3. Если произведение совпало с p-1, то рекурсивно проверим, что каждый сомножитель является простым.4)Если не все сомножители q являются простыми, угадаем значение x и проверим неравенство $x^{(p-1)/q} \neq 1$ для каждого q, делящего p-1. Тем самым устанавливается, что *ord x* равен p-1, иначе *ord x* должен делиться на один из множителей (p-1) /q, что противоречит полученному выше неравенству. Возведение в степень осуществляется эффективным алгоритмом, сделав не более k умножений ($k< n$), затратив времени $O(n^3)$, так что общее время – $O(n^4)$. Построенный недетерминированный алгоритм полиномиален вдоль каждой ветви, кроме шага 3. Рекурсивное вычисление на шаге 3, представим в виде дерева, в корне которого находится n-битовое число p, сыновьями являются угаданные сомножители числа p-1, под каждым q_i – угаданные сомножители числа q_i –1 и т.д. Таким образом, время работы на каждой ветке $O(n^5)$.

УДК 519.6

О точных решениях линейных уравнений в комплексных круговых интервалах

В.С. Дронов, Н.А. Кузнецов
АлтГУ, г. Барнаул

Несмотря на то, что расширение подхода интервального анализа с действительного случая на комплексный является давней идеей (см., например, [1]), и существует достаточно обширный класс задач, приводящих к появлению интервальной неопределённости в комплексных данных (см. в [2] примеры задач, растущих из практики, и в [3] примеры теоретических), в целом комплексные интервальные методы развиты ощутимо хуже действительных.

Одной из проблем переноса интервальных методов на комплексный случай являются свойства операций над комплексными числами, во многих случаях «ломающие» простоту действительных подходов. Во многом из-за разных взглядов на то, что в комплексных данных заслуживает интервализации, не существует и единого подхода к определению комплексного интервала. Двумя имеющими давнюю историю вариантами являются прямоугольные и круговые комплексные интервалы (естественным образом связанные с алгебраической и тригонометрической формой записи комплексного числа). Не менее естественной в этом смысле, но менее известной формой являются секторные интервалы в терминах [2]:

$$\{x \epsilon C : x = \rho e^{i\theta}, \rho \in \boldsymbol{\rho}, \theta \in \boldsymbol{\theta}\}$$

Классическим результатом для так называемого объединённого множества решений систем линейных уравнений в действительном интервальном случае является теорема Бека-Никеля, обеспечивающая возможность оценки объединённого множества решений по крайним точкам исходных интервальных данных. Из-за свойств операций над комплексными числами, прямой перенос этой теоремы на комплексный случай или прямо неверен (для прямоугольных и секторных интервалов), или существенно менее полезен из-за отсутствия порядка на комплексных числах (для круговых интервалов). В действительном случае объединённое множество решений интервальной системы линейных уравнений представляет собой «звёздчатое» множество – пересечение которого с каждым ортантом представляет собой выпуклое многогранное множество. Для комплексного случая это неверно. На рисунке 1 приводится пример из [4], где рассмотрено устройство объединённого множества решений для прямоугольных комплексных интервалов.

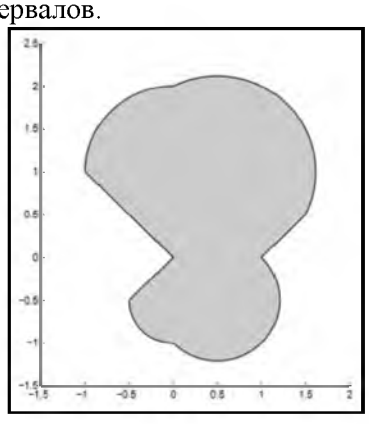

Рисунок 1 – объединённое множество решений уравнения
[1-i, 5+i]**z**=[-i, 1+2i] в прямоугольных интервалах

Стандартной проблемой, вызывающей расширение интервалов при использовании интервальных операций является «эффект обёртывания», вызванный несовпадением интервальной оболочки результата операции и точного множества. Рисунок 2 показывает множества представителей результатов умножения и деления в прямоугольной комплексной арифметике (для умножения тускло-серым показана интервальная оболочка).

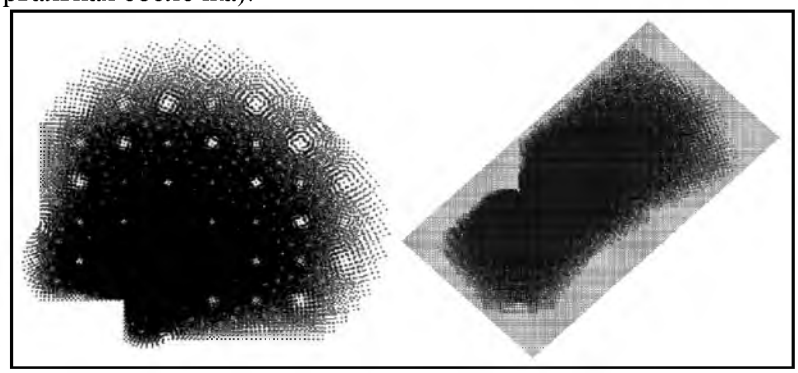

Рисунок 2 – результаты деления (слева) и умножения (справа) прямоугольных интервалов

Операции в круговых интервалах также подвержены «эффекту обёртывания», что видно на рисунке 3.

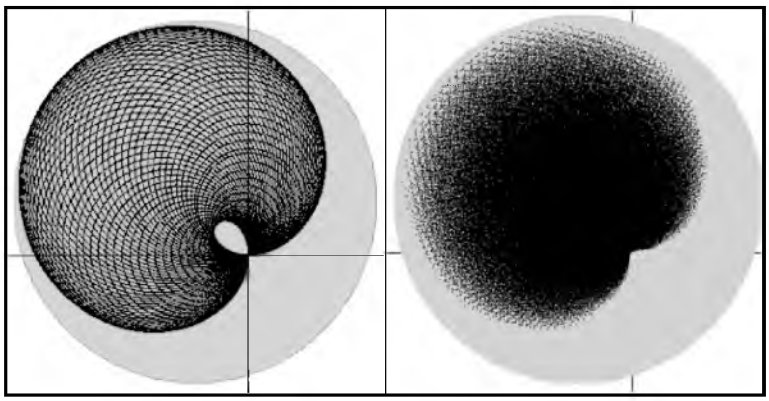

Рисунок 3 – интервальная оболочка (серая) и границы точного произведения для круговых интервалов радиуса 1 с центрами в 1 и -1+i

Рисунок 3 можно считать изображением точного множества решения для системы в круговых интервалах из единственного уравнения (наглядная визуализация случаев большей размерности не столь удобна). Левая часть лучше показывает границы, однако внутренняя петля множества – артефакт подхода; рисунок получен перемножением границ круговых интервалов. Свойства операций над круговыми интервалами обеспечивают в этом случае надёжность внешней границы множества, но не захват внутренних точек, что видно по правой части рисунка, полученного перемножением представителей: границы здесь более размыты, но видно отсутствие пустоты на месте петли.

Можно утверждать, что границы множеств точных решений линейных уравнений в круговых интервалах представляют собой кривые четвёртого порядка, что выгодно отличает их от прямоугольных. При этом, в отличие от тривиальных операций сложения и вычитания, умножение и деление на нольнесодержащий интервал приводит ко множеству, граница которого описывается улиткой Паскаля. При этом при удалении от нуля происходит улучшение оценки результата секторным интервалом на фоне кругового, что может говорить о перспективности смешанных секторно-круговых оценок.

Библиографический список

1. Boche. R. Complex interval arithmetic with some applications. – Lockheed Missules and Space company, Sunnyvale, California, 1966. – 34 с.

2. Candau Y., Raissi T., Ramdani N., Ibos L. Complex interval arithmetic using polar form //Reliable Computing. – 2006. – №1 – С. 1–20.

3. Petcovic M., Petcovic L., Complex interval arithmetic and its applications. – Mathematical Research, Vol. 105 – Berlin, VILEY-VCH, 1998.

4. Hladík M. Solution sets of complex linear interval systems of equations. //Reliable Computing – 2010 – №14 – С. 78–87.