МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

DOI 10.17223/20710410/8/9

УДК 591.1

ЭЛАСТИЧНОСТЬ АЛГОРИТМОВ

В. В. Быкова

Институт математики Сибирского федерального университета, г. Красноярск, Россия

E-mail: bykvalen@mail.ru

Приведены характерные особенности эластичности субполиномиальных, полиномиальных, субэкспоненциальных, экспоненциальных и гиперэкспоненциальных классов алгоритмов. Дана методика сравнения алгоритмов по асимптотике поведения эластичности функций вычислительной сложности.

Ключевые слова: *сложность вычислений, анализ алгоритмов.*

Современная индустрия программного обеспечения и средств информационной безопасности компьютерных систем диктует необходимость развития специальных методов анализа и классификации алгоритмов. В теории сложности вычислений классификация алгоритмов традиционно осуществляется с точки зрения вычислительной сложности — трудоемкости продуцируемых алгоритмами вычислительных процессов. При этом вычислительная сложность алгоритма формально описывается функцией временной сложности $t(n)$, отражающей максимальное количество элементарных шагов, которое необходимо алгоритму для достижения запланированного результата в зависимости от n — длины входа алгоритма [1]. Обычно ограничиваются рассмотрением поведения функций сложности в асимптотике при стремлении n к бесконечности, а изложение результатов ведется в терминах O-большое и o-малое [2 – 4]. До недавнего времени алгоритмы подразделяли на низкозатратные (полиномиальные) и высокозатратные (экспоненциальные). В сегодняшней программной инженерии используется пять сложностных классов алгоритмов. Выделены субполиномиальные (быстрые) алгоритмы из полиномиального класса, субэкспоненциальные и гиперэкспоненциальные алгоритмы из экспоненциального класса. Субполиномиальные и субэкспоненциальные алгоритмы — область повышенного интереса современных криптографических систем [5 – 7]. Использование непосредственного асимптотического оценивания для распознавания всех пяти сложностных классов алгоритмов в большинстве случаев сопряжено с трудностями вычислительного характера. В данной работе в качестве меры вычислительной сложности алгоритма взята эластичность функции $t(n)$.

1. Характеристика исследуемого семейства функций сложности

Относительно функции сложности сделан ряд допущений. Во-первых, полагается, что $t(n)$ — монотонно неубывающая функция, областью значений которой выступает множество неотрицательных действительных чисел, а областью определения — множество неотрицательных целых чисел. Во-вторых, допускается отступление от дискретности изменения n (с формальной заменой n на x), т. е. предположение о том, что

аргумент x непрерывен, а необходимые значения функции $t(n)$ вычисляются в целочисленных точках $x = n$. В-третьих, анализируемое множество функций ограничивается семейством $\mathfrak{L}$ — «по-существу положительных» логарифмически-экспоненциальных функций. Установление указанных границ рассматриваемого множества функций обеспечивает существование эластичности и возможность сравнения любых двух функций сложности алгоритмов по скорости роста.

Семейство $\mathfrak{L}$-функций было введено и исследовано Г. Х. Харди [8]. Напомним, что $f(x)$ считается «по-существу положительной» функцией, если существует x_0, такое, что $f(x) > 0$ для всех $x > x_0$. Известно, что каждая $\mathfrak{L}$-функция непрерывна и дифференцируема в той области, где она определена. Теорема Харди о $\mathfrak{L}$-функциях констатирует, что эти функции образуют асимптотическую иерархию [8]: если $f(x)$, $q(x) \in \mathfrak{L}$, то при $x \to \infty$ верно одно из трех соотношений $f(x) \prec q(x)$, $f(x) \succ q(x)$, $f(x) = O[q(x)]$. Заметим, что здесь и далее

$$f(x) = O[g(x)] \Leftrightarrow f(x) \sim cq(x) \Leftrightarrow \lim_{x\to\infty} \frac{f(x)}{g(x)} = c > 0;$$

$$f(x) \prec g(x) \Leftrightarrow f(x) = o[g(x)] \Leftrightarrow \lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$$

В асимптотической иерархии $\mathfrak{L}$-функций можно выделить пять классов функций с различным порядком роста:

$$\text{Subpoly} = \left\{ f(x) \,\middle|\, f(x) \prec e^{O(\ln x)} \right\};$$

$$\text{Poly} = \left\{ f(x) \,\middle|\, f(x) = O[e^{O(\ln x)}] \right\};$$

$$\text{Subexp} = \left\{ f(x) \,\middle|\, e^{O(\ln x)} \prec f(x) \prec e^{O(x)} \right\};$$

$$\text{Exp} = \left\{ f(x) \,\middle|\, f(x) = O[e^{O(x)}] \right\};$$

$$\text{Hyperexp} = \left\{ f(x) \,\middle|\, e^{O(x)} \prec f(x) \right\}.$$

Эта классификация основана на том, что всякая $\mathfrak{L}$-функция $f(x)$ представима в виде $f(x) = e^{w(x)}$, где $w(x) = \ln f(x) \in \mathfrak{L}$, а экспоненты вида $e^{w(x)}$ подчиняются асимптотической иерархии, при этом

$$e^{w_1(x)} \prec e^{w_2(x)} \Leftrightarrow \lim_{x\to\infty} [w_1(x) - w_2(x)] = -\infty, \quad 1 \prec w_1(x) \prec w_2(x) \Rightarrow e^{w_1(x)} \prec e^{w_2(x)}. \quad (1)$$

Кроме того, для произвольных вещественных положительных констант ξ_1, ξ_2, ξ_3, τ_1, τ_2, τ_3 отношение

$$x^{\xi_1}(\ln x)^{\xi_2}(\ln\ln x)^{\xi_3} \prec x^{\tau_1}(\ln x)^{\tau_2}(\ln\ln x)^{\tau_3} \quad (2)$$

справедливо, если и только если $\xi_1 < \tau_1$, или если $\xi_1 = \tau_1$, $\xi_2 < \tau_2$, или если $\xi_1 = \tau_1$, $\xi_2 = \tau_2$, $\xi_3 < \tau_3$ [9].

2. Эластичность и ее свойства

Эластичный (гр. *elastikos*) — упругий, гибкий, легко приспособляющийся. С физической точки зрения эластичность — это свойство вещества оказывать механическое сопротивление силе, которая на него воздействует, и принимать исходную форму после спада данной силы. Изучается в теории упругости. С экономической точки зрения эластичность — это характеристика изменения одного показателя (например, спроса)

по отношению к другому показателю (например, цене товара). Используется в эконометрике для анализа производственных функций [10]. С математической точки зрения эластичность $E_x(y)$ — это коэффициент пропорциональности между темпами роста величин $y = t(x)$ и x. Формально, это дифференциальная характеристика функции $y = t(x)$, определяемая как предел отношения относительного приращения этой функции к относительному приращению аргумента [11]:

$$E_x(y) = \lim_{\Delta x \to 0} \left(\frac{\Delta y}{y} : \frac{\Delta x}{x} \right) = \frac{x}{y} \lim_{\Delta x \to 0} \frac{\Delta y}{\Delta x} = \frac{x}{y} y' = x(\ln y)' = \frac{(\ln y)'}{(\ln x)'}. \tag{3}$$

Таким образом, если $E_x(t)$ — эластичность функции временной сложности $y = t(x)$, то при повышении значения x (длины входа алгоритма) на один процент значение t (время выполнения алгоритма) увеличится приблизительно на $E_x(t)$ процентов.

Справедливы следующие свойства эластичности [11, 12].

1. Всякая постоянная имеет нулевую эластичность.
2. Эластичность — безразмерная величина: $E_x(y) = E_{ax}(by)$.
3. Эластичность обратной функции $x = f^{-1}(y)$ — обратная величина: $E_y(x) = 1/E_x(y)$
4. Эластичность произведения функций $u = u(x)$ и $w = w(x)$ равна сумме их эластичностей: $E_x(u \cdot w) = E_x(u) + E_x(w)$. Так, умножение функции на отличную от нуля константу не изменяет эластичности.
5. Эластичность отношения функций $u = u(x)$ и $w = w(x)$ равна разности их эластичностей: $E_x(u/w) = E_x(u) - E_x(w)$.
6. Эластичность суммы функций $u = u(x)$ и $w = w(x)$ — сумма эластичностей слагаемых, взятых с соответствующими весами:
   $E_x(u + w) = (u/(u + w))E_x(u) + (w/(u + w))E_x(w)$.
7. Эластичность показательно-степенной функции вида $y = u^w$, где $u = u(x)$ и $w = w(x)$, задается соотношением $E_x(y) = w(E_x(w) \ln u + E_x(u))$. В частности, $E_x[e^{w(x)}] = wE_x(w)$.
8. Эластичность композиции функций $y = f(w)$ и $w = w(x)$ равна
   $E_x(y) = E_w(f)E_x(w)$.

Непосредственное применение (3) и свойств 1–8 дает формулы эластичностей основных $\mathfrak{L}$-функций. В табл. 1 указаны асимптотические оценки эластичностей основных $\mathfrak{L}$-функций при $x \to \infty$. Здесь везде полагается, что значения x такие большие, что значения аргумента всякого логарифма и значения самого логарифма всегда остаются строго больше нуля.

Таблица 1

Эластичность основных $\mathfrak{L}$-функций

Функция $y = f(x)$	Эластичность $E_x[f(x)]$	Принадлежность к классу функций
Константа $c > 0$	0	$f(x) \in \mathrm{Subpoly}$
Каскад из k логарифмов $\underbrace{\ln\ln\ldots\ln}_{k\text{ раз}} x$, $x > 1, k = 1, 2, \ldots$	$\dfrac{1}{\ln x \cdot \ldots \cdot \underbrace{\ln\ln\ldots\ln}_{k\text{ раз}} x} = o(1)$	$f(x) \in \mathrm{Subpoly}$
Полилогарифм $(\ln x)^m$, $x > 1, m > 0$	$\dfrac{m}{\ln x} = o(1)$	$f(x) \in \mathrm{Subpoly}$
Показательный полилогарифм $e^{\lambda(\ln x)^m} = x^{\lambda(\ln x)^{m-1}}$ $x > 1, \lambda > 0, 0 < m < 1$	$\lambda m(\ln x)^{m-1} = o(1)$	$f(x) \in \mathrm{Subpoly}$
Степенная функция $e^{k(\ln x)^m} = x^{k(\ln x)^{m-1}} = x^k$ $x > 1, k > 0, m = 1$	$k = O(1)$	$f(x) \in \mathrm{Poly}$
Показательно-степенной логарифм $e^{m \ln x \ln\ln x} = x^{m \ln\ln x} =$ $= (\ln x)^{m \ln x}$, $x > 1, m > 0$	$m(1 + \ln\ln x) =$ $= O(\ln\ln x)$	$f(x) \in \mathrm{Subexp}$
Показательный полилогарифм $e^{\lambda(\ln x)^m} = x^{\lambda(\ln x)^{m-1}}$, $x > 1, \lambda > 0, m > 1$	$\lambda m(\ln x)^{m-1} = O[(\ln x)^{m-1}]$	$f(x) \in \mathrm{Subexp}$
Частный случай показательного полилогарифма $e^{\lambda x^\xi (\ln x)^{1-\xi}}$, $x > 1, 0 < \xi < 1$	$\lambda x^\xi (\ln x)^{1-\xi}(\xi + \dfrac{1-\xi}{\ln x}) =$ $= O[x^\xi (\ln x)^{1-\xi}]$	$f(x) \in \mathrm{Subexp}$
Экспонента конечного порядка роста $e^{\lambda x^k}$, $x > 0, \lambda > 0, k > 0$	$\lambda k x^k = O(x^k)$	$f(x) \in \mathrm{Subexp}, 0 < k < 1$ $f(x) \in \mathrm{Exp}, k = 1$ $f(x) \in \mathrm{Hyperexp}, k > 1$
«Башня» $\underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2^x}}}}}}_{k\text{ этажей}}$, $k \geqslant 1$	$k 2^x 2^{2^x} \cdots \underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2^x}}}}}}_{k-1\text{ этажей}} (\ln 2)^k$	$f(x) \in \mathrm{Exp}, k = 1$ $f(x) \in \mathrm{Hyperexp}, k > 1$

3. Классы логарифмически-экспоненциальных функций и их эластичности

В работе [12] доказана теорема, устанавливающая характеризацию эластичности для пяти классов $\mathfrak{L}$-функций.

Теорема 1 (о классификации $\mathfrak{L}$-функций) [12]. Разбиение семейства монотонно неубывающих «по-существу положительных» $\mathfrak{L}$-функций на классы Subpoly, Poly, Subexp, Exp, Hyperexp в соответствии с порядком их роста эквивалентно надлежащему разбиению по асимптотике эластичности этих функций на бесконечности:

$$\text{Subpoly} = \left\{ f(x) \,\middle|\, f(x) \prec e^{O(\ln x)} \right\} \equiv \left\{ f(x) \,|E_x(f) = o(1) \right\}; \tag{4}$$

$$\text{Poly} = \left\{ f(x) \,\middle|\, f(x) = O[e^{O(\ln x)}] \right\} \equiv \left\{ f(x) \,|E_x(f) = O(1) \right\}; \tag{5}$$

$$\text{Subexp} = \left\{ f(x) \,\middle|\, e^{O(\ln x)} \prec f(x) \prec e^{O(x)} \right\} \equiv \left\{ f(x) \,|1 \prec E_x(f) \prec x \right\}; \tag{6}$$

$$\text{Exp} = \left\{ f(x) \,\middle|\, f(x) = O[e^{O(x)}] \right\} \equiv \left\{ f(x) \,|E_x(f) = O(x) \right\}; \tag{7}$$

$$\text{Hyperexp} = \left\{ f(x) \,\middle|\, e^{O(x)} \prec f(x) \right\} \equiv \left\{ f(x) \,|x \prec E_x(f) \right\}. \tag{8}$$

Из данной теоремы и свойств эластичности вытекают важные следствия.

Следствие 1. Разбиение $\mathfrak{L}$-функций на классы Subpoly, Poly, Subexp, Exp, Hyperexp инвариантно относительно полиномиального преобразования, т. е. если $f(x) \in \mathfrak{F}$, $\mathfrak{F} \in \{\text{Subpoly, Poly, Subexp, Exp, Hyperexp}\}$, то также $p(f(x)) \in \mathfrak{F}$, где $p(x) \in \text{Poly}$.

Действительно, по свойству 8 имеем: $E_x[p(f(x))] = E_f(p)Ex(f) = O(1)Ex(f)$. Согласно (4) – (8), умножение эластичности на асимптотическую константу не меняет принадлежность $\mathfrak{L}$-функции к классу $\mathfrak{F} \in \{\text{Subpoly, Poly, Subexp, Exp, Hyperexp}\}$.

Следствие 2. Класс Subpoly замкнут относительно суперпозиции (композиции) $\mathfrak{L}$-функций, т. е. если $f(x), q(x) \in \text{Subpoly}$, то $q(f(x)) \in \text{Subpoly}$.

Следствие 3. Класс Poly замкнут относительно суперпозиции $\mathfrak{L}$-функций, т. е. если $f(x), q(x) \in \text{Poly}$, то $q(f(x)) \in \text{Poly}$.

Следствие 4. Класс Hyperexp замкнут относительно суперпозиции $\mathfrak{L}$-функций, т. е. если $f(x), q(x) \in \text{Hyperexp}$, то $q(f(x)) \in \text{Hyperexp}$.

Композиция $\mathfrak{L}$-функций из классов Subexp, Exp может изменить их принадлежность к этим классам.

4. Систематизация алгоритмов

Теорема о классификации $\mathfrak{L}$-функций позволяет формально описать пять современных сложностных классов алгоритмов. Класс быстрых алгоритмов — множество алгоритмов с функциями сложности $t(x) \in \text{Subpoly}$. Таким алгоритмам присуща тождественно нулевая или бесконечно малая эластичность. Класс полиномиальных алгоритмов — множество алгоритмов с $t(x) \in \text{Poly}$ и асимптотически постоянной эластичностью $E_x(t)$. Класс субэкспоненциальных алгоритмов — алгоритмы, для которых $t(x) \in \text{Subexp}$. Эластичность $E_x(t)$ субэкспоненциального алгоритма — бесконечно большая величина, такая, что $1 \prec E_x(t) \prec x$. Для такого алгоритма темп роста времени выполнения значительно выше темпа роста длины входа. Класс экспоненциальных алгоритмов — это алгоритмы, для которых $t(x) \in \text{Exp}$. Для них эластичность $E_x(t) = O(x)$ — бесконечно большая величина, асимптотически пропорциональная линейной функции. Функции с подобной эластичностью описывают законы естественного

роста: скорость увеличения такой функции прямо пропорциональна ей самой. Класс гиперэкспоненциальных алгоритмов — это алгоритмы, для которых $t(x) \in \text{Hyperexp}$ и $x \prec E_x(t)$. Темп роста гиперэкспоненциальных функций настолько высок, что не укладывается в законы естественного роста.

Исходя из следствий 1 – 4, классификации алгоритмов на основе асимптотического поведения эластичности функций сложности присущи следующие практически значимые особенности:

- инвариантность относительно модели вычислений, поскольку переход от одной модели вычислений к другой меняет вычислительную сложность алгоритма полиномиальным образом. Это отвечает традиции измерять вычислительную сложность алгоритма с точностью до $O(1)$ и сопоставлять алгоритмы с точностью до полинома [1];
- неизменность сложностного класса алгоритма при полиномиальном преобразовании входа алгоритма. Подобные преобразования могут возникать при учете в модели вычислений времени доступа к исходным данным алгоритма;
- суперпозиция быстрых алгоритмов приводит к быстрому алгоритму;
- суперпозиция полиномиальных алгоритмов приводит к алгоритму полиномиальной сложности.

5. Методика сравнения алгоритмов по асимптотическому поведению эластичности

Если необходимо установить класс, к которому принадлежит алгоритм с функцией сложности $t(n) \in \mathfrak{L}$, то следует выполнить следующие действия:

- осуществить формальный переход от $t(n)$ к $t(x)$, т. е. от дискретного аргумента n к непрерывному x;
- вычислить $E_x(t)$ и найти асимптотическую оценку для $E_x(t)$ при $x \to \infty$;
- определить класс функций, используя эквивалентности (4) – (8).

Пусть требуется сравнить алгоритмы α_1 и α_2, вычислительная сложность которых описывается функциями $t_1(x)$ и $t_2(x)$ соответственно. Для этого сначала надлежит установить классы сложности для α_1 и α_2. Если данные алгоритмы принадлежат разным классам сложности, то иерархия этих классов задает соответствующее отношение между α_1 и α_2 в смысле их быстродействия. Если оказалось, что алгоритмы α_1 и α_2 принадлежат одному классу, то многое зависит от самого этого класса:

- если $t_1(x), t_2(x) \in \text{Subpoly, Subexp, Hyperexp}$, то при $E_x(t_1) \prec E_x(t_2)$ всегда $t_1(x) \prec t_2(x)$, т. е. алгоритм α_1 асимптотически быстрее алгоритма α_2;
- если $t_1(x), t_2(x) \in \text{Poly, Exp}$, то $E_x(t_1) \sim cE_x(t_2), c > 0$. При большой длине входа и $0 < c < 1$ время выполнения алгоритма α_1 меньше времени работы алгоритма α_2 приблизительно в $1/c$ раз. При $c > 1$, наоборот, алгоритм α_1 работает медленнее алгоритма α_2 примерно в c раз. При $c = 1$ требуется исследование в $E_x(t_1), E_x(t_2)$ членов более низкого порядка, нежели константа.

Проиллюстрируем последний случай. Рассмотрим два алгоритма, осуществляющих операцию умножения двух длинных n-разрядных целых чисел: алгоритм Шенхаге — Штрассена, имеющий функцию сложности

$$t_1(n) = c_1 n \ln n \ln\ln n,$$

и алгоритм Тоома — Кука, характеризующийся трудоемкостью

$$t_2(n) = c_2 n e^{(2\ln n)^{1/2}} \ln n,$$

где $c_1 > 0$, $c_2 > 0$ — некоторые константы [4]. Если выполнить формальный переход от n к x, то $t_1(x)$, $t_2(x)$ — «по-существу положительные» монотонно возрастающие $\mathfrak{L}$-функции. Определим для них эластичности:

$$E_x(t_1) = E_x(c_1 x \ln x \ln\ln x) = E_x(c_1) + E_x(x) + E_x(\ln x) + E_x(\ln\ln x) =$$
$$= 0 + 1 + \frac{1}{\ln x} + \frac{1}{\ln x \ln\ln x} = 1 + \gamma_1(x) > 0,$$
$$E_x(t_2) = E_x(c_2 x e^{(2\ln x)^{1/2}} \ln x) = E_x(c_2) + E_x(x) + E_x(e^{(2\ln n)^{1/2}}) + E_x(\ln x) =$$
$$= 0 + 1 + \frac{\sqrt{2}}{(\ln x)^{1/2}} + \frac{1}{\ln x} = 1 + \gamma_2(x) > 0.$$

Поскольку $\gamma_1(x) = o(1)$, $\gamma_2(x) = o(1)$, то $t_1(x), t_2(x) \in \mathrm{Poly}$ и $E_x(t_1) \sim E_x(t_2)$. Выполним сравнение бесконечно малых величин $\gamma_1(x) > 0$, $\gamma_2(x) > 0$ при $x \to \infty$:

$$\lim_{x\to\infty} \frac{\gamma_1(x)}{\gamma_2(x)} = \lim_{x\to\infty} \left(\frac{\ln\ln x + 1}{\ln x \ln\ln x} : \frac{(2\ln x)^{1/2} + 1}{\ln x} \right) = \lim_{x\to\infty} \left(\frac{\ln\ln x + 1}{\ln x \ln\ln x} \cdot \frac{\ln x}{(2\ln x)^{1/2} + 1} \right) =$$
$$= \lim_{x\to\infty} \left(\frac{\ln\ln x + 1}{\ln\ln x} \cdot \frac{1}{(2\ln x)^{1/2} + 1} \right) = \lim_{x\to\infty} \left(1 + \frac{1}{\ln\ln x} \right) \cdot \left(\frac{1}{(2\ln x)^{1/2} + 1} \right) = 1 \cdot 0 = 0.$$

Отсюда $\gamma_1(x) \prec \gamma_2(x)$ и $E_x(t_1) \prec E_x(t_2)$ при $x \to \infty$. Следовательно, алгоритм Шенхаге — Штрассена асимптотически быстрее алгоритма Тоома — Кука. Как следует из данного примера, в ряде случаев при сравнении алгоритмов не удается избежать непосредственного сравнения функций при помощи O-большое и o-малое. Это касается полиномиальных и экспоненциальных алгоритмов с асимптотически пропорциональными эластичностями. Здесь могут оказаться полезными соотношения (1), (2), относящиеся к иерархии $\mathfrak{L}$-функций.

6. Сложность и эластичность теоретико-числовых алгоритмов

Разработка и анализ теоретико-числовых алгоритмов — предмет исследований алгоритмической теории чисел, имеющей приложения в криптографии [6, 7]. В криптографии (для обоснования стойкости криптографических систем и для разработки методов их вскрытия) важны следующие методы и алгоритмы [5]: тесты на простоту целых чисел, методы факторизации (разложения целых чисел на множители), алгоритмы дискретного логарифмирования, алгоритмы выполнения арифметических операций с длинными целыми числами, алгоритмы полиномиальной арифметики и др.

Традиционно функции сложности теоретико-числовых алгоритмов являются функциями от n — количества двоичных разрядов (битов), требуемых для записи исходного длинного целого числа N. Таким образом, $n = O(\log_2 N) = O(\ln N)$. В табл. 2 приведены классы сложности и эластичности наиболее известных тестов на простоту и алгоритмов факторизации длинных целых чисел. Функции сложности этих алгоритмов взяты из работы [5]. В функциях сложности осуществлен формальный переход от дискретного аргумента n к непрерывному x.

Таблица 2

Эластичность некоторых теоретико-числовых алгоритмов

Алгоритм	Функция сложности $t(x)$ алгоритма	Эластичность $E_x[t(x)]$ алгоритма	Класс сложности алгоритма
Тест на простоту Конягина — Померанса	$O(1)\dfrac{x^{17/7}}{\ln x}$	$o(1)+\dfrac{17}{7}-\dfrac{1}{\ln x}=$ $=O(1)$	Poly
Тесты на простоту Адлемана — Померанса — Румели и Ленстры	$O(1)x^{c\ln\ln x}, c>0$	$o(1)+$ $+c(1+\ln\ln x)=$ $=O(\ln\ln x)$	Subexp
Тест на простоту Аггравала — Кайала — Саксены	$O(1)x^{12}(\ln x)^c, c>0$	$o(1)+12+\dfrac{c}{\ln x}=$ $=O(1)$	Poly
Факторизация целых чисел по методу Диксона	$e^{cx^{\xi}(\ln x)^{1-\xi}}$ $\xi=\frac{1}{2}, c>0$	$o(1)+cx^{1/2}(\ln x)^{1/2}\cdot$ $\cdot(\dfrac{1}{2}+\dfrac{1}{2\ln x})=$ $=O\left[x^{1/2}(\ln x)^{1/2}\right]$	Subexp
Факторизация целых чисел по методу GNFS (general number field sieve)	$e^{cx^{\xi}(\ln x)^{1-\xi}}$ $\xi=\dfrac{1}{3}, c>0$	$o(1)+cx^{1/3}(\ln x)^{1/3}\cdot$ $\cdot(\dfrac{1}{3}+\dfrac{2}{3\ln x})=$ $=O\left[x^{1/3}(\ln x)^{2/3}\right]$	Subexp
Факторизация целых чисел по методу Шермана — Лемана	$O(1)e^{x/3}$	$o(1)+x/3=O(x)$	Exp
Факторизация целых чисел по методу Полларда — Штрассена	$O(1)x^4e^{x/4}$	$o(1)+4+x/4=O(x)$	Exp

Заключение

Классификация алгоритмов на основе асимптотического поведения эластичности функций сложности не разрушает прежней, традиционной классификации с полиномиальными и экспоненциальными алгоритмами, а лишь дополняет и уточняет ее. Свойства эластичности позволяют без особого труда находить эластичность для любой $\mathfrak{L}$-функции. К ограничениям рассмотренной классификации следует отнести требование принадлежности функций сложности алгоритмов к семейству Харди. Однако в большинстве реальных случаев это требование является вполне естественным и не вызывает особых трудностей при анализе алгоритмов.

Представленные в работе результаты (следствия 1 – 4, методика сравнения алгоритмов по асимптотическому поведению эластичности, формулы эластичностей для основных $\mathfrak{L}$-функций и теоретико-числовых алгоритмов) могут быть полезны в определении стойкости современных криптографических систем и для разработки методов их вскрытия.

ЛИТЕРАТУРА

1. *Юдин Д. Б., Юдин А. Д.* Математики измеряют сложность. М.: Книжный дом «Либроком», 2009. 192 с.
2. *Быкова В. В.* Математические методы анализа рекурсивных алгоритмов // Журнал СФУ. Математика и физика. 2008. № 1(3). С. 236–246.
3. *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982. 416 с.
4. *Кормен Т., Лейзерсон Ч., Ривест Р.* Алгоритмы: построение и анализ. М.: МЦНМО, 1999. 960 с.
5. *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2006. 336 с.
6. *Чмора А. Л.* Современная прикладная криптография. М.: Гелиос АРВ, 2001. 256 с.
7. *Варновский Н. П.* Криптография и теория сложности // Математическое просвещение. 1998. Сер. 3. Вып. 2. С. 71–86.
8. *Харди Г. Х.* Курс чистой математики. М.: ИЛ, 1949. 512 с.
9. *Грэхем Р., Кнут Д., Поташник О.* Конкретная математика. М.: Мир; Бином. Лаборатория знаний, 2006. 703 с.
10. *Доугерти К.* Введение в эконометрику. М.: ИНФРА-М, 2001. 402 с.
11. *Солодовников А. С., Бабайцев В. А., Браилов А. В., Шандра И. Г.* Математика в экономике. М.: Финансы и статистика, 2001. 376 с.
12. *Быкова В. В.* Метод распознавания классов алгоритмов на основе асимптотики эластичности функций сложности // Журнал СФУ. Математика и физика. 2009. № 2(1). С. 48–61.