Модел. и анализ информ. систем. Т. **19**, № **3** (2012) 124–135

УДК 519.61

О порядке роста числа инъективных и сверхрастущих рюкзачных векторов

Мурин Д. М.

Ярославский государственный университет им. П.Г. Демидова

e-mail: nirum87@mail.ru, d.murin@secst.ru

получена 6 ноября 2011

Ключевые слова: инъективные рюкзачные векторы, сверхрастущие рюкзачные векторы, компьютерная алгебра

В 1978 году Р. Меркль и М. Хеллман предложили использовать для построения криптосистем одномерную аддитивную задачу об укладке рюкзака. В основе предложенной криптосистемы лежал класс рюкзаков, обладающих сверхрастущими векторами. Указанный класс является подмножеством множества рюкзаков с инъективными (криптографическими) векторами, допускающих однозначное декодирование (дешифрование). В настоящей работе рассмотрены вопросы о порядке роста числа рюкзаков с инъективными векторами и о порядке роста числа рюкзаков со сверхрастущими векторами при росте максимального элемента рюкзака.

> «В действительности он только выглядит как произвольный, потому что очень немногие векторы рюкзака могут быть получены таким способом ...»
>
> *Саломаа А. «Криптография с открытым ключом»*

Задача о рюкзаке

Р. Меркль и М. Хеллман [1] предложили использовать для построения криптосистем с открытым ключом следующую частную задачу об укладке рюкзака. Пусть $A = \{a_1, a_2, \ldots, a_n\}$ – множество натуральных (положительных целых) чисел (множество весов, рюкзачный вектор). Число n – мощность множества весов A – называется *размерностью* рюкзака. Для произвольного подмножества A^* множества A ($A^* \subset A$) обозначим через $S(A^*)$ сумму элементов подмножества A^* и назовем ее весом подмножества A^*.

Напомним некоторые определения.

Определение 1. ***Задача о рюкзаке.*** *По заданному множеству A и числу S, определить, существует ли такое подмножество $A^* \subset A$, что $S(A^*) = S$, т.е. существует ли в A подмножество веса S.*

Задачу о рюкзаке можно переформулировать следующим образом: имеет ли уравнение $\sum_{i=1}^{n} x_i a_i = S$, где $x_1, \ldots, x_n$ – неизвестные, решение в числах 0 и 1.

В криптологии интерес представляет несколько измененная задача о рюкзаке: известно, что уравнение $\sum_{i=1}^{n} x_i a_i = S$, где $x_1, \ldots, x_n$ – неизвестные, имеет решение в числах 0 и 1, необходимо найти это решение.

Определение 2. Рюкзачный вектор $A = (a_1, \ldots, a_n)$ называется *упорядоченным* или *возрастающим* (соответственно *сверхрастущим*), если и только если $a_j > a_{j-1}$ (соответственно $a_j > \sum_{i=1}^{j-1} a_i$) выполняется для всех j, таких что $2 \leq j \leq n$. [2]

Определение 3. Рюкзачный вектор $A = (a_1, \ldots, a_n)$ называется *инъективным* или *криптографическим*, если для любых различных подмножеств $A^* \subset A$ и $A^{**} \subset A$, $A^* \neq A^{**}$ суммы элементов данных подмножеств будут различны: $S(A^{**}) \neq S(A^*)$.

Результаты экспериментов

Обозначим через $F_1(n, M)$ число упорядоченных инъективных рюкзачных векторов $A = (a_1, \ldots, a_n)$ размерности n, максимальный элемент которых равен M. Обозначим через $F_2(n, M)$ число сверхрастущих рюкзачных векторов размерности n, максимальный элемент которых равен M.

Для изучения свойств функций $F_1(n, M)$ и $F_2(n, M)$ нами было разработано программное обеспечение, позволяющее в параллельном режиме генерировать рюкзачные векторы и определять, принадлежит ли сгенерированный вектор множеству упорядоченных инъективных векторов или множеству сверхрастущих векторов.

В ходе проведения серии компьютерных экспериментов были установлены значения функций $F_1(n, M)$ для $2 \leq n \leq 4$ при $1 \leq M \leq 1024$, $n = 5$ при $1 \leq M \leq 512$, $n = 6$ при $1 \leq M \leq 256$, $7 \leq n \leq 8$ при $1 \leq M \leq 128$ и $F_2(n, M)$ для $2 \leq n \leq 9$ при $1 \leq M \leq 1024$. Это позволило выдвинуть предположения относительно порядка роста функций $F_1(n, M)$ и $F_2(n, M)$.

На рисунках 1-2 приводятся результаты проведенных компьютерных экспериментов.

При анализе результатов компьютерных экспериментов было установлено, что график функции $\sqrt[n-1]{F_1(n, M)}$ при фиксированном n и $M \geq M_n$, где M_n – наименьшее натуральное число такое, что $F_1(n, M_n) \neq 0$, в значительной степени «схож» с графиком прямой, т.е. функция $\sqrt[n-1]{F_1(n, M)}$ при фиксированном n и $M \geq M_n$ ведет себя подобно полиному первой степени от M (рисунок 3[1]). И можно предположить, что функция $F_1(n, M)$ при фиксированном n и $M \geq M_n$ должна вести себя подобно полиному степени $n - 1$ от M.

На наш взгляд, особый интерес представляет тот факт, что функция $F_2(n, M)$ при фиксированном n и $M \geq 2^{n-1}$ также ведет себя подобно полиному степени $n-1$ от M (рисунок 4).

[1]На рисунке 3 для сравнения приведен также график функции $y = 2M$.

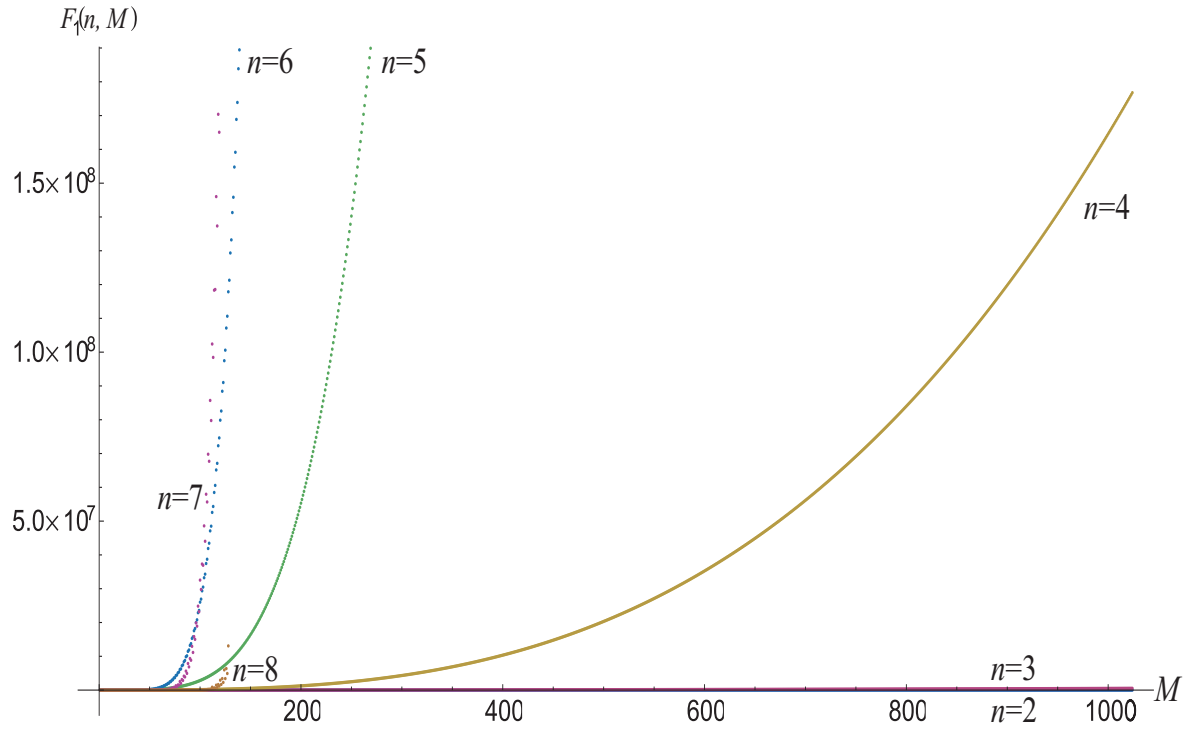

Рис. 1. Поведение функции $F_1(n, M)$ при $2 \leq n \leq 8$

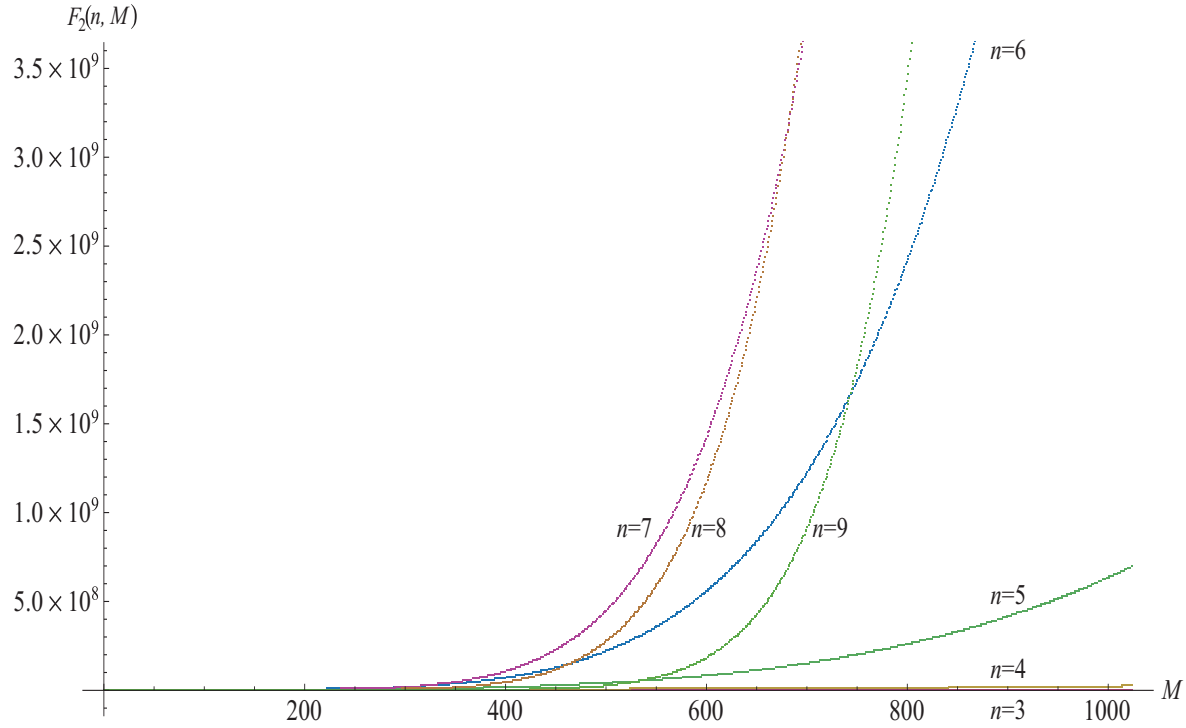

Рис. 2. Поведение функции $F_2(n, M)$ при $3 \leq n \leq 9$

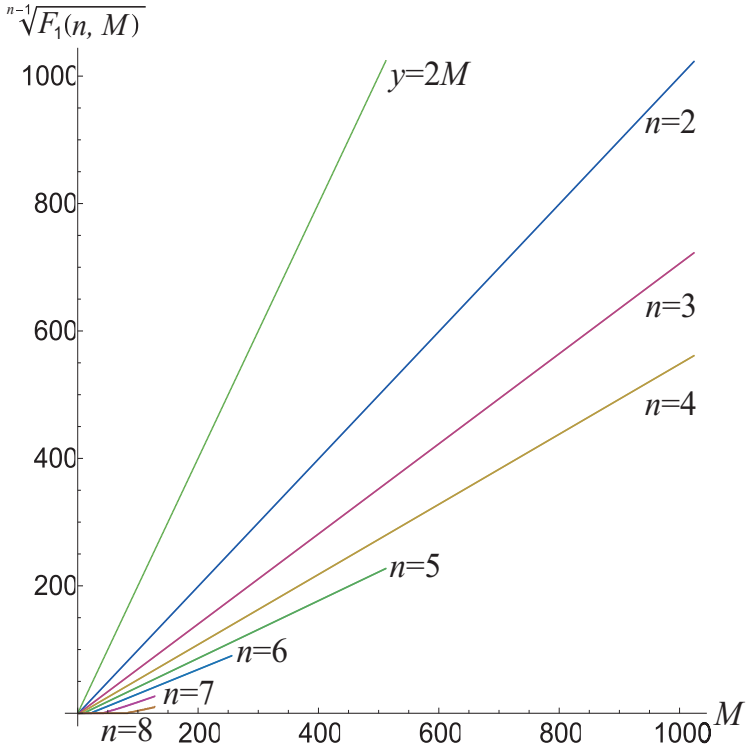

Рис. 3. Поведение функции $\sqrt[n-1]{F_1(n, M)}$ при $2 \leq n \leq 8$

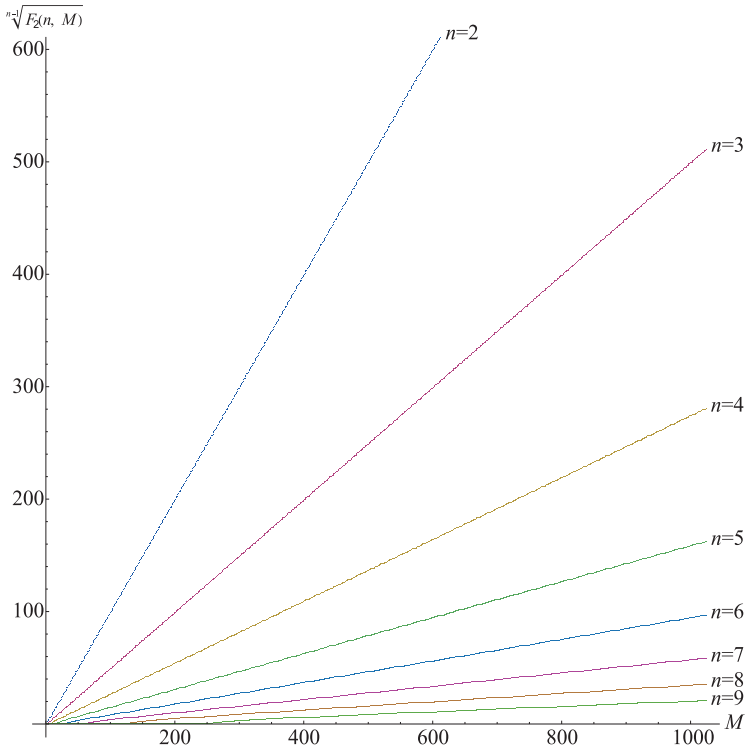

Рис. 4. Поведение функции $\sqrt[n-1]{F_2(n, M)}$ при $2 \leq n \leq 9$

Оценка сверху для $F_1(n, M)$

Оценим $F_1(n, M)$:

Теорема 1. При фиксированном $n \in \mathbb{N}$ и любом натуральном M (за исключением случая $n = 1, M = 1$, при котором $F_1(n, M) = 1$) выполняется неравенство

$$F_1(n, M) \leq \frac{(M-1)^{n-1}}{(n-1)!}.$$

Доказательство. Число произвольных неупорядоченных рюкзачных векторов размерности n с максимальным элементом равным M равно $M^n - (M-1)^n = \sum_{k=1}^{n} C_n^k (M-1)^{n-k}$, т.е. ведет себя как полином степени $n-1$ от M.

В сумме $\sum_{k=1}^{n} C_n^k (M-1)^{n-k}$ слагаемые $C_n^k (M-1)^{n-k}$ при $k = 2, \ldots, n$ отвечают за векторы, в которых имеются два и более максимальных элементов равных M. Вектор, удовлетворяющий такому условию, заведомо не является инъективным, поэтому $F_1(n, M) \leq n(M-1)^{n-1}$.

И, поскольку нас интересуют только упорядоченные векторы, то

$$F_1(n, M) \leq \frac{n(M-1)^{n-1}}{n!}.$$

□

Оценка снизу для $F_2(n, M)$

Нетрудно понять, что рюкзачный вектор $(1, 2, 2^2, \ldots, 2^{n-1})$ является единственным сверхрастущим вектором размерности n с максимальным элементом, не превосходящим 2^{n-1}.

Теорема 2. Все сверхрастущие векторы могут быть получены из вектора $(1, 2, 2^2, \ldots, 2^{n-1})$ путем применения к нему некоторого набора следующих операций:

$$P_1^n : (a_1 + 1, a_2 + 1, a_3 + 2, \ldots, a_{n-1} + 2^{n-3}, a_n + 2^{n-2})$$

$$\vdots$$

$$P_k^n : (a_1, a_2, a_3, \ldots, a_k + 1, a_{k+1} + 1, \ldots, a_{n-1} + 2^{n-k-2}, a_n + 2^{n-k-1})$$

$$\vdots$$

$$P_{n-1}^n : (a_1, a_2, a_3, \ldots, a_{n-1} + 1, a_n + 1)$$

$$P_n^n : (a_1, a_2, a_3, \ldots, a_{n-1}, a_n + 1)$$

$$P_0^n : (a_1, a_2, a_3, \ldots, a_{n-1}, a_n)$$

Доказательство. Вектор $(1, 2, 2^2, \ldots, 2^{n-1})$ - сам является сверхрастущим и $(1, 2, 2^2, \ldots, 2^{n-1}) = P_0^n((1, 2, 2^2, \ldots, 2^{n-1}))$.

Рассмотрим сверхрастущий вектор $(a_1, \ldots, a_n) \neq (1, 2, 2^2, \ldots, 2^{n-1})$. Пусть $1 \leq k \leq n$ – первый (наименьший) номер такой, что $a_k > 2^{k-1}$, тогда $a_k \geq 2^{k-1} + 1$,

$$a_{k+1} > \sum_{i=1}^{k} a_i \geq 2^{k-1} - 1 + 2^{k-1} + 1 = 2^k \quad \Rightarrow \quad a_{k+1} \geq 2^k + 1,$$

$$a_{k+2} > \sum_{i=1}^{k+1} a_i \geq 2^{k-1} - 1 + 2^{k-1} + 1 + 2^k + 1 = 2^{k+1} + 1 \quad \Rightarrow \quad a_{k+2} \geq 2^{k+1} + 2,$$

$$\vdots$$

$$a_n > \sum_{i=1}^{n-1} a_i \geq 2^{k-1} - 1 + 2^{k-1} + 1 + 2^k + 1 + 2^{k+1} + 2 + \ldots + 2^{n-k-2} = 2^{n-1} + 2^{n-k-1} - 1 \Rightarrow$$

$$a_n \geq 2^{n-1} + 2^{n-k-1}.$$

И мы можем применить к вектору $(a_1, \ldots, a_n)$ преобразование

$$(P_k^n)^{-1} : (a_1, a_2, a_3, \ldots, a_k - 1, a_{k+1} - 1, \ldots, a_{n-1} - 2^{n-k-2}, a_n - 2^{n-k-1}),$$

причем результирующий вектор будет сверхрастущим. Действительно:

$$a_k - 1 \geq 2^{k-1} > 2^{k-1} - 1 = \sum_{i=1}^{k-1} a_i, \quad a_{k+1} - 1 > \sum_{i=1}^{k-1} a_i + (a_k - 1),$$

$$a_{k+2} - 2 > \sum_{i=1}^{k-1} a_i + (a_k - 1) + (a_{k+1} - 1),$$

$$\vdots$$

$$a_n - 2^{n-k-1} > \sum_{i=1}^{k-1} a_i + (a_k - 1) + \sum_{i=k+1}^{n-1} (a_i - 2^{i-k-1}).$$

Заметим, что при применении преобразования $(P_k^n)^{-1}$ a_k уменьшается ровно на 1. Рассмотрим следующую процедуру.

Процедура. Сведение сверхрастущего вектора к вектору $(1, 2, \ldots, 2^{n-1})$**.**

Процедуре на вход поступает $A = (a_1, \ldots, a_n)$ – исходный сверхрастущий вектор. k, n – натуральные числа, $b[1..n]$ – массив натуральных чисел размерности n.

Тело процедуры:

1. $k := 1$;

2. Пока $k < n + 1$ выполнять:

2.1. Если $a_k > 2^{k-1}$,

2.1.1. То запомним k и $b_k := a_k - 2^{k-1}$;

2.1.2. $A := (P_k^n)^{-b_k}(A)$;

(где для любых натуральных чисел i, k, n : $(P_k^n)^{-i} = (P_k^n)^{-i+1}(P_k^n)^{-1}$);

2.2. Иначе

2.2.1. $b_k := 0$;

2.3. $k := k + 1$.

Конец процедуры.

После завершения процедуры $A = (1, 2, \ldots, 2^{n-1})$. Действительно, после применения преобразования $(P_k^n)^{-(a_k - 2^{k-1})}$, a_k уменьшится на $a_k - 2^{k-1}$. Кроме того, поскольку мы запомнили преобразования $(k,\ b_k)$, с помощью которых привели исходный сверхрастущий вектор к вектору $(1, 2, \ldots, 2^{n-1})$, то мы сможем восстановить исходный сверхрастущий вектор из вектора $(1, 2, \ldots, 2^{n-1})$. А именно:

$$(a_1, \ldots, a_n) = (P_n^n)^{b_n}(P_{n-1}^n)^{b_{n-1}} \ldots (P_1^n)^{b_1}((1, 2, \ldots, 2^{n-1})).$$

Поскольку исходный сверхрастущий вектор выбирается произвольно, то из вышесказанного следует, что любой сверхрастущий вектор $A = (a_1, \ldots, a_n)$ представим в виде

$$(a_1, \ldots, a_n) = (P_n^n)^{x_n}(P_{n-1}^n)^{x_{n-1}} \ldots (P_1^n)^{x_1}((1, 2, \ldots, 2^{n-1})),$$

для некоторых неотрицательных целых чисел $x_1, \ldots, x_n$.

□

Теорема 3. Операции $P_0^n, P_1^n, \ldots, P_n^n$ коммутируют.

Доказательство. Для любого натурального n и натурального i, такого что $1 \leq i \leq n$ выполняется следующее соотношение:

$$P_i^n(P_0^n((a_1, a_2, \ldots, a_n))) = P_i^n((a_1, a_2, \ldots, a_n)) = P_0^n(P_i^n((a_1, a_2, \ldots, a_n))),$$

и, следовательно, $P_i^n P_0^n = P_0^n P_i^n$.

Для любого натурального n и натуральных i и k, таких что $1 \leq i < k \leq n$, выполняется следующее соотношение:

$$P_i^n(P_k^n((a_1, \ldots, a_n))) = P_i^n((a_1, \ldots, a_k + 1, a_{k+1} + 1, \ldots, a_{n-1} + 2^{n-k-2}, a_n + 2^{n-k-1})) =$$

$$(a_1, \ldots, a_i + 1, a_{i+1} + 1, \ldots, a_k + 1 + 2^{k-i-1}, a_{k+1} + 1 + 2^{k-i}, \ldots, a_n + 2^{n-k-1} + 2^{n-i-1}) =$$

$$(a_1, \ldots, a_i + 1, a_{i+1} + 1, \ldots, a_k + 2^{k-i-1} + 1, a_{k+1} + 2^{k-i} + 1, \ldots, a_n + 2^{n-i-1} + 2^{n-k-1}) =$$

$$= P_k^n((a_1, \ldots, a_i + 1, a_{i+1} + 1, \ldots, a_{n-1} + 2^{n-i-2}, a_n + 2^{n-i-1})) = P_k^n(P_i^n((a_1, \ldots, a_n)))$$

и, следовательно, $P_i^n P_k^n = P_k^n P_i^n$.

□

Следствие. Каждый сверхрастущий вектор размерности n определяется только набором операций $\{P_i^n\}$, позволяющих получить его из вектора $(1, 2, 2^2, \ldots, 2^{n-1})$, а не последовательностью применения данных операций.

Пусть $(a_1, a_2, \ldots, a_n, M)$ – сверхрастущий вектор с максимальным элементом M. Такой вектор может иметь своим началом только сверхрастущий вектор $(a_1, a_2, \ldots, a_n)$, сумма элементов которого меньше M. Следовательно, количество сверхрастущих векторов с максимальным элементом равным M равно количеству сверхрастущих векторов $(a_1, a_2, \ldots, a_n)$, сумма элементов которых меньше M. Или количеству таких наборов операций $\{P_i^n\}$ при $1 \leq i \leq n$, что применение набора операций к вектору $(1, 2, 2^2, \ldots, 2^{n-1})$ переводит его в вектор, сумма элементов которого меньше M. Другими словами, нас интересуют все такие наборы неотрицательных целых чисел $x_0, \ldots, x_{n-1}$, что $(a_1, \ldots, a_n) = (P_n^n)^{x_0}(P_{n-1}^n)^{x_1} \ldots (P_1^n)^{x_{n-1}}((1, 2, \ldots, 2^{n-1}))$ и $\sum_{i=1}^n a_i < M$.

Заметим, что при применении операции P_i^n при $1 \leq i \leq n$ сумма элементов рюкзачного вектора увеличивается на 2^{n-i}. Поэтому наборы $x_0, \ldots, x_{n-1}$ можно рассматривать как решения в $\mathbb{N}_0$ неравенства

$$2^n - 1 + \sum_{i=1}^{n} x_{n-i} \cdot 2^{n-i} < M,$$

где $x_0, x_1, \ldots, x_{n-1}$ – неизвестные.

Оценим снизу $F_2(n, M)$:

Теорема 4. При фиксированном $n \geq 2$ и любом натуральном $M \geq 2^{n-1}$ выполняется неравенство $F_2(n, M) \geq P(M)$, где $P(M)$ – некоторый полином $n-1$ степени от M.

Доказательство. Обозначим $T(n, S)$ количество решений в $\mathbb{N}_0$ неравенства

$$\sum_{i=1}^{n} x_{n-i} \cdot 2^{n-i} < S,$$

где $S \in \mathbb{N}_0$, $x_0, x_1, \ldots, x_{n-1}$ – неизвестные. Тогда $T(n-1, S)$ – количество решений в $\mathbb{N}_0$ неравенства $\sum_{i=1}^{n-1} x_{n-1-i} \cdot 2^{n-1-i} < S$. Заметим также, что неравенство $x_0 < S$ имеет ровно S решений, поэтому $T(1, S) = S$. Тогда

$$T(n,S) = \sum_{k_1=0}^{\left[\frac{S}{2^{n-1}}\right]} T(n-1, S-k_1 2^{n-1}) = \sum_{k_1=0}^{\left[\frac{S}{2^{n-1}}\right]} \sum_{k_2=0}^{\left[\frac{S-k_1 2^{n-1}}{2^{n-2}}\right]} T(n-2, S-k_1 2^{n-1}-k_2 2^{n-2}) =$$

$$= \sum_{k_1=0}^{\left[\frac{S}{2^{n-1}}\right]} \sum_{k_2=0}^{\left[\frac{S-k_1 2^{n-1}}{2^{n-2}}\right]} \ldots \sum_{k_{n-1}=0}^{\left[\frac{S-k_1 2^{n-1}-k_2 2^{n-2}-\ldots-k_{n-2}2^2}{2}\right]} T(1, S-k_1 2^{n-1}-k_2 2^{n-2}-\ldots-k_{n-1}2) \geq$$

$$\geq \sum_{k_1=0}^{\left[\frac{S}{2^n}\right]} \sum_{k_2=0}^{\left[\frac{S}{2^n}\right]} \ldots \sum_{k_{n-1}=0}^{\left[\frac{S}{2^n}\right]} T(1, S-k_1 2^{n-1}-k_2 2^{n-2}-\ldots-k_{n-1}2) \geq$$

$$\geq \sum_{k_1=0}^{\left[\frac{S}{2^n}\right]} \sum_{k_2=0}^{\left[\frac{S}{2^n}\right]} \ldots \sum_{k_{n-1}=0}^{\left[\frac{S}{2^n}\right]} T(1, \left[S - \frac{S}{2^n}2^{n-1} - \frac{S}{2^n}2^{n-2} - \ldots - \frac{S}{2^n}2\right]) =$$

$$= \sum_{k_1=0}^{\left[\frac{S}{2^n}\right]} \sum_{k_2=0}^{\left[\frac{S}{2^n}\right]} \ldots \sum_{k_{n-1}=0}^{\left[\frac{S}{2^n}\right]} T(1, \left[\frac{S}{2^{n-1}}\right]) = \left[\frac{S}{2^{n-1}}\right] \left(\left[\frac{S}{2^n}\right] + 1\right)^{n-1} \geq \left[\frac{S}{2^{n-1}}\right] \left(\frac{S}{2^n}\right)^{n-1}$$

Откуда следует, что

$$F_2(n+1, M) = T(n, M-2^n+1) \geq \left[\frac{M-2^n+1}{2^{n-1}}\right] \left(\frac{M-2^n+1}{2^n}\right)^{n-1}.$$

И, следовательно, при фиксированном $n \geq 2$ и любом натуральном $M \geq 2^{n-1}$ (при $M < 2^{n-1}$ $F_2(n, M) = 0$) выполняется неравенство

$$F_2(n, M) \geq P(M) = \left(\frac{M-2^{n-1}+1}{2^{n-2}} - 1\right) \left(\frac{M-2^{n-1}+1}{2^{n-1}}\right)^{n-2}.$$

□

Из вышесказанного следует, что при любом фиксированном $n \geq 2$ существуют пределы

$$\lim_{M\to\infty} \frac{n! \cdot F_1(n, M)}{nM^{n-1}}, \lim_{M\to\infty} \frac{n! \cdot F_2(n, M)}{nM^{n-1}} \text{ и } \lim_{M\to\infty} \frac{F_2(n, M)}{F_1(n, M)}.$$

Определим функции $f_1(n)$ и $f_2(n)$ равенствами

$$f_1(n) = \lim_{M\to\infty} \frac{n!\cdot F_1(n,M)}{M^{n-1}}, f_2(n) = \lim_{M\to\infty} \frac{F_2(n,M)}{F_1(n,M)}.$$

Тогда из полученных выше результатов следует, что при фиксированном $n \geq 2$ функции $\frac{f_1(n)}{M}$, $\frac{f_2(n)}{M}$ должны вести себя подобно функции $P^{-1}(M)$, где $P(M)$ – некоторый полином первой степени от M, а функции $f_1(n)$, $f_2(n)$ – подобно константе. Это иллюстрируют рисунки 5 – 7.

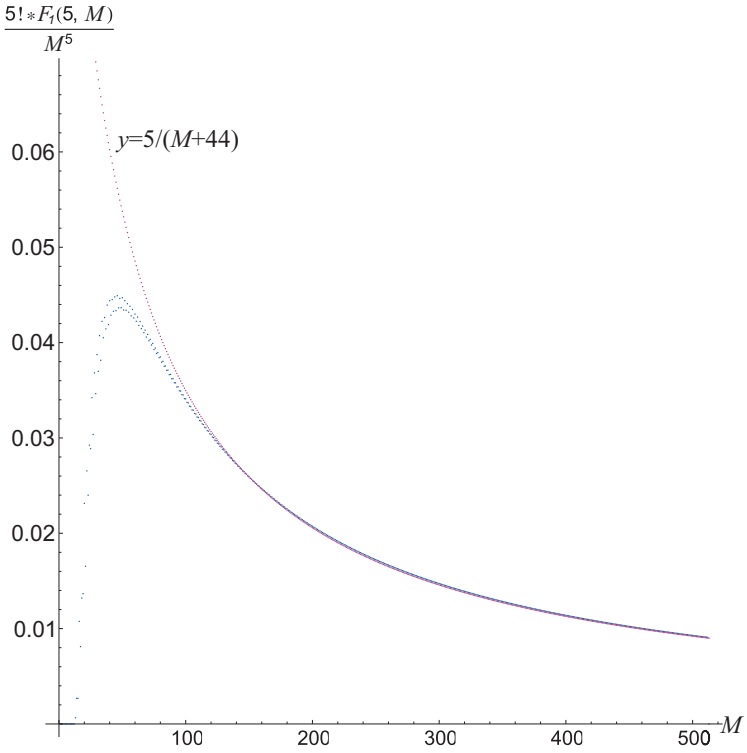

Рис. 5. Поведение функции $\frac{5!\cdot F_1(5,M)}{M^5}$

Алгоритм перечисления всех сверхрастущих рюкзаков с фиксированным максимальным элементом

Мы предлагаем следующий алгоритм перечисления всех сверхрастущих рюкзаков размерности $n+1$ с фиксированным максимальным элементом M в лингвистическом порядке. Поскольку нам заранее известен $n+1$-й элемент строящихся рюкзаков (он равен M), постольку мы будем заниматься построением только начальных векторов $(a_1, \ldots, a_n)$. Мы предполагаем, что $M > 2^n - 1$, иначе ни одного вектора построить не удастся.

Алгоритм.

$A[1..n]$ – массив рюкзачных векторов размерности n.

$I[1..n], S[1..n]$ – массивы неотрицательных целых чисел размерности n.

S – целое неотрицательное число.

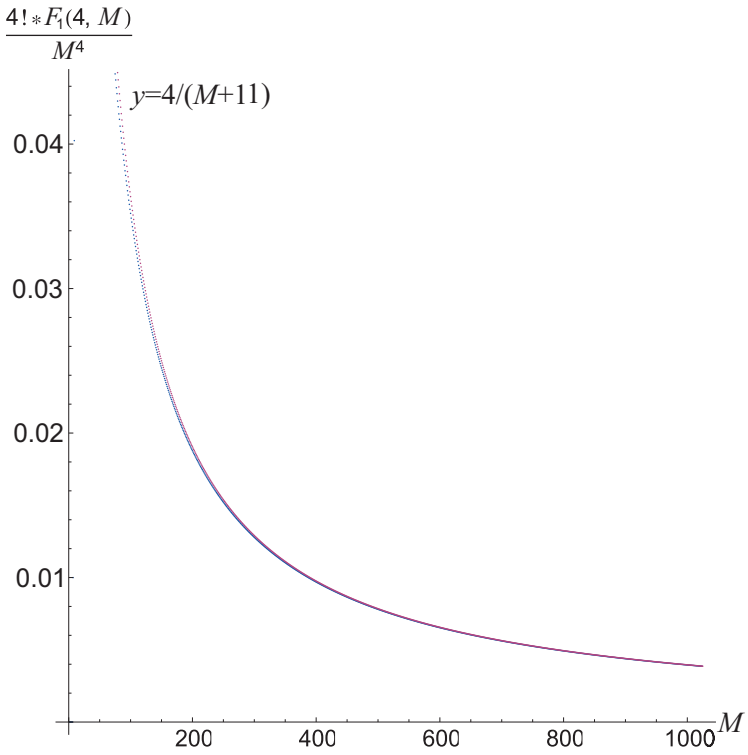

Рис. 6. Поведение функции $\frac{4!\cdot F_1(4,M)}{M^4}$

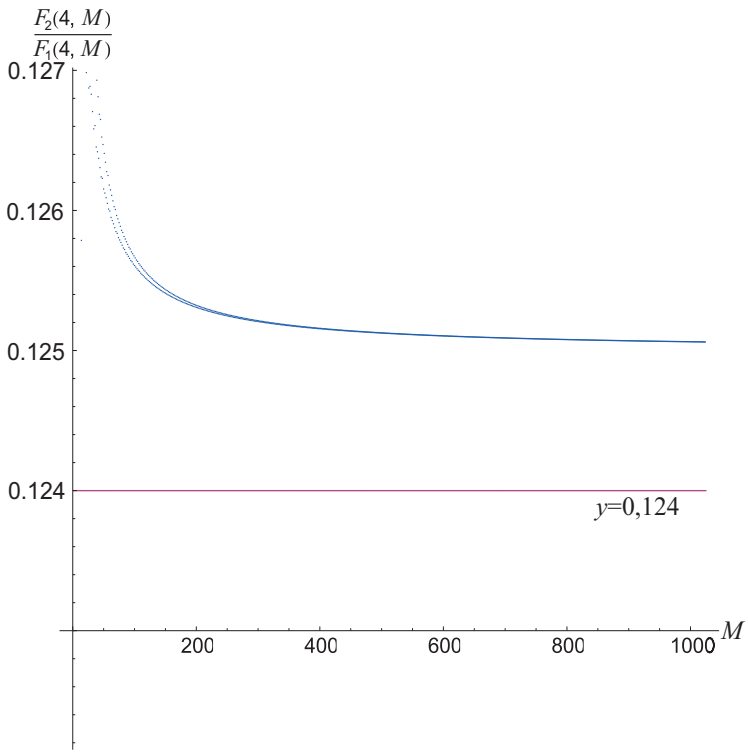

Рис. 7. Поведение функции $\frac{F_2(4,M)}{F_1(4,M)}$

$P_1^n, \dots P_n^n$ – рассмотренные выше операции со сверхрастущими векторами.

Тело алгоритма:

$A_1 := (1, 2, \dots, 2^{n-1})$;
$S := M - 2^n + 1$;
print (A_1);
for($I_1 := 0$; $I_1 \le \left[\frac{S}{2^{n-1}}\right]$; $I_1 := I_1 + 1$)
{
if($I_1 \neq 0$)
{
$A_1 := P_1^n(A_1)$;
print (A_1);
}
$A_2 := A_1$;

$\dots$

for($I_k := 0$; $I_k \le \left[\frac{S - I_1 \cdot 2^{n-1} - \dots - I_{k-1} \cdot 2^{n-k+1}}{2^{n-k}}\right]$; $I_k := I_k + 1$)
{
if($I_k \neq 0$)
{
$A_k := P_k^n(A_k)$;
print (A_k);
}
$A_{k+1} := A_k$;

$\dots$

for($I_n := 1$; $I_n < S - I_1 \cdot 2^{n-1} - \dots - I_{n-1} \cdot 2$; $I_n := I_n + 1$)
{
$A_n := P_n^n(A_n)$;
print (A_n);
}

$\dots$

}

$\dots$

}

Конец алгоритма.

Проиллюстрируем работу алгоритма таблицей его пошагового исполнения при $n = 4$, $M = 24$. Алгоритм выдает начальные сверхрастущие векторы размерности 4, пятый элемент искомых векторов размерности $n + 1$ равен 24 (Таблица 1).

Список литературы

1. *Merkle R.C., Hellman M.E.* Hiding information and signatures in trap-door knapsacks // IEEE Trans. Inform. Theory. 1978. V. IT-24. P. 525–530.

2. *Саломаа А.* Криптография с открытым ключом. М.: Мир, 1995.

I_1	I_2	I_3	I_4	Выводимый вектор	I_1	I_2	I_3	I_4	Выводимый вектор
x	x	x	x	$(1,2,4,8)$	0	0	2	2	$(1,2,6,12)$
0	0	0	1	$(1,2,4,9)$	0	0	2	3	$(1,2,6,13)$
0	0	0	2	$(1,2,4,10)$	0	0	2	4	$(1,2,6,14)$
0	0	0	3	$(1,2,4,11)$	0	0	3	x	$(1,2,7,11)$
0	0	0	4	$(1,2,4,12)$	0	0	3	1	$(1,2,7,12)$
0	0	0	5	$(1,2,4,13)$	0	0	3	2	$(1,2,7,13)$
0	0	0	6	$(1,2,4,14)$	0	0	4	x	$(1,2,8,12)$
0	0	0	7	$(1,2,4,15)$	0	1	x	x	$(1,3,5,10)$
0	0	0	8	$(1,2,4,16)$	0	1	0	1	$(1,3,5,11)$
0	0	1	x	$(1,2,5,9)$	0	1	0	2	$(1,3,5,12)$
0	0	1	1	$(1,2,5,10)$	0	1	0	3	$(1,3,5,13)$
0	0	1	2	$(1,2,5,11)$	0	1	0	4	$(1,3,5,14)$
0	0	1	3	$(1,2,5,12)$	0	1	1	x	$(1,3,6,11)$
0	0	1	4	$(1,2,5,13)$	0	1	1	1	$(1,3,6,12)$
0	0	1	5	$(1,2,5,14)$	0	1	1	2	$(1,3,6,13)$
0	0	1	6	$(1,2,5,15)$	0	1	2	x	$(1,3,7,12)$
0	0	2	x	$(1,2,6,10)$	0	2	x	x	$(1,4,6,12)$
0	0	2	1	$(1,2,6,11)$	1	x	x	x	$(2,3,6,12)$

Таблица 1. Пошаговое исполнение алгоритма

The Order in the Growth of the Injective and Super-Increasing Vectors Knapsacks Quantity

Murin D. M.

Keywords: injective vectors, super-increasing vectors, computer algebra

In 1978 R. Mercle and M. Hellman offered to use the subset sum problem for constructing cryptographic systems. The proposed cryptosystems were based on a class of the knapsacks with super-increasing vectors. This class is a subset of the set of knapsacks with injective (cryptographic) vectors that allow the single-valued decoding (decryption) result. In this paper we consider the problems related to the order in the growth of the injective vectors knapsacks quantity and to the order in the growth of knapsacks quantity with the super-increasing vectors through the knapsack maximal element increasing.

Сведения об авторе: Мурин Дмитрий Михайлович,
Ярославский государственный университет им. П.Г. Демидова, аспирант