

## МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УДК 512.54

### О coNP-ПОЛНОТЕ ЗАДАЧИ «ИНЪЕКТИВНЫЙ РЮКЗАК»

В. Г. Дурнев, О. В. Зеткина, А. И. Зеткина, Д. М. Мурин

*Ярославский государственный университет им. П. Г. Демидова, г. Ярославль, Россия*

Устанавливается coNP-полнота задачи «Инъективный рюкзак».

**Ключевые слова:** NP-полные и coNP-полные задачи, инъективный рюкзак, m-инъективный рюкзак.

DOI 10.17223/20710410/33/7

### ABOUT THE coNP-COMPLETE “INJECTIVE KNAPSACK” PROBLEM

V. G. Durnev, O. V. Zetkina, A. I. Zetkina, D. M. Murin

*P. G. Demidov Yaroslavl State University, Yaroslavl, Russia***E-mail:** durnev@uniyar.ac.ru, oks\_68@mail.ru, aizetkina@gmail.ru, nirum87@mail.ru

It is proved that the “Injective knapsack” problem is coNP-complete.

**Keywords:** NP-complete and coNP-complete problems, injective knapsack, m-injective knapsack.

#### 1. Задачи о рюкзаках

Хорошо известно [1–3], что «Проблема рюкзака», или «Проблема суммы элементов подмножеств», является NP-полной. Она может быть сформулирована как вопрос о разрешимости в числах 0, 1 уравнения вида

$$a_1x_1 + \dots + a_nx_n = b, \quad (1)$$

где  $a_1, \dots, a_n$  и  $b$  — произвольные натуральные числа;  $x_1, \dots, x_n$  — неизвестные.

В 1978 г. Р. Меркль и М. Хеллман [4] предложили первую (в открытых источниках) асимметричную систему шифрования, которая базировалась на «Проблеме рюкзака». Спустя четыре года А. Шамир показал, что метод генерации открытых ключей по закрытым в криптосистеме Меркля — Хеллмана не является надёжным и практически все индивидуальные представители «Проблемы рюкзака», возникающие при использовании этой системы, поддаются решению.

Несмотря на результаты А. Шамира, «Проблема рюкзака» обладает полезными для криптографии свойствами: во-первых, о ней известно, что она является достаточно сложной, и, во-вторых, процесс шифрования в криптосистеме Меркля — Хеллмана существенно быстрее, чем процесс шифрования в криптосистеме RSA, и представляется вероятным, что можно построить стойкие криптосистемы, основанные на «Проблеме рюкзака», с высокой скоростью шифрования и расшифрования, что является

крайне важным прикладным свойством, например для задачи синхронизации центров обработки данных по неконтролируемому (незащищённому) каналу связи. Благодаря этим свойствам работы по созданию криптосистем, базирующихся на «Проблеме рюкзака», не прекращаются [5–8].

В работе [7] введена в рассмотрение «Проблема обобщённого рюкзака», которая для фиксированного натурального числа  $m \geq 2$  состоит в ответе на вопрос, разрешимо ли уравнение (1) в числах  $0, 1, \dots, m-1$ .

В связи с шифрсистемой с открытым ключом, предложенной Р. Мерклем и М. Хелманом на основе «супервозрастающего» рюкзака, стали представлять особый интерес так называемые «Инъективные рюкзаки».

Будем говорить, что набор различных натуральных чисел  $a_1, \dots, a_n$  определяет «Инъективный рюкзак» (соответственно « $m$ -инъективный рюкзак»), если не существует двух различных наборов чисел  $0, 1$  (соответственно наборов чисел  $0, \dots, m-1$ , где натуральное число  $m \geq 2$ )  $\alpha_1, \dots, \alpha_n$  и  $\beta_1, \dots, \beta_n$ , таких, что

$$a_1\alpha_1 + \dots + a_n\alpha_n = a_1\beta_1 + \dots + a_n\beta_n.$$

В противном случае набор натуральных чисел  $a_1, \dots, a_n$  определяет «Неинъективный рюкзак» (соответственно « $m$ -неинъективный рюкзак»).

#### **Задача «Инъективный рюкзак»**

Дано: набор различных натуральных чисел  $a_1, \dots, a_n$ .

Определить: является ли определяемый ими рюкзак инъективным.

#### **Задача «Неинъективный рюкзак»**

Дано: набор различных натуральных чисел  $a_1, \dots, a_n$ .

Определить: является ли определяемый ими рюкзак неинъективным.

#### **Задача « $m$ -инъективный рюкзак»**

Дано: набор различных натуральных чисел  $a_1, \dots, a_n$ , натуральное число  $m \geq 2$ .

Определить: является ли определяемый числами  $a_1, \dots, a_n$  рюкзак  $m$ -инъективным.

#### **Задача « $m$ -неинъективный рюкзак»**

Дано: набор различных натуральных чисел  $a_1, \dots, a_n$ , натуральное число  $m \geq 2$ .

Определить: является ли определяемый числами  $a_1, \dots, a_n$  рюкзак  $m$ -неинъективным.

Очевидно, что задача «2-инъективный рюкзак» эквивалентна задаче «Инъективный рюкзак», поэтому задача « $m$ -инъективный рюкзак» включает в себя задачу «Инъективный рюкзак».

Ясно, что задача «Неинъективный рюкзак» является дополнением задачи «Инъективный рюкзак» и принадлежит классу NP. Аналогично задача « $m$ -неинъективный рюкзак» является дополнением задачи « $m$ -инъективный рюкзак» и, в силу включения задачи «Неинъективный рюкзак», принадлежит классу NP.

## **2. Теорема о coNP-полноте задачи «Инъективный рюкзак»**

**Теорема 1.** Задача «Инъективный рюкзак» является coNP-полной.

**Доказательство.** Необходимо доказать, что задача «Неинъективный рюкзак» (дополнение задачи «Инъективный рюкзак») является NP-полной. Так как она принадлежит классу NP, то остаётся доказать её NP-трудность. Для этого достаточно установить полиномиальную сводимость к ней некоторой подходящей NP-полной задачи. В качестве таковой возьмём задачу о разрешимости в числах  $0, 1$  уравнения вида

$$2(a_1x_1 + \dots + a_nx_n) = \sum_{i=1}^n a_i, \quad (2)$$

где  $a_1, \dots, a_n$  — произвольные натуральные числа. Эта задача хорошо известна под названием «Разбиение». Столь же хорошо известна и её NP-полнота. При построении полиномиальной сводимости воспользуемся некоторыми идеями работы [9], с которой нас любезно познакомил М. В. Волков.

По коэффициентам уравнения (2) по аналогии с работой [9] построим последовательность из  $3n$  натуральных чисел

$$\bar{a}_1, \dots, \bar{a}_n, b_1, \dots, b_n, c_1, \dots, c_n, \quad (3)$$

полагая

$$\begin{aligned} \bar{a}_i &= a_i \cdot 10^{2n} + 10^{n+i-1} + 10^{i-1} \quad \text{для } i = 1, \dots, n, \\ b_i &= 10^{n+i-1} + 10^i \quad \text{для } i = 1, \dots, n-1, \\ b_n &= 10^{2n-1} + 1, \\ c_i &= 2 \cdot 10^{i-1} \quad \text{для } i = 1, \dots, n. \end{aligned}$$

Покажем, что уравнение (2) имеет решение в числах 0, 1 тогда и только тогда, когда натуральные числа (3) образуют «Неинъективный рюкзак». Рассмотрим функцию

$$f(x_1, \dots, x_n, y_1, \dots, y_n, z_1, \dots, z_n) = \bar{a}_1 x_1 + \dots + \bar{a}_n x_n + b_1 y_1 + \dots + b_n y_n + c_1 z_1 + \dots + c_n z_n.$$

Для произвольных десятичных цифр  $d_1, \dots, d_k$  через  $\overline{d_k \dots d_{10}}$ , как обычно, будем обозначать число

$$d_k \cdot 10^{k-1} + \dots + d_2 \cdot 10 + d_1.$$

Рассмотрим  $f$  как отображение множества  $\{0, 1\}^{3n}$  в множество натуральных чисел. Тогда натуральные числа (3) задают «Неинъективный рюкзак» в том и только в том случае, когда это отображение не является инъективным.

Нетрудно понять, что для произвольных чисел  $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n, \gamma_1, \dots, \gamma_n$  из множества  $\{0, 1\}$  справедливо равенство

$$\begin{aligned} f(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n, \gamma_1, \dots, \gamma_n) &= (a_1 \alpha_1 + \dots + a_n \alpha_n) 10^{2n} + \overline{(\beta_n + \alpha_n) \dots (\beta_1 + \alpha_1)}_{10} \cdot 10^n + \\ &+ \overline{(\beta_{n-1} + \alpha_n + 2\gamma_n)(\beta_{n-2} + \alpha_{n-1} + 2\gamma_{n-1}) \dots (\beta_1 + \alpha_2 + 2\gamma_2)(\beta_n + \alpha_1 + 2\gamma_1)}_{10}. \end{aligned}$$

Поэтому для произвольных чисел  $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n, \gamma_1, \dots, \gamma_n, \alpha'_1, \dots, \alpha'_n, \beta'_1, \dots, \beta'_n, \gamma'_1, \dots, \gamma'_n$  из множества  $\{0, 1\}$  равенство

$$f(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n, \gamma_1, \dots, \gamma_n) = f(\alpha'_1, \dots, \alpha'_n, \beta'_1, \dots, \beta'_n, \gamma'_1, \dots, \gamma'_n)$$

равносильно системе равенств

$$\left\{ \begin{aligned} a_1 \alpha_1 + \dots + a_n \alpha_n &= a_1 \alpha'_1 + \dots + a_n \alpha'_n, \\ \beta_n + \alpha_n &= \beta'_n + \alpha'_n, \\ \beta_{n-1} + \alpha_{n-1} &= \beta'_{n-1} + \alpha'_{n-1}, \\ &\dots \\ \beta_2 + \alpha_2 &= \beta'_2 + \alpha'_2, \\ \beta_1 + \alpha_1 &= \beta'_1 + \alpha'_1, \\ \beta_{n-1} + \alpha_n + 2\gamma_n &= \beta'_{n-1} + \alpha'_n + 2\gamma'_n, \\ \beta_{n-2} + \alpha_{n-1} + 2\gamma_{n-1} &= \beta'_{n-2} + \alpha'_{n-1} + 2\gamma'_{n-1}, \\ &\dots \\ \beta_1 + \alpha_2 + 2\gamma_2 &= \beta'_1 + \alpha'_2 + 2\gamma'_2, \\ \beta_n + \alpha_1 + 2\gamma_1 &= \beta'_n + \alpha'_1 + 2\gamma'_1. \end{aligned} \right.$$

Предположим, что уравнение (2) имеет решение  $\alpha_1, \dots, \alpha_n$  в числах 0, 1. Покажем, что найдутся такие числа  $\beta_1, \dots, \beta_n, \gamma_1, \dots, \gamma_n, \alpha'_1, \dots, \alpha'_n, \beta'_1, \dots, \beta'_n, \gamma'_1, \dots, \gamma'_n \in \{0, 1\}$ , которые нарушают инъективность рюкзака (3), т. е. наборы

$$(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n, \gamma_1, \dots, \gamma_n) \quad \text{и} \quad (\alpha'_1, \dots, \alpha'_n, \beta'_1, \dots, \beta'_n, \gamma'_1, \dots, \gamma'_n)$$

различны, но выполняется равенство

$$f(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n, \gamma_1, \dots, \gamma_n) = f(\alpha'_1, \dots, \alpha'_n, \beta'_1, \dots, \beta'_n, \gamma'_1, \dots, \gamma'_n).$$

Уравнение (2) даёт равенство  $a_1\alpha_1 + \dots + a_n\alpha_n = a_1(1 - \alpha_1) + \dots + a_n(1 - \alpha_n)$ , поэтому в качестве чисел  $\alpha'_1, \dots, \alpha'_n$  можно взять  $1 - \alpha_1, \dots, 1 - \alpha_n$ . Тогда  $\alpha_i \neq \alpha'_i$  при произвольном  $i$ ,  $1 \leq i \leq n$ . Для нахождения чисел  $\beta_1, \dots, \beta_n, \gamma_1, \dots, \gamma_n, \beta'_1, \dots, \beta'_n, \gamma'_1, \dots, \gamma'_n$  получаем две системы

$$\left\{ \begin{array}{l} \beta_n + 2\alpha_n = 1 + \beta'_n, \\ \beta_{n-1} + 2\alpha_{n-1} = 1 + \beta'_{n-1}, \\ \dots \\ \beta_2 + 2\alpha_2 = 1 + \beta'_2, \\ \beta_1 + 2\alpha_1 = 1 + \beta'_1 \end{array} \right. \quad \text{и} \quad \left\{ \begin{array}{l} \beta_{n-1} + 2\alpha_n = 1 + \beta'_{n-1} + 2(\gamma_n - \gamma'_n), \\ \beta_{n-2} + 2\alpha_{n-1} = 1 + \beta'_{n-2} + 2(\gamma_{n-1} - \gamma'_{n-1}), \\ \dots \\ \beta_1 + 2\alpha_2 = 1 + \beta'_1 + 2(\gamma_2 - \gamma'_2), \\ \beta_n + 2\alpha_1 = 1 + \beta'_n + 2(\gamma_1 - \gamma'_1). \end{array} \right.$$

Из первой системы при произвольном  $i$ ,  $1 \leq i \leq n$ , получаем  $\beta_i - \beta'_i = 1 - 2\alpha_i$ . Правая часть этого равенства равна  $\pm 1$ , что позволяет при любом значении  $\alpha_i$  однозначно определить числа  $\beta_i$  и  $\beta'_i$ . При этом  $\beta_i - \beta'_i = \pm 1$ , поэтому  $\beta_i + \beta'_i = 1$ .

Для нахождения чисел  $\gamma_1, \dots, \gamma_n, \gamma'_1, \dots, \gamma'_n$  воспользуемся системой

$$\left\{ \begin{array}{l} \beta_{n-1} + 2\alpha_n = 1 + \beta'_{n-1} + 2(\gamma_n - \gamma'_n), \\ \beta_{n-2} + 2\alpha_{n-1} = 1 + \beta'_{n-2} + 2(\gamma_{n-1} - \gamma'_{n-1}), \\ \dots \\ \beta_1 + 2\alpha_2 = 1 + \beta'_1 + 2(\gamma_2 - \gamma'_2), \\ \beta_n + 2\alpha_1 = 1 + \beta'_n + 2(\gamma_1 - \gamma'_1). \end{array} \right.$$

При  $2 \leq i \leq n$  получаем равенство  $2(\gamma'_i - \gamma_i) = 2\alpha_i - (1 + (\beta_{i-1} - \beta'_{i-1}))$ . Так как  $\beta_i + \beta'_i = 1$ , то  $\gamma'_i - \gamma_i = \alpha_i - 1 + \beta_{i-1}$ . Это уравнение разрешимо при любых  $\alpha_i$  и  $\beta_{i-1}$ . Для нахождения  $\gamma_1$  и  $\gamma'_1$  воспользуемся уравнением  $\gamma'_1 - \gamma_1 = \alpha_1 - 1 + \beta_n$ .

Для доказательства обратного предположим, что для двух различных наборов  $\langle \alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n, \gamma_1, \dots, \gamma_n \rangle$  и  $\langle \alpha'_1, \dots, \alpha'_n, \beta'_1, \dots, \beta'_n, \gamma'_1, \dots, \gamma'_n \rangle$  чисел 0, 1 выполняется равенство

$$f(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n, \gamma_1, \dots, \gamma_n) = f(\alpha'_1, \dots, \alpha'_n, \beta'_1, \dots, \beta'_n, \gamma'_1, \dots, \gamma'_n).$$

Это даёт равенство  $a_1\alpha_1 + \dots + a_n\alpha_n = a_1\alpha'_1 + \dots + a_n\alpha'_n$  и две системы равенств

$$\left\{ \begin{array}{l} \beta_n + \alpha_n = \beta'_n + \alpha'_n, \\ \beta_{n-1} + \alpha_{n-1} = \beta'_{n-1} + \alpha'_{n-1}, \\ \dots \\ \beta_2 + \alpha_2 = \beta'_2 + \alpha'_2, \\ \beta_1 + \alpha_1 = \beta'_1 + \alpha'_1 \end{array} \right. \quad \text{и} \quad \left\{ \begin{array}{l} \beta_{n-1} + \alpha_n + 2\gamma_n = \beta'_{n-1} + \alpha'_n + 2\gamma'_n, \\ \beta_{n-2} + \alpha_{n-1} + 2\gamma_{n-1} = \beta'_{n-2} + \alpha'_{n-1} + 2\gamma'_{n-1}, \\ \dots \\ \beta_1 + \alpha_2 + 2\gamma_2 = \beta'_1 + \alpha'_2 + 2\gamma'_2, \\ \beta_n + \alpha_1 + 2\gamma_1 = \beta'_n + \alpha'_1 + 2\gamma'_1, \end{array} \right.$$

которыми воспользуемся для доказательства равенств  $\alpha'_1 = 1 - \alpha_1, \dots, \alpha'_n = 1 - \alpha_n$ .

Перепишем эти системы в более наглядном виде:

$$\left\{ \begin{array}{l} \beta_n - \beta'_n = \alpha'_n - \alpha_n, \\ \beta_{n-1} - \beta'_{n-1} = \alpha'_{n-1} - \alpha_{n-1}, \\ \dots \\ \beta_2 - \beta'_2 = \alpha'_2 - \alpha_2, \\ \beta_1 - \beta'_1 = \alpha'_1 - \alpha_1 \end{array} \right. \quad \text{и} \quad \left\{ \begin{array}{l} (\beta_{n-1} - \beta'_{n-1}) + (\alpha_n - \alpha'_n) + 2(\gamma_n - \gamma'_n) = 0, \\ (\beta_{n-2} - \beta'_{n-2}) + (\alpha_{n-1} - \alpha'_{n-1}) + 2(\gamma_{n-1} - \gamma'_{n-1}) = 0, \\ \dots \\ (\beta_1 - \beta'_1) + (\alpha_2 - \alpha'_2) + 2(\gamma_2 - \gamma'_2) = 0, \\ (\beta_n - \beta'_n) + (\alpha_1 - \alpha'_1) + 2(\gamma_1 - \gamma'_1) = 0. \end{array} \right.$$

Предположим, что при некотором  $i$  выполняется равенство  $\alpha_i = \alpha'_i$ . Если  $i < n$ , то, двигаясь по системам вверх, последовательно получаем

- 1)  $\beta_i = \beta'_i$ ,
- 2)  $(\alpha_{i+1} - \alpha'_{i+1}) + 2(\gamma_{i+1} - \gamma'_{i+1}) = 0$ ,
- 3)  $(\alpha_{i+1} = \alpha'_{i+1})$  и  $(\gamma_{i+1} = \gamma'_{i+1})$ ,
- 4)  $\beta_{i+1} = \beta'_{i+1}$ ,
- 5)  $(\alpha_{i+2} - \alpha'_{i+2}) + 2(\gamma_{i+2} - \gamma'_{i+2}) = 0$ ,
- 6)  $(\alpha_{i+2} = \alpha'_{i+2})$  и  $(\gamma_{i+2} = \gamma'_{i+2})$ ,
- ...
- 3(n - i)  $(\alpha_n = \alpha'_n)$  и  $(\gamma_n = \gamma'_n)$ ,
- 3(n - i) + 1)  $\beta_n = \beta'_n$ ,
- 3(n - i) + 2)  $(\alpha_1 - \alpha'_1) + 2(\gamma_1 - \gamma'_1) = 0$ ,
- 3(n - i) + 3)  $(\alpha_1 = \alpha'_1)$  и  $(\gamma_1 = \gamma'_1)$ .

Продолжая двигаться по системам вверх, получим, что наборы

$$\langle \alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n, \gamma_1, \dots, \gamma_n \rangle \quad \text{и} \quad \langle \alpha'_1, \dots, \alpha'_n, \beta'_1, \dots, \beta'_n, \gamma'_1, \dots, \gamma'_n \rangle$$

совпадают, что противоречит предположению. Значит, при любом  $i$  выполняется равенство  $\alpha'_i = 1 - \alpha_i$ . Поэтому набор  $\langle \alpha_1, \dots, \alpha_n \rangle$  является решением уравнения (2). Это завершает доказательство теоремы. ■

**Следствие 1.** Задача « $m$ -инъективный рюкзак» является coNP-полной.

### Заключение

В работе доказано, что задача «Неинъективный рюкзак» является NP-полной, а задача «Инъективный рюкзак» — coNP-полной. При этом интересно отметить, что с определённой точки зрения «Инъективных рюкзаков» практически столько же, сколько «Неинъективных».

В работах [10, 11] устанавливается, что число «Инъективных рюкзаков» размерности  $n$  с фиксированным максимальным элементом  $M$  ограничено снизу величиной

$$n! \left( \frac{M - 2^{n-1} + 1}{2^{n-2}} - 1 \right) \left( \frac{M - 2^{n-1} + 1}{2^{n-1}} \right)^{n-2}, \quad \text{где полагаем } M \geq 2^{n-1},$$

а сверху —  $n!C_{M-1}^{n-1}$ , где полагаем  $M \geq n$ ;  $C_r^s$  — число сочетаний. Отметим, что оценки эти достаточно грубые, поскольку нижняя оценка получена фактически для «Супервозрастающих рюкзаков», а если рассмотреть верхнюю оценку для числа «Инъективных рюкзаков», максимальный элемент которых принимает значения от  $n$  до  $M$ , то

получим

$$\begin{aligned} n! \sum_{k=n}^M C_{k-1}^{m-1} &= n! \left( \frac{1}{0!} + \frac{n}{1!} + \frac{(n+1)n}{2!} + \frac{(n+2)(n+1)n}{3!} + \dots + \frac{(M-1) \dots (n+1)n}{(M-n)!} \right) = \\ &= n! \left( \frac{(n+2)(n+1)}{2!} + \frac{(n+2)(n+1)n}{3!} + \dots + \frac{(M-1) \dots (n+1)n}{(M-n)!} \right) = \\ &= n! \frac{M(M-1) \dots (n+1)}{(M-n)!} = \frac{M!}{(M-n)!}, \end{aligned}$$

и поскольку  $\lim_{M \rightarrow \infty} \frac{M!}{(M-n)!M^n} = 1$ , то «практически все» рюкзаки должны быть инъективными.

Действуя по аналогии, можно установить, что число « $m$ -инъективных рюкзаков» размерности  $n$  с фиксированным максимальным элементом  $M$  ограничено снизу величиной

$$n! \left( \frac{M - m^{n-1} + 1}{(m-1)m^{n-2}} - 1 \right) \left( \frac{M - m^{n-1} + 1}{m^{n-1}} \right)^{n-2}, \text{ где полагаем } M \geq m^{n-1},$$

а сверху —  $n!C_k^{n-1}$ , где полагаем  $M \geq n(m-1)$ ;  $k = [(M-m+1)/(m-1)]$ .

Если посмотреть на все оценки, как на полиномы от  $M$ , то окажется, что каждый полином имеет степень  $n-1$ . При этом общее число «рюкзаков» размерности  $n$  с фиксированным максимальным элементом  $M$  составляет  $M^n - (M-1)^n = \sum_{k=1}^n C_n^k (M-1)^{n-k}$  и также является полиномом степени  $n-1$  от  $M$ . Это означает, что доля «Инъективных рюкзаков» размерности  $n$  среди всех рюкзаков зависит только от  $n$ , то есть при фиксированном  $n$  эта доля является константой, соответственно является константой и доля «Неинъективных рюкзаков».

## ЛИТЕРАТУРА

1. Karp R. M. Reducibility among combinatorial problems // Complexity of Computer Computations. N. Y.: Plenum Press, 1972. P. 85–103.
2. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.
3. Пападимитриу Х., Стайглиц К. Комбинаторная оптимизация. Алгоритмы и сложность. М.: Мир, 1984.
4. Merkle R. and Hellman M. Hiding information and signature in trapdoor knapsacks // IEEE Trans. Inform. Theory. 1978. V. 24. No. 5. P. 525–530.
5. Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory // Problems Control Inform. Theory. 1986. No. 15(2). P. 159–166.
6. Chor B. and Rivest R. A knapsack-type public key cryptosystem based on arithmetic in finite fields // CRYPTO'84. LNCS. 1985. V. 196. P. 54–65.
7. Осипян В. О. О криптосистемах с заданным рюкзаком // Материалы VI Междунар. науч.-практич. конф. «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2004. С. 269–271.
8. Осипян В. О. О системе защиты информации на основе проблемы рюкзака // Известия Томского политехнического университета. 2006. Т. 309. № 2. С. 209–212.
9. Woeginger G. J. and Yu Z. On the equal-subset-sum problem // Inform. Proc. Lett. 1992. V. 42. P. 299–302.

10. Мурин Д. М. О порядке роста числа инъективных и сверхрастающих рюкзачных векторов // Моделирование и анализ информационных систем. 2012. Т. 19. № 3. С. 124–135.
11. Мурин Д. М. О порядке роста числа инъективных и сверхрастающих векторов и некоторых особенностях сильного модульного умножения // Прикладная дискретная математика. Приложение. 2012. № 5. С. 19–21.

## REFERENCES

1. Karp R. M. Reducibility among combinatorial problems. Complexity of Computer Computations, N. Y., Plenum Press, 1972, pp. 85–103.
2. Garey R. and Johnson D. Computers and Intractability. N. Y., USA, W. H. Freeman & Co, 1979.
3. Papadimitriou C. H. and Steiglitz K. Combinatorial Optimization: Algorithms and Complexity. Prentice-Hall, 1982.
4. Merkle R. and Hellman M. Hiding information and signature in trapdoor knapsacks. IEEE Trans. Inform. Theory, 1978, vol. 24, no. 5, pp. 525–530.
5. Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory. Problems Control Inform. Theory, 1986, no. 15(2), pp. 159–166.
6. Chor B. and Rivest R. A knapsack-type public key cryptosystem based on arithmetic in finite fields. CRYPTO'84, LNCS, 1985, vol. 196, pp. 54–65.
7. Osipyan V. O. O kriptosistemakh s zadannym ryukzakom [About cryptosystems with a given knapsack]. Proc. VI Int. Conf. "Information security". Taganrog, TRTU Publ., 2004, pp. 269–271. (in Russian)
8. Osipyan V. O. O sisteme zashchity informatsii na osnove problemy ryukzaka [Information protection system based on the knapsack problem]. Bull. TPU, 2006, vol. 309, no 2, pp. 209–212. (in Russian)
9. Woeginger G. J. and Yu Z. On the equal-subset-sum problem. Inform. Proc. Lett., 1992, vol. 42, pp. 299–302.
10. Murin D. M. O poryadke rosta chisla in'ektivnykh i sverkh rastushchikh ryukzachnykh vektorov [The order in the growth of the injective and super-increasing vectors knapsacks quantity]. Modelirovanie i Analiz Informatsionnykh Sistem, 2012, vol. 19, no 3, pp. 124–135. (in Russian)

11. *Murin D. M.* O poryadke rosta chisla in"ektivnykh i sverkhkrastushchikh vektorov i nekotorykh osobennostyakh sil'nogo modul'nogo umnozheniya [About the order of the increasing in the number of the injective and super-increasing vectors and some particularities in the strong modular multiplying]. *Prikladnaya diskretnaya matematika. Prilozhenie*, 2012, no. 5, pp. 19–21. (in Russian)