ОДНОРОДНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ
(Вычислительные системы)
1981 год Выпуск 90

УДК 519.15:681.323

О СУЩЕСТВОВАНИИ ПРЕДЕЛЬНЫХ КАИС-СТРУКТУР

С.А. Сыскин

В книге [1] сформулирована следующая

ГИПОТЕЗА. Для любых натуральных N и n существует предельная КАИС-структура порядка N и размерности n.

Все определения можно найти в [1]. При $n \geq 3$ эта гипотеза, вообще говоря, неверна: при $n = 3$ и $N = 25$ не существует предельных КАИС-структур. В настоящей заметке будет доказана

ТЕОРЕМА. Для любого целого $N \geq 1$ существует предельная КАИС-структура порядка N и размерности 2, обладающая циклической группой автоморфизмов.

Сделаем сначала несколько пояснений.

Все встречающиеся далее числа будут целыми. Выберем на плоскости прямоугольную систему координат и два числа a, b. Отметим каждую точку плоскости с координатами (x,y) числом $ax + by$. Для каждого $m \geq 1$ определим R_m как множество точек (x,y) с $|x|+|y| \leq m$. Легко видеть, что R_m - ромб, содержащий ровно $2m(m+1) + 1$ точек с целыми координатами. Наша теорема утверждает, что если m таково, что $2m(m-1) + 1 < N \leq 2m(m+1) + 1$, то числа a и b можно взять так, что в ромбе R_{m-1} все числа $ax + by$ различны по модулю N, и для любого n найдется такое $(x,y) \in R_m$, что $ax+by \equiv n \pmod N$. Более точно, мы покажем, что

при $N \leq 2m^2 - 2$ можно взять $a = m$, $b = m-1$; (1)

при $N > 2m^2 - 2$ можно взять $a = m+1$, $b = m$. (2)

ДОКАЗАТЕЛЬСТВО теоремы. Пусть сначала $N \leq 2m^2 - 2$. Положим $a = m$, $b = m-1$. Мы должны доказать, что

а) в ромбе R_{m-1} стоят различные по модулю N числа;

б) для каждого n существуют такие x,y с $(x,y) \in R_m$, что $ax + by \equiv n \pmod N$.

Проверим "а". Индукция по m дает, что теорема справедлива для $N_1 = 2m(m-1) + 1$. Так как $N_1 > 2(m-1)^2 - 2$, то для N_1 мы должны, согласно формулировке теоремы, выбрать параметры $a = m$, $b = m-1$, как и для N. Другими словами, все числа $ax+by$, лежащие в ромбе R_{m-1}, различны по модулю N_1. Так как максимальное из них равно $m(m-1)$, а минимальное равно $-m(m+1)$, то все эти числа различны и по модулю N, что и доказывает "а". Более того, отсюда следует, что в R_{m-1} стоят в точности все числа от $-m(m+1)$ до $m(m+1)$.

Теперь проверим "б". Можно считать ввиду предыдущего, что $n > m(m-1)$ или $n < -m(m-1)$. Далее, мы можем считать, что $|n| \le N$. Легко видеть, что на правом верхнем ребре ромба (которое является отрезком прямой $x+y=n$) стоят числа от $m(m-1)$ до m^2, а на левом нижнем ребре – числа от $-m^2$ до $-m(m-1)$. Другими словами, в ромбе R_m стоят все числа от $-m^2$ до m^2. Так как $2m^2 > N$ по условию, то среди этих $2m^2+1$ чисел находятся все остатки от деления на N, что и доказывает (I).

Теперь рассмотрим случай $N > 2m^2-2$. Положим $a=m+1$ и $b=m$. Нам надо, как и в предыдущем случае, доказать "а" и "б".

Проверим "а". (К сожалению, здесь нельзя так же применить индукцию.) Допустим, что существуют такие числа x, y, i, j, что $(x,y) \ne (i,j)$, $|x| + |y| \le m-1$, $|i| + |j| \le m-1$ и $x(m+1) + ym \equiv i(m+1) + jm \pmod N$, или $(x-i)(m+1) + (y-j)m \equiv 0 \pmod N$. Умножив, если необходимо, последнее равенство на -1, мы можем считать, что в его левой части стоит неотрицательное число. Заметим, что оно меньше N. В самом деле, $(x-i)(m+1) + (y-j)m = (x+y)m - (i+j)m + (x-i) \le (m-1)m + (m-1)m + 2(m-1) = 2m^2 - 2 < N$ по условию, что и требовалось. Следовательно, $(x-i)(m+1) + (y-j)m = 0$, поэтому $(x-i)$ делится на m, а $y-j$ делится на $m+1$. Если $x - i = 0$, то $y-j = 0$, т.е. $(x,y) = (i,j)$, поэтому $|x-i| \ge m$, $|y-j| \ge m+1$, откуда $2m+1 \le |x-i| + |y-j| \le |x| + |y| + |i| + |j| \le 2m-2$, противоречие. Утверждение "а" доказано.

Теперь докажем "б". Здесь мы можем считать, что $N = 2m(m+1) + 1$. В самом деле, если все числа из R_m дадут ровно $2m(m+1) + 1$ различных остатков от деления на $2m(m+1) + 1$, то они дадут и все N остатков от деления на N. Таким образом, пусть $N = 2m(m+1) + 1$. Нам достаточно доказать теперь, что в R_m нет двух одинаковых чисел, а это делается как и в предыдущем абзаце.

Теорема доказана.

Автор выражает благодарность В.В.Корнееву, беседы с которым настроили на решение этой задачи.

Литература

I. ЕВРЕИНОВ Э.В., ХОРОШЕВСКИЙ В.Г. Однородные вычислительные системы. - Новосибирск: Наука, 1978. - 308 с.

Поступила в ред.-изд.отд.
16 июня 1981 года