ЖЭТФ, 2021, том 159, вып. 3, стр. 434–447

О ПРОСТОМ ЭВРИСТИЧЕСКОМ ВЫВОДЕ ФОРМУЛЫ ШЕННОНА ДЛЯ КАНАЛА СВЯЗИ С НЕПРЕРЫВНЫМИ ПЕРЕМЕННЫМИ В КВАНТОВОМ СЛУЧАЕ

И. М. Арбеков [a], ***С. Н. Молотков*** [a,b,c*], ***И. В. Синильщиков*** [c]

[a] *Академия криптографии Российской Федерации*
121552, Москва, Россия

[b] *Институт физики твердого тела Российской академии наук*
142432, Черноголовка, Московская обл., Россия

[c] *Центр квантовых технологий, Московский государственный университет им. М. В. Ломоносова*
119899, Москва, Россия

Поступила в редакцию 22 декабря 2020 г.,
после переработки 22 декабря 2020 г.
Принята к публикации 23 декабря 2020 г.

Цель статьи — вывод на простом эвристическом и понятном на физическом интуитивном уровне формул пропускных способностей для классически-квантового канала связи с гауссовским шумом, которые являются аналогами классических пропускных способностей и которые возникают во многих задачах квантовой теории информации. Классическая пропускная способность классического канала связи с ограниченной частотной полосой и гауссовскими информационными состояниями при стремлении шума к нулю имеет расходимость. При последовательном квантовом рассмотрении расходимость устраняется, что является следствием фундаментального физического принципа тождественности частиц — бозонов в информационных состояниях.

DOI: 10.31857/S0044451021030056

1. ВВЕДЕНИЕ

Определение условий для безошибочной передачи информации при помощи классических сигналов через канал с шумом является фундаментальным результатом теории информации Шеннона [1–3]. В квантовой области существует также значительное количество разнообразных задач, связанных с передачей и обработкой информации [4–6]. Одной из таких задач является передача классической информации при помощи квантовых состояний. Верхняя граница безошибочной передачи классической информации при помощи квантовых состояний в асимптотическом пределе длинных последовательностей дается фундаментальной величиной (информацией) Холево [4–6]. Квантовая теория информации является достаточно обширной и разработанной теорией, которая использует специфический для данной области математический аппарат, для понимания и освоения которого требуется определенное время и усилия. В классической теории информации для многих результатов имеется качественная интерпретация, тогда как в квантовой области часть фундаментальных понятий и результатов не может быть в принципе интерпретирована в классических терминах. К ним можно отнести понятие запутанности и результаты, связанные с передачей информации при помощи запутанных состояний, поскольку само явление запутанности отсутствует в классической области. Тем не менее, при исследовании некоторых понятий, таких как пропускная способность классически-квантового канала связи или скорость безошибочной передачи классической информации при помощи квантовых состояний, можно провести аналогию с соответствующими классическими величинами, несмотря на то, что полное сведение к классическому случаю невозможно. Для осмысленной постановки и проведения экспериментальных исследований часто необходима простая и интуитивно понятная на физическом

* E-mail: sergei.molotkov@gmail.com

уровне интерпретация используемых теоретико-информационных конструкций, не перегруженная математическим аппаратом. Цель данной заметки — дать простой эвристический вывод квантового аналога формулы Шеннона для пропускной способности классического канала с непрерывной переменной. При выводе используются привычная в физике интерпретация вероятности как предела частоты событий при большом числе испытаний (измерений), а также стандартная борновская интерпретация матрицы плотности как ансамбля квантовых состояний. Речь пойдет о пропускной способности канала связи в единицу времени (бит/с) с непрерывными сигналами, имеющими конечную частотную полосу Ω (Гц) и наблюдаемыми на фоне белого гауссовского шума [1–3]:

$$C = \frac{1}{2}\Omega \log\left(1 + \frac{S}{N_0\Omega}\right), \tag{1}$$

где

$$\frac{1}{T}\int\limits_{-T/2}^{T/2} x^2(t)\,dt$$

— ограничение на мощность (дисперсию) случайного сигнала $x(t)$, $N_0\Omega$ — мощность (дисперсия) белого шума в полосе $[0,\Omega]$[1)], $\log \equiv \log_2$.

Неформальный смысл (1) состоит в определении верхней границы числа битов информации в единицу времени, которые можно передать безошибочно при помощи сигналов с ограниченной полосой Ω и мощностью S через канал связи с гауссовским белым шумом, имеющим постоянную одностороннюю (для положительных частот) спектральную плотность N_0. Отношение сигнал/шум $S/N_0\Omega$ в том или ином контексте возникает во многих физических ситуациях. Для самодостаточности и связности изложения, а также для того, чтобы проследить аналогии с классическим случаем, приведем эвристический вывод формулы для пропускных способностей дискретного классического канала без памяти, а также непрерывного классического канала с гауссовским белым шумом. Этот вывод потребуется для получения формулы в квантовом случае. В определенном смысле вывод формулы для пропускной способности в квантовом случае может быть основан на выводе формулы для пропускной способности дискретного канала связи в классическом случае.

2. КЛАССИЧЕСКИЙ ДИСКРЕТНЫЙ КАНАЛ СВЯЗИ

Каждому физическому сигналу, передаваемому через канал связи, сопоставляется символ алфавита $x_i \in X = \{x_i\}_{i=1}^N$. При передаче информации каждый символ (сигнал) посылается в канал с вероятностью $P_X(x_i)$. Канал используется n раз, каждая посылка независима от предыдущих. На приемной стороне принимаются искаженные состояния — один из символов алфавита $y_i \in Y = \{y_i\}_{i=1}^N$. Размерности N и сами алфавиты (множества) на приемной и передающей сторонах не обязательно совпадают. Размерности считаем одинаковыми, чтобы не загромождать выкладки несущественными деталями.

Физические свойства канала с искажениями (шумом) формализуются заданием переходных вероятностей $P_{Y|X}(y|x)$ — послан символ x, принят символ y. Совместное распределение символов на входе и выходе канала,

$$P_{XY}(x,y) = P_X(x)P_{Y|X}(y|x) = \\ = P_Y(y)P_{X|Y}(x|y), \tag{2}$$

— это вероятность обнаружить пару (x,y), если одновременно имеется доступ ко входу и выходу.

Вероятность получить последовательность $Y_n = (y_{i_1},\ldots,y_{i_n})$ при условии переданной последовательности (сообщения) $X_n = (x_{i_1},\ldots,x_{i_n})$ равна

$$P(Y_n|X_n) = \prod_{j=1}^{n} P_{Y|X}(y_{i_j}|x_{i_j}). \tag{3}$$

Тем самым задается стационарный дискретный канал связи с искажениями (шумом) без памяти. Заметим, что вероятность сообщения $P(X_n)$ на передающей стороне, в соответствии с независимым выбором символов, имеет вид

$$P(X_n) = \prod_{j=1}^{n} P_X(x_{i_j}) = \\ = (P_X(x_1))^{n(x_1)}\ldots(P_X(x_n))^{n(x_n)}, \tag{4}$$

где $(n(x_1),\ldots,n(x_n))$ — частота появления символов в сообщении X_n, $0 \le n(x_1) \le n,\ldots,0 \le n(x_n) \le n$ и $n(x_1)+\ldots+n(x_n) = n$.

В асимптотическом пределе длинных последовательностей, при $n \to \infty$, частоты $n(x_i)$ появления

[1)] Отметим, что для ширины частотной полосы ω используется условие $|\omega| \le W$. Поскольку для физической устойчивой системы отрицательные частоты невозможны, используем для ширины полосы $0 \le \omega \le \Omega$ (положение интервала на оси частот несущественно), поэтому ширина полосы в наших обозначения вдвое больше по сравнению, например, с шириной полосы в [3].

символов стремятся к своим математическим ожиданиям: $n(x_i) \approx nP_X(x_i)$.

Тогда можно сказать, что при больших n практически все последовательности (сообщения) имеют одинаковую вероятность:

$$P(X_n) = \prod_{j=1}^{n} P_X(x_{i_j}) = \\ = (P_X(x_1))^{nP_X(x_1)} \dots (P_X(x_n))^{nP_X(x_n)} = \\ = 2^{-nH(X)}, \quad (5)$$

$$H(X) = -\sum_{i=1}^{N} P_X(x_i) \log(P_X(x_i)). \quad (6)$$

Число таких типичных последовательностей [2] равно $2^{nH(X)}$, $H(X)$ — энтропия Шеннона.

Аналогичным образом на приемной стороне вероятность типичной последовательности равна $P(Y_n) = 2^{-nH(Y)}$, их число равно

$$2^{nH(Y)}, \quad H(Y) = -\sum_{i=1}^{N} P_Y(y_i) \log(P_Y(y_i)). \quad (7)$$

Неформально (5) и (7) означают, что при использовании источника n раз на передающей и принимающей сторонах с вероятностью практически единица возникнет одна из типичных последовательностей (5).

Энтропии Шеннона $H(X)$, $H(Y)$ имеют смысл числа битов — бинарных разрядов, минимально необходимых для записи типичных последовательностей (5), (7).

Для анализа процесса передачи информации требуется знать, как каждая последовательность на передающей стороне переходит в последовательность на приемной стороне.

Пусть задана типичная последовательность $X_n = (x_{i_1}, \dots, x_{i_n})$, где частоты появления символов равны

$$n(x_1) = nP_X(x_1), \dots, n(x_n) = nP_X(x_n).$$

Там, где был символ, скажем, x_1, появление на выходе символов y_k $(k = 1, \dots, N)$ происходит в соответствии с условными вероятностями

$$P_{Y|X}(y_1|x_1), P_{Y|X}(y_2|x_1), \dots, P_{Y|X}(y_N|x_1). \quad (8)$$

Число входных символов x_1 (длина последовательности из символов x_1) равно $nP_X(x_1)$. Тогда при $nP_X(x_1) \to \infty$, в соответствии со сказанным выше, вероятность любой части выходной последовательности, порождаемой частью входной типичной последовательности, состоящей только из x_1, равна

$$(P_{Y|X}(y_1|x_1))^{nP_X(x_1)P_{Y|X}(y_1|x_1)} \dots \\ \dots (P_{Y|X}(y_N|x_1))^{nP_X(x_1)P_{Y|X}(y_N|x_1)} = \\ = \prod_{i=1}^{N} (P_{Y|X}(y_i|x_1))^{nP_X(x_1)P_{Y|X}(y_i|x_1)} = \\ = 2^{-P_X(x_1)H(Y|x_1)}, \quad (9)$$

где

$$H(Y|x_1) = -\sum_{i=1}^{N} P_{Y|X}(y_i|x_1) \log(P_{Y|X}(y_i|x_1))$$

— условная энтропия выхода при условии входа x_1.

Собирая все входные символы вместе, получаем, что любая последовательность на выходе, порождаемая отдельной типичной последовательностью на входе, имеет вероятность

$$\prod_{k=1}^{N} \prod_{i=1}^{N} (P_{Y|X}(y_i|x_k))^{nP_X(x_k)P_{Y|X}(y_i|x_k)} = \\ = 2^{-nH(Y|X)}, \quad (10)$$

где

$$H(Y|X) = \sum_{k=1}^{N} P_X(x_k) H(Y|x_k) = -\sum_{k=1}^{N} P_X(x_k) \times \\ \times \sum_{i=1}^{N} P_{Y|X}(y_i|x_k) \log(P_{Y|X}(y_i|x_k) \quad (11)$$

— средняя условная энтропия выхода.

Таким образом, каждая типичная последовательность на передающей стороне порождает множество последовательностей мощности $2^{nH(Y|X)}$.

Для того чтобы группы порождаемых последовательностей на выходе канала связи не перекрывались и, следовательно, не возникало ошибки на приемной стороне, передаваемых последовательностей должно быть не более

$$\frac{2^{nH(Y)}}{2^{nH(Y|X)}} = 2^{nI(X,Y)}, \\ I(X,Y) = H(Y) - H(Y|X) = H(X) - H(X|Y), \quad (12)$$

$I(X,Y)$ — взаимная информация между входом и выходом канала.

Переходные вероятности задаются физическими свойствами канала, поэтому единственной пе-

ременной величиной является распределение вероятностей $P_X(x)$ на входе канала связи и, следовательно, максимального значения взаимной информации $I(X,Y)$ можно добиться выбором распределения $P_X(x)$.

Тогда пропускная способность канала связи равна

$$C = \max_{P_X(x)} I(X,Y) \tag{13}$$

и имеет смысл числа битов информации на одну посылку, которые можно безошибочно передать через канал связи с шумом.

Таким образом, чтобы различить каждую передаваемую последовательность, их должно быть не более 2^{nC}.

Более точно, утверждение о кодировании в канале с шумом [1–3] говорит о существовании набора последовательностей размером $2^{n(C-\varepsilon)}$, ошибка различения которых при любом сколь угодно малом $\varepsilon > 0$ стремится к нулю. Соответственно число битов информации в пересчете на одну посылку, которое безошибочно можно передать через канал связи с шумом, не превосходит C. Данное утверждение есть теорема существования, поскольку не дает алгоритмически эффективного построения набора последовательностей — кодовых слов на передающей стороне, которые можно безошибочно различить на приемной стороне.

3. КЛАССИЧЕСКИЕ КАНАЛЫ С НЕПРЕРЫВНЫМИ ПЕРЕМЕННЫМИ

Дальнейшая цель — вывести формулы для пропускной способности канала с непрерывными переменными сначала в классическом случае, а затем и в квантовом, используя интуитивно понятные на физическом уровне результаты для дискретного классического канала связи.

Пусть имеется один классический канал с непрерывной случайной величиной (сигналом) x — сигналом на входе канала — с плотностью распределения вероятностей $f_X(x)$, а также с ограничением на второй момент

$$\mathbf{E}x^2 = \int\limits_{-\infty}^{\infty} x^2 f_X(x)\,dx \le S \tag{14}$$

и дифференциальной энтропией

$$H_d(X) = \int\limits_{-\infty}^{\infty} f_X(x)\log(f_X(x))\,dx. \tag{15}$$

Шум в канале представим в виде гауссовской случайной величины z, независимой от x, с нулевым средним и дисперсией σ^2_{noise}, плотностью вероятности

$$\varphi(z,\sigma^2_{noise}) = \frac{1}{\sqrt{2\pi\sigma^2_{noise}}}\exp\left(-\frac{z^2}{2\sigma^2_{noise}}\right), \tag{16}$$

и дифференциальной энтропией

$$H_d(Z) = \int\limits_{-\infty}^{\infty} \varphi(z,\sigma^2_{noise})\log(\varphi(z,\sigma^2_{noise}))\,dz = \\ = \frac{1}{2}\log(2\pi e\sigma^2_{noise}). \tag{17}$$

Отметим, что дифференциальная энтропия $H_d(Z)$ гауссовского распределения определяется только его дисперсией и не зависит от математического ожидания (сдвига) — «центра» распределения вероятностей.

Наблюдения на выходе канала связи — это сумма сигнала и шума $y = x + z$ с плотностью распределения вероятностей $f_Y(y)$ и дифференциальной энтропией

$$H_d(Y) = -\int\limits_{-\infty}^{\infty} f_Y(y)\log(f_Y(y))\,dy. \tag{18}$$

Для использования результатов предыдущего раздела представим алфавит на входе и выходе канала связи как разбиение числовой прямой на совпадающие интервалы Δx_i, Δy_i одинаковой малой длины Δ.

Соответствующие вероятности $P_X(x_i)$, $P_Y(y_i)$ определим как

$$\begin{aligned} P_X(x_i) &= f_X(x_i)\cdot\Delta, \quad x_i \in (x_i, x_i+\Delta), \\ P_Y(y_i) &= f_Y(y_i)\cdot\Delta, \quad y_i \in (y_i, y_i+\Delta). \end{aligned} \tag{19}$$

После такого разбиения канал с непрерывным алфавитом на входе и выходе превращается в дискретный канал с распределением вероятности символов на входе и на выходе (19). После дискретизации можно напрямую воспользоваться результатами разд. 2 для дискретного канала связи.

Забегая вперед, отметим, что, как будет видно ниже, «мелкость» дискретизации не входит в ответ — формально сокращается, однако это не снимает вопроса о нижней границе дискретизации сигнала. В классическом случае нет ограничений на нижнюю границу дискретизации, что в итоге приводит к расходимости пропускной способности канала

в классическом случае в пределе нулевого шума в канале. Этот вопрос последовательно разрешается только в квантовом случае (см. ниже).

Заметим, что при любом фиксированном x наблюдение $y = x + z$ имеет гауссовское распределение с дисперсией σ^2_{noise}. Тогда с учетом (19) и свойства независимости энтропии гауссовского распределения от сдвига, при малых Δ можно проследить цепочку приближенных равенств:

$$I(X,Y) = H(Y) - H(Y|X) = \\ = -\sum_{i=1}^{N} P_Y(y_i)\log(P_Y(y_i)) - \left(-\sum_{k=1}^{N} P_X(x_k) \times \right. \\ \left. \times \sum_{i=1}^{N} P_{Y|X}(y_i|x_k)\log(P_{Y|X}(y_i|x_k))\right) \approx \\ \approx \left(-\int\limits_{-\infty}^{\infty} f_Y(y)\log(f_Y(y))\,dy - \log(\Delta)\right) - \\ -\left(\int\limits_{-\infty}^{\infty} f_X(x)\left(-\int\limits_{-\infty}^{\infty} f_{Y|X}(y|x)\log(f_{Y|X}(y|x))\,dy\right)dx - \right. \\ \left. - \log(\Delta)\right) = H_d(Y) - \frac{1}{2}\log(2\pi e\sigma^2_{noise}). \quad (20)$$

Пропускная способность представляется как

$$C = \max_{f_X(x)}\left(H_d(Y) - \frac{1}{2}\log(2\pi e\sigma^2_{noise})\right). \quad (21)$$

Ограничение (14), (16) на сигнал x дает ограничение на y вида

$$\mathbf{E}y^2 = \mathbf{E}(x+z)^2 \le S + \sigma^2_{noise}. \quad (22)$$

Максимум дифференциальной энтропии при ограничении (22) достигается на гауссовском распределении с дисперсией $\sigma^2 = S + \sigma^2_{noise}$ [1–3], поэтому

$$\max_{f_X(x)} H_d(Y) = \frac{1}{2}\log(2\pi e(S+\sigma^2_{noise})) \quad (23)$$

и, следовательно,

$$C = \frac{1}{2}\log(2\pi e(S+\sigma^2_{noise})) - \frac{1}{2}\log(2\pi e\sigma^2_{noise}) = \\ = \frac{1}{2}\log\left(1 + \frac{S}{\sigma^2_{noise}}\right). \quad (24)$$

При наличии L независимых каналов с ограничениями на входе $S_1, \ldots, S_L$ и дисперсиями шума $\sigma^2_{noise,1} \ldots \sigma^2_{noise,L}$ пропускная способность представляет собой сумму [1–3]:

$$C_L = \frac{1}{2}\sum_{m=1}^{L}\log\left(1 + \frac{S_m}{\sigma^2_{noise,m}}\right). \quad (25)$$

В частном случае нескольких независимых каналов с одинаковыми дисперсиями шума σ^2_{noise} и общим ограничением

$$\mathbf{E}x_2^1 + \ldots + \mathbf{E}x_L^2 \le S \quad (26)$$

пропускная способность достигается на «равномощных» входах и выходах:

$$C_L = \frac{L}{2}\log\left(1 + \frac{S}{\sigma^2_{noise}L}\right). \quad (27)$$

Как видно из (27), при стремлении шума к нулю, $\sigma^2_{noise} \to 0$, пропускная способность — скорость передачи информации стремится к бесконечности, это означает, что через канал без шума можно передать сколь угодно много информации в единицу времени, причем энергия сигнала ограничена (26), что является физическим абсурдом. Данный факт в скрытом виде есть следствие отсутствия нижней границы Δ — дискретизации сигнала в классической области.

4. КЛАССИЧЕСКИЕ НЕПРЕРЫВНЫЕ КАНАЛЫ

Следующий шаг, который нам потребуется, прежде чем перейти к рассмотрению классически-квантового канала с ограниченной частотной полосой и гауссовским шумом, — рассмотреть классический канал с ограниченной частотной полосой и гауссовским шумом. Эти результаты будут использованы ниже.

Рассмотрим каналы, в которых сигналы на входе $x(t)$ и выходе $y(t)$ являются случайными процессами или случайными функциями времени.

Мы дадим простой интуитивно понятный вывод формулы для пропускной способности (в единицу времени) канала связи. Пусть вход — приготовление сигнала на передающей стороне — имеет вид

$$y(t) = x(t) + n(t), \quad (28)$$

сигнал $x(t)$ задан (приготавливается) на интервале времени $[-T/2, T/2]$, имеет ограниченную частотную полосу Ω и наблюдается (измеряется на приемной стороне) на фоне белого гауссовского шума $n(t)$ с постоянной спектральной плотностью $N_0/2$.

Формула (28) имеет асимптотический характер при $\Omega T \to \infty$ в следующем смысле. Функции с ограниченным частотным спектром Ω не могут быть строго локализованы на конечном временном интервале T, однако, как будет видно ниже, существует

набор функций с ограниченным частотным спектром, которые экспоненциально сильно по параметру ΩT локализованы в интервале T. То есть весь сигнал $x(t)$ сосредоточен в окне T, кроме «хвостов», которые выходят за интервал T лишь с вероятностью $\approx \exp(-\Omega T)$. Число ортогональных функций с ограниченным частотным спектром, экспоненциально локализованных в окне T, есть $N_\Omega \approx \Omega T$, данные функции используются как базисные, по которым разлагается сигнал $x(t)$. Неформально говоря, сказанное означает, что сигнал с ограниченным частотным спектром может быть сколь угодно точно приготовлен передатчиком во временном окне T.

Перейдем к более точным формулировкам. Следуя [3], мы используем представление любой заданной действительной или комплексной функции с помощью разложения в ряд по ортонормальным функциям. При этом случайная функция описывается с помощью совместного распределения коэффициентов такого разложения.

Любая (интегрируемая с квадратом) функция $x(t)$, заданная на интервале $[-T/2, T/2]$, может быть представлена в виде разложения по системе ортогональных функций $\{\overline{\varphi}_m(t)\}_{m=1}^{\infty}$:

$$x(t) = \sum_{m=1}^{\infty} x_m \overline{\varphi}_m(t), \quad x_m = \int\limits_{-T/2}^{T/2} x(t)\overline{\varphi}_m(t)\,dt. \quad (29)$$

Ограничение по частоте Ω можно представить как прохождение функции $x(t)$ через фильтр с частотной характеристикой

$$H(\omega) = \begin{cases} 1, & 0 \le \omega \le \Omega, \\ 0, & \omega \ge \Omega, \end{cases} \quad (30)$$

или импульсной переходной функцией

$$h(t) = \frac{\sin(2\pi\Omega t)}{\pi t}. \quad (31)$$

Тогда для любой функции с ограничением Ω имеет место представление

$$x(t) = \sum_{m=1}^{\infty} h(t-\tau)\overline{\varphi}_m(\tau)\,d\tau, \quad t \in \left[-\frac{T}{2}, \frac{T}{2}\right]. \quad (32)$$

Можно выбрать систему $\{\overline{\varphi}_m(t)\}_{m=1}^{\infty}$ исходных функций не произвольно, а как решения интегрального уравнения [7–9]

$$\int\limits_{-T/2}^{T/2} \mathcal{K}(\tau_1, \tau_2)\overline{\varphi}_m(\tau_2)\,d\tau_2 = \lambda_m \overline{\varphi}_m(\tau_1), \quad (33)$$

где

$$\mathcal{K}(\tau_1, \tau_2) = h^*(t, \tau_1)h^*(t, \tau_2)\,dt, \quad (34)$$

$$h^*(t, \tau) = \begin{cases} h(t-\tau), & |t| \le \dfrac{T}{2}, \quad |\tau| \le \dfrac{T}{2}, \\ 0 & \text{в других точках.} \end{cases} \quad (35)$$

Тогда

$$x(t) = \sum_{m=1}^{\infty} x_m \int\limits_{-T/2}^{T/2} h(t-\tau)\overline{\varphi}_m(\tau)\,d\tau = \\ = \sum_{m=1}^{\infty} x_m \sqrt{\lambda_m}\varphi_m(t), \quad t \in \left[-\frac{T}{2}, \frac{T}{2}\right]. \quad (36)$$

Здесь $\{\overline{\varphi}_m(t)\}$ — система волновых функций вытянутого сфероида [7–9], ортогональных на всей числовой прямой $(-\infty, \infty)$ и ортогональных на интервале $[-T/2, T/2]$. Данное свойство ортогональности позволит аккуратно осуществить предельный переход $T \to \infty$ при вычислении скорости в единицу времени безошибочной передачи информации.

Собственные числа $\lambda_1 > \lambda_2 > \ldots > 0$ отвечают за долю энергии — степени локализации функций $\theta_m(t)$ в интервале $[-T/2, T/2]$:

$$\int\limits_{-T/2}^{T/2} \overline{\varphi}_m^2(t)\,dt = \lambda_m. \quad (37)$$

Имеет место следующее свойство функций вытянутого сфероида [7–9]: при $\Omega T \to \infty$ и для любых сколь угодно малых значений $\varepsilon \approx \ln(\Omega T)/(\Omega T)$ собственные числа $\lambda_m \to 1$ для всех $m \le \Omega T(1-\varepsilon)$ и $\lambda_m \to 0$ для всех $m \ge \Omega T(1+\varepsilon)$. При этом стремление собственных чисел λ_m к единице при $m \le \le \Omega T(1-\varepsilon)$ определяется параметром $\exp(-\Omega T)$.

Отсюда следует, что функция $x(t)$ с ограниченным по частоте спектром, представленная в (36), определяется, по существу, только первыми $N_\Omega = = \Omega T$ коэффициентами $x_1, \ldots, x_{N_\Omega}$:

$$x(t) = \sum_{m=1}^{N_\Omega} = x_m \varphi_m(t), \quad (38)$$

функции $\varphi_m(t)$ ортонормированы на интервале $[-T/2, T/2]$. При этом $\varphi_m(t)$, $m = 1, \ldots, N_\Omega$ практически полностью локализованы на интервале $[-T/2, T/2]$.

Раскладывая по системе $\{\varphi_m(t)\}$ реализацию белого гауссовского шума, получаем коэффициенты — случайные величины:

$$n_m = \int\limits_{-T/2}^{T/2} n(t)\varphi_m(t)\,dt, \quad m = 1, \ldots, N_\Omega. \tag{39}$$

Коэффициенты n_m при разных m статистически независимы друг от друга и от x_m, и

$$\mathbf{E}n_m^2 = N_0. \tag{40}$$

Таким образом, канал связи с непрерывным временем

$$y(t) = x(t) + n(t) \tag{41}$$

представляем в виде дискретного по времени канала

$$(y_1, \ldots, y_{N_\Omega}) = (x_1 + n_1, \ldots, x_{N_\Omega} + n_{N_\Omega}) \tag{42}$$

с независимыми компонентами шума $(n_1, \ldots, n_{N_\Omega})$, имеющими гауссовское распределение. Предположим, что мощность на входе канала ограничена [1, 3]:

$$\frac{1}{T}\int\limits_{-T/2}^{T/2} \mathbf{E}x^2(t)\,dt \le S. \tag{43}$$

С учетом ортогональности $\{\varphi_m(t)\}$ отсюда получаем соотношение

$$\sum_{m=1}^{N_\Omega} \mathbf{E}x_M^2 \le ST. \tag{44}$$

Передача информации в многомодовом случае осуществляется аналогично передаче информации в случае одной моды. После дискретизации передатчик выбирает в соответствии с вероятностью, аналогичной (19), в каждой моде символ алфавита (уровень сигнала) на входе. Фактически такой выбор отвечает выбору амплитуды сигнала в каждой моде. На принимающей стороне приемник определяет выходной символ — уровень сигнала в каждой независимой моде. Именно ортогональность сигналов в каждой моде — ортогональность базисных функций, по которым разлагается сигнал, позволяет это сделать.

Далее, используя свойство энтропийной функции и соотношение (27) предыдущего раздела для пропускной способности независимых гауссовских каналов, окончательно получаем выражение для пропускной способности дискретного по времени канала:

$$\begin{aligned} C_L(T) = \max_{f_{Y_1,\ldots,Y_{N_\Omega}}(y_1,\ldots,y_{N_\Omega})} (H_d(Y_1, \ldots, Y_{N_\omega}) - \\ - H_d(Y_1, \ldots, Y_{N_\Omega}|X_1, \ldots, X_{N_\Omega})) = \\ = \sum_{m=1}^{N_\Omega} \left(\max_{f_Y(y)} H_d(Y) - \frac{1}{2}\log(2\pi e N_0) \right) = \\ = \frac{N_\Omega}{2}\log\left(1+\frac{ST}{N_\Omega N_0}\right) = \frac{1}{2}\Omega T \log\left(1+\frac{S}{N_0\Omega}\right). \end{aligned} \tag{45}$$

Для пропускной способности в единицу времени получаем

$$C = \lim_{T\to\infty}\frac{C_L(T)}{T} = \frac{1}{2}\Omega\log\left(1+\frac{S}{N_0\Omega}\right). \tag{46}$$

Как видно из (46), расходимость пропускной способности при нулевом шуме в канале ($N_0 \to 0$) сохраняется и в многомодовом случае.

5. КВАНТОВЫЙ КАНАЛ, ОДНОМОДОВЫЙ СЛУЧАЙ

Перейдем к обсуждению квантового случая. Рассмотрим классически-квантовый канал. Целью является передача классической информации при помощи квантовых состояний. Данную задачу можно свести в определенном смысле к эффективному классическому каналу связи, чтобы можно было провести аналогию с соответствующими классическими величинами, несмотря на то, что полное сведéние к классическому случаю невозможно.

В классически-квантовом канале связи на передающей стороне символам классического алфавита — классической информации — сопоставляются квантовые состояния, которые передаются через квантовый канал с шумом. На приемной стороне посредством измерений квантовых состояний, искаженных шумом в канале связи, требуется получить классическую информацию, закодированную в квантовые состояния. Аналогом непрерывной классической переменной является когерентное состояние $|\zeta\rangle_j$, которое при большом среднем числе фотонов $|\zeta|^2 \gg 1$ переходит в классический сигнал. Индекс j отвечает за пространственную моду состояния.

Аналогично предыдущим разделам будем рассматривать пространственные моды с конечной частотной полосой, и в качестве базисных одночастичных функций выберем волновые функции вытянутого сфероида. Операторы рождения в различных

модах коммутируют (базисные состояния ортогональны),

$$[a(\varphi_j), a^\dagger(\varphi_i)] = (\varphi_j, \varphi_i) = \delta_{ji},$$
$$(\varphi_j, \varphi_i) = \int\limits_\Omega \varphi_j(\omega)\varphi_i^*(\omega)\,d\omega = \delta_{ji}, \qquad (47)$$

$$(\overline{\varphi}_j, \overline{\varphi}_i) = \int\limits_\Omega \overline{\varphi}_j(\omega)\overline{\varphi}_i^*(\omega)\,d\omega = \delta_{ji}, \quad \varphi_j = \frac{1}{\sqrt{\lambda_j}}\overline{\varphi}_j,$$

где $\varphi_j(\omega)$ — j-я функция вытянутого сфероида, нормированная на единицу во временном окне $[-T/2, T/2]$, $\overline{\varphi}_j(\omega)$ — функция, нормированная на интервале $(-\infty, \infty)$, λ_j — собственное число (см. (37)).

Для связи с предыдущими разделами удобнее рассмотреть сначала случай одной моды j. Любое многочастичное квантовое состояние тождественных частиц бозонов [10] может быть представлено как

$$|\Phi\rangle_j = \begin{pmatrix} \Phi_{0j} \\ \Phi_{1j}(\omega_1, \omega_2) \\ \dots \\ \Phi_{nj}(\omega_1, \omega_2, \dots, \omega_n) \\ \dots \end{pmatrix} = \sum_{n=0}^{\infty} \frac{1}{\sqrt{n!}} \times$$
$$\times \int\limits_\Omega \dots \int\limits_\Omega d\omega_1 d\omega_2 \dots d\omega_n \Phi_{nj}(\omega_1, \omega_2, \dots, \omega_n) \times$$
$$\times (a^\dagger(\varphi_j))^n |\mathrm{vac}\rangle_j, \quad (48)$$

где $\Phi_{nj}(\omega_1, \omega_2, \dots, \omega_n)$ — амплитуды состояний с разными фоковскими числами фотонов в моде j. Одномодовое когерентное состояние, локализованное во временном окне T, имеет вид

$$|\zeta\rangle_j = \exp\left(-\frac{|\zeta|^2}{2}\right) \sum_{n=0}^{\infty} \frac{\zeta^n}{\sqrt{n!}} (a^\dagger(\varphi_j))^n |\mathrm{vac}\rangle_j =$$
$$= \exp\left(-\frac{|\zeta|^2}{2}\right) \sum_{n=0}^{\infty} \frac{\zeta^n}{\sqrt{n!}} |n(\varphi_j)\rangle, \quad (49)$$

где $|n(\varphi_j)\rangle$ — фоковское состояние с n фотонами в моде j. Аналогично классическому одномодовому случаю кодирование осуществляется в энергию сигнала — амплитуду $(x, x + dx)$, которая выбирается в соответствии с распределением вероятностей $P_X(x)\,dx$. В квантовом случае аналогом энергии является среднее число фотонов $|\alpha|^2$, которое при кодировании выбирается случайно в соответствии с распределением вероятностей $P(\alpha)\,d\alpha$, где $d\alpha = d\alpha_{Re} d\alpha_{Im}$ — вещественная и мнимая части параметра α. По этой причине число степеней свободы в когерентном состоянии в два раза больше, чем в классическом сигнале (см. ниже). Пусть на передающей стороне задана интенсивность когерентного состояния α. После прохождения через канал связи чистое когерентное состояние превращается в матрицу плотности, искаженную гауссовским шумом. Искаженную матрицу плотности можно представить в виде

$$\rho_j(\alpha) = \frac{1}{2\pi N_{noise}} \int d\zeta |\zeta\rangle_{jj}\langle\zeta| \times$$
$$\times \exp\left(-\frac{|\zeta - \alpha|^2}{2N_{noise}}\right), \quad (50)$$

здесь N_{noise} — дисперсия среднего числа фотонов в j-моде шума, имеет размерность числа фотонов, поскольку $|\zeta - \alpha|^2$ — среднее число фотонов. Распределение вероятностей числа фотонов $\mu = |\alpha|^2$ в квантовых сигнальных состояниях аналогично классическому случаю имеет гауссовский вид:

$$P(\alpha) = \frac{1}{2\pi M} \exp\left(-\frac{|\alpha|^2}{2M}\right), \qquad (51)$$

где M — дисперсия среднего числа фотонов в информационных состояниях — аналог энергии в классическом случае (см. формулы (8), (19)). Формулу (51) нужно понимать как

$$P(\alpha_{Re}, \alpha_{Im}) = \frac{1}{\sqrt{2\pi M}} \frac{1}{\sqrt{2\pi M}} \exp\left(-\frac{\alpha_{Re}^2 + \alpha_{Im}^2}{2M}\right),$$

где α_{Re}, α_{Im} — независимые классические гауссовские случайные величины с одной и той же дисперсией, $d\alpha = d\alpha_{Re} d\alpha_{Im}$.

Непрерывный диапазон изменений α разбивается на дискретные интервалы $(\alpha_k, \alpha_k + d\alpha)$, вероятность α из этого интервала равна $P(\alpha_k)\,d\alpha$, аналогично классическому случаю. После этого источник становится дискретным, число интервалов разбиения k есть N. Каждому классическому символу α_k, выбираемому с вероятностью $P(\alpha_k)\,d\alpha$, сопоставляется когерентное квантовое состояние, которое после прохождения через канал связи становится равным (50). Итак, сигнальные состояния — набор с разными энергиями $\rho_j(\alpha)$ — выбираются с вероятностями $P(\alpha)\,d\alpha$. На приемной стороне возникают последовательности $\rho_j(k) = \rho_j(\alpha_k)P(\alpha_k)\,d\alpha$. Последовательность посылок длины n в полной аналогии с дискретным классическим источником (4) имеет вид

$$(\rho_j(k_1))^{\otimes n_{k_1}} \otimes (\rho_j(k_2))^{\otimes n_{k_2}} \otimes \dots \otimes (\rho_j(k_n))^{\otimes n_{k_n}},$$
$$n_{k_1} + n_{k_2} + \dots + n_{k_n} = n, \qquad (52)$$

где n_{k_1} — число вхождений символа α_{k_1}, n_{k_2} — число вхождений символа α_{k_2} и т. д. Все последовательности (52) получаются как результат разложения

$$(\rho_j(\alpha_1)P(\alpha_1)\,d\alpha + \rho_j(\alpha_2)P(\alpha_2)\,d\alpha + \\ + \ldots + \rho_j(\alpha_N)P(\alpha_N)\,d\alpha)^{\otimes n} = \\ = \left(\sum_k \rho_j(\alpha_k)P(\alpha_k)\,d\alpha\right)^{\otimes n} \to \overline{\rho}_j^{\otimes n}, \quad (53)$$

$$\overline{\rho}_j = \int \rho_j(\alpha)P(\alpha)\,d\alpha. \quad (54)$$

Диагонализуем матрицу плотности $\overline{\rho}_j$ в (53), (54), получаем

$$\overline{\rho}_j = \sum_{K=0}^{\infty} \Lambda_j(K)|K(\varphi_j)\rangle\langle K(\varphi_j)|, \\ \Lambda_j(K) = \frac{1}{N_{noise}+M+1}\left(\frac{N_{noise}+M}{N_{noise}+M+1}\right)^K, \quad (55)$$

где $\Lambda_j(K)$, $|K(\varphi_j)\rangle$ — собственные числа и векторы, которые нумеруем буквой K. После диагонализации задача становится эффективно «классической». Собственные векторы (состояния) матрицы плотности (53)–(55) являются ортогональными, достоверно различимыми — в этом смысле классическими. Поэтому состояния на передающей стороне выглядят как состояния классического источника, который генерирует символы классического алфавита (индекс K) с вероятностями $\Lambda_j(K)$, равными собственным числам матрицы плотности (53)–(55).

В асимптотическом пределе длинных последовательностей число вхождений каждого состояния $|K(\varphi_j)\rangle\langle K(\varphi_j)|$ определяется соответствующим собственным числом — вероятностью $\Lambda_j(K)$. Число вхождения дается математическим ожиданием аналогично классическому случаю (4), (5): $n\Lambda_j(K_i)$. На приемной стороне имеются последовательности квантовых состояний:

$$|K_1(\varphi_j)\rangle\langle K_1(\varphi_j)| \otimes |K_2(\varphi_j)\rangle \times \\ \times \langle K_2(\varphi_j)| \otimes \ldots \otimes |K_n(\varphi_j)\rangle\langle K_n(\varphi_j)|, \quad (56)$$

число таких типичных последовательностей и их вероятности равны

$$2^{nH(\overline{\rho}_j)}, \quad \prod_{K=0}^{\infty} \Lambda_j(K)^{n\Lambda_j(K)} = 2^{-nH(\overline{\rho}_j)}, \\ H(\overline{\rho}_j) = -\mathrm{Tr}\{\overline{\rho}_j \log(\overline{\rho}_j)\} = \\ = -\sum_{K=0}^{\infty} \Lambda_j(K)\log(\Lambda_j(K)). \quad (57)$$

Все типичные последовательности (57) равновероятны, квантовые состояния последовательностей ортогональны, т. е. достоверно различимы. Для их различения, чтобы выяснить, какая последовательность была передана с приемной стороны, нужно делать квантовомеханические измерения на приемной стороне. Такие измерения даются набором проекторов

$$I = \sum_{\ell=1}^{2^{nH(\overline{\rho}_j)}} \mathcal{P}_\ell + \mathcal{P}_{nontyp}, \quad (58)$$

где I — единичный оператор, проектор на все последовательности, $\mathcal{P}_\ell$ — проектор на типичную последовательность, сумма проекторов есть проектор на пространство типичных последовательностей, $\mathcal{P}_{nontyp}$ — проектор на пространство нетипичных последовательностей, вероятность «попасть» в это подпространство стремится к нулю в асимптотическом пределе. Измерение (58) проводится во временном окне T — проекторы «локализованы» в этом окне.

Важно отметить, что измерение является коллективным — отвечает проекциям не на индивидуальные состояния в каждой посылке, а проекциям сразу на состояния всей последовательности длины n.

При вычислении энтропии фон Неймана удобно воспользоваться соотношением

$$\frac{x}{(1-x)^2} = \sum_{k=1}^{\infty} k \cdot x^k,$$

получаем

$$H(\overline{\rho}_j) = (N_{noise}+M+1)\log(N_{noise}+M+1) - \\ - (N_{noise}+M)\log(N_{noise}+M). \quad (59)$$

Дадим физическую интерпретацию формул (57), (59). Неформально, все последовательности на приемной стороне занимают объем (57) в пространстве состояний, пространство натянуто на состояния типичных последовательностей (57).

Если целью было бы различить каждую типичную последовательность, то она достигнута: измерение (58) позволяет достоверно (в асимптотике) различить каждую типичную последовательность (57). Однако целью является не просто различить типичные последовательности, а установить, из какой типичной последовательности на передающей стороне возникла та или иная последовательность на приемной стороне. То есть цель — определить информационную последовательность $(\alpha_{k_1}, \alpha_{k_2}, \ldots, \alpha_{k_n})$ символов по результатам измерения на приемной сто-

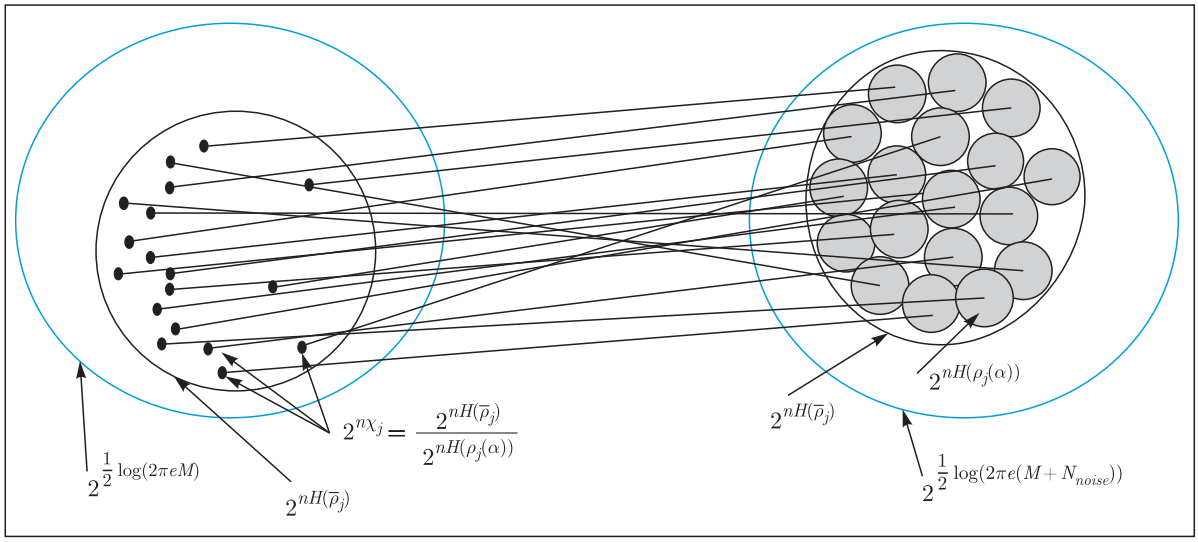

Рис. 1. Схематически показаны множества последовательностей на передающей и приемной сторонах. Число типичных классических последовательностей $2^{(1/2)\log(2\pi eS)}$, множество типичных классических последовательностей на приемной стороне $2^{(1/2)\log(2\pi e(S+\sigma^2_{noise}))}$. Каждая последовательность на приемной стороне «размазывается» в $2^{(1/2)\log(2\pi e\sigma^2_{noise})}$ последовательностей. В квантовом случае число различимых последовательностей на приемной стороне $2^{H(\overline{\rho}_j)}$, это множество также показано на передающей стороне. Каждая последовательность из данного множества переходит в множество на приемной стороне $2^{H(\rho(\alpha))}$. Множество последовательностей, передаваемых с приемной стороны — кодовые последовательности (показаны черными точками). Число последовательностей, которые могут быть безошибочно различимы на приемной стороне, есть $2^{n\chi_j} = 2^{H(\overline{\rho}_j)}/2^{H(\rho(\alpha))}$

роне. Матрица плотности в каждой посылке «занимает» некоторый объем пространства состояний, каждая последовательность на передающей стороне переходит в некоторое количество последовательностей на приемной стороне, каждая последовательность на передающей стороне будет занимать некоторый объем пространства состояний на приемной стороне, аналогично классическому случаю. Шум в канале размазывает каждую последовательность в некоторый объем (см. рис. 1 и пояснения к нему).

Матрица плотности в каждой посылке «имеет объем», который не зависит от индекса k (это справедливо только для гауссовского распределения среднего числа фотонов в сигнале и шуме). Диагонализуя матрицу плотности в (50), получаем

$$\rho_j(\alpha_k) = \sum_{k=0}^{\infty} \lambda_j(k) |k(\varphi_j)\rangle\langle k(\varphi_j)|, \qquad \lambda_j(k) = \frac{1}{N_{noise}+1}\left(\frac{N_{noise}}{N_{noise}+1}\right)^k, \tag{60}$$

где $\lambda_j(k)$, $|k(\varphi_j)\rangle$ — собственные числа и векторы $\rho_j(\alpha_k)$. Отметим, что собственные числа и векторы (60) не зависят от индекса разбиения k и определяются только шумом в канале. Неформально говоря, внутри типичных последовательностей имеют место внутренние типичные последовательности — каждая типичная последовательность на передающей стороне в среднем превращается в одинаковый набор внутренних типичных последовательностей, число которых и вероятность есть

$$2^{nH(\rho_j(\alpha))}, \quad \prod_{k=0}^{\infty} \lambda_j(k)^{n\lambda_j(k)} = 2^{-nH(\rho_j(\alpha))}, \tag{61}$$

для энтропии частичной матрицы плотности получаем

$$H(\rho_j(\alpha_k)) = -\sum_{n=0}^{\infty} \lambda_j(n)\log(\lambda_j(n)) = (N_{noise}+1)\times \\ \times \log(N_{noise}+1) - N_{noise}\log(N_{noise}). \tag{62}$$

Для того чтобы различить при помощи измерений (58) каждую передаваемую последовательность со стороны передатчика, число таких последовательностей на передающей стороне должно быть таково, чтобы образы от них на приемной стороне не перекрывались. При выборе числа последовательностей на передающей стороне в асимптотическом пределе равным

$$2^{n\chi_j} = \frac{2^{nH(\overline{\rho}_j)}}{2^{nH(\rho_j(\alpha))}}, \quad \chi_j = H(\overline{\rho}_j) - H(\rho_j(\alpha)), \tag{63}$$

приемник сможет безошибочно различить данное число последовательностей. Естественно, набор этих последовательностей — кодовая таблица — оговаривается заранее. Приемник точно знает, что будет послана одна из последовательностей из кодовой таблицы, только заранее неизвестно, какая именно. Измерение позволяет отличить каждую последовательность из кодовой таблицы. Величина $C = \chi_j = H(\overline{\rho}_j) - H(\rho_j(\alpha))$ представляет собой фундаментальную величину Холево [4–6] — пропускную способность классически-квантового канала связи с гауссовским шумом. Данная величина дает верхнюю фундаментальную границу безошибочной передачи классической информации при помощи квантовых состояний, т. е. числа битов информации в пересчете на посылку.

Данная величина достижима на коллективных измерениях (58) (см. также [4–6]).

Обратим внимание, что «размазка» состояний на приемной стороне определяется только интенсивностью шума (в (62) входит только N_{noise} и не входит энергия/число фотонов M информационного сигнала, в полной аналогии с классическим случаем (см. формулу (17)).

6. КВАНТОВЫЙ КАНАЛ, МНОГОМОДОВЫЙ СЛУЧАЙ

В многомодовом случае имеется N_Ω параллельных независимых классически-квантовых каналов. Сигнальные состояния $\rho_j(\alpha)$ $(j = 1, 2, \ldots, N_\Omega)$ в независимых каналах выбираются с вероятностями $P(\alpha_k)\,d\alpha$ в каждой моде. Каждая мода j выбирается независимо. Последовательности в каждой посылке во всех модах могут быть представлены аналогично предыдущему случаю с одной модой, $\rho(k,j) = \rho_j(\alpha_k)P(\alpha_k)\,d\alpha$ (индекс k нумерует интервалы разбиения, число интервалов N). Все последовательности имеют вид

$$\rho(k_1,j_1)^{\otimes n(k_1,j_1)} \otimes \\ \otimes \rho(k_2,j_2)^{\otimes n(k_2,j_2)} \otimes \ldots \otimes \rho(k_n,j_n)^{\otimes n(k_n,j_n)}, \quad (64)$$

где $n(k_1,j_1)$ — число вхождений в последовательность состояний $\rho(k_1,j_1)$ с k_1,j_1 с энергией α_{k_1} в моде j_1 и т. д. Все последовательности длины n могут быть представлены как результат разложения:

$$\prod_{j=1}^{N_\Omega} (\rho_j(\alpha_1)P(\alpha_1)\,d\alpha + \\ + \rho_j(\alpha_2)P(\alpha_2)\,d\alpha + \ldots + \rho_j(\alpha_N)P(\alpha_N)\,d\alpha)^{\otimes n} = \\ = \prod_{j=1}^{N_\Omega} \left(\int \rho_j(\alpha)P(\alpha)\,d\alpha \right)^{\otimes n} = \prod_{j=1}^{N_\Omega} \overline{\rho}_j^{\otimes n}. \quad (65)$$

Число типичных последовательностей и их вероятности по всем каналам (модам) равны

$$2^{nN_\Omega H(\overline{\rho}_j)}, \quad \prod_{j=1}^{N_\Omega} \left(\prod_{K=0}^{\infty} \Lambda_j(K)^{n\Lambda_j(K)} \right) = \\ = 2^{-nN_\Omega H(\overline{\rho}_j)}. \quad (66)$$

Аналогично одномодовому случаю каждая типичная последовательность в каждом канале (моде) на передающей стороне в среднем превращается в одинаковый набор внутренних типичных последовательностей, число которых и вероятность есть

$$2^{N_\Omega n H(\rho_j(\alpha))}, \quad \prod_{j=1}^{N_\Omega} \left(\prod_{k=0}^{\infty} \lambda_j(k)^{n\lambda_j(k)} \right) = \\ = 2^{-N_\Omega n H(\rho_j(\alpha))}. \quad (67)$$

При выборе числа последовательностей на передающей стороне в асимптотическом пределе равным

$$2^{N_\Omega n \chi_j} = \frac{2^{N_\Omega n H(\overline{\rho}_j)}}{2^{nH(\rho_j(\alpha))}}, \\ \chi = \sum_{j=1}^{N_\Omega} \big(H(\overline{\rho}_j) - H(\rho_j(\alpha)) \big) = \\ = N_\Omega \left(H(\overline{\rho}_j) - H(\rho_j(\alpha)) \right), \quad (68)$$

приемник сможет безошибочно различить их все. Для скорости безошибочной передачи информации в многомодовом случае с учетом (67), (68) получаем

$$C_Q = \lim_{T\to\infty} \frac{\chi}{T} = \\ = \Omega \left([(N_{noise} + M + 1)\log(N_{noise} + M + 1) - \right. \\ - (N_{noise} + M)\log(N_{noise} + M)] - \\ - [(N_{noise} + 1)\log(N_{noise} + 1) - \\ \left. - N_{noise}\log(N_{noise})] \right). \quad (69)$$

Зависимости пропускных способностей в квантовом и классическом случаях от M приведены на рис. 2. Как видно из рис. 2, с ростом интенсивности шума и при одном и том же отношении M/N_{noise} пропускная способность в квантовом случае C_Q стремится

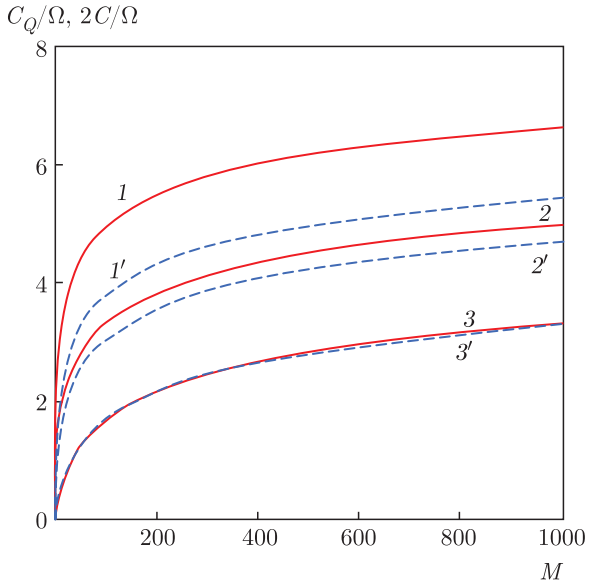

Рис. 2. Зависимости пропускных способностей в классическом случае (штриховые линии) и квантовом случае (сплошные линии) как функции среднего числа фотонов в моде M (энергии $S \to M$ в формуле (1)) при различных значениях интенсивности шума $N_{noise}(N_0) = 0.1$ (*1*, *1′*), 1.0 (*2*, *2′*), 10.0 (*3*, *3′*)

к классическому значению $2C$ (множитель 2 возникает из удвоенного числа степеней свободы в квантовом случае — комплексности параметра α в когерентном состоянии). При большой интенсивности сигнала и шума пропускная способность в квантовом и классическом случаях практически совпадают (кривые *3*, *3′* на рис. 2).

7. СРАВНЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ В КЛАССИЧЕСКОМ И КВАНТОВОМ СЛУЧАЯХ

Как было отмечено выше, формула для пропускной способности Шеннона для частотно-ограниченного канала расходится при нулевом шуме в канале:

$$C = \frac{1}{2}\Omega \log\left(1 + \frac{S}{N_0\Omega}\right) \to \infty, \quad N_0 \to 0. \qquad (70)$$

Данный факт свидетельствует об ограниченности классического подхода.

Отметим, что подозрение о том, что формулу (70) нужно модифицировать, высказывались еще в классических работах по теории информации [3] R. G. Gallager, *Information Theory and Reliable Communication*, p. 390 (формула (8.3.23)): "Physically, of course, the problem can be easily resolved by observing that N_0 cannot be strictly zero. To put it another way, when an analysis of a mathematical model of a physical problem is indeterminate, it means that the model has been over-idealized and the model must be changed".

В квантовом случае при большом числе фотонов пропускная способность частотно-ограниченного классически-квантового канала (69) имеет вид

$$C_Q = \Omega \log(1 + M) = \Omega \log\left(1 + \frac{m}{\Omega}\right), \qquad N_{noise} = 0. \qquad (71)$$

Удобно ввести обозначение $M = m/\Omega$, где m имеет смысл числа фотонов в состоянии в единичной частотной полосе. Как видно из (71), при нулевом шуме расходимость отсутствует.

Формула (70) является чисто классической [3], при стремлении энергии шума к нулю ($N_{noise} \to 0$) скорость передачи информации расходится. Для того чтобы явно локализовать причину расходимости, рассмотрим пример.

Действительно, разобьем диапазон изменений непрерывной случайной величины (энергии сигнала) на интервалы Δ таким образом, чтобы вероятности попадания в каждый интервал были одинаковыми. Передача информации осуществляется выбором энергии сигнала в том или ином интервале. Припишем каждому интервалу его номер в лексикографическом порядке, начиная с 0. Бинарное представление номера (энергии сигнала) и будет передаваемой информацией — блоком 0 и 1. Очевидно, что при стремлении масштаба дискретизации к нулю, $\Delta \to 0$, за одну посылку и один акт измерения энергии сигнала приемником (канал идеальный) можно получить сколь угодно много информации — сколь угодно большой блок 0 и 1.

Для того чтобы устранить данное противоречие со здравым смыслом, часто произносятся слова, что процесс измерений сам вносит шум, поэтому интервал дискретизации нельзя выбирать меньше амплитуды шума. С логической точки зрения такой подход непоследователен, поскольку измеряется общее значение переменной, которое содержит вклад от всех процессов, включая шум, и процесс дискретизации не зависит от шума — является внешним.

Неформально говоря, количество передаваемой информации за одну посылку зависит от волевого решения по дискретизации.

Физически ясно, что любой физический сигнал нельзя дискретизировать до бесконечности в сторону уменьшения интервала Δ. На каком-то этапе неизбежно возникнут ограничения, диктуемые квантовой природой сигнала. Причем нижняя гра-

ница дискретизации диктуется квантовой механикой и не зависит от интенсивности сигнала. Нельзя дискретизировать сигнал до «масштабов, меньших отдельного фотона». Любой интенсивный сигнал содержит хоть и макроскопически большое, но все же конечное число фотонов.

Квантовая природа микромира должна ограничивать степень дискретизации, что неизбежно должно приводить к конечности энтропии сигнала, соответственно, накладывать фундаментальные ограничения на скорость передачи информации. Для того чтобы выяснить фундаментальные ограничения на скорость передачи информации, необходимо сразу рассматривать сигнал как квантовое состояние, которое может содержать любое число фотонов. Чтобы прояснить глубокую физическую причину, стоящую за устранением расходимости в классической формуле, рассмотрим вывод пропускной способности классически-квантового канала связи в идеальном случае — канала без шума, где интенсивность шума N_{noise} сразу равна нулю.

8. ПРОПУСКНАЯ СПОСОБНОСТЬ ИДЕАЛЬНОГО ЧАСТОТНО-ОГРАНИЧЕННОГО КЛАССИЧЕСКИ-КВАНТОВОГО КАНАЛА СВЯЗИ И ПРИНЦИП ТОЖДЕСТВЕННОСТИ ЧАСТИЦ

Как сейчас покажем, за отсутствием расходимости при нулевом шуме в формуле (71) стоит фундаментальный физический принцип тождественности частиц — бозонов. Вычисление пропускной способности для идеального канала связи сводится к подсчету скорости генерации энтропии источником информационных состояний. Формально отсутствие шума означает, что распределение сигнальных квантовых состояний в (50) сконцентрировано в окрестности числа фотонов M во всех состояниях, которые становятся равновероятными.

В этом случае задача вычисления скорости генерации энтропии сводится к подсчету числа квантовых состояний с M фотонами, локализованных в интервале времени $[-T/2, T/2]$.

Пусть квантовое состояние поля содержит M фотонов — бозе-частиц. Состояние имеет носитель в конечной частотной полосе Ω. В качестве одночастичных базисных состояний выберем волновые функции вытянутого сфероида $\varphi_n(\omega)$. Таких функций $N_\Omega = \Omega T$. Число многочастичных ортогональных векторов состояний с M фотонами, локализованных во временном окне T, равно числу способов размещения M фотонов по N_Ω одночастичным состояниям. Число размещений бозе-частиц по N_Ω состояниям равно

$$C^M_{N_\Omega-1+M} = \frac{(N_\Omega-1+M)!}{(N_\Omega-1)!M!}. \tag{72}$$

Вектор состояния, отвечающий размещению — разбиению числа $n_1+n_2+\ldots+n_{N_\Omega}=M$, имеет вид

$$\begin{aligned}|\Phi_{n_1,n_2,\ldots,n_{N_\Omega}}\rangle = \int\limits_\Omega \ldots \int\limits_\Omega d\omega_1 d\omega_2 \ldots d\omega_{n_1} d\omega_{n_1+1} \times \\ \times d\omega_{n_1+2}\ldots d\omega_{n_2}\ldots d\omega_{n_{N_\Omega-1}+1} d\omega_{n_{N_\Omega-1}+2}\ldots d\omega_{n_{N_\Omega}} \times \\ \times \varphi_1(\omega_1)\varphi_1(\omega_2)\ldots\varphi_1(\omega_{n_1})\varphi_2(\omega_{n_1+1}) \times \\ \times \varphi_2(\omega_{n_1+2})\ldots\varphi_2(\omega_{n_2})\ldots\varphi_{N_\Omega}(\omega_{n_{N_\Omega-1}+1}) \times \\ \times \varphi_{N_\Omega}(\omega_{n_{N_\Omega-1}+2})\ldots\varphi_{N_\Omega}(\omega_{n_{N_\Omega}}) \times \\ \times |\omega_1,\omega_2,\ldots,\omega_{n_1},\omega_{n_1+1},\omega_{n_1+2},\ldots,\omega_{n_2}, \\ \ldots,\omega_{n_{N_\Omega-1}+1},\omega_{n_{N_\Omega-1}+2},\ldots,\omega_{n_{N_\Omega}}\rangle. \end{aligned} \tag{73}$$

Дальнейшая логика рассуждений следующая. При заданном числе фотонов в состоянии M имеется (72) ортогональных, а значит достоверно различимых, квантовых состояний на интервале $[-T/2, T/2]$, которые локализованы почти целиком в этом окне. Измерения во временном окне позволяют различить все ортогональные состояния. Максимальная энтропия источника достигается в том случае, когда источник генерирует равновероятно все $C^M_{N_\Omega-1+M}$ ортогональных различимых состояний. Состояния (73) ортогональны, поэтому достоверно различимы. Передатчик посылает состояния (73) равновероятно. Приемник использует измерения, сводящиеся к проекции на набор состояний (73). В каждом акте измерения во временном окне $[-T/2, T/2]$ возникает случайно один из $C^M_{N_\Omega-1+M}$ исходов.

Вероятность каждого состояния, генерируемого передатчиком, есть $1/C^M_{N_\Omega-1+M}$, соответственно, энтропия источника, генерируемая за время T, есть

$$H_T = \log\left(C^M_{N_\Omega-1+M}\right). \tag{74}$$

Поскольку $N_\Omega \gg 1$, воспользовавшись формулой Стирлинга для значения факториала в главном приближении, получаем

$$\begin{aligned} C^M_{N_\Omega-1+M} \approx \frac{(N_\Omega+M)^{N_\Omega}(N_\Omega+M)^M}{N_\Omega^{N_\Omega}M^M} = \\ = \left(1+\frac{M}{N_\Omega}\right)^{N_\Omega}\left(1+\frac{N_\Omega}{M}\right)^M, \end{aligned} \tag{75}$$

где M — число фотонов во временном окне $[0, T]$. Удобно для дальнейшего ввести обозначение $M = mT$, где m имеет смысл числа фотонов в единицу

времени и имеет такую же размерность, как частота Ω [1/с], поэтому отношение m/Ω является безразмерным.

Используя (74), (75), находим, что энтропия, генерируемая источником в единицу времени (пропускная способность) равна

$$C_Q = \lim_{T\to\infty} \frac{H_T}{T} = \\ = \Omega \left[\log\left(1+\frac{m}{\Omega}\right) + \frac{m}{\Omega}\log\left(1+\frac{\Omega}{m}\right)\right]. \quad (76)$$

При малых числах фотонов (предельно квантовый сигнал), $m/\Omega \ll 1$, выражение для скорости генерации энтропии принимает вид

$$C_Q = m, \quad (77)$$

она пропорциональна числу фотонов в единичной частотной полосе. Скорость генерации энтропии фактически определяется частотной полосой сигнала. Формально ширина частотной полосы в формуле (78) сокращается, скорость генерации энтропии пропорциональна числу фотонов. При большом числе фотонов, $m/\Omega \gg 1$, (классический предел) второе слагаемое в правой части (76) остается конечным и стремится к

$$\frac{m}{\Omega}\log\left(1+\frac{\Omega}{m}\right) \to \frac{1}{\ln(2)}, \quad \frac{m}{\Omega}\to\infty. \quad (78)$$

Первое слагаемое в (76) логарифмически растет с увеличением числа фотонов (интенсивности сигнала):

$$C_Q = \Omega \log\left(1+\frac{m}{\Omega}\right), \quad (79)$$

что совпадает с пропускной способностью (71) канала с гауссовскими информационными состояниями после устремления к нулю интенсивности шума в канале.

9. ЗАКЛЮЧЕНИЕ

В заключение отметим, что при выводе пропускной способности канала с гауссовскими информационными состояниями и шумом предыдущим способом (разд. 5–7) за кадром остается фундаментальный факт — устранение расходимости, фактически невозможность дискретизировать сигнал до сколь угодно малых масштабов. Нижняя граница дискретизации ограничивается числом ортогональных различимых квантовых состояний при заданном числе фотонов M (в классическом случае интенсивностью), которые можно сформировать в данной частотной полосе. Число различных способов размещения M бозонов при использовании N_Ω одночастичных базисных состояний диктуется фундаментальным физическим принципом тождественности частиц — бозонов, формула (72). При квантовом рассмотрении проблема дискретизации сигнала отсутствует, при заданном количестве частиц M число состояний определяется числом способов размещения тождественных частиц по N_Ω уровням — набору одночастичных состояний.

Благодарности. Выражаем благодарность коллегам по Академии криптографии Российской Федерации за обсуждения и поддержку, а также К. А. Балыгину, А. Н. Климову, С. П. Кулику за многочисленные обсуждения и замечания.

Финансирование. Работа выполнена при поддержке Российского научного фонда (проект № 21-12-00005).

ЛИТЕРАТУРА

1. C. E. Shannon, Bell System Techn. J. **XXVII**, 379 (1948).

2. T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley (1991).

3. R. G. Gallager, *Information Theory and Reliable Communication*, John Willey&Sons, New York, Chichester, Brisbane, Toronto, Singapore (1968).

4. A. S. Holevo, Probl. Inf. Transm. **9**, 177 (1973).

5. А. С. Холево, УМН **53**, 193 (1998).

6. А. С. Холево, *Квантовые системы, каналы, информация*, МЦНМО, Москва (2010).

7. H. J. Landau and H. O. Pollak, Bell System Techn. J. **40**, 65 (1961).

8. D. Slepian and H. O. Pollak, Bell System Techn. J. **40**, 43 (1961).

9. W. H. J. Fuchs, J. Math. Analysis Applications **9**, 317 (1964).

10. Ф. А. Березин, *Метод вторичного квантования*, сер. Шедевры мировой физико-математической литературы, ИО НФМИ, Новокузнецк (2000), 230 с.