УДК 004.056.5

В. П. Цветов

НЕКОРРЕКТНЫЕ ЗАДАЧИ И ЗАЩИТА ДАННЫХ

По Адамару корректно поставленная задача обладает свойствами существования, единственности и устойчивости своего решения. Некорректные задачи не обладают хотя бы одним из перечисленных свойств, чаще всего свойством устойчивости решения относительно начальных данных. Решение подобных задач чувствительно даже к небольшому изменению значений входных параметров, что не позволяет гарантировать приемлемое приближение к точному решению на уровне существующей погрешности в измерении начальных значений. В статье рассматривается применение эффекта неустойчивости для синтеза криптографических преобразований, использующих естественные шумы в каналах передачи данных.

Well posed (by Hadamard) problem has properties of existence, uniqueness and stability of its solution. Ill posed problems do not have at least one of the above properties, often this is the stability property of the solution with respect to initial conditions. The solution of such problems is sensitive even to a small change in the values of the input data, and so we do not guarantee an acceptable approximation to the answer at the level of the existing error in the measurement of initial values. The paper discusses the use of the instability effect for the synthesis of cryptographic transformations using natural noise in radio channels.

Ключевые слова: некорректные задачи, криптографическая защита информации.

Keywords: ill posed problem, secure cryptographic systems.

Введение

Понятие корректно поставленной задачи было сформулировано Ж. Адамаром в 1902 г. для дифференциальных уравнений [1]. Им же был приведен пример некорректной постановки задачи Коши для уравнения Лапласа. В операторной форме критерий корректной постановки задачи определяется следующим образом.

Пусть $\langle X, \rho_X \rangle$ и $\langle Y, \rho_Y \rangle$ – два метрических пространства и $A : X \mapsto Y$ – определенный на них оператор. $Dom(A)$ и $Im(A)$ - область определения и множество значений оператора A соответственно, и $X' \subseteq Dom(A)$, $Y' \subseteq Im(A)$. Задача нахождения решения уравнения

$$A(x) = y \tag{1}$$

Вестник Балтийского федерального университета им. И. Канта.
Сер.: Физико-математические и технические науки. 2019. № 4. С. 86 – 93.

считается поставленной корректно (по Адамару) на паре пространств $\langle X', \rho_X \rangle$ и $\langle Y', \rho_Y \rangle$, если

1) решение $x \in X' \subseteq Dom(A) \subseteq X$ существует для любого значения $y \in Y' \subseteq Im(A) \subseteq Y$;

2) решение единственно, то есть если $A(x') = A(x'')$, то $x' = x''$;

3) решение устойчиво относительно изменений правой части, то есть если для каждого вещественного числа $\varepsilon > 0$ существует такое вещественное число $\delta > 0$, что $\rho_X(x', x'') < \varepsilon$ как только $\rho_Y(y', y'') < \delta$, где $y' = A(x') \in Y', y'' = A(x'') \in Y'$.

Условия 1, 2 означают существование обратного оператора $A^{-1} : Y' \mapsto X'$, а условие 3 — возможность его непрерывного продолжения на замыкание множества Y' в случае полноты пространств $\langle X, \rho_X \rangle$ и $\langle Y, \rho_Y \rangle$.

Если хотя бы одно из условий нарушается, то задача нахождения решения уравнения (1) считается некорректно поставленной или некорректной. В частности, некорректна задача решения уравнения (1) с вполне непрерывным линейным оператором $A : X \mapsto X$, тотально определенным на бесконечномерном сепарабельном гильбертовом пространстве $\langle X, \langle \cdot, \cdot \rangle_X \rangle$.

Напомним, следуя [2], что гильбертовым пространством называется линейное векторное пространство (над полем вещественных или комплексных чисел) со скалярным произведением, полное относительно метрики (нормы):

$$\rho_X(x', x'') = \|x' - x''\|_X = \sqrt{\langle x' - x'', x' - x'' \rangle_X}. \qquad (2)$$

Полнота метрического пространства $\langle X, \rho_X \rangle$ означает существование предела любой фундаментальной последовательности $\{x_n\}_{n=1}^{\infty}$, а сепарабельность — существование счетного всюду плотного подмножества $X' \subseteq X$.

Оператор $A : X \mapsto Y$ называется вполне непрерывным, если он непрерывен и компактен, то есть отображает всякое ограниченное подмножество множества X в относительно компактное подмножество множества Y. Подмножество $X' \subset X$ называется относительно компактным, если его замыкание компактно, то есть если из любой последовательности $\{x_n\}_{n=1}^{\infty} \subseteq X'$ можно выделить подпоследовательность $\{x_{n_k}\}_{k=1}^{\infty} \subseteq X'$, сходящуюся к некоторой точке $x_0 \in X$ по метрике ρ_X.

В любом сепарабельном гильбертовом пространстве существует счетный ортонормированный базис, то есть такая система попарно различных ненулевых векторов $\{e_n\}_{n=1}^{\infty}$, что $\langle e_i, e_j \rangle_X = 0$ в случае, если $i \neq j$, и $\|e_i\|_X^2 = \langle e_i, e_i \rangle_X = 1$, через которую любой вектор $x \in X$ может

быть представлен в виде ряда $x = \sum_{n=1}^{\infty} \langle x, e_n \rangle_X \cdot e_n$, сходящегося в смысле метрики (2). Понятно, если $i \neq j$, то $\rho_X(e_i, e_j) = \sqrt{2}$, а множество $\{e_n\}_{n=1}^{\infty} \subseteq S(0,1) = \{x \mid x \in X \wedge \rho_X(0,x) = \|x\|_X = 1\} \subseteq X$ ограничено.

Если оператор $A : X \mapsto Y$ тотален, вполне непрерывен и обратим, то из последовательности $\{A(e_n)\}_{n=1}^{\infty} \subseteq Y$ можно выделить подпоследовательность $\{A(e_{n_k})\}_{k=1}^{\infty}$, сходящуюся к некоторой точке $y_0 \in Y$. Обозначим $y_k = A(e_{n_k})$. В силу фундаментальности последовательности $\{y_k\}_{k=1}^{\infty}$ для всякого $\delta > 0$ будут существовать значения k' и k'', для которых $\rho_Y(y_{k'}, y_{k''}) < \delta$, однако $\rho_X(e_{n_{k'}}, e_{n_{k''}}) = \sqrt{2}$. Таким образом, в данном случае задача решения уравнения (1) неустойчива, то есть некорректна по Адамару.

В случае нормированных линейных векторных пространств $\langle X, \|\cdot\|_X \rangle$ и $\langle Y, \|\cdot\|_Y \rangle$ рассматривают нормированные линейные векторные пространства определенных на них непрерывных тотальных линейных операторов $\langle \mathfrak{B}(X,Y), \|\cdot\|_{\mathfrak{B}(X,Y)} \rangle$, где $\|A\|_{\mathfrak{B}(X,Y)} = \sup_{x \in X} \frac{\|A(x)\|_Y}{\|x\|_X}$. По определению $\|A(x)\|_Y \leq \|A\|_{\mathfrak{B}(X,Y)} \cdot \|x\|_X$. Непрерывные линейные операторы также называют ограниченными, поскольку только для них существует конечное значение нормы $\|\cdot\|_{\mathfrak{B}(X,Y)}$.

В общем случае $\langle Dom(A), \|\cdot\|_X \rangle$ и $\langle Im(A), \|\cdot\|_Y \rangle$ являются подпространствами нормированных линейных векторных пространств $\langle X, \|\cdot\|_X \rangle$ и $\langle Y, \|\cdot\|_Y \rangle$ соответственно. Если $Dom(A)$ конечномерно, то и $Im(A)$ конечномерно, при этом $\dim(Im(A)) \leq \dim(Dom(A))$, а линейный оператор A обратим только и только в случае выполнения равенства $\dim(Im(A)) = \dim(Dom(A))$. Операторы, действующие в конечномерных пространствах, называются конечномерными. Все линейные конечномерные операторы ограничены (непрерывны).

Операторная норма $\|\cdot\|_{\mathfrak{B}(X,Y)}$ удобна для оценки зависимости погрешности решения уравнения (1) от погрешности его правой части. Наряду с (1) рассмотрим уравнение

$$A(x') = y' = y + \delta y \in Im(A). \qquad (1')$$

Обозначим $\delta x = x' - x$ и, вычитая из (1′) исходное уравнение (1), получим $A(\delta x) = \delta y$ или, в предположении существования непрерывного обратного к оператору A, $\delta x = A^{-1}(\delta y)$.

С учетом оценок

$\|\delta x\|_X = \|A^{-1}(\delta y)\|_X \le \|A^{-1}\|_{\mathfrak{B}(Im(A),X)} \cdot \|\delta y\|_Y$ и $\|y\|_Y = \|A(x)\|_Y \le \|A\|_{\mathfrak{B}(X,Y)} \cdot \|x\|_X$ получаем

$$\frac{\|\delta x\|_X}{\|x\|_X} \le \|A\|_{\mathfrak{B}(X,Y)} \cdot \|A^{-1}\|_{\mathfrak{B}(Im(A),X)} \cdot \frac{\|\delta y\|_Y}{\|y\|_Y}. \quad (3)$$

Таким образом, относительная погрешность решения уравнения (1) определяется через относительную погрешность его правой части при помощи константы $\mu(A) = \|A\|_{\mathfrak{B}(X,Y)} \cdot \|A^{-1}\|_{\mathfrak{B}(Im(A),X)}$, которая называется числом обусловленности непрерывного линейного оператора A. Если оператор A^{-1} не непрерывен (не ограничен), как, например, в случае вполне непрерывного оператора A в бесконечномерном гильбертовом пространстве, то полагают $\mu(A) = \infty$.

Если $\mu(A) = \infty$, то задача решения уравнения (1) становится неустойчивой и малым вариациям правой части $\|\delta y\|_Y$ могут соответствовать сколь угодно большие вариации решения $\|\delta x\|_X$.

Модель канала связи и кодирование сообщений

В качестве модели канала передачи сигналов рассмотрим бесконечномерное сепарабельное гильбертово пространство $\langle X, \langle\cdot,\cdot\rangle_X \rangle$ с ортонормированным базисом $\{e_n\}_{n=1}^{\infty}$ и аддитивное преобразование

$$T(x,\xi) = x + \xi,$$

где $x \in X$, а ξ - случайное отображение со значениями в шаре $B(0,\varepsilon) = \{x \mid \|x\|_X < \varepsilon\} \subseteq X$. Модель описывает технологии, применяемые в современной радиосвязи, и учитывает наличие естественных и искусственных шумов в радиоканалах [3].

Рассмотрим алфавит $\mathcal{A} = \{\alpha_1, \alpha_2, .., \alpha_m\}$ мощности $|\mathcal{A}| = m$ и множество сообщений $W_N = \mathcal{A}^N = \{w = \alpha_{i_1}\alpha_{i_2}...\alpha_{i_N} \mid k \in 1..N \wedge i_k \in 1..m \wedge \alpha_{i_k} \in \mathcal{A}\}$ фиксированной длины *N*. Понятно, что мощность $|W| = m^N$.

1. Кодирование сообщений. Определим множество

$$C_N = \left\{ \tilde{i} = \frac{1}{m} \cdot [i_1, .., i_N] \mid k \in 1..N \wedge i_k \in 1..m \right\}$$

и тотальную биекцию $F_1 : W_N \mapsto C_N$, полагая

$$F_1(w) = F_1(\alpha_{i_1}\alpha_{i_2}...\alpha_{i_N}) = \frac{1}{m} \cdot [i_1, .., i_N] = \tilde{i} \in C_N.$$

Обозначим как $X_N \subset X$ линейную оболочку множества базисных векторов $\{e_n\}_{n=1}^N$. Определим тотальную инъекцию $F_2 : C_N \mapsto X_N$, полагая $F_2\left(\tilde{i}\right) = F_2\left(F_1\left(\alpha_{i_1}\alpha_{i_2}...\alpha_{i_N}\right)\right) = \sum_{n=1}^{N} \frac{i_n}{m} \cdot e_n = \tilde{x}_w \in X_N$.

Понятно, что $\min_{w \in W} \|\tilde{x}_w\|_X = \min_{w', w'' \in W \wedge w' \neq w''} \|\tilde{x}_{w'} - \tilde{x}_{w''}\|_X = \frac{1}{m}$ и одновременно $\max_{w \in W} \|\tilde{x}_w\|_X = \max_{w', w'' \in W} \|\tilde{x}_{w'} - \tilde{x}_{w''}\|_X = \sqrt{N}$.

Обозначим $X_N^{\perp}$ - ортогональное дополнение X_N. Рассмотрим факторпространство $X / X_N^{\perp}$. По построению каждый класс эквивалентности содержит единственный вектор $\tilde{x} \in X_N$, поэтому $[\tilde{x}'] \cap [\tilde{x}''] = \varnothing$, если $\tilde{x}' \neq \tilde{x}''$. Кодом сообщения $w \in W$ будем считать произвольный вектор $x_w \in [\tilde{x}_w]$.

2. Декодирование сообщений. Поскольку $x_w = \tilde{x}_w + x^{\perp}$, где $x^{\perp} \in X_N^{\perp}$, то $\tilde{x}_w = P_{X_N}\left(x_w\right) = \sum_{n=1}^{N} \langle x_w, e_n \rangle_X \cdot e_n$, где $P_{X_N} : X \mapsto X_N$ - проектор на X_N.

Таким образом, алгоритм декодирования сообщения $w \in W_N$ по его коду $x_w \in [\tilde{x}_w]$ задается формулой $w = F_1^{-1}\left(F_2^{-1}\left(P_{X_N}\left(x_w\right)\right)\right)$.

3. Модель канала. Под передачей сигнала с сообщением w по каналу связи с шумами будем понимать преобразование кода $T\left(x_w, \xi\right) = \tilde{x}_w + x^{\perp} + \xi$. В силу ранее сказанного

$$P_{X_N}\left(T\left(x_w, \xi\right)\right) = P_{X_N}\left(\tilde{x}_w + x^{\perp} + \xi\right) = \tilde{x}_w + P_{X_N}\left(\xi\right), \tag{4}$$

где $\left\|P_{X_N}\left(\xi\right)\right\|_X = \left\|\sum_{n=1}^{N} \langle \xi, e_n \rangle_X \cdot e_n\right\|_X = \sqrt{\sum_{n=1}^{N} \langle \xi, e_n \rangle_X^2} \leq \sqrt{\sum_{n=1}^{\infty} \langle \xi, e_n \rangle_X^2} = \|\xi\|_X < \varepsilon$.

4. Декодирование на фоне шумов. В случае $\varepsilon < \frac{1}{2m}$ для определения $\tilde{x}_w$ по принятому зашумленному сигналу $\theta = T\left(x_w, \xi\right)$ достаточно использовать критерий «ближайшего соседа» $\tilde{x}_w = \arg \min_{x \in F_2(C_N)} \left\|P_{X_N}\left(\theta\right) - x\right\|_X$, где $F_2\left(C_N\right) \subset X_N$ - образ C_N при действии F_2.

Таким образом, алгоритм декодирования сообщения $w \in W_N$ по его зашумленному сигналу $\theta = T\left(x_w, \xi\right)$ задается формулой

$$w = F_1^{-1}\left(F_2^{-1}\left(\arg \min_{x \in F_2(C_N)} \left\|P_{X_N}\left(\theta\right) - x\right\|_X\right)\right).$$

Рассмотренный способ кодирования можно трактовать как криптографическое преобразование исходного сообщения $w \in W$, в котором секретом является базис $\{e_n\}_{n=1}^N$ подпространства $X_N \subset X$, а подпро-

странство $X_N^{\perp}$ используется для противодействия методам частотного анализа шифротекста $x_w = \tilde{x}_w + x^{\perp}$ за счет возможности произвольной вариации вектора $x^{\perp} \in X_N^{\perp}$.

Шифрование сообщений

Перейдем к изучению случая, когда подпространство X_N известно и не является секретом как, например, в ситуации с известным рабочим диапазоном частот. Рассмотрим вполне непрерывный линейный обратимый оператор $A : X \mapsto X$ и его сужение A_N на подпространство X_N. Как уже отмечалось выше, оператор $A_N : X_N \mapsto X$ конечномерен и $\dim\left(Im(A_N)\right) = \dim\left(X_N\right) = N$.

1. Криптографическое преобразование в канале без шумов. Как и ранее, поставим в соответствие сообщению $w \in W$ вектор $\tilde{x}_w = F_2\left(F_1\left(w\right)\right)$. Зафиксируем некоторый вектор $x_0^{\perp} \in X_N^{\perp}$, положим $x_w = \tilde{x}_w + x_0^{\perp}$ и определим криптографическое преобразование $y_w = A\left(x_w\right)$. Понятно, что обратное криптографическое преобразование задается формулой

$$P_{X_N}\left(A^{-1}\left(y_w\right)\right) = P_{X_N}\left(x_w\right) = P_{X_N}\left(\tilde{x}_w + x_0^{\perp}\right) = \tilde{x}_w, \qquad (5)$$

а декодирование сообщения проводится на основании пункта 2 предыдущего раздела. Очевидно, (5) справедливо для произвольных $x_0^{\perp} \in X_N^{\perp}$.

Под передачей сигнала с зашифрованным сообщением w по каналу связи с шумами будем понимать преобразование $T\left(y_w, \xi\right) = A\left(x_w\right) + \xi$. В силу вполне непрерывности оператора A задача решения уравнения

$$A\left(x'_w\right) = y'_w = T\left(y_w, \xi\right) = y_w + \xi = A\left(x_w\right) + \xi, \qquad (6)$$

будет неустойчива относительно изменений правой части, и ее решение x'_w может значительно отличаться от значения x_w так же, как и значение $P_{X_N}\left(x'_w\right)$ от значения $\tilde{x}_w$. Таким образом, обратное криптографическое преобразование (5), примененное непосредственно к зашумленному сигналу $y'_w = T\left(y_w, \xi\right) = A\left(x_w\right) + \xi$, будет приводить к систематическим ошибкам декодирования на приемной стороне.

2. Криптографическое преобразование в канале с шумами. Указанное свойство оператора $A : X \mapsto X$ не позволяет непосредственно использовать его для шифрования сообщений в каналах с шумами, однако оно оказывается полезным в качестве средства защиты от перехвата даже в том случае, когда атакующему становится известен секрет $\left\langle \left\{e_n\right\}_{n=1}^{N}, A \right\rangle$. Рассмотрим следующую криптографическую схему.

Обозначим $P_{Im(A_N)} : X \mapsto Im(A_N)$ - проектор на $Im(A_N)$. По аналогии с предыдущим,

$$P_{Im(A_N)}\left(T\left(y_w,\xi\right)-A\left(x_0^{\perp}\right)\right)=P_{Im(A_N)}\left(A\left(\tilde{x}_w\right)\right)+P_{Im(A_N)}\left(\xi\right)= \\ =A_N\left(\tilde{x}_w\right)+P_{Im(A_N)}\left(\xi\right) \quad (7)$$

где, как и ранее, $\left\|P_{Im(A_N)}\left(\xi\right)\right\|_X \le \left\|\xi\right\|_X < \varepsilon$.

Запишем (7) в виде

$$A_N\left(\tilde{x}'_w\right)=A_N\left(\tilde{x}_w+\delta\tilde{x}_w\right)=\tilde{y}_w+\delta\tilde{y}_w=\tilde{y}'_w, \quad (8)$$

где

$$\tilde{x}'_w=\tilde{x}_w+\delta\tilde{x}_w;\ \tilde{y}'_w=\tilde{y}_w+\delta\tilde{y}_w;\ \tilde{y}_w=A_N\left(\tilde{x}_w\right);$$
$$\delta\tilde{y}_w=P_{Im(A_N)}\left(T\left(y_w,\xi\right)-A\left(x_0^{\perp}\right)\right)-A_N\left(\tilde{x}_w\right);\ A_N\left(\delta\tilde{x}_w\right)=P_{Im(A_N)}\left(\xi\right).$$

Поскольку по построению оператор A_N имеет ограниченный обратный A_N^{-1}, то

$$\tilde{x}'_w=A_N^{-1}\left(\tilde{y}'_w\right). \quad (9)$$

Кроме того, норма разности $\left\|\tilde{x}'_w-\tilde{x}_w\right\|_X$ будет удовлетворять неравенству

$$\left\|\tilde{x}'_w-\tilde{x}_w\right\|_X=\left\|\delta\tilde{x}_w\right\|_X=\left\|A_N^{-1}\left(P_{Im(A_N)}\left(\xi\right)\right)\right\|_X \le \\ \le\left\|A_N^{-1}\right\|_{\mathfrak{B}\left(Im(A_N),X^N\right)}\cdot\left\|P_{Im(A_N)}\left(\xi\right)\right\|_X \le \\ \le\left\|A_N^{-1}\right\|_{\mathfrak{B}\left(Im(A_N),X^N\right)}\cdot\left\|\xi\right\|_X<\left\|A_N^{-1}\right\|_{\mathfrak{B}\left(Im(A_N),X^N\right)}\cdot\varepsilon \quad (10)$$

Принимая во внимание (9) и (10), делаем заключение: если $\varepsilon<\dfrac{1}{2m\left\|A_N^{-1}\right\|_{\mathfrak{B}\left(Im(A_N),X^N\right)}}$, то для определения $\tilde{x}_w$ по принятому зашумленному и зашифрованному сигналу применим критерий «ближайшего соседа» $\tilde{x}_w=\arg\min\limits_{x\in F_2(C_N)}\left\|A_N^{-1}\left(P_{Im(A_N)}\left(T\left(y_w,\xi\right)-A\left(x_0^{\perp}\right)\right)\right)-x\right\|_X$ и, следовательно, $w=F_1^{-1}\left(F_2^{-1}\left(\tilde{x}_w\right)\right)$.

Предложенная схема использует в качестве секрета только вектор $x_0^{\perp}\in X_N^{\perp}$, а естественные шумы канала усиливают ее криптостойкость за счет неустойчивости алгоритма шифрования.

Выводы

В статье рассмотрен способ организации криптозащищенного радиоканала связи, одним из элементов которого являются естественные или наведенные помехи. Способ опирается на неустойчивость задачи решения операторных уравнений первого рода с вполне непрерывным линейным оператором. Наиболее простой вид криптографическая схема будет принимать в случае самосопряженного вполне непрерывного

линейного оператора с проекторами на подпространства его собственных векторов, то есть в случае использования ортонормированного базиса $\{e_n\}_{n=1}^{\infty}$, где $A(e_n) = \lambda_n \cdot e_n$.

Для численных реализаций следует использовать конечномерные обратимые (матричные) операторы с большим числом обусловленности $\mu(A)$ 1.

Список литературы

1. *Hadamard J.* Sur les probl`emes aux derivees partielles et leur signification physique // Bull. Univ. Princeton. 1902. Vol. 13. P. 49—52.

2. *Канторович Л.В., Акилов Г.П.* Функциональный анализ. М., 1984.

3. *Цветов В.П.* Об одной задаче декодирования символов по неполным данным в радиоканале // Сб. науч. тр. III Междунар. конф. и молодежной школы ИТНТ-2017. Самара, 2017. С. 954—957.

Об авторе

Виктор Петрович Цветов — канд. физ.-мат. наук, доц., Самарский национальный исследовательский университет им. академика С.П. Королева, Россия.
E-mail: tsf-su@mail.ru

The author

Dr Victor P. Tsvetov, Associate Professor, Samara University, Russia.
E-mail: tsf-su@mail.ru