Аналитическая сложность и кодирование сигналов

В.К.Белошапка

12.11.2023

Аннотация

Существуют два способа описания геометрического объекта L: объект как образ отображения и объект как прообраз. У каждого способа есть свои достоинства и недостатки, вместе они дают полноту картины. Для того чтобы сравнить эти описания по сложности, можно использовать подход Колмогорова: т.е. после уточнения системы базовых операций сложность описания – это минимальная длина определяющего текста. Соответственно, мы получаем две колмогоровских сложности: в первом случае – $K^+(L)$, а во втором – $K^-(L)$. Пусть Cl^n – класс функций двух переменных, допускающих представление аналитическими функциями одного переменного и сложения глубины не больше n, а $K^+(Cl^n)$ и $K^-(Cl^n)$ – соответствующие им колмогоровские сложности. Имеются аргументы в пользу того, что при $n \geq 2$ значение $K^-(Cl^n)$ очень велико и задача построения описания Cl^n в виде прообраза (определяющими соотношениями) даже при $n = 2$ вычислительно нереализуема. На основе этого наблюдения предлагается схема кодирования-декодирования сигнала, а также приводятся аргументы в пользу того, что декодирование сигнала, закодированного по такой схеме, недоступно для квантового компьютера.

[1]

[1]Механико-математический факультет Московского университета им.Ломоносова, Воробьевы горы, 119991 Москва, Россия, vkb@strogino.ru.
Московский центр фундаментальной и прикладной математики МГУ им.М.В.Ломоносова,
vkb@strogino.ru

1. Координатные описания: объект как образ и как прообраз

При координатном описании геометрических объектов широко используются описания двух типов. Прямой (+) – объект как образ пространства параметров под действием отображения и обратный (-) – объект как подмножество объемлющего пространства, заданного некоторыми определяющими соотношениями. Вот простейший пример.

Прямая в вещественном пространстве $\mathbf{R}^3$. В первом представлении прямая l, проходящая через точку (a, b, c) в направлении вектора (α, β, γ), – это *образ* отображения $\varphi = (x(t), y(t), z(t))$ вещественной прямой с координатой t в пространство $\mathbf{R}^3$ с координатами (x, y, z). А во втором – подмножество этого $\mathbf{R}^3$, выделенное двумя соотношениями:

$$(+) \qquad x(t) = a + \alpha\, t, \quad y(t) = b + \beta\, t, \quad z(t) = c + \gamma\, t,$$

$$(-) \qquad t = \frac{x-a}{\alpha} = \frac{y-b}{\beta} = \frac{z-c}{\gamma} \quad \text{или}$$

$$u(x, y) = -\beta\, a + \alpha\, b - \alpha\, y + \beta\, x = 0,$$
$$v(x, y) = -a\gamma + \alpha\, c - \alpha\, z + \gamma\, x = 0.$$

Т.е. во втором случае прямая – это *прообраз* начала координат для отображения ψ из $\mathbf{R}^3$ в плоскость переменных (u, v), где $\psi = (u(x, y, z), v(x, y, z))$.

Эти два представления, прямое (+), в виде образа, и обратное (-), в виде прообраза, дополняют друг друга и являются по отношению к друг другу двойственными. Первое представление ориентировано на явное генерирование точек объекта (прямой). Однако если имеется некая точка $p = (x_0, y_0, z_0) \in \mathbf{R}^3$ и нас интересует вопрос о ее принадлежности данной прямой, то мы должны перейти ко второму представлению. Причем это второе представление решает две задачи. Оно дает критерий принадлежности точки p данной прямой, а также вычисляет значение $t = t_0$, при котором $\varphi(t_0) = p$. По отношению к первой подзадаче, задаче вычисления t_0, вторая, критерий принадлежности прямой, – это условие разрешимости.

В этом простейшем примере оба представления просты и переход от одного представления к другому также прост. Если за меру сложности

выражения χ принять $N(\chi)$ – число арифметических операций, нужных для его вычисления, то сложность для прямого представления $N^+ = 6$, а для обратного $N^- = 8$.

Рассмотрим еще один пример.

Пусть Cl^1 – это совокупность аналитических функций $z(x, y)$ двух переменных, имеющих представление вида $z = c(a(x) + b(y))$, где (a, b, c) – аналитические функции одного переменного. Это определение Cl^1, очевидно, есть определение первого типа, т.е. определение в виде образа. Если $\mathcal{A}$ – пучок ростков голоморфных функций на комплексной плоскости $\mathbf{C}$ (аналитические функции одного переменного), то пространство параметров – это прямая сумма $\mathcal{A} \oplus \mathcal{A} \oplus \mathcal{A}$. Отображение в пучок аналитических функций двух переменных имеет вид

$$z(x, y) = \varphi(a, b, c)(x, y) = c(a(x) + b(y)). \tag{1}$$

Это представление обладает всеми достоинствами и недостатками прямого представления (в виде образа): мы имеем явное выражение, которое позволяет, варьируя параметры (a, b, c), генерировать все функции $z(x, y) \in Cl^1$. Однако если у нас имеется конкретная аналитическая функция $z(x, y)$ и нам требуется выяснить, принадлежит ли z классу Cl^1, то мы нуждаемся в представлении второго типа. Для того чтобы перейти от представления (1) к обратному представлению, мы должны из соотношения $z(x, y) - c(a(x) + b(y)) = 0$ исключить параметры (a, b, c). Это нетрудно проделать (см. [1]), в итоге получаем соотношение вида:

$$\psi(z) = z'_x\, z'_y\, (z'''_{xxy}\, z'_y - z'''_{xyy}\, z'_x) + z''_{xy}\, ((z'_x)^2\, z''_{yy} - (z'_y)^2\, z''_{xx}) = 0. \tag{2}$$

Это соотношение является критерием принадлежности z семейству Cl^1 в следующем смысле. Если z имеет локальное представление вида (1), то $\psi(z)(x, y)$ – тождественный ноль всюду, где определена z. Если же $\psi(z)$ – тождественный ноль, то имеется две возможности. Либо z – это функция одного переменного, и тогда она, очевидно, имеет искомое представление, либо в окрестности любой точки, где $z'_x\, z'_y \neq 0$, росток функции z имеет представление (1), которое аналитически продолжается по всем тем путям, по которым продолжается z и на которых не обращается в ноль выражение $z'_x(x, y)\, z'_y(x, y)$. Отметим также, что $\psi(z)$ – это числитель дифференциальной дроби $R(z) = (\log(z'_x/z'_y))''_{xy}$. Соотношение (2)

– это решение второй подзадачи (-), т.е. критерий существования функций (a, b, c). При выполнении этого критерия компоненты представления (a, b, c) восстанавливаются с помощью интегрирования однозначно с точностью до выбора трех постоянных.

В этом примере для подсчета сложности выражения будем считать число входящих в него функций одного переменного, дифференцирований и арифметических операций. Тогда для прямого представления получаем $N^+ = 4$, а для обратного $N^- = 7$. Здесь мы посчитали N^- для R, для ψ получим больше.

Класс Cl^1 функций вида $c(a(x) + b(y))$ можно включить в расширяющуюся иерархию классов, определяемых индуктивно.

$Cl^0 = \{a(x) \text{ или } b(y),\ a, b \in \mathcal{A}\}$,
$Cl^{n+1} = \{z(x, y) = c(A_n(x, y) + B_n(x, y)),\ A_n, B_n \in Cl^n, c \in \mathcal{A}\}$.

Все классы Cl^n этой иерархии, по определению, получают явное прямое описание (+). Например, функции 2-го класса параметризуются семеркой функций одного переменного $(a(t), b(t), c(t), p(t), q(t), r(t), s(t))$, при этом произвольная функция 2-го класса имеет вид

$$z = \varphi_2(a, b, c, p, q, r, s)(x, y) = s\,(c(a(x) + b(y)) + r(p(x) + q(y)))$$

В соответствии с нашим правилом подсчета сложности $N^+(\varphi_0) = 1,\ N^+(\varphi_1) = 4,\ N^+(\varphi_2) = 10$ и далее $N^+(\varphi_{n+1}) = 2\,N^+(\varphi_n)+2$. Каждый класс Cl^n имеет конечный набор определяющих дифференциальных полиномов $\psi_n(z) = (P_n^1(z), \ldots, P_n^{m_n}(z))$, которые дают обратное (-) описание класса, т.е. $Cl^n = \{z : \psi_n(z) = 0\}$. Задача построения $\psi_n(z)$ – это задача того же типа, что и рассмотренная выше задача построения $\psi_1(z)$. Мы должны последовательно исключать неизвестные функции одного переменного и получать условия разрешимости. После исключения последней функции мы получим условия разрешимости только на функцию z. Это и есть уравнения класса. Для целей исключения можно пользоваться различной техникой (результанты, методы построения базисов дифференциальных идеалов).

Рассмотренные выше классы Cl^n – это классы функций, допускающих представление функциями одного переменного и сложения глубины не выше чем n. Можно рассматривать классы $Cl(S)$, построен-

ные из функций одного переменного и сложения по произвольной схеме композиции S. Схемой композиции мы называем способ расстановки скобок для построения композиции. И та же аргументация позволяет утверждать, что $Cl(S)$ имеет свой конечный набор определяющих дифференциальных полиномов $P(Cl(S))$. Для того чтобы охарактеризовать сложность конечного набора дифференциальных полиномов P, введем в рассмотрение следующие величины: $k(P)$ – максимальный дифференциальный порядок, $d(P)$ – максимальная алгебраическая степень, $m(P)$ – число полиномов, $M(P)$ – общее число мономов. В работе [2] было продемонстрировано, насколько резко возрастает сложность определяющих полиномов при небольшом усложнении схемы по сравнению со схемой первого класса. Приведем здесь некоторые результаты из этой работы.

Если $P = P(Cl^0)$, то $k = 1,\ d = 2,\ m = M = 1.$

Если $P = P(Cl^1)$, то $k = 3,\ d = 4,\ m = 1,\ M = 4.$

Если $P = P(Cl^{1+})$, где $Cl^{1+} = \{z = c(a(x) + b(y)) + p(x)\}$, то
$k = 5,\ d = 6,\ m = 2,\ M = 68.$

Если $P = P(Cl^{1++})$, где $Cl^{1++} = \{z = c(a(x) + b(y)) + p(x + y)\}$, то
$k = 7,\ d = 435,\ m = 6.$

Точных вычислений для Cl^2 нет. Однако можно предложить некоторые оценки. Дифференциальные соотношения для Cl^2 начинаются в 11-струе и заканчиваются в 32-й. При этом определяющие полиномы – это соотношения только на производные z. Если ограничиться порядком 11, то переменных в такой струе 77. Оценка алгебраической степени соответствующего алгебраического подмногообразия 11-струи по теореме Безу дает $\approx 10^{90}$. Оценка числа мономов $\approx 10^{2000}$.

Таким образом, можно резюмировать:

Задача построения $\psi_n(z)$, т.е. построения обратного описания Cl^n, является очень сложной для всех $n \geq 2$

Причем очень сложным является не только способ получения ответа, но и сам ответ, т.е. определяющие дифференциальные полиномы $(P_n^1(z), \ldots, P_n^{m_n}(z))$. И мы оказываемся в ситуации, когда с вычислительной точки зрения прямая задача (+) довольно проста, а обратная (-) – абсолютно недоступна.

Хорошим примером такой ситуации из теории чисел является пара взаимообратных целочисленных задач: вычисление показательной функции и логарифма в мультипликативной группе конечного поля. Как известно, на высокой сложности задачи целочисленного логарифмирования основаны распространенные алгоритмы шифрования информации [3].

2. Асимметрия колмогоровской сложности в задачах описания классов Cl^n

В работе [4] 1965-го года А.Н.Колмогоров обсудил два известных подхода к определению "количества информации": комбинаторный и вероятностный, а также предложил новый – алгоритмический. В контексте дискретной математики этот алгоритмический подход принято понимать как способ измерения "сложности" конечной последовательности элементов некоторого дискретного множества. Причем за меру сложности последовательности предложено взять длину "оптимальной" программы (на некотором языке программирования), которая выписывает эту последовательность.

С точки зрения двух способов описания объекта, рассмотренных выше, алгоритм, генерирующий последовательность Z, – это прямое описание (+) объекта Z, т.е. как образа некоторого отображения отрезка натурального ряда f (частично рекурсивная функция), т.е. $Z = \{f(1), f(2), \ldots, f(m)\}$. Ей, несомненно, можно сопоставить обратную задачу (-) – задачу идентификации, т.е. задачу проверки выполнения условия $z \in Z$. Как у первой, так и у второй задачи есть колмогоровская сложность: $K^+(Z)$ и $K^-(Z)$.

О вычислимости и алгоритмах можно говорить и за пределами дискретной математики (см., например, [5]). Перейдем в аналитический контекст, в котором можно обсуждать сложность прямой и обратной задач описания классов Cl^n. Для этого, как и выше при обсуждении сложности Cl^1, в список элементарных операций включаем функции одного пере-

менного, дифференцирования и арифметические операции. В результате мы получим две колмогоровские сложности класса $K^+(Cl^n)$ и $K^-(Cl^n)$.

Сформулированный в предыдущем пункте тезис теперь можно переформулировать так:

При $n \geq 2$ сложность алгоритма идентификации класса $K^-(Cl^n)$ значительно выше сложности алгоритма порождения класса $K^+(Cl^n)$.

3. Алгоритм кодирования сигнала

Основываясь на наблюдении, сформулированном выше, можно предложить способ кодирования-декодирования сигнала. Современная криптография почти полностью погружена в дискретную парадигму. Поэтому подчеркнем, что речь идет о способе, который сам по себе дискретизации не требует.

Пусть передаваемый физический сигнал – это функция $F(t)$, определенная на отрезке $\alpha_1 \leq t \leq \alpha_2$. Известно много способов заменить функцию $F(t)$ на отрезке на ее приближение на этом отрезке вещественной функцией $f(t)$, голоморфной или мероморфной на всей комплексной плоскости. Это может быть полином (теорема Вейерштрасса), тригонометрический полином (разложение в ряд Фурье), целая функция ограниченного роста (теорема Котельникова, [6]) и пр. Итак, $f(t)$ – это такая аналитическая на всей прямой функция, которая хорошо приближает F на $[\alpha_1, \alpha_2]$. Причем, учитывая физическую природу сигнала, мы можем предполагать, что все такие функции равномерно ограничены на $[\alpha_1, \alpha_2]$, т.е. $|f(t)| \leq M_f$.

Рассмотрим выражение из Cl^2 вида

$$z(x,t) = s\left(c(a(x) + b(t)) + r(p(x) + f(t))\right).$$

Причем $f(t)$ – это построенное нами приближение $F(t)$. Оставшиеся шесть функций $K = (a, b, p, c, r, s)$ – это ключ для процедур кодирования-декодирования. Относительно функций r и s будем предполагать, что их производные строго положительны на всей вещественной прямой, т.е. обратные функции r^{-1} и s^{-1} – аналитические функции, однозначные на всей прямой. Оставшиеся четыре функции (a, b, c, p) – произвольные вещественно-аналитические функции на прямой. При этом как в качестве функций (a, b, c, p), так и

функций (r, s) следует выбирать функции *достаточно общего вида*. Например, если все эти функции – полиномы (это вполне допустимо), то степени должны выбираться не слишком малыми, а в конечномерных пространствах наборов коэффициентов таких полиномов следует выбирать точку *достаточно общего положения*.

Далее полагаем ключ K фиксированным и не подлежащим разглашению. Кодирование осуществляется применением к $f(t)$ оператора Φ, декодирование – применением к $z(x,t)$ оператора Ψ:

$$f(t) \to \Phi(K,f) = s(c(a(x)+b(t)) + r(p(x)+f(t))) = z(x,t),$$
$$z(x,t) \to \Psi(K,f) = r^{-1}(s^{-1}(z(x,t)) - w) - p(x) = f(t),$$
$$\text{где } w = c(a(x)+b(t)).$$

Процедура такова.

Отправитель:
(1) преобразует сигнал $F(t)$ в аналитическое выражение $f(t)$, приближающее F на $[\alpha_1, \alpha_2]$,
(2) с помощью ключа K и оператора Φ преобразует $f(t)$ в $z(x,t)$ (изображение),
(3) по открытому каналу связи передает $z(x,t)$ получателю.
Получатель:
(4) с помощью ключа K и оператора Ψ преобразует $z(x,t)$ в $f(t)$, т.е. в приближение исходного сигнала $F(t)$ на отрезке $\alpha_1 \le t \le \alpha_2$.

Данная процедура устойчива по отношению к ошибкам в передаче изображения $z(x,y)$. Пусть

$$|f(t)| \le M_f \text{ при } \alpha_1 \le t \le \alpha_2, \quad |p(x)| \le M_p \text{ при } \beta_1 \le x \le \beta_2,$$
$$|w(x,t)| \le M_w \text{ при } \alpha_1 \le t \le \alpha_2,\ \beta_1 \le x \le \beta_2,$$
$$|r(u)| \le M_r \text{ при } |u| \le M_p + M_f, \quad |s(v)| \le M_s \text{ при } |v| \le M_w + M_r.$$

Тогда $|z| \le M_s$ при $\alpha_1 \le t \le \alpha_2,\ \beta_1 \le x \le \beta_2$. Пусть N_s – это минимум $|s'(v)|$ при $|v| \le M_w + M_r$, а N_r – это минимум $|r'(u)|$ при $|u| \le M_p + M_f$.

Пусть в результате ошибок при формировании и передаче сообщения z трансформировалось в $\tilde{z} = z + \delta z$. Соответственно, $\Psi(K, z+\delta z) =$

$f + \delta f = \tilde{f}$. Тогда

$$|\delta f| = |r^{-1}(s^{-1}(z(x,t) + \delta z(x,t)) - w) - r^{-1}(s^{-1}(z(x,t)) - w)| \leq$$
$$\frac{1}{N_r} |s^{-1}(z(x,t) + \delta z(x,t)) - s^{-1}(z(x,t))| \leq \frac{1}{N_r N_s} |\delta z(x,t)|.$$

Заметим, что f не зависит от x, чего нельзя сказать о $\tilde{f}$.

Приведенная схема кодирования-декодирования использует ключ K, которым пользуются оба участника. Отправитель для кодирования, получатель – для декодирования. В отсутствие ключа задача декодирования (задача декомпозиции функции 2-го класса) становится очень трудной.

Это весьма гибкая конструкция, и у нас имеется много возможностей для ее усложнения и модификации. От схемы композиции функций из класса Cl^2, мы можем перейти к схеме, основанной на представлении функции из Cl^n (ключ – это $2\,(2^n - 1)$ функций одного переменного). Или же к $Cl(S)$ для произвольной схемы композиции S.

В более общей ситуации конструкция выглядит следующим образом. Выбираем одну из функций, которые находятся на самом нижнем уровне композиции (функция от t), и резервируем ее для передаваемого сигнала $F(t)$ (точнее, его аналитического приближения $f(t)$). Фиксируем все остальные аналитические функции одного переменного, необходимые для построения композиции со схемой S, выбирая функции достаточно общего положения, т.е. ключ K. Получаем оператор кодирования $f(t) \to \Phi(S, K, f)(x,t) = z(x,t)$. Оператор декодирования $z(x,t) \to \Psi(S, K, z)(t) = f(t)$ строится аналогично тому, что мы описали выше для Cl^2. Декодирование осуществляется путем пошагового уменьшения сложности композиции. При этом естественно возникают операторы декодирования для выражений меньшей сложности, которые используют части нашего ключа. При построении оператора Ψ используются обращения некоторых функций, входящих в ключ. Поэтому при формировании ключа мы накладываем условие их монотонности.

Еще одно направление обобщения конструкции связано с использованием иерархий сложности для функций не двух, а бóльшего числа переменных [7]. Для функций трех переменных можно рассмотреть две задачи: вопрос о представимости суперпозициями функций одного переменного и сложения (суперпозиции (3) $\to$ (1)) или о представимости

суперпозициями функций двух переменных (суперпозиции (3) $\to$ (2)). Давайте встанем на вторую точку зрения, и пусть теперь $\mathcal{A}$ – это пучок ростков аналитических функций двух переменных. Рассмотрим иерархию классов аналитических функций трех переменных $w = g(x, y, z)$, определяемых индуктивно:

$$Cl^0 = \{a(x, y) \text{ или } b(y, z) \text{ или } c(z, x), \quad a, b, c \in \mathcal{A}\},$$
$$Cl^{n+1} = \{w(x, y, z) = c(A_n(x, y, z), B_n(x, y, z)),\ A_n, B_n \in Cl^n, c \in \mathcal{A}\}.$$

Задача идентификации для Cl^2 весьма сложна. Это можно использовать для схемы кодирования 2-мерного сигнала (изображения) $f(t, s)$.

Общаяя схема композиции функции $w \in Cl^2$ использует семь функций двух переменных. Каждая из четырех функций нижнего уровня зависит от каких-то двух переменных из набора (x, t, s), необходимо уточнить каких. Фиксируем этот выбор, например, так:

$$w(x, t, s) = \varphi(a, b, c, p, f, r, s)(x, t) = s(c(a(x, t), b(x, s)), r(p(x, s), f(t, s))),$$

Резервируем одну из функций нижнего уровня под наш сигнал, а оставшиеся шесть фиксируем и объявляем ключом K. Таким образом, мы получаем преобразование

$$f(t, s) \to \Phi(K, f)(x, t, s) = s(c(a(x, t), b(x, s)), r(p(x, s), f(t, s))) = w(x, t, s).$$

Для обратимости преобразования (аналог монотонности) мы должны иметь два ключа (K, K'). Причем каждая из трех пар функций (s, s') и (r, r') должна определять глобально обратимое преобразование $\mathbf{R}^2$. Кодирование

$$f(t, s) \to (\Phi(K, f)(x, t, s), \Phi(K', f)(x, t, s)) = (w_1(x, t, s), w_2(x, t, s)),$$

т.е. к получателю отправляются $(w_1(x, t, s), w_2(x, t, s))$. Декодирование осуществляется с помощью отображений $\mathbf{R}^2$, обратных к $(s(u, v), s'(u, v))$ и $(r(u, v), r'(u, v))$. Отметим, что эта конструкция позволяет за один сеанс передавать два закодированных изображения: f с помощью K и h с помощью K'. Но равенство $h = f$ не мешает процедуре. Также можно отметить, что в качестве f может быть передана функция одного переменного $f(t)$.

Дальнейшее усложнение конструкции можно получить, рассматривая иерархии, связанные с задачей суперпозиций вида $(k) \to (l)$, где $k > l$ (разложение функций от k переменных в суперпозиции функций l переменных).

Приведем аргументы в пользу того, что схема шифрования с помощью функций из Cl^2 от двух переменных *недоступна для декодирования с помощью квантового компьютера*, т.е. вычислительной системы построенной из кубитов [8]. Состояние одного кубита описывается комплекснозначной функцией времени t, принимающей значения на единичной окружности комплексной плоскости, т.е. $\exp(i\,\nu(t))$. Это функция одного переменного. Квантовая суперпозиция – это переход к линейной комбинации. Пусть имеется вычислительное устройство, которое в качестве простых базовых операций допускает набор из четырех арифметических операций, выполняет все (аналитические) функции одного переменного, а также аналитические операции над ними (суперпозицию, дифференцирование и интегрирование). Такое устройство, как представляется, мажорирует квантовый компьютер. Приведенная в [2] демонстрация направлена на то, чтобы показать, что задача построения декомпозиции для функции из Cl^2 (в отсутствии ключа), по-видимому, недоступна даже для такого мощного устройства.

Конечно, если представить себе, что успехи физических наук приведут к тому, что вместо кубита будет предложена единица, состояние которой – это функция не одной, а двух переменных, и также будет предложен аппарат для свободного манипулирования с системой таких единиц, то наша аргументация к такой вычислительной машине не применима. Тогда потребуется схема кодирования (рассмотренная нами выше), основанная на сложности задачи идентификации Cl^2 для функций трех переменных.

Список литературы

[1] Valery K. Beloshapka, “Decomposition of functions of finite analytical complexity”, Журн. СФУ. Сер. Матем. и физ., 11:6 (2018), 680–685.

[2] В. К. Белошапка, “О сложности дифференциально-алгебраического описания классов аналитической сложности”, Матем. заметки, 105:3 (2019), 323–331; Math. Notes, 105:3 (2019), 309–315

[3] Введение в криптографию. Под ред.В.В.Ященко, МЦНМО – ЧеРо, Москва, 1998. — 273 с.

[4] А. Н. Колмогоров, “Три подхода к определению понятия “количество информации””, Пробл. передачи информ., 1:1 (1965), 3–11

[5] L.Blum, M.Shub, S.Smale "On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines". Bull. Amer. Math. Soc. New Series. v.21 (1), 1989, p.1–46.

[6] Котельников В. А. О пропускной способности «эфира» и проволоки в электросвязи, Материалы к I съезду по вопросам технической реконструкции дела связи и развития слаботочной промышленности, 1933 // Успехи физических наук : Журнал. — 2006. — № 7. — С. 762—770.

[7] В. К. Белошапка, Аналитическая сложность функций многих переменных // Математические заметки, том 100, выпуск 6, декабрь 2016, стр. 795-803.

[8] Китаев А., Шень А., Вялый М, Классические и квантовые вычисления, МЦНМО, ISBN: 5-900916-35-9, 1999, 192 с.