Выразимость в арифметике

1. Теория делимости

Выразимо a делится на b. Легко выразимо, что a простое: у a нет делителей, кроме a и 1.

Выражение a — степень двойки: все делители a делятся на 2 или равны 1.

Удвоенная степень двойки — тоже степень двойки.

Лемма о чётности: каждое число имеет ровно один из двух видов: $2 \times k$ или $2 \times k + 1$. Доказываем по индукции: $0 = 2 \times 0$, $0e2 \times k + 1$. Далее говорим, что $(2 \times k + 1) + 1 = 2 \times (k + 1)$ и что если $x + 1 = 2 \times k$, то $ke0$, $k = l + 1$, $x = 2 \times l + 1$.

Действительно, пусть $2 \times k = a \times b$, a — нечётно, $ae1$. Тогда если b чётно, то $b = 2 \times c$, $2 \times k = 2 \times c \times a$, $k = a \times c$. Иначе же $a - 1$ и $b - 1$ чётны, тогда $a \times b$ нечётно.

Легко выразить, что a — ближайшая большая степень двойки к x. Разумеется, при этом a — степень двойки и $x < a < 2 * x$

Для каждого x есть такое a, что ясно по индукции.

Легко определить, что q и r — неполное частное и остаток от деления a на b.

Их существование легко доказать по обобщённой индукции: либо $a < b$, либо существует c, такое что $c + b = a$. Поделим c с остатком на a и прибавим к неполному частному 1. Единственность доказывается как обычно.

2. Работа с двоичными словами

Кодирование пар. Например, $(a, b) \to 4 \times (a + b) \times (a + b) + b + 1$.

c — конкатенация a и b Обозначим $\odot$. Легко доказать тотальность. При этом, при аккуратном определении оказывается, что двоичная запись числа 0 окажется пустым словом. Но это ничем не плохо. Кроме того, если $a \odot b = x \odot y = s$, то для некоторого t либо $s = a \odot t \odot y$, либо $s = x \odot t \odot b$.

Если множество задано парой M, l, где l — степень двойки, то можно написать $x \times 64 < l \wedge \exists a, b : a \odot (4 \times (l - 1)) \odot (4 \times x) \odot (4 \times (l - 1)) \odot b$. Это можно считать утверждением, что $x \in (M, l)$.

Можно наложить дополнительное требование, что каждое x может быть так найдено лишь в одном месте M и что M начинается на $4 * (l - 1)$, то есть на блок из единиц с двумя нулями после него, и заканчивается на $(l - 1)$. При этом надо бы уметь делать перекалибровку, то есть доказывать, что для любого l_2 существует M', такое что множество с кодом M', l_2 совпадает как набор элементов с множеством M, l_1. Это доказывается, например, через принцип минимального элемента про M при фиксированных l_1, l_2. Если M пустое, то можно явно записать перекалибровку; иначе можно взять самый левый элемент (тот, наличие которого в M, l_1 демонстрируется при минимальном a), отрезать связанный с ним блок от M, перекалибровать остальное и склеить с куском $4 \times (l-1) \odot x \times 4$. При этом для доказательства, что лишних элементов при приклеивании x не появится, надо будет проводить рассуждения с блоками единиц. В арифметике они пользуются утверждениями вида ``для всех степеней двойки в данном диапазоне неполное частное от деления M на них нечётно''. Нетрудно доказать, что с помощью перекалибровки можно добавлять и выкидывать элементы.

При этом, если хранить множество пар натуральных чисел, то можно получить не только конечное множество, но и последовательность

Пример: выразимость $x = 2^k$.

Существует последовательность пар, такая что в ней есть (0,1) и для каждого (n+1,s) есть (n, s/2). Кроме того, в ней есть (k, n). Существование 2^k для любого k доказывается по индукции.

Вычисление можно описать как последовательность изменений состояния по определённым правилам. Ответ - часть последнего состояния.

Выразимость понятия доказательства просто потому, что есть способ алгоритмической проверки.

Создадим через понятие вычислимости предикат proof(p, s), предполагая нумерацию доказательств и утверждений. $\Phi(n) : ot \exists p : proof(p, s_n(n))$, предполагая нумерацию формул с одним параметром. Подставим в качестве n номер $\Phi(x)$. Если эта формула доказуема, она не верна.