Формула расчёта данной величины:

$$R_\sigma = \frac{ULC^*}{Q}.$$

Данное выражение демонстрирует отношение между суммарной пропускной способностью U пользователей и максимально допустимой пропускной способностью системы – Q .

На рис. 3 представлен график зависимости R_σ от числа активных пользователей U при $S \in \{32, 64, 128, 256, 512, 1024\}$ и $Q = 1024$.

Из рис. 3 следуют выводы:

1. Чем меньше число S , тем на меньшем числе пользователей достигается максимальная величина R_σ .
2. Скорость изменения функции $R_\sigma(U)$ зависит только от величины S .
3. Величина R_σ^{max} достигает своего наибольшего значения, при числе пользователей U , большем чем S на $\approx \frac{9S}{16}$, где S – максимальное число пользователей, ведущих ортогональную передачу данных.

3. СИГНАЛЬНО-КОДОВАЯ КОНСТРУКЦИЯ ДЛЯ ВЕКТОРНОГО ДИЗЬЮНКТИВНОГО КАНАЛА

Итак, нами были получены предельные значения суммарной относительной скорости передачи. Следующий этап – разрешение коллизии для данной модели канала.

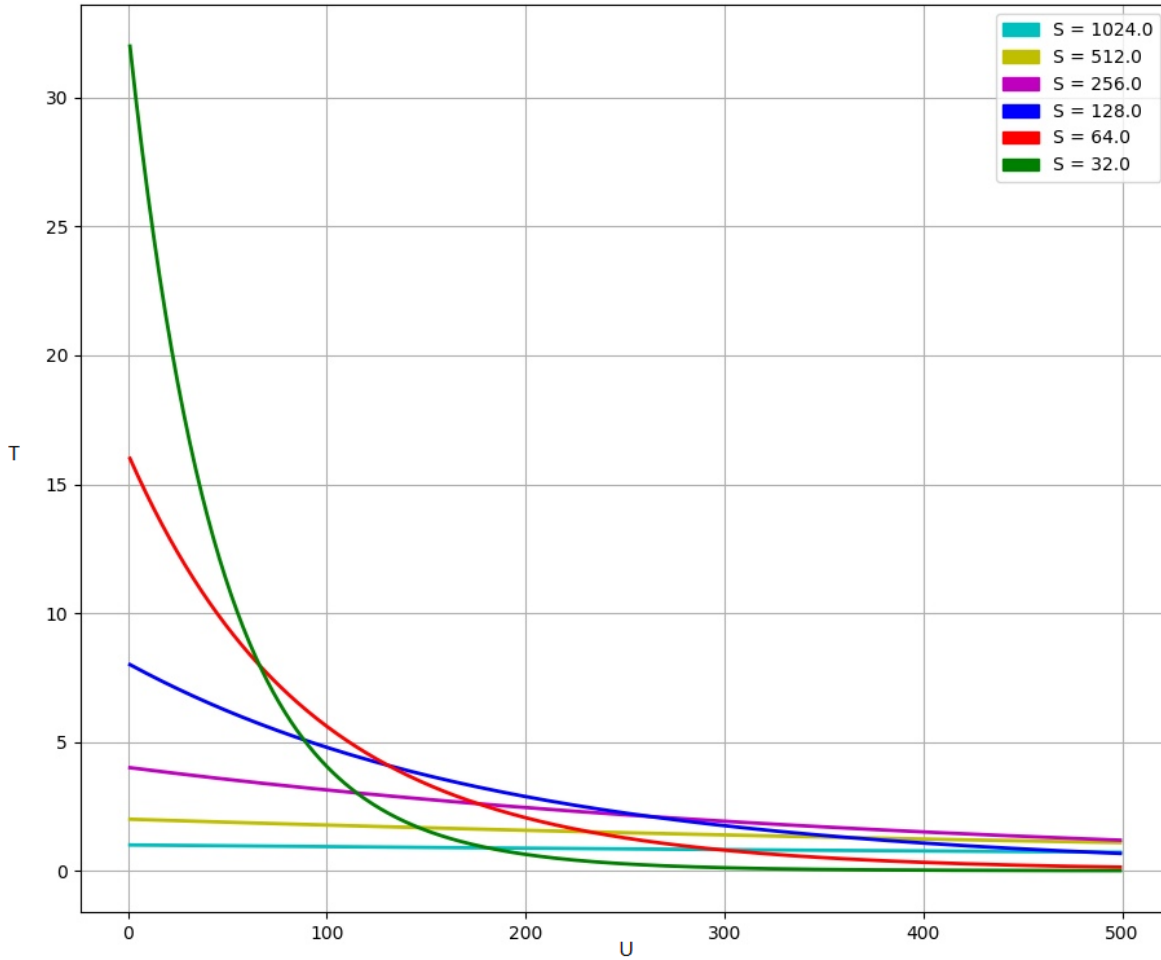


Рис. 2. Зависимость количества пользователей U от скорости передачи информации T при различных значениях независимых каналов S .

3.1. Постановка задачи разрешения коллизий

Пусть пользователю необходимо передать $K = Lm$ бит через канал. Чтобы осуществить передачу, нужно выбрать m случайных чисел $i_1, i_2, \dots, i_m, 1 \leq i_\tau \leq S$ и затем в каждый τ -ый момент времени осуществить передачу L бит в i_τ -ом слоте.

Ввиду того, что предложенная модель передачи допускает наличие коллизий, для достоверной передачи K бит требуется, чтобы пользователи вводили некоторую избыточность в передаваемые сообщения, которая бы позволила базовой станции разрешать возникающие коллизии.

Более детально: если информационный вектор i -ого пользователя имеет вид $\mathbf{X}_i = (\mathbf{X}_{i1}, \mathbf{X}_{i2}, \dots, \mathbf{X}_{im})$, где $\mathbf{X}_{ij} = (x_{ij}^{(1)}, x_{ij}^{(2)}, \dots, x_{ij}^{(L)}, x_{ij}^{(\tau)} \in \{0, 1\})$, то для разрешения коллизий пользователь вводит проверочные векторы (т. е. векторы из проверочных символов) $\mathbf{P}_i = (\mathbf{P}_{i1}, \mathbf{P}_{i2}, \dots, \mathbf{P}_{ih})$, где $\mathbf{P}_{ij} = (p_{ij}^{(1)}, p_{ij}^{(2)}, \dots, p_{ij}^{(L)}, p_{ij}^{(\tau)} \in \{0, 1\})$ и затем отправляет в канал слово $\mathbf{C} = (\mathbf{X} \mathbf{P})$. Если $n = m + h$, то для того, чтобы реализовать описанную выше передачу, пользователи должны использовать или (nL, mL) двоичные коды, или (n, m) коды над полем $GF(2^L)$, или некоторые каскадные конструкции кодов.

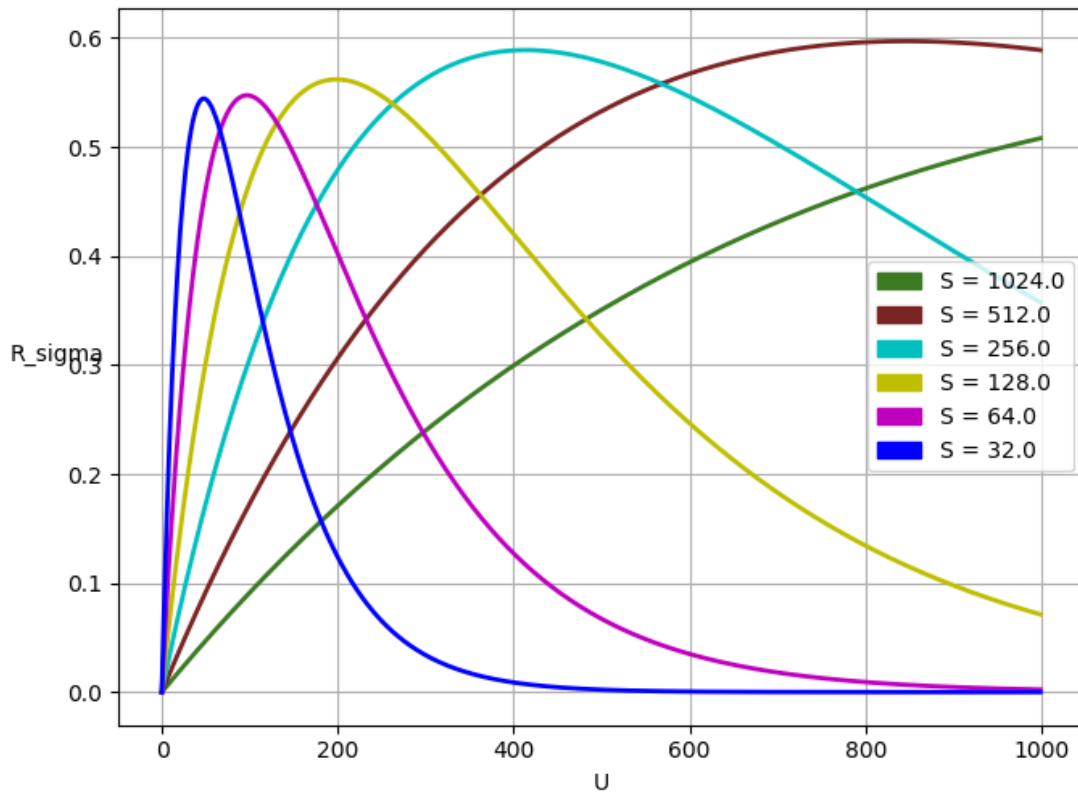


Рис. 3. Зависимость целевой скорости R_σ от числа пользователей U при различных значениях независимых каналов S

Важно напомнить о том, что в рассматриваемом канале коллизии могут возникнуть только в случае, когда несколько пользователей выбирают один и тот же слот для передачи в некоторый момент времени. Следовательно, это коллизии, группированные по L символов, при чем в каждой такой группе происходит в среднем $\frac{L}{4}$ искажений переданных символов (которые могут быть интерпретированы как ошибки). Данное наблюдение позволяет сделать вывод: двоичные коды (nL, mL) не оптимальны в данной ситуации, так как они предназначены для исправления независимых, а не группированных ошибок.

На рис. 4 изображена модель передачи, которая представлена в данном разделе. Эллипсы – это коллизии, произошедшие во время передачи.

3.2. Асимптотическая граница Варшавова–Гилберта

Отметим, что задача разрешения коллизий для данной модели канала была рассмотрена в работах [8]–[10]. В частности, в работе [8] для разрешения коллизий были использованы перемеженные двоичные коды, а в работе [10] – перемеженные коды Рида-Соломона. Работа [9] также посвящена перемеженным кодами Рида-Соломона, в частности, в ней были рассмотрены оптимальные параметры данного класса кодов с точки зрения вероятности ошибки на блок.

В данной работе мы рассмотрим асимптотическое поведение “хороших” кодов в задаче разрешения коллизий. Для этого нами была использована граница Варшавова–Гилберта (ВГ), и далее мы будем предполагать, что исследуемые нами коды лежат на данной границе.

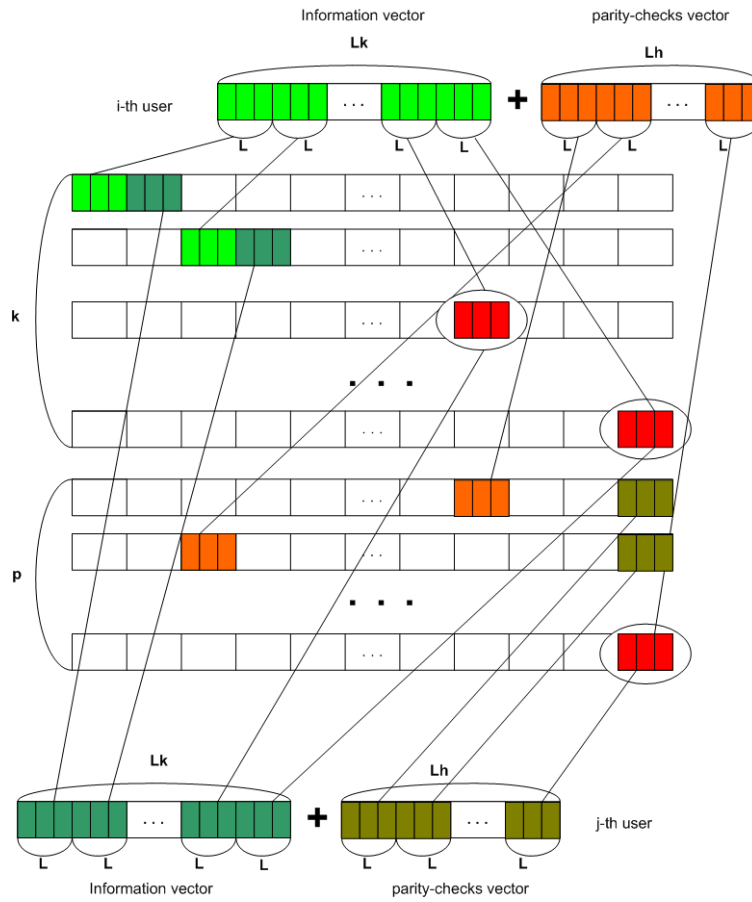


Рис. 4. Передача через канал – случай для двух пользователей.

По определению граница Варшамова–Гилберта – это граница существования линейного $(n, k, \geq d)_q$ кода.

В данной работе была использована асимптотическая граница Варшамова–Гилберта. R_{VG} – максимальная возможная мощность q -го кода.

$$R_{VG} \geq 1 - H_q(\delta),$$

где $\delta = \frac{d}{n} \in [0, 1 - \frac{1}{q}]$ и $H_q(x) = x \log_q(q - 1) - x \log_q x - (1 - x) \log_q(1 - x)$ – q -ичная энтропия.

Итак, чтобы найти суммарную относительную скорость передачи в векторном дизъюнктивном канале, рассмотрим формулу:

$$(\star) R_\sigma^c = \frac{UL}{Q} R_{VG}(1 - P_w),$$

где P_w – это вероятность ошибочного декодирования

$$1 - P_w = \sum_{i=0}^{n\delta-1} \binom{n}{i} (1 - P_s)^{n-i} P_s^i,$$

где P_s – вероятность коллизии.

3.3. Численные результаты

Итак, рассмотрим полученные результаты скорости передачи информации на границе Варшамова–Гилберта.

Для примера возьмём векторный дизъюнктивный канал, состоящий из $Q = 1024$ независимых подканалов. Ввиду того, что параметры n , q , l , d и U могут быть практически произвольными для заданного Q , в зависимости от их выбора, будут получаться различные сценарии передачи. Следовательно, чтобы оценить эффективность кодов, воспользуемся формулой (*).

Тем не менее, первым шагом было получение наилучших значений n и $\delta = \frac{d}{n}$. Было сделано два вывода:

1. Чем больше значение длины кода n , тем больше максимальное значение относительной скорости передачи (рис. 5).
2. Максимальное значение относительной скорости передачи достигается при $\delta = (0.6 \pm 0.05)$ (рис. 6).

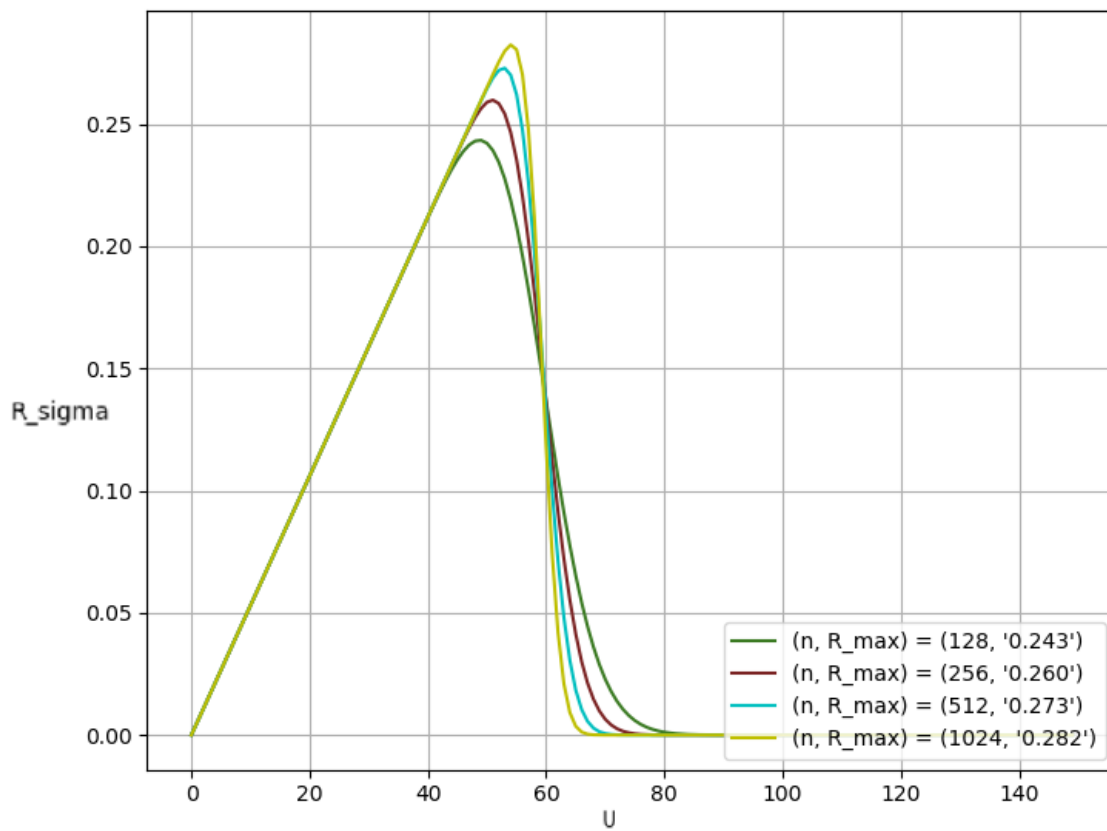


Рис. 5. Зависимость между максимальным значением целевой скорости передачи R_{σ} и длиной кода n при $L = 16$, $Q = 1024$, $U = 100$.

Итак, при $\delta = (0.6 \pm 0.05)$ и при $n \rightarrow \infty$ максимальное значение значения R_{σ} будет наибольшим. Но теперь важно проверить, как будет варьироваться величина R_{σ} при изменении L , Q и U .

В данных экспериментах использовались параметры: $n = 256$ и $\delta = 0.6$.

Было рассмотрено, как влияет изменение величины L при различных $Q \in [1024, 2048, 4096]$ на R_{σ}^{max} и при каком количестве пользователей этот максимум достигается:

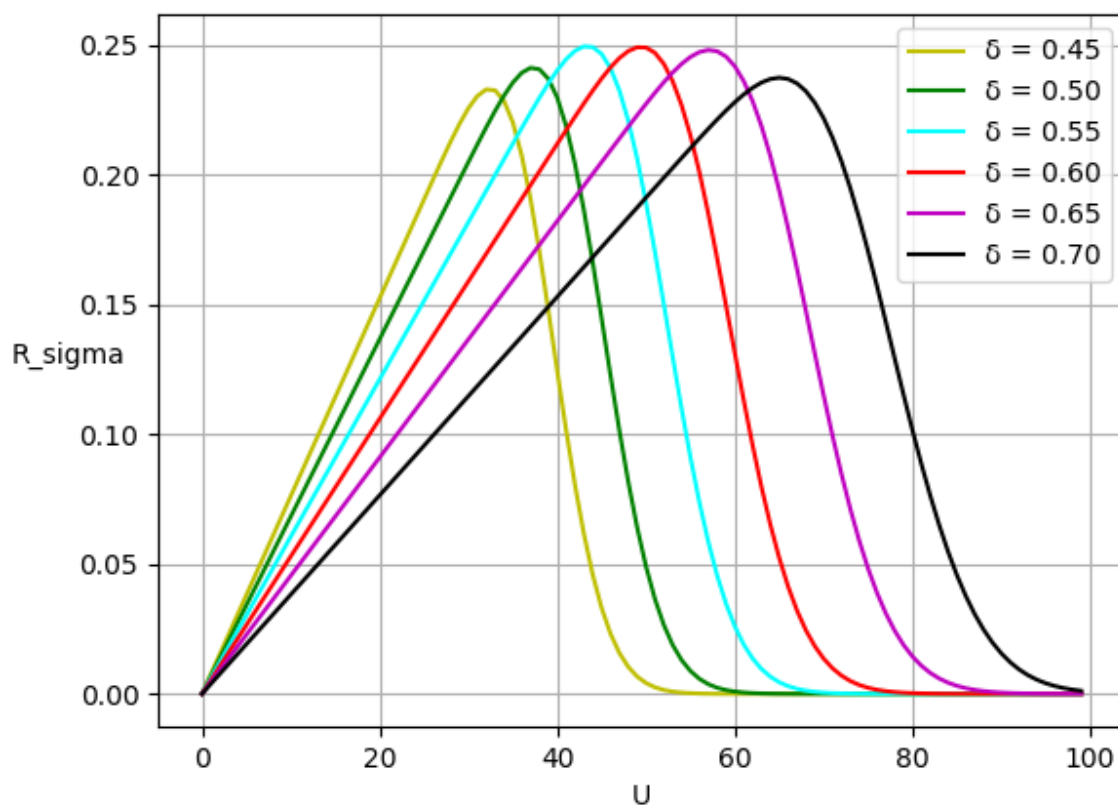


Рис. 6. Влияние δ на максимальное значение целевой скорости R_σ при $L = 16$, $Q = 1024$, $U = 100$.

Таблица

L	Q	S	U	R_σ^{max}
8	1024	128	100	0.212
8	2048	256	200	0.212
8	4096	512	400	0.211
16	1024	64	50	0.260
16	2048	128	100	0.258
16	4096	256	200	0.257
32	1024	32	25	0.286
32	2048	64	50	0.283
32	4096	128	100	0.281
64	1024	16	13	0.305
64	2048	32	25	0.298
64	4096	64	50	0.295

Итак:

- При фиксированном значении L : чем больше значение Q , тем меньше значение максимума суммарной относительной скорости.
- При фиксированном значении Q : чем больше значение L , тем больше значение максимума суммарной относительной скорости.

- При фиксированном значении L : число пользователей при максимальной величине R_σ увеличивается примерно в 2 раза, если увеличить значения $\frac{Q}{L}$ в 2 раза, но важно отметить, что R_σ при этом уменьшается.
- Из проведённых экспериментов удалось определить, что максимальная величина $R_\sigma = 0.305$ была получена при условии: $L = 16$, $Q = 1024$. Но максимум достигается лишь при 13 активных пользователях.

Ниже представлены графики при $L = 8$ (рис.7) и $L = 64$ (рис.8) на границе Варшавова–Гилберта в сравнении с теоретическим пределом R_σ^{max} :

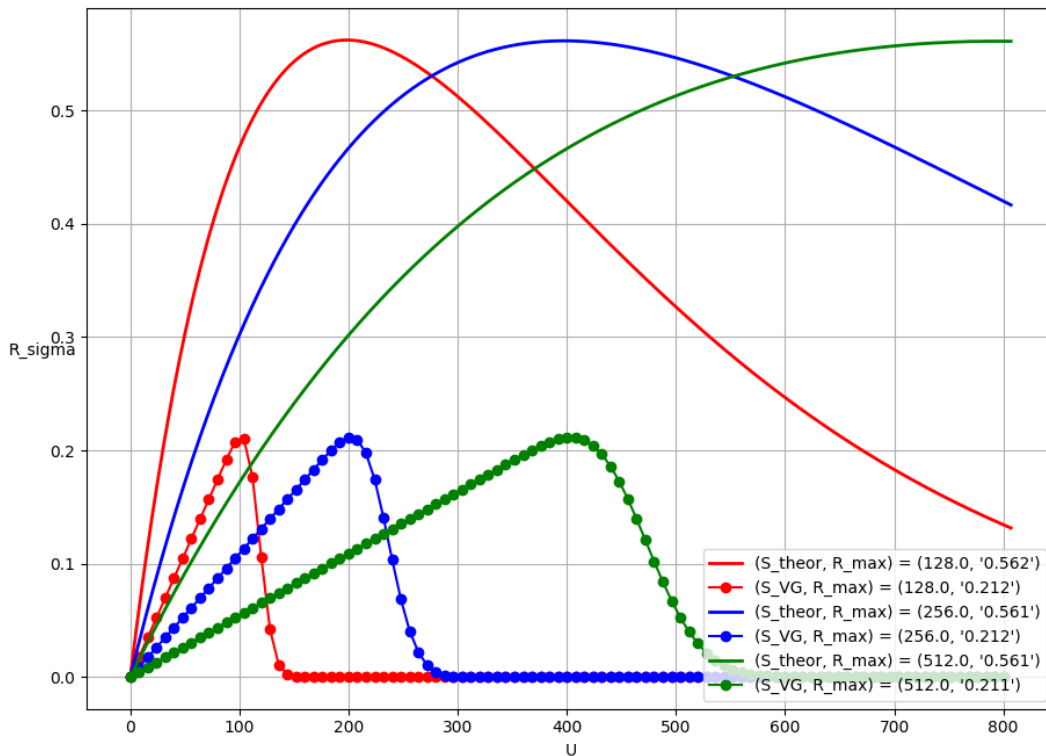


Рис. 7. Сравнение общей скорости передачи R_σ с теоретической оценкой R_σ^{max} при $L = 8$.

Из рис. 7 и рис. 8 видно, что при различных значениях L максимумы суммарной относительной скорости различаются примерно в 2 раза. Данный факт проистекает из “симметричности” границы Варшавова–Гилберта. В будущем будет рассматриваться граница случайного кодирования, которая, возможно, уменьшит данную разницу.

4. ЗАКЛЮЧЕНИЕ

В данной работе был предложен специальный класс векторных дизъюнктивных каналов, в которых пользователи передают пакеты бит некоторой заданной длины. Для данного класса каналов получена оценка на его пропускную способность при различном числе пользователей и различных гиперпараметрах канала. Кроме того, в работе была предложена сигнально-кодированная конструкция для разрешения коллизий, возникающих на этапе передачи, в предполо-

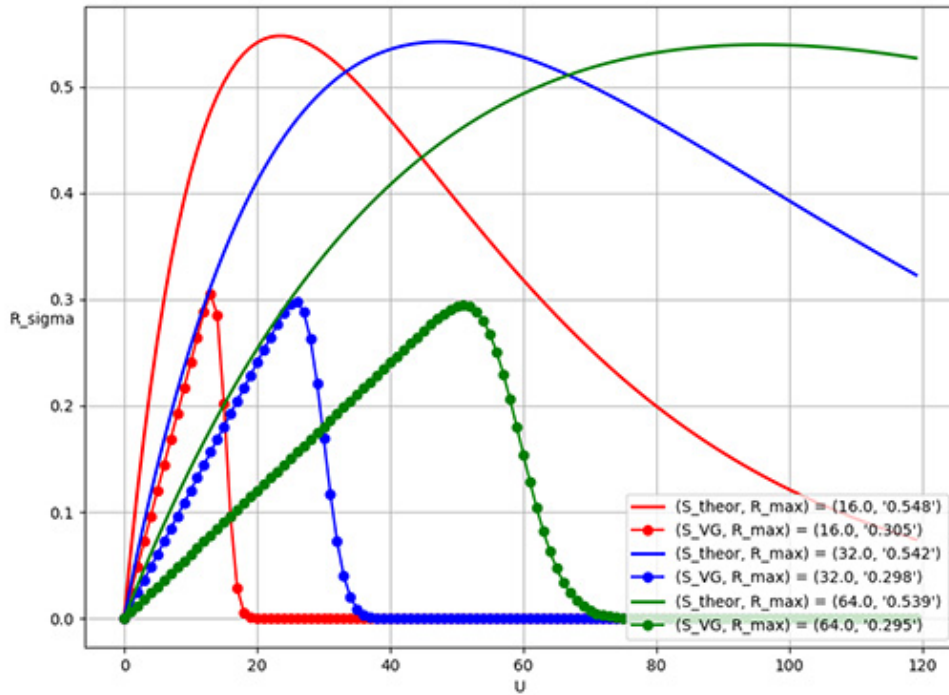


Рис. 8. Сравнение общей скорости передачи R_σ с теоретической оценкой R_σ^{max} при $L = 64$.

жении, что код, входящий в конструкцию, лежит на границе Варшавова–Гилберта. Для этой конструкции были получены численные результаты для относительной суммарной скорости передачи на блок при различном числе пользователей.

СПИСОК ЛИТЕРАТУРЫ

1. B. Rimoldi and R. Urbanke, "A rate-splitting approach to the Gaussian multiple-access channel," IEEE Transactions on Information Theory, vol. 42, no. 2, pp. 364–375, 1996.
2. L. Ping, L. Liu, K. Wu, and W. K. Leung, "Interleave division multiple-access," IEEE Transactions on Wireless Communications, vol. 5, no. 4, pp. 938–947, 2006.
3. A. R. Cohen, J. A. Heller and A. J. Viterbi, "A new coding technique for asynchronous multiple access communication," IEEE Transactions on Communication Technology, vol. 19, pp. 849–855, October 1971.
4. S. C. Chang and J. Wolf, "On the t-User m-Frequency Noiseless Multiple- Access Channel with and without Intensity Information," IEEE Transactions on Information Theory, vol. 27, no. 1, pp. 41–48, Jan. 1981.
5. L. Wilhelmsson and K. S. Zigangirov, "On the Asymptotic Capacity of a Multiple-Access Channel," Problems of Information Transmission, vol. 33, no. 1, pp. 9–16, 1997.
6. L. A. Bassalygo and M. S. Pinsker, "Evaluation of the Asymptotics of the Summarized Capacity of an m-Frequency t-User Noiseless Multiple-Access Channel," Problems of Information Transmission, vol. 36, no. 2, pp. 91–97, 2000.
7. A. Han Vinck and K. Keuning, "On the Capacity of the Asynchronous t-User m-Frequency Noiseless Multiple-Access Channel without Intensity Information," IEEE Transactions on Information Theory, vol. 42, no. 6, pp. 2235–2238, Nov. 1996.

Researching of Correcting Properties of Codes Lying on Varshamov–Gilbert Bound for a System of Non-Orthogonal Multiple Access

F.I. Ivanov, D.V. Rollov

This paper deals with the error exponent of the regular graph-based binary low-density parity-check (LDPC) codes under the maximum likelihood (ML) decoding algorithm in the binary symmetric channel (BSC). Unlike other papers where error exponents are considered for the case when the length of LDPC codes tends to infinity (asymptotic analysis) we considered the finite length case (finite length analysis). In this paper we describe the method of deriving the lower bound on the error exponent for regular graph-based LDPC code with finite length under ML decoding and analyze the dependency of the error exponent on various LDPC code parameters. The numerical results, obtained for the considered lower bound, are represented and analyzed at the end of the paper.

KEYWORDS: LDPC code, error exponent, finite length.