Об элементарной выразимости в логике предикатов

Капустин Ю.С.

В математике часто новые понятия вводятся с помощью некоторых кванторных определений. При наличии достаточно большого запаса таких понятий они могут позволить переформулировать новые кванторные определения бескванторным образом. Это делает заслуживающей рассмотрения задачу отыскания базисных понятий в заданной предметной области, которые делают избыточным дальнейшее кванторное определение. Интересной также является задача создания компьютерных программ, автоматически вводящих такие базисы.

В данной работе рассматриваются 3 простых случая сведения кванторной выразимости к бескванторной. Исследуются предикаты и функции, определенные через $\in$ и заданные на множестве $Z \cup 2^Z$, где Z — множество целых чисел. Кроме того, рассматриваются предикаты, выразимые через тот же предикат на множестве точек плоскости и прямых, лежащих в ней. Также рассмотрены предикаты, выразимые на множестве натуральных чисел с отношением делимости на нем. Во всех случаях удалось найти базисы бескванторной выразимости.

Ключевые слова: кванторная выразимость, логика предикатов.

1. Общие определения, используемые в работе

Пусть M — некоторое множество, содержащее $\varnothing$. Интерпретацией сигнатуры S над M будем называть отображение $\Sigma : S \to F$, сопоставляющее элементам множества символов S предикаты и операции, определенные на M. Множество M с заданной на нём системой операций и предикатов будем называть универсумом. Формулы и термы в интерпретации Σ определяются следующим образом:

1) x_i, где x_i – переменная из фиксированного счетного списка – терм.

2) Если $\Sigma(s) = f$ – n—местная операция на M, $t_1, \ldots, t_n$ – термы, то слово $s(t_1, \ldots, t_n)$ – терм.

3) Если $\Sigma(s) = p$ – n—местный предикат, определенный на M, $t_1, \ldots, t_n$– термы, то слово $s(t_1, \ldots, t_n)$ – терм.

4) Если $P_1, \ldots P_k$ — формула, то слова $(P_1 \bigvee \cdots \bigvee P_k), (P_1 \& \ldots \& P_k)$, $\neg P_1$,$P_1 \to P_2$ – формулы.

5) Если P – формула, $x_1, \ldots, x_n$ — символы переменных, то слова $\forall x_1, \ldots, x_n(P), \exists x_1, \ldots, x_n(P)$ – формулы.

6) Если P – формула, x – переменная, S содержит $\in$, то $set_x(P)$ — терм.

Каждая формула определяет естественным образом некоторый предикат, заданный на наборах элементов множества M. Каждый терм определяет естественным образом некоторую операцию, заданную на наборах элементов M, и принимающий значения в M. $set_x(P)$, где P – формула от свободной переменной x и свободных переменных $x_1, \ldots, x_n$ $set_x(P)$ интерпретируется как $\{y \in M : P(y) = \text{И}\}$ — операция от переменных $x_1, \ldots, x_n$, значение которой равно множеству всех x, на которых верен предикат, задаваемый формулой P. Если это множество при некоторых значениях свободных переменных, входящих в формулу P, не принадлежит M, то на этом значении переменных значение $set_x(P)$ равно $\varnothing$.

Если предикат или операция f определяется какой-либо формулой или термом в сигнатуре $\Sigma : S \to F$, то говорим, что f логически выразимо над F (через F). Если f определяется формулой или термом в Σ, не содержащим кванторов и описателей set, то говорим, что f элементарно выразимо над F.

2. Элементарная выразимость в универсуме U_1

Определим универсум U_1:

Пусть U_0 — произвольное счетное множество элементов, не являющихся множествами, $U_1 = 2^{U_0} \bigcup U_0$, и отношение $\in$ определяется на U_1 следующим образом:

— Если $x_1 \in U_1 \backslash U_0$ или $x_2 \in U_0$, то $x_1 \in x_2 = \text{Л}$

— Иначе значение $x_1 \in x_2$ определено естественным образом.

В данном простейшем случае оказалось возможным найти такой набор предикатов и операций, что все предикаты и операции, выразимые через $\in$ в U_1, элементарно выражаются через него. Верна теорема:

Теорема 1. *Все предикаты и операции, логически выразимые в U_1 через $\in$ – это те и только те, которые элементарно выражаются над Q=$\{a = \varnothing, \varnothing, U_0 \backslash a, a \bigcup b, \{a\}, Card_n(a)\}$, где первые пять предикатов и операций определены естественным образом:*

$U_0 \backslash a = set_x(\neg(x \in a)\&(x \in U_0))$

$a \bigcup b = set_x((x \in a)\&(x \in b))$ — *то есть, если один из операндов не является множеством, то с точки зрения значений операции он считается пустым множеством.*

$\{x\} = \varnothing$, *если* $\neg(x \in U_0)$, *иначе определяется стандартным образом. То есть* $\{z\} = set_x(x \in U_0\&(x = z))(= set_x(x \in U_0\&(\forall y(z \in y) \to (x \in y))))$

$Card_n(x) = U_0$ - *счетный набор операций с параметром n, проверяющих, является ли множество x n-элементным:*

$Card_n(x) = U_0$, *если n—элементно,* $\varnothing$ *иначе.*

Доказательство:

Доказательство теоремы можно разбить на несколько шагов:

1) Докажем, что $\in$ элементарно выразимо над данным набором.

2) Докажем, что все описанные предикаты и операции выразимы.

3) Докажем, что множество предикатов и операций, элементарно выразимых над данным набором, замкнуто относительно однократного применения квантора общности.

4) Докажем, что множество предикатов и операций, элементарно выразимых над данным набором, замкнуто относительно однократного применения описателя set_x.

Тогда из 3) и 4) будет следовать, что множество предикатов и операций, элементарно выразимых над Q, замкнуто относительно применения set_x и кванторов. Кроме того, по определению оно замкнуто относительно элементарной выразимости. Значит, оно замкнуто относительно выразимости. Так как оно согласно 1) включает $\in$, все предикаты и операции, выразимые над $\in$, будут содержаться в этом множестве. Из 2) будет следовать обратное включение, и теорема будет доказана.

В доказательстве будут использоваться предикаты $Crd_n(x)$ (которые не следует путать с операциями $Card_n(x)$), определяемые следующим образом:

$Crd_n(x)$ =И, если x n-элементно.

Иначе $Crd_n(x)$ =Л.

Эти предикаты элементарно выразимы над Q:

$Crd_n(x) \equiv (Card_n(x) = \varnothing)$

Также отметим, что операция $a \bigcap b$ элементарно выразима над Q:

$a \bigcap b = U_0 \backslash ((U_0 \backslash a) \bigcup (U_0 \backslash b))$

Лемма 1. $\in$ *элементарно выразимо над данным набором.*

Действительно:

$a \in b \equiv (a \in U_0)\&(\neg(b \in U_0))\&Crd_1(b \bigcap \{a\})$. При этом:

$(a \in U_0) \equiv (Crd_1(\{a\})) \equiv (\neg((Card_1(\{a\})) = \varnothing)$

(так как для элементов не из U_0 $\{x\} = \varnothing$ по определению)

$Crd_1(b \bigcap \{a\}) \equiv Crd_1(U_0 \backslash ((U_0 \backslash b) \bigcup (U_0 \backslash \{a\}))) \equiv$

$\neg((Card_1(U_0 \backslash ((U_0 \backslash b) \bigcup (U_0 \backslash \{a\})))) = \varnothing)$

Следовательно, отношение $a \in b$ - выразимо.

Так как $a \in b \equiv (a \in U_0)\&(\neg(b \in U_0))\&Crd_1(b \bigcap \{a\})$, подставляя выражения для конъюнктов, получим бесквантворную формулу, задающую $\in$, что доказывает лемму.

Лемма 2. *Все описанные предикаты и операции выразимы через* $\in$.

Действительно, $U_0 = set_x(\exists y(x \in y))$

Пусть f_1 и f_2– выразимы. Тогда описанные операции можно выразить так:

$U_0 \backslash f_1 \equiv set_x(\neg(x \in f_1)\&x \in U_0)$

$f_1 \bigcup f_2 \equiv set_x(x \in f_1\&x \in f_2\&x \in U_0)$

$Card_m(f) \equiv set_x(Crd_m(F)\&x \in U_0)$, где x не является свободной переменной терма f (выразимость предиката $Crd_m(F)$ покажем далее)

$(f = \varnothing) \equiv (\neg(\exists x(f \in x)))\&(\neg(\exists x(x \in f)))$ (f не из U_0 и f не содержит элементов)

$\varnothing = set_x(x \in x)$

$\{z\} = set_x(x \in U_0\&(\forall y(z \in y) \to (x \in y)))$

Покажем выразимость всех предикатов $Crd_n(x)$

Докажем ее индукцией по n:

$Crd_0(x) \equiv \forall y(\neg y \in x)$

$Crd_1(x) \equiv \exists y(y \in x\&\forall z((z \in x) \to \forall u((z \in u) \to (y \in u)))$

(в x есть элемент y такой,что любой элемент x ему равен)

$Crd_{n+1}(x) \equiv \exists y, z(\forall a(((a \in y) \to ((a \in x)\&\neg(a \in z)))\&$

$((a \in z) \to (a \in x)))\&(Crd_n(y))\&Crd_1(z))\&$

$\forall a((a \in x) \to ((a \in y) \bigvee (a \in z))$

(у x есть два непересекающихся подмножества – n—элементное y и 1—элементное z – такие, что их объединение включает x)

Следовательно, все данные предикаты и операции выразимы над $\{\in\}$, а значит, и любое отношение или операция, выразимое бесквантворной формулой или термом над этими предикатами и операциями, выразима над $\{\in\}$. Лемма доказана.

Покажем, что система предикатов и операций, элементарно выразимых через данное множество, замкнута относительно применения квантора, то есть ей принадлежат все предикаты, выразимые через нее однократным применением квантора.

Докажем утверждение для предикатов:

Лемма 3. *Система Q замкнута относительно кванторной выразимости формулой с одним квантором.*

Без ограничения общности можно считать, что используется квантор всеобщности. Необходимо доказать, что $q(x_1, \ldots, x_n)$, выражающийся как $\forall x(p(x, x_1, \ldots, x_n))$, где $p(x, x_1, \ldots, x_n)$ – элементарно выразимый через Q предикат, элементарно выражается через Q.

Заметим, что любое вхождение условной операции $Card_n(f)$ можно исключить из p, добавив предикаты $Crd_n(f)$: $p(x, x_1, \ldots, x_n) \equiv p_1(x, x_1, \ldots, x_n)\&(Crd_n(f)) \bigvee p_2(x, x_1, \ldots, x_n)\&\neg(Crd_n(f))$, где p_1 - формула p, в которой все вхождения $Card_n(f)$ заменены на U_0, а p_2 - формула p, в которой все вхождения $Card_n(f)$ заменены на $\varnothing$. Исключим все такие вхождения в порядке вложенности, начиная с самых вложенных. Устранив по индукции все вложения условных операций, получим формулу $\forall x(p'(x, x_1, \ldots, x_n))$, равносильную исходной, где формула p' не содержит условных операций $Card_n$ (который мог быть вложенным), но содержит предикаты Crd_n (которые не могут быть вложены друг в друга, так как в них вложены только операции).

Пример Пусть $p(x, x_1, \ldots, x_n)$ имеет вид $Card_3(x_1 \bigcup x \bigcup U_0 \backslash (Card_2(x_2))) = \varnothing$. Тогда результаты последовательно примененных преобразований будут иметь вид:

$Card_3(x_1 \bigcup x \bigcup (U_0 \backslash (Card_2(x_2)))) = \varnothing$

$\equiv Card_3(x_1 \bigcup x \bigcup (U_0 \backslash U_0)) = \varnothing\&Crd_2(x_2) \bigvee Card_3(x_1 \bigcup x \bigcup (U_0 \backslash \varnothing)) = \varnothing\&\neg Crd_2(x_2)$

$\equiv U_0 = \varnothing\&Crd_2(x_2)\&Crd_3(x_1 \bigcup x \bigcup (U_0 \backslash U_0)) \bigvee$

$\varnothing = \varnothing\&Crd_2(x_2)\&\neg Crd_3(x_1 \bigcup x \bigcup (U_0 \backslash U_0)) \bigvee$

$U_0 = \varnothing\&\neg Crd_2(x_2)\&Crd_3(x_1 \bigcup x \bigcup (U_0 \backslash \varnothing)) \bigvee$

$\varnothing = \varnothing\&\neg Crd_2(x_2)\&\neg Crd_3(x_1 \bigcup x \bigcup (U_0 \backslash \varnothing))$

Так как любой элемент U_1 принадлежит либо U_0, либо $U_1 \backslash U_0$, полученная формула $\forall x(p'(x, x_1, \ldots, x_n))$ эквивалентна формуле

$\forall x((x \in U_0) \to p'(x, x_1, \ldots, x_n))\&\forall x(\neg(x \in U_0) \to p'(x, x_1, \ldots, x_n))$.

Так как любой элемент из U_0 при применении операций $U_0 \backslash$ и $\bigcup$, а также при применении предиката $Crd_n(x)$ ведет себя как $\varnothing$, то в консеквенте в первом конъюнкте вхождение x в эти операции в этой формуле

можно заменить на $\varnothing$ (кроме случая, когда x не вложен ни в какую операцию, и p имеет вид $x = \varnothing$ или $Crd_n(x)$, в случае чего весь квантор равен Л или И, если $n = 0$), и останутся только вхождения в виде $\{x\}$. Формулу $\forall x((x \in U_0) \to p'(\{x\}, x_1, \ldots, x_n))$ можно заменить эквивалентной:

$\forall y((Crd_1(y)) \to p'(y, x_1, \ldots, x_n))$. (произведена замена переменных: $y = \{x\}$, биективно отображающая U_0 на множество одноэлементных множеств)

Что эквивалентно следующей формуле:

$\forall x((\neg(x \in U_0)) \to ((Crd_1(x)) \to p'(x, x_1, \ldots, x_n)))$.

Под вторым квантором, в подформуле $\forall x(\neg(x \in U_0) \to P_2(x, x_1, \ldots, x_n))$, все вхождения $\{x\}$ можно заменить на $\varnothing$, так как $\{x\} = \varnothing$ для любого x из $U_1 \backslash U_0$

Так как образ всех операций из множества Q включается в $U_1 \backslash U_0$, а для любого элемента оттуда $\{x\} = \varnothing$, все подформулы вида $\{g(x, x_1, \ldots, x_n)\}$ можно заменить на $\varnothing$, кроме подформул вида $\{x_i\}$

Пример Пусть формула p' имеет вид

$Crd_2(x_1 \backslash x \backslash (x_2 \backslash x) \& (Crd_3(x_2 \backslash x) \bigvee Crd_2(x_2 \backslash x))$.

Применим к формуле $\forall x(p'(x, x_1, \ldots, x_n))$ указанные преобразования:

$\forall x Crd_2(x_1 \backslash x \backslash (x_2 \backslash x) \& (Crd_3(x_2 \backslash \{x\}) \bigvee Crd_2(x_2 \backslash \{x\}))$;

$\forall x(x \in U_0 \to Crd_2(x_1 \backslash x \backslash (x_2 \backslash x) \& (Crd_3(x_2 \backslash \{x\}) \bigvee Crd_2 \backslash \{x\}))) \&$

$\& \forall x(\neg x \in U_0 \to Crd_2(x_1 \backslash x) \backslash (x_2 \backslash x) \& (Card_3(x_2 \backslash \{x\}) \bigvee Crd_2(x_2 \backslash \{x\})))$;

$\forall x(x \in U_0 \to Crd_2(x_1 \backslash \varnothing \backslash (x_2 \backslash \varnothing) \& (Crd_3(x_2 \backslash \{x\}) \bigvee Crd_2(x_2 \backslash \{x\}))) \&$

$\& \forall x(\neg x \in U_0 \to Crd_2(x_1 \backslash x) \backslash (x_2 \backslash x) \& (Crd_3(x_2 \backslash \varnothing) \bigvee Card_2(x_2 \backslash \varnothing)))$;

$\forall x(x \in U_0 \to Crd_2(x_1 \backslash x_2 \& (Crd_3(x_2 \backslash \{x\}) \bigvee Crd_2 \backslash \{x\}))) \&$

$\& \forall x(\neg x \in U_0 \to Crd_2(x_1 \backslash x) \backslash (x_2 \backslash x) \& (Crd_3(x_2) \bigvee Crd_2(x_2)))$.

Таким образом, достаточно показать элементарную выразимость предикатов, задаваемых формулами:

$\forall x(\neg(x \in U_0) \to q(x, x_1, \ldots, x_n, \{x_1\}, \ldots, \{x_n\}))$, где q элементарно выражается через $U_0 \backslash a, a \bigcup b, \varnothing$ и $Crd_n(a)$.

Рассмотрим (для произвольных $x_1, \ldots, x_n$) алгебру множеств, порожденную множествами $U_0, x_1, \ldots, x_n, \{x_1\}, \ldots, \{x_n\}$. Все элементы этой алгебры множеств выразимы как дизъюнктное объединение множеств вида $U_0 \bigcap (\bigcap_{a \in A} a) \backslash (\bigcup_{a \in B} a)$, где $A \sqcup B = \{x_1, \ldots, x_n, \{x_1\}, \ldots, \{x_n\}\}$ (через $A \sqcup B$ обозначено дизъюнктное объединение множеств A и B, то есть в каждом выражении $U_0 \bigcap (\bigcap_{a \in A} a) \backslash (\bigcup_{a \in B} a)$ встречаются все элементы $\{x_1, \ldots, x_n, \{x_1\}, \ldots, \{x_n\}\}$ по одному разу.)

Действительно, два различных множества такого вида не пересекаются ни при каких значениях $x_1, \ldots, x_n$, так как если $a \in A$, $\neg a \in A'$, то множество $v_{AB} = U_0 \bigcap (\bigcap_{a \in A} a) \backslash (\bigcup_{a \in B} a)$ включается в a, а множество

$v_{A'B'} = U_0 \bigcap (\bigcap_{a \in A'} a) \backslash (\bigcup_{a \in B'} a)$ не пересекается с a, а следовательно, и с v_{AB}.

Покажем, что любой элемент алгебры множеств выразим в виде объединения множеств заданного вида (вида $U_0 \bigcap (\bigcap_{a \in A} a) \backslash \bigcup_{a \in B} a)$). Действительно, применим к терму $F(x_1 \dots x_n)$ над $U_0 \backslash$ и $\bigcup$ преобразования, заданные следующими эквивалентностями:

$U_0 \backslash (a \bigcup b) \equiv (U_0 \backslash a) \bigcap (U_0 \backslash b)$

$U_0 \backslash (a \bigcap b) \equiv (U_0 \backslash a) \bigcup (U_0 \backslash b)$

$U_0 \backslash (U_0 \backslash b) \equiv b$

$(b \bigcup a) \bigcap c \equiv (b \bigcap c) \bigcup (a \bigcap c)$, получим формулу с внешней операцией $\bigcup$, затем$\bigcap$, и внутренней операцией $U_0 \backslash$.

Проведя обратное преобразование $(U_0 \backslash a) \bigcup (U_0 \backslash b) \equiv U_0 \backslash (a \bigcap b)$, приведем выражение к виду:

$\bigcup_k (U_0 \backslash (a_{ki_1} \bigcup \dots \bigcup a_{ki_n}))$, что выражается как объединение множеств заданного вида (вида $U_0 \bigcap (\bigcap_{a \in A} a) \backslash (\bigcup_{a \in B} a)$).

Пользуясь данным утверждением докажем, что формула вида

(1)$\forall x (\neg (x \in U_0) \to F(Crd_{m_1}(f_1(x, x_1, \dots, x_n, \{x_1\}, \dots, \{x_n\})), \dots,$

$Crd_{m_k}(f_k(x, x_1, \dots, x_n, \{x_1\}, \dots, \{x_n\})))$,

где f_i – операции, выразимые через $U_0 \backslash$ и $\bigcup$, истинна или ложна только в заисимости от числа элементов в множествах вида $U_0 \bigcap (\bigcap_{a \in A} a) \backslash \bigcup_{a \in B} a$, причем найдется M такое, что если среди чисел элементов множеств $v_{AB} = U_0 \bigcap (\bigcap_{a \in A} a) \backslash \bigcup_{a \in B} a$ и множеств $v_{A'B'} = U_0 \bigcap \bigcap (\bigcap_{a \in A'} a) \backslash \bigcup_{a \in B} a$ для любых A, B, где:

— $A \sqcup B = \{x_1, \dots, x_n, \{x_1\}, \dots, \{x_n\}\}$,

$A' \sqcup B' = \{x'_1, \dots, x'_n, \{x'_1\}, \dots, \{x'_n\}\}$,

— $x_1, \dots, x_n, x'_1, \dots, x'_n$ — произвольные элементы U_1

— $x_j \in A \equiv x'_j \in \backslash A'$, $\{x_j\} \in A \equiv \{x'_j\} \in A'$,

различаются только те, которые больше M, то значения формулы совпадают на наборах x_j и x'_j.

Возьмем $M = 2max_k m_k + 3$. Тогда по любому множеству x из $U_1 \backslash U_0$, для которого консеквент в формуле(1) ложен (зафиксируем), можно построить множество x', содержащее:

— по столько элементов из каждого из множеств $v_{A'B'}$, сколько элементов x содержится в соответствующем множестве v_{AB}, для v_{AB}, пересечение которых с x содержит не более $max_k m_k$ элементов;

— из множеств $v_{A'B'}$, для которых это число больше $max_k m_k$ – по столько элементов, чтобы число элементов в дополнении x' до этих множеств было таким же, как в дополнении до соответствующего множества v_{AB};

— если же и пересечение с v_{AB}, и дополнение x до v_{AB}содержат более $max_k m_k$ элементов, то из соответствующего $v_{A'B'}$ в x' добавляем по $max_k m_k + 1$ элементов.

(Так как различные множества вида $v_{A'B'}$ не пересекаются, мы всегда можем взять множество, содержащее по данному числу элементов из каждого такого множества, если это число не превосходит мощности множества, что в данном случае выполнено).

Так как $f_i(x, x_1, \ldots, x_n, \{x_1\}, \ldots, \{x_n\})$ выражается как дизъюнктивное объединение множеств вида v_{AB}, то значение предиката $Crd_{m_i}(f_i(x, x_1, \ldots, x_n, \{x_1\}, \ldots, \{x_n\})$ – булева функция от значений предикатов $Crd_n(v_{AB})$, где v_{AB} выразимо через $U_0\backslash$ и $\bigcup$, а n принимает все значения от 0 до m_i (так как зная значения всех этих предикатов, мы или сможем назвать число элементов в $f_i(x, x_1, \ldots, x_n, \{x_1\}, \ldots, \{x_n\})$, или сказать, что это число больше m_i, если одна из компонент вида v_{AB} содержит более m_i элементов).

Следовательно, по x такому, что неверен консеквент формулы (1), мы построим x' такое, что оно становится неверным при замене на x' и x_j на x'_j при условии, что числа элементов множеств v_{AB}и $v_{A'B'}$ для каждого различаются только для пар тех множеств, мощность каждого из которых больше $2max_k m_k + 3$.

Отсюда следует, что формула (1) эквивалентна некоторой булевой функции от предикатов $(Crd_n(v_{AB}))$, где $v_{AB} = U_0 \bigcap (\bigcap_{a\in A} a)\backslash(\bigcup_{a\in B} a)$, $A \sqcup B = \{x_1, \ldots, x_n, \{x_1\}, \ldots, \{x_n\}\}$, $n < M$. Следовательно, предикат, ей задаваемый, элементарно выражается через них, а значит, (учитывая, что $a \bigcap b \equiv U_0\backslash(U_0\backslash a \bigcup \backslash U_0\backslash b)$ и $Crd_n(a) \equiv \neg(Card_n(a)) = \varnothing$), и через Q, так как $a \bigcap b$ и $Crd_n(a)$ элементарно выражается через Q. Лемма 3 доказана.

Пример Пусть необходимо элементарно выразить предикат

$\forall x(\neg(x \in U_0) \to (\neg Crd_2(x \bigcup (U_0\backslash x_1) \bigcup \{x_2\}))))$.

Для этого рассмотрим все возможные значения мощностей множеств $U_0\backslash x_1\backslash\{x_2\}, U_0\backslash x_1 \bigcap \{x_2\}, U_0\backslash\{x_2\} \bigcap x_1, \{x_2\} \bigcap x_1$, не различая значения больше 6. Например, для U_0 - множества целых чисел, $x_1 = U_0\{1, 2\}, x_2 = 1$, предикат не выполнен - например, при $x = 2$ подкванторное выражение ложно. Следовательно, для любых x_1, x_2, для которых мощность $U_0\backslash x_1\backslash\{x_2\}$ равна 1, мощность $U_0\backslash x_1 \bigcap \{x_2\}$ равна 1, мощность $U_0\backslash\{x_2\} \bigcap x_1$ больше 6 (выразимый предикат - мощность не равна 0,1,2,3,4, 5, 6), мощность $\{x_2\} \bigcap x_1$ равна 0, можно выбрать x состоящий из одного элемента - элемента множества $U_0\backslash x_1\backslash\{x_2\}$, следовательно, все такие x_1, x_2 не удовлетворяют предикату. Рассмотрев все возможные варианты возможных мощностей множеств

$U_0\backslash x_1\backslash\{x_2\}, U_0\backslash x_1 \bigcap \{x_2\}, U_0\backslash\{x_2\} \bigcap x_1, \{x_2\} \bigcap x_1$, не различая значения больше 6, элементарно выразим $\forall x(\neg(x \in U_0) \to (\neg Crd_2(x \bigcup (U_0\backslash x_1) \bigcup \{x_2\})))$ через предикаты, выражающие мощности этих множеств, а значит, и через Q.

Докажем утверждение для операций.

Лемма 4. *Система Q замкнута относительно выразимости термом без кванторов с одним описателем set_x.*

Нужно доказать, что через данный набор выражаются все операции вида $set_x p(x, x_1, \ldots, x_n)$, где p элементарно выражается через Q.

Сначала заметим, что операция, задаваемая этой формулой, выразима через Q с использованием описателя вида $set_x(x \in U_0 \& p(x, x_1, \ldots, x_n))$. Действительно, если существует x не из U_0, для которого выполнено $p(x, x_1, \ldots, x_n)$, то значение операции $set_x(x \in U_0 \& p(x, x_1, \ldots, x_n))$ равно $\varnothing$, иначе равно значению операции $set_x(x \in U_0 \& p(x, x_1, \ldots, x_n))$. По доказанному ранее, предикат, выражающийся формулой $\exists x(\neg(x \in U_0) \& p(x, x_1, \ldots, x_n))$ элементарно выражается через предикаты вида $Crd_n(f(x_1, \ldots, x_n))$ только с использованием булевых функций $\bigvee$ и $\neg$, так как они образуют базис булевых функций. Заменяя в выражающей формуле подформулы вида $Crd_n(f(x_1, \ldots, x_n))$ на $Card_n(f(x_1, \ldots, x_n))$, $\neg$ на $U_0\backslash$, и $\bigvee$ на $\bigcup$, получим выражение g, равное $\varnothing$ на значениях $x, x_1, \ldots, x_n$, на которых $\exists x(\neg(x \in U_0) \& p(x, x_1, \ldots, x_n))$ ложно, и U_0, если эта формула истинна. Следовательно, $set_x p(x, x_1, \ldots, x_n) = set_x(x \in U_0 \& p(x, x_1, \ldots, x_n)) \bigcap g$, и истинность утверждения достаточно проверить для операций, выразимых термом вида $set_x(x \in U_0 \& p(x, x_1, \ldots, x_n))$, где элементарно выразимо над Q.

Пример Рассмотрим терм $set_x(Card_2(\{x\} \bigcup x_1) = \varnothing)$. Так как $Card_2(\{x\} \bigcup x_1) = \varnothing$ аналогично началу доказательства предыдущей леммы можно привести к виду $Crd_2(\{x\} \bigcup x_1)$ - виду без описателей Card, а $\exists x(\neg(x \in U_0) \& Crd_2(\{x\} \bigcup x_1))$ равносильно бесквантворной формуле $Card_2(x_1)$, терм $set_x(Crd_2(\{x\} \bigcup x_1) = \varnothing)$ равносилен терму

$set_x(x \in U_0 \& Crd_2(\{x\} \bigcup x_1)) \bigcap U_0\backslash(Card_2(x_1))$

Путем преобразований, задаваемых данными формулами (заменяя выражения из левой части формул на выражения из правой части формул):

$set_x(x \in U_0 \& f \& g) = set_x(x \in U_0 \& f) \bigcap set_x(x \in U_0 \& g)$,

$a \bigcap b = U_0\backslash((U_0\backslash a) \bigcup (U_0\backslash b))$

$set_x((x \in U_0) \& (f \bigvee g)) = set_x((x \in U_0) \& f) \bigcup set_x((x \in U_0) \& g)$

$set_x(x \in U_0 \& \neg f) = U_0\backslash set_x(x \in U_0 \& f)$

заменим терм вида $set_x(x \in U_0 \& p(x, x_1, \ldots, x_n))$ на эквивалентный ему терм вида $f(set_x(x \in U_0 \& Crd_{n_i}(f_i(x, x_1, \ldots, x_n))))$, где f - операция от i переменных, выразимая через $U_0 \backslash a$, $a \bigcup b$.

Осталось выразить $set_x(x \in U_0 \& Crd_{n_i}(f_i(x, x_1, \ldots, x_n)))$ через Q.

Если x входит в f_i, то во всех его вхождениях, кроме его вхождения в виде $\{x\}$, его можно заменить на $\varnothing$, так как все остальные операции из Q действуют на элементы U_0 так же, как на $\varnothing$.

Если после этого x не входит в полученный терм вида f, то значение этого терма равно значению терма $Card_{n_i}(f_i(x, x_1, \ldots, x_n))$. Иначе его можно записать в равносильном виде:

$\bigcup_{\sigma \in B^{2n}}(Card_{n_i} f_i(x, x_1, \ldots, x_n))) \bigcap(\bigcap_{i=1}^{n}(x \in x_i)^{\sigma_i}) \bigcap(\bigcap_{i=1}^{n}(x = x_i)^{\sigma_i})$,

где B^{2n} – булев куб,

$(x \in y)^{\sigma_i} = (x \in y)?$ при $\sigma = 1$,$U_0 \backslash (x \in y)?$ иначе

(где $x \in y?$ определяется как $Card_1(U_0 \backslash (U_0 \backslash \{x\} \bigcup (U_0 \backslash y))$ — выразимая операция)

$(x = y)^{\sigma_i} = (x = y)?$ при $\sigma = 1$, $U_0 \backslash (x = y)?$ иначе

$(x = y?Card_1(U_0 \backslash (U_0 \backslash \{x\} \bigcup (U_0 \backslash \{y\})))$ — выразимая операция)

Пример $set_x(x \in U_0 \& Crd_2(\{x\} \bigcup x_1))$ можно записать в виде

$(set_x(x \in U_0 \& Crd_2(\{x\} \bigcup x_1)) \bigcap (x = x_1)? \bigcap (x \in x_1)?) \bigcup$

$(set_x(x \in U_0 \& Crd_2(\{x\} \bigcup x_1)) \bigcap (x = x_1)? \bigcap (U_0 \backslash (x \in x_1)?))$

$\bigcup (set_x(x \in U_0 \& Crd_2(\{x\} \bigcup x_1)) \bigcap (U_0 \backslash (x = x_1)?) \bigcap (x \in x_1)?)$

$\bigcup (set_x(x \in U_0 \& Crd_2(\{x\} \bigcup x_1)) \bigcap (U_0 \backslash (x = x_1)?) \bigcap (U_0 \backslash (x \in x_1)?))$

Введем новое обозначение — пусть $[a \backslash \{x\}]$ означает $a \backslash \{x\}$, подразумевая, что $x \in a$ (аналогично тому, как дизъюнктное объединие означает объединение множеств, подразумевая, что они не пересекаются). Преобразуем каждое вхождение $Card_{n_i}(f_i(x, x_1, \ldots, x_n))$ при соответствующих условиях (то есть при условиях на равенство и принадлежность множествам, обозначенным свободными переменными, заданных выражениями $(x \in x_i)^{\sigma_i}$ и $(x = x_i)^{\sigma_i}$, с которыми данное вхождение выражения $Card_{n_i}(f_i(x, x_1, \ldots, x_n))$ связано через $\bigcap$) и на принадлежность и равенство элементам $x_1, \ldots, x_n$ следующим образом:

$a \backslash \{x\}$ заменим на a там, где $\neg(x \in a)$; $a \backslash \{x\}$ заменим на $[a \backslash \{x\}]$ там, где $(x \in a)$;

$\{x\} \backslash a = \varnothing$ там, где $(x \in a)$; $\{x\} \backslash a = \{x\}$ там, где $\neg(x \in a)$;

$\{x\} \bigcup a = a$ там, где $(x \in a)$; $\{x\} \backslash a = a \sqcup \{x\}$ там, где $\neg(x \in a)$; (здесь $\sqcup$ обозначает дизъюнктивное объединение)

$b \backslash [a \backslash \{x\}] = b \backslash a \sqcup x$ или $b \backslash a$

$b \backslash (a \sqcup \{x\}) = b \backslash a \backslash x$ или $b \backslash a$

$b \bigcup (a \sqcup \{x\}) = b \bigcup a \sqcup x$ или $b \bigcup a$

$\{x\} \bigcup [a \backslash \{x\}] = a$
$\{x\} \bigcup (a \sqcup \{x\}) = a \sqcup x$
$\{x\} \backslash [a \backslash \{x\}] = \{x\}$
$\{x\} \backslash (a \sqcup \{x\}) = \varnothing$
$b \backslash \{x\} \bigcup (a \backslash \{x\}) = (a \bigcup b) \backslash \{x\}$
$(b \bigcup \{x\}) \backslash (a \bigcup \{x\}) = b \backslash a$ или $[(b \backslash a) \backslash \{x\}]$
$(b \bigcup \{x\}) \backslash (a \backslash \{x\}) = (b \backslash a) \bigcup \{x\}$
И т.д.

С помощью этих преобразований выражение $f(x, x_1, \ldots, x_n)$ можно привести к одному из видов: $g(x_1, \ldots, x_n)$, $[g(x_1, \ldots, x_n) \backslash \{x\}]$, или $g(x_1, \ldots, x_n) \sqcup \{x\}$.

Тогда:

$set_x(x \in U_0 \& g(x_1, \ldots, x_n) = m)$ можно заменить на тождественно равный терм $Card_m g(x_1, \ldots, x_n)$

$set_x(x \in U_0 \& [g(x_1, \ldots, x_n) \backslash \{x\}] = m)$ можно заменить на тождественно равный терм $Card_{m+1} g(x_1, \ldots, x_n)$

$set_x(x \in U_0 \& (g(x_1, \ldots, x_n) \sqcup \{x\}) = m)$ можно заменить на тождественно равный терм $Card_{m-1} g(x_1, \ldots, x_n)$, считая, что $Card_{-1}(g(x_1, \ldots, x_n))$ равно $\varnothing$.

Пример Терм
$(set_x(x \in U_0 \& Crd_2(\{x\} \bigcup x_1)) \bigcap (U_0 \backslash (x = x_1)?) \bigcap (x \in x_1)?)$
преобразуется к виду
$(set_x(x \in U_0 \& Crd_2(x_1)) \bigcap (U_0 \backslash (x = x_1)?) \bigcap (x \in x_1)?)$,
так как в рамках данного терма $set_x(x \in U_0 \& Crd_2(x_1))$ можно рассматривать при условии $x \in x_1$ (и $\neg(x = x_1)$).

Лемма доказана.

Как уже было показано ранее, доказательство лемм доказывает теорему.

Выделим базис в системе предикатов и операций, элементарно выразимых над Q.

$\varnothing = \{U_0 \backslash \{x\}\}$ для любого x.

ПримерОстальные элементы системы Q образуют базис:

Нужно доказать, что никакой из этих предикатов и операций не выразим через другие.

$a = \varnothing$ – единственный предикат

$\{a\}$ – единственная операция, различающая элементы U_0

$a \bigcup b$ – единственная многоместная операция.

$Crd_n(x)$ – остальные операции, примененные к элементу x, вне зависимости от того, n—элементный он или счетный со счетным допол-

нением, сохраняют $\{U_0, U_0\backslash x, x, \varnothing\}$ и какое множество из этих является результатом этих операций не зависит от того, n—элементно x или счетно. То есть, если некоторая формула от одной переменной, элементарно выраженная через $Q\backslash Crd_n(x)$, примененная к произвольному n-элементному множеству, дает несчетное множество, то и при применении к счетному множеству со счетным дополнением она также должна давать счетное множество, следовательно, она не может выражать $Crd_n(x)$.

$U_0\backslash a$ – остальные операции склеивают счетные множества.

Следовательно, получен базис.

3. Элементарная выразимость в универсуме натуральных чисел с отношением делимости.

Теперь рассмотрим в качестве множества M множество всех натуральных чисел с предикатом "a|b". Так как это множество не содержит $\varnothing$, мы не будем рассматривать формулы, содержащие описатель set_x, и будем рассматривать только предикаты, выразимые с использованием кванторов. Каждый элемент этого множества – это конечное произведение простых в каких-то степенях, то есть его можно рассматривать как набор простых с некоторыми индексами. Следовательно, некоторые операции над U_1 имеют аналоги здесь. Например, a$\bigcap$b соответствует операция , а $a\backslash b$ соответствует операция "произведение простых, входящих в a, но не в b, со степенями, с которыми они входили в a". Оказывается, для (M,|) верна теорема, в чем—то аналогичная теореме для U_1:

Теорема 2. *Любой предикат, выразимый в N с использованием кванторных формул (не содержащих описателя set_x) над {|} элементарно выражается над следующим счетным набором R предикатов и операций:*

— aУЧb, где aУЧb – это произведение простых, входящих в a, но не в b, со степенями, с которыми они входили в a (усеченное частное). Например: $100\,УЧ15 = 4, 8\,УЧ2 = 1$

— НОД(a, b)

— aПЧ$_n b$, где n—параметр, aПЧ$_n b$ = (произведение простых, входящих в разложение a в большей степени, чем b, как минимум на n.) Например: $8ПЧ_2 2 = 2, 100ПЧ_1 5 = 10$

— ЧП$_n(a)$, так обозначим предикат, истинный, если в разложении a ровно n простых, n – параметр (число простых).

Доказательство.

Доказательство можно разбить на те же три шага, что и в прошлом разделе:

— Выразимость отношения делимости через R;

— Выразимость R через отношение делимости;

— Замкнутость R относительно выразимости.

1) Отношение делимости выражается через данный набор. Действительно, $(a|b) \equiv (\text{ЧП}_0(a\text{ПЧ}_1 b))$.

2) Все предикаты, элементарно выразимые через данный набор, выражаются через $|$.

Для этого достаточно показать, что каждый из заданных предикатов и операций выразим формулой, где под выразимостью операции $u(x_1, \ldots, x_n)$ имеется в виду существование формулы $f(x, x_1, \ldots, x_n)$ со свободными переменными $x, x_1, \ldots, x_n$, которая при любых значениях $x_1, \ldots, x_n$ принимает значение И только при $x = u(x_1, \ldots, x_n)$. Покажем, что этого достаточно.

Действительно, в этом случае от любого вхождения в формулу $p(u)$ операции u, выразимой формулой $f(x, x_1, \ldots, x_n)$, можно избавиться с сохранением равносильности:

$p(u(x_1, \ldots, x_n)) \equiv (\exists x(f(x, x_1, \ldots, x_n)\&p(x)))$. Поэтому если все предикаты и операции из R выражаются формулой над $|$, то и все предикаты, элементарно выразимые над R, также будут выразимы формулой над $|$.

Покажем, что все предикаты и операции из R выразимы через отношение делимости:

НОД(a, b) выражается формулой $(x|a\&x|b\&(\forall y((y|a\&y|b) \to y|x)))$

aУЧb – формулой (НОД$(x, b) = 1\&(x|a)\&\forall y((\text{НОД}(y, b) = 1\&(y|a)) \to y|x)))$, где единица выражается формулой $(\forall y(x|y))$

Предикат “x—простое” – формулой $\forall y(y|x \to (y = x \bigvee y = 1))$

(Предикат $x = y$ выражает формула $\forall z((z|x \to z|y)\&(z|y \to z|x)))$

Предикат $\text{ЧП}_n(a)$ выразим формулой $\exists x_1, \ldots, x_n$ ($x_1, \ldots, x_n$— попарно не равные, простые, делители a и $\forall x_{n+1}(x_{n+1}$или равен одному из x_i, или не простой, или не делитель a)).

aПЧ$b(n)$, где n—параметр, aПЧ$b(n)$ = (произведение простых, входящих в разложение a в большей степени, чем b, как минимум на n.) выражается так:

$\exists x_1, \ldots, x_n$ ($x_1, \ldots, x_n$— попарно различные простые, каждый из них входит в разложение a в степени минимум на n большей, чем в b, и $\forall x_{n+1}(x_{n+1}$ или совпадает с одним из x_i, или не простое, или не входит в разложение a в степени минимум на n большей, чем в b),

где предикат “x – простое, входящее в a в большей степени, чем в b, как минимум на n” можно выразить таким образом:

$\exists x_0, x_1, \ldots, x_n$ (x—простое&$\forall y((y|x_0$&y—простое)$\to y = x)$&$\ldots$&

$\forall y((y|x_n$&y—простое$) \to y = x)$&$(x_0|x_1$&$\neg(x_0 = x_1))$&$\ldots$&

$(x_{n-1}|x_n$&$\neg(x_{n-1} = x_n))$&$\forall y((\forall z(z|y$&z—простое$\to z = x))$&

$y|b \to (y|x_0))$&$(x_n|a))$

(то есть существуют $n-1$ различных степеней простого числа x, образующие цепочку по делимости, причем первая степень – как минимум та степень, в которой x входит в b, а последняя делит a)

Следовательно, все предикаты и операции из набора R выразимы над $|$, а следовательно, и все операции, элементарно выразимые над R, выразимы над $|$.

3) Остается доказать, что система операций и предикатов, элементарно выразимых над R, замкнута относительно однократного применения квантора.

Докажем это утверждение таким образом. Рассмотрим систему R', состоящую из операций НОД, УЧ и предикатов $\text{ЧП}_m(a\text{ПЧ}_n b)$. Как было указано в пункте 1), отношение $|$ выражается через данный набор. Так как этот набор элементарно выражается через R, он логически выразим над $|$. Следовательно, если мы докажем полноту этого набора, то отсюда будет следовать вывод, что все предикаты, выразимые над $|$, это те и только те, которые выразимы над R'. Так как R' элементарно выразим над R, а R выразим над $|$, отсюда будет следовать утверждение теоремы для R.

Без ограничения общности будем считать, что формула, выразимость которой над R мы хотим доказать, имеет вид: $\exists x p(x, x_1, \ldots, x_n)$, где p – дизъюнкция элементарных формул или их отрицаний. Так как $\text{ЧП}_m(a\text{ПЧ}_n b)$ - единственные предикаты в R', каждая элементарная формула имеет вид $\text{ЧП}_m(a\text{ПЧ}_n b)$, где a – операция, элементарно выразимая над НОД и УЧ. Для удобства в дальнейшем будем обозначать УЧ как $\backslash$.

Рассмотрим систему всех чисел вида

$a_k = (\text{НОД}(x_{11} \ldots x_{1n})\backslash x_{21}\backslash \ldots \backslash x_{2n})$,

где $x_{11}, \ldots, x_{1n}, x_{21}, \ldots, x_{2n}$ – все переменные, входящие в формулу, включая x (если под НОДом нет переменных, считаем, что выражение равно $1 = x\backslash x$ – тоже элементарно выразимая операция). Если рассматривать каждое число только как множество простых, не учитывая степеней, то любая операция, выразимая над $\backslash$ и НОД, будет тождественно

равна дизъюнктному объединению данных множеств. Чтобы учесть и степени, поступим таким образом:

Заметим, что $x = \text{ДНОК}_k(x\backslash(x\backslash a_k))$, где ДНОК обозначает НОК попарно взаимно простых чисел, a_k - взаимно простые и каждый простой делитель x является простым делителем некоторого a_k, и заменим все вхождения переменных в терм такими выражениями.

Пример Если x - это x_1 или x_2, или выразимый через них с помощью НОК и УЧ терм, то $x = \text{ДНОК}(x\backslash(x\backslash(x_1\backslash x_2)), x\backslash(x\backslash(x_2\backslash x_1)), x\backslash(x\backslash(x_1, x_2)))$, так как любой простой делитель x является простым делителем $(x_1\backslash x_2)$, $(x_2\backslash x_1)$ или (x_1, x_2). Например, если $x = x_1 = 15, x_2 = 6$, $\text{ДНОК}(x\backslash(x\backslash(x_1\backslash x_2)), x\backslash(x\backslash(x_2\backslash x_1)), x\backslash(x\backslash(x_1, x_2))) = \text{ДНОК}(5, 1, 3) = 15 = x_1$

Преобразуем полученные термы, используя следующие преобразования:

$\text{ДНОК}_k(x_{1k}\backslash(x_{1k}\backslash(a_k)))\backslash\text{ДНОК}_k(x_{2k}\backslash(x_{2k}\backslash(a_k))) =$

$= \text{ДНОК}(x_{3k}\backslash(x_{3k}\backslash(a_k)))$, где: $x_{3k} = x_{1k}$, если терм x_{2k} не содержит a_k в своем дизъюнктном разложении по a_i

(так как по термам a_i можно разложить терм – формальное выражение – а не его значение при конкретных x, то содержание a_k в разложении терма можно определить, посмотрев на терм, и оно не зависит от значения переменных), иначе $x_{3k} = 1$.

$\text{НОД}(\text{ДНОК}_k(x_{1k}\backslash(x_{1k}\backslash a_k)), \text{ДНОК}_k(x_{2k}\backslash(x_{2k}\backslash a_k))) =$

$= \text{ДНОК}((x_{1k}\text{НОД}x_{2k})\backslash((x_{1k}\text{НОД}x_{2k})\backslash a_k))$.

(Все a_k взаимно простые, и все $(\text{ДНОК}_k(x\backslash(x\backslash a_k)))$ имеют общие делители только с a_k и взаимно просты с a_n, если n не равно k)

Получим, что любое выражение для a или b (где

$\forall x(\text{ЧП}_m(a\text{ПЧ}_n b) = p)$ - предикат, элементарную выразимость которого нам нужно доказать) можно записать в виде

$\text{ДНОК}_k(\text{НОД}_j(x_{ijk})\backslash(\text{НОД}_j(x_{ijk})\backslash a_k))$

(i=1 в выражении для a, i=2 в выражении для b). Тогда предикат $\text{ЧП}_m(a\text{ПЧ}_n b)$ равносилен предикату

$\text{ЧП}_m(\text{ДНОК}_k(\text{НОД}_j(x_{1jk})\backslash(\text{НОД}_j(x_{1jk})\backslash a_k))$

$\text{ПЧ}_n\text{ДНОК}_k(\text{НОД}_j(x_{2jk})\backslash(\text{НОД}_j(x_{2jk})\backslash a_k)))$.

Так как каждое из чисел, входящих в ДНОК, содержит в разложение те и только те простые, которые содержатся в разложении a_k, причем все a_k взаимно простые, $\text{ЧП}_m(\text{ДНОК}_k(\text{НОД}_j(x_{1jk})\backslash(\text{НОД}_j(x_{1jk})\backslash a_k))$

$\text{ПЧ}_n\text{ДНОК}_k(\text{НОД}_j(x_{2jk})\backslash(\text{НОД}_j(x_{2jk})\backslash a_k)))$ тождественно равен

$\text{ЧП}_m(\text{ДНОК}_k((\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk}))\backslash$

$((\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk}))\backslash a_k)))$.

Число простых делителей ДНОК – это просто сумма чисел простых делителей операндов ДНОК. Рассмотрев все возможные разложения числа m на $2^{\text{число переменных}}$ слагаемых, получим, что подкванторную формулу можно записать, как формулу над элементарными формулами

$\text{ЧП}_m((\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk}))\backslash$

$((\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk}))\backslash a_k))$.

Следовательно, нужно доказать, что над R' выразим предикат, задаваемый формулой: $\exists x(A_1\& \ldots \& A_n)$, где a_i – элементарная формула вида $\text{ЧП}_m((\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk}))\backslash$

$((\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk}))\backslash a_k)) = m$ или её отрицание.

Покажем существование таких M, N, что истинность или ложность формулы $\exists x(A_1\& \ldots \& A_n)$ зависит только от значений предикатов вида $\text{ЧП}_m((\text{НОД}_j(x_{1jk})\text{ПЧ}_n\ \text{НОД}_j(x_{2jk}))\backslash((\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk}))\backslash b_k))$

(что равно $\text{ЧП}_m((\text{НОД}_j(x_{1jk})\backslash(\text{НОД}_j(x_{1jk})\backslash b_k))\text{ПЧ}_n$

$(\text{НОД}_j(x_{2jk})\backslash(\text{НОД}_j(x_{2jk})\backslash b_k)))$ - выразимо над R')

и $\text{ЧП}(b_k) = m$, где b_k определяются как a_k, но только над множеством свободных переменных, все $n < N$, все $m < M$, и формулы не содержат x. (Таких формул конечное число, и если зависимость есть, то она задается булевой функцией).

Действительно, пусть значения всех таких формул совпадают для наборов x_i и x_i', и для набора x_i существует такой , что $(A_1\& \ldots \& A_n)$ =И. Докажем, что тогда существует и x_i', такой, что $(A_1'\& \ldots \& A_n')$ =И, где a_i' получены заменой первого набора на второй.

В качестве x' нужно взять такое число, чтобы число простых в разложении $\text{НОК}(x', b_k')$ совпадало с числом простых в разложении $\text{НОК}(x, b_k)$, а число простых в разложении $b_k\backslash x$ с числом простых в разложении $\text{НОК}(x', b_k')$, если эти числа не больше максимального m, содержащегося в формулах a_i. Получим $M >= 2m + 2$.

Посмотрим, от чего зависит вхождение простого в разложение $\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk})$. Если x входит в левый НОД, то простое делит $\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk})$ тогда и только тогда, когда оно делит значение аналогичного выражения без , и выражения $x\text{ПЧНОД}_j(x_{2jk})$ (х из правого НОДа, если он там есть, можно убрать с сохранением вхождения простых). Если только в правый – то тогда и только тогда, когда оно входит или в разложение выражения $\text{НОД}_j(x_{1jk})\text{ПЧ}_n(x)$ или выражения $\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk})$, где из правого а изъято x.

Посмотрим, в какой степени может входить простое число в разложении x на множители. Степень, в которой p входит в разложение в $\text{НОД}_j(x_{1jk})$ и в $\text{НОД}_j(x_{2jk})$ — это одна из степеней, в которой p входит

в одно из x_i или в x. С точки зрения значения всех предикатов важно лишь, входит ли простое в x в степени, большей или меньшей, чем степень каждого x_i, а также взаимное расположение степеней, в которых в них входят p (это определяет, в чьей именно степени p входит в этот предикат), и разница между степенью вхождения p в x и каждый из x_i, но только в том случае, если она не больше n.

Следовательно, если взять x', который содержит столько же простых из каждой категории b'_k (если их не больше m) в степенях, на столько же больших или меньших каждого вхождения в x'_k (если эти разности степеней не больше n), на сколько это выполнено для . Получим, что достаточно взять $N = 2n + 2$, $M = (2^{\text{число свободных переменных}} * (\text{число свободных переменных}+1) * (2n + 2)) * (m + 1)$ (т.к. всего возможно максимум $2^{\text{число свободных переменных}}$ расстановки свободных переменных в порядке убывания степени вхождения заданного простого, и имеет значение, находится ли степень между заданными 2 числами, меньше ли она большего на заданное число, не большее n, или больше меньшего на заданное число, меньшее n, — всего не более $=((2^{\text{число свободных переменных}} * (\text{число свободных переменных}+1) * (2n+2))$ позиций – и важно, чтобы числа простых на каждой позиции совпадали, если хоть одно меньше m – максимум на каждую "позицию" придется "поместить" по $m + 1$ простому делителю из соответствующего b_k). Теорема доказана.

4. Элементарная выразимость в универсуме точек плоскости.

Два разобранных множества были во многом схожи. Их можно было рассматривать как набор "простых" элементов и набор "составных", которые могут быть "составлены" из любых простых. Возникает вопрос: что может происходить, если "составные" имеют определённую структуру. Например, рассмотрим в качестве универсума множество прямых и точек плоскости, и, как и в первом случае, множеством операций будет $\{\in\}$. Для того, чтобы можно было рассматривать операции, образованные при помощи описателя set_x, добавим к универсуму $\varnothing$ и множества, состоящие только из одной точки, для того, чтобы результатом операции могла быть точка. Обозначим полученный универсум W.

Какие операции можно выразить таким образом, используя только set_x, причем однократно (достаточно проверить это, так как тогда любой оператор set_x можно будет заменить на соответствующее выражение)? Эти формулы будут иметь вид:

$set_x(P(A_1, \ldots, A_n))$, где P – формула, задающая некоторую булеву функцию от предикатов $A_1, \ldots, A_n$. Заменим формулу P на КНФ булевой функции, задаваемой P:

$set_x((A_{11}\& \ldots \& A_{1m}) \bigvee \cdots \bigvee (A_{k1}\& \ldots \& A_{km}))$, где a_{ij} – атомарные формулы или их отрицания.

Рассмотрим множества точек x, для которых верны атомарные формулы или их отрицания (не учитывая, что кроме точек предикатам могут удовлетворять другие объекты):

$set_x(x \in a) = a$. a может быть пустым множеством, одноточечным множеством или прямой. Если a – точка, то значение предиката равно $\varnothing$.

$set_x(\neg(x \in a))$ =П$\backslash a$, где П – плоскость, в которой мы рассматриваем точки и прямые.

$set_x(\neg(a \in x))$ =П, $set_x(a \in x) = \varnothing$

$set_x(a \in b) = (a \in b)?$

$set_x(\neg(a \in b)) = (\neg a \in b)?$

Теперь рассмотрим все возможные пересечения таких множеств, соответствующие описателю set_x, примененному к описателю класса .

1) Если пересечение содержит хоть один элемент $\varnothing$, то и все пересечение будет равно $\varnothing$.

2) Иначе, если оно содержит только тождественные операторы, то это пересечение – $A_1 \bigcap \cdots \bigcap A_n$.

3) Если оно содержит только условные операторы $(a \in b)?$ или $(\neg a \in b)?$, то это пересечение условных операторов.

4) Если оно содержит и условные операторы, и хоть один тождественный, но не содержит элементов вида П$\backslash a$, то оно элементарно выражается через$\bigcap$ и операторы видов $(a \in b?)$ и $(\neg a \in b?d)$, где:

$(a \in b?c) = c$, если $a \in b$, $\varnothing$ иначе.

$(\neg a \in b?d)$= $\varnothing$, если a$\in$b, d иначе.

5—6) Если пересечение содержит элемент вида П$\backslash a$, то:

5)Если есть хоть один тождественный оператор, то пересечение имеет вид O$\backslash A_1 \ldots \backslash A_n$, где O – оператор, выразимый над$\bigcap$, $(a \in b?)$ и $(\neg a \in b?d)$,

6)Иначе оставим его в виде пересечения.

Теперь рассмотрим объединения множеств шести полученных типов, соответствующие дизъюнкциям в формуле

$set_x((A_{11}\& \ldots \& A_{1m}) \bigvee \cdots \bigvee (A_{k1}\& \ldots \& A_{km}))$.

Это прямая в том случае, если одно из этих множеств – прямая, а другие – такие же прямые, или одно – прямая без точек, принадлежащих

другим множествам, причем все точки из остальных множеств принадлежат этой прямой. Точка – если одно из множеств — точка, остальные пустые или эта же точка. Иначе значение оператора, заданного описателем set_x будет равно $\varnothing$.

Прямой или прямой без точек может являться только значение операторов типов 5), 4) или 2). Иначе в случае 1) оно пустое, в случаях 3 и 6) – пустое, если хоть один входящий туда условный оператор принимает значение $\varnothing$, иначе является плоскостью без нескольких точек. Чтобы объединение было прямой или точкой, хотя бы один из операторов должен иметь вид 2), 4) или 5). Введём новую операцию – $diz(A_1, \ldots, A_n)$, равную $\varnothing$ во всех случаях, кроме случая, когда среди множеств ровно одно непустое; в этом случае она равна этому множеству. Тогда $set_x(x \in b_1 \bigvee \cdots \bigvee x \in B_n \bigvee x \in (\Pi \backslash A_1 \backslash \ldots \backslash a_m \bigcap (b_1 \in c_1)? \bigcap \cdots \bigcap (B_n \in c_p)) = set_x(\bigvee in = 1(x \in diz((b_1 \in c_1?B_i), \neg(b_1 \in c_1?B_i) \bigcap (b_2 \in c_2?B_i), \ldots, \neg(b_1 \in c_1?B_i) \bigcap \cdots \bigcap (b_{p-1} \in c_{p-1}?B_i) \bigcap (b_p \in c_p?B_i)))$.

Добавим условные предикаты (b—прямая)? = b, если b прямая, $\varnothing$ иначе. (a=b)? , (a—точка)?, (a—одноточечное множество)? – аналогично.

Заменим операции $(a \in b?)$ и $(\neg a \in b?)$ на операции $(a \subset b?)$, $(\neg a \subset b?)$ и $\{a\}$.

Используя пересечения этих операций и diz полученных пересечений, можно получить операцию, которая в случае, если один из этих элементов – прямая или прямая без точек, которыми являются результаты других операций, или прямая без точек, которые лежат в результате другой операции – такой же прямой, а остальные элементы – такая же прямая или пустые множества, или точки, лежащие на этой прямой, равна этой прямой; в случае, когда один из элементов – точка, а другой – такие же точки или пустые множества, равна $\varnothing$; в остальных случаях равна $\varnothing$.

Следовательно, доказано утверждение:

Утверждение. Любой терм, выразимый над $\in$ в универсуме W термом, содержащим одно вхождение set_x и не солержащим кванторов, элементарно выразим через следующие операции:

$a \bigcap b = set_x(\in a \& x \in b)$, $(a -$ прямая$)?$, $(a = b)?$, $(a -$ точка$)?$, $(a -$ одноточечное множество$)?$, $\{a\}$, $diz(a_1, \ldots, a_n)$, $(a \subset b?)$, $(\neg a \subset b?)$.

Как видно, использование только описателя set_x приводит к появлению большого числа условных операторов, но почти не добавляет существенных операций в случае, когда универсум содержит не все множества данных элементов. Поэтому рассмотрим, какие предикаты выразимы формулами над универсумом W, не использующими set_x.

Сначала рассмотрим, какие аналоги операций из U_n выражаются в данном универсуме. Аналогом пересечения двух множеств здесь является точка пересечения двух прямых. Аналогом объединения множеств – прямая, проходящая через две данные точки. Аналогом числа элементов – предикаты а—прямая, а—одноточечное множество. Аналогом $\{a\}$ – также операция $\{a\}$. Аналогов разности здесь нет. Также можно ввести предикат принадлежности одноточечного множества прямой. Все эти предикаты выразимы над $\in$:

$(a \bigcap b)$ задается формулой $\exists x((x \in a)\&(x \in b))$

$(a \subset b)$ задается формулой $\exists x(x \in a \& x \in b \& a$—точка$\& b$—прямая$)$

$(a \bigcup b)$ задается формулой $\exists x((a \subset x)\&(b \subset x) \bigvee \neg\exists y((a \subset x)\&$ $(b \subset x))\&x = \varnothing)$

(а—прямая) задается формулой $\exists xyz(\in a \& x \in z \& y \in a \& \neg y \in z)$

(а—одноточечное множество) задается формулой $\exists x(x \in a \&$ $\neg(a$—прямая$))$

а—точка задается формулой ({а} – одноточечное множество).

$\{a\}$ задается формулой $\exists x(x$—одноточечное множество$\& a \in x)$.

С помощью этих предикатов элементарно выражается довольно большой класс отношений. Например, $a \backslash = b$ эквивалентно $a \bigcap b$—точка. Или три точки лежат на одной прямой – $a \in (\{b\} \bigcup \{c\})$ Однако не все отношения, элементарно выразимые через $\in$, элементарно выражаются через данный набор предикатов.

На самом деле верна теорема:

Теорема 3. *Все предикаты, выразимые в W через $\in$ – это те и только те, которые элементарно выразимы через следующие предикаты и операторы:*

1—7)$(a \bigcap b)$, $(a \bigcup b)$, (а—прямая), (а—одноточечное множество), $(a \subset b)$, $\{a\}$, (прямая, проходящая через точку одноточечного подмножества а параллельно прямой b),

8)(точки из одноточечных множеств $A_1, A_2, A_3, \ldots A_n$ лежат на одной прямой, $A_1, A_2, A_3, \ldots, A_n$ различны, и x_i такие, что $(A_1 - A_i) = x_i(A_1, A_2)$, m>2, лежат в полуалгебраическом множестве A, задаваемом алгебраическими неравенствами с рациональными коэффициентами).

9)(прямые $A_1, A_2, A_3, \ldots A_n$ параллельны, $A_1, A_2, A_3, \ldots, A_n$ различны, и x_i такие, что отношения направленных расстояний между прямыми $l(A_1 - A_i) = x_i l(A_1, A_2)$, m>2, лежат в полуалгебраическом множестве A, задаваемом алгебраическими неравенствами с рациональными коэффициентами).

10)(прямые $b_0, b_1, b_2, b_3, \dots b_n$ проходят через одну точку, $b_0, b_1, b_2, b_3 \dots, b_n$ различны, и если провести прямую, параллельную b_0, и обозначить за $A_1, A_2, A_3, \dots A_n$ точки её пересечения с $b_1, b_2, b_3, \dots b_n$, то x_i такие, что вектор $(A_1 — A_m) = x_i(A_1, A_2)$, $m>2$, лежат в полуалгебраическом множестве A, задаваемом алгебраическими неравенствами с рациональными коэффициентами).

Данная теорема представляет собой лишь перенос теоремы Тарского-Зайденберга[1] на множества точек плоскости. Далее представлена схема её доказательства. В ней не прописывается каждый раз,что все вырожденные случаи можно рассмотреть отдельно. Например, если мы рассматриваем точку пересечения двух прямых в предикате $p(a \bigcup b)$, мы можем задать ему любое значение в случае, если a и b параллельны, или a и b не прямые - (a—прямая)&(b—прямая)& $(a \bigcup b)$ — одноточечное множество & $p(a \bigcup b) \bigvee$ (a—прямая)&(b—прямая)& $\neg(a \bigcup b)$ — одноточечное множество & $p_2 \bigvee \neg$ (a—прямая)&$p_3 \bigvee \neg$ (b—прямая)&p_4

Доказательство.

1)$a \in b = \{a\} \subset b$. В дальнейшем, чтобы не оговаривать специально, не будем различать точку и одноточечное множество (предикат $\{a\}$ ставит в соответствие точке одноточечное множество, а остальные предикаты “работают” с одноточечными множествами), а также не будем проверять операции на корректность, то есть неравенство пустому множеству их результатов, так как случай равенства всегда можно рассматривать отдельно – $((P(U))\&(\neg(U = \varnothing))) \bigvee (U = \varnothing \& \dots)$. Специально вырожденные случаи описывать не будем.

2) Покажем, что все данные предикаты и операции выразимы формулой над $\in$. Выразимость первых шести была показана ранее. Седьмой выражается так: $\exists x$(x—прямая&a—одноточечное множество&b—прямая&$a \subset x \& x \setminus = b$).

Девятые тривиально выражаются с использованием восьмых: (прямые $A_1, A_2, A_3, \dots A_n$ параллельны) & $(A_1, A_2, A_3, \dots, A_n$ различны) &$\exists x(x -$ прямая&$\neg(x = A_1)\&(x \bigcap A_1, \dots, x \bigcap A_n$ удовлетворяют соответствующему восьмому предикату). Десятые выражаются через восьмые аналогично.

Покажем выразимость остальных предикатов. Для этого нам необходимо показать, как строя однозначно заданные прямые со свойствами, выразимыми формулами (т.е. добавляя кванторы $\exists x_1 \dots x_n$ (f$(x_1 \dots x_n)\& \dots)$)

— Умножить данный вектор на целый коэффициент. (то есть задать свойство: вектор, заданный данными двумя точками, равен n*вектор, заданный другими двумя данными точками).

— Сложить данные два коллениарных вектора

— Умножить вектор на отношение двух коллениарных векторов

— Определить сонаправленность данных двух векторов с общим началом.

Пункт II) (пункт 1 из него легко выводится). Пусть мы хотим сложить коллениарные векторы OA и XY. Построим на отрезке OA параллелограмм OABC, и обозначим за D точку пересечения прямой XY с прямой, проходящей через C параллельно XY. Отрезок XC будет требуемой суммой.

Пункт III) Отложим(как в пункте 2) все векторы от одной точки O. Пусть OB нужно умножить на отношение OC и OD. Рассмотрим прямую, не параллельную этим векторам, и проходящую через O. Пусть E, F – точки пересечения этой прямой с двумя параллельными прямыми, проходящими через OC и OD соответственно. Точка пересечения прямой OB и прямой, проходящей через F параллельно ED, и будет концом требуемого вектора.

Пункт IV) OB и OC сонаправленны, если существует D такое, что OB=c(OD) и OD=c(OC). Следовательно, все данные предикаты выразимы.

3) Докажем замкнутость данной системы предикатов.

По теореме Тарского-Зайденберга[1] любая формула над множеством вещественных чисел, кванторно выразимая через операции принадлежности полуалгебраическому множеству, элементарно выразима через эти операции.

Пусть некоторый предикат P задается формулой p. Без ограничения общности можно считать, что в формуле P содержатся условия на классы всех входящих в него переменных (точка/прямая), все прямые, проведенные через любую пару точек, взаимное положение всех точек и прямых и параллельность любой пары прямых. Тогда возможны случаи:

— Имеется только одна точка, пара точек и прямая, проходящая через них, три попарно пересекающиеся прямые, пара параллельных или пересекающихся прямых, на одной из которых, возможно, отмечена точка, три прямые, проходящие через одну точку, возможно, с одной отмеченной точкой. В этом случае данную совокупность прямых и точек можно перенести аффинным преобразованием в любую другую совокупность прямых и точек с таким же попарным расположением. Следовательно,

все выразимые предикаты выражаются через взаимное расположение прямых. Так как три точки, лежащие на одной прямой, не отмечены,

— Имеется хотя бы пара пересекающихся прямых и пара отмеченных на них точек (возможно, точек пересечения с другими прямыми). Рассмотрим все переменные, входящие в формулу – и свободные, и связанные. Можно ввести систему координат с двумя осями – двумя прямыми и единичными отрезками с концами в данной точке. В этом случае точками на этих прямых можно задать координаты каждой точки и каждой прямой (под координатами прямой подразумеваются координаты её пересечения с координатными осями или с одной осью, если она параллельна другой оси). Рассмотрим прямую, проходящую через концы единичных отрезков, и перенесём параллельно ей все отмеченные соответствующие координатам точки с одной из прямых на другую. Все соотношения, задаваемые данным наборов предикатов и отношений полуалгебраические относительно координат в любой аффинной системе координат. По теореме Тарского—Зайденберга любая проекция полуалгебраического множества полуалгебраическая, то есть любая кванторная формула над (+, *, =) имеет равносильную ей бескванторную формулу. Так как при условии, что на плоскости задана декартова система координат, каждая прямая однозначно задается координатами точек её пересечения с осями или фактом её параллельности одной из осей и координатой точки пересечения с другой из осей, а точка задается своими координатами, причем все операции из условия теоремы являются алгебраическими операциями над координатами. Следовательно, от кванторов можно избавиться, сохранив выразимость через данный набор предикатов.

— Имеется только набор параллельных прямых, возможно, на одной из них отмечена точка, или проведена прямая, их пересекающая. Тогда можно взять систему координат, содержащую одну из этих прямых (содержащую отмеченную точку, если есть) и прямую, их пересекающую. Тогда все данные параллельные прямые будут иметь только одну координату, поэтому все предикаты (по теореме Тарского – Зайденберга) можно выразить через алгебраические соотношения отношений только этих координат, то есть через предикаты 8—го типа и предикаты 1)—6).

— Имеется набор прямых, проходящих через одну точку. На одной из них выбираем начало координат, и берем её в качестве первой оси. Вторую координатную ось направляем параллельно одной из прямых. В качестве одного единичного отрезка берем отрезок от начала координат до точки пересечения прямых, в качестве второго – отрезок от начала координат до точки пересечения соответствующей оси до третьей

заданной прямой. В этом случае соотношения координат прямых полностью задаются вторыми координатами прямых, следовательно, отношения координат прямых в полученной системе координат выражаются через предикаты 9—го типа и предикаты 1)—6).

Итак, данная система предикатов и операций замкнута, ч.т.д.

5. Благодарности.

Выражаю благодарность проф. А.С.Подколзину за постановку задачи и помощь в работе.

Список литературы

[1] Н. К. Верещагин, А. Шень, *Языки и исчисления*, МЦНМО, М., 2012.

On the elementary expressibility in predicate logic

Kapustin I.S.

New mathematics concepts are often introduced with some quantifier definitions. If we have a sufficiently large stock of such notions, it can allow to reformulate the new quantifier definitions in a quantifier-free form. This makes the problem of finding basic concepts, which make further quantifiable definition redundant, worth considering. Creating computer programs that automatically introduce such bases is also worth considering.

In this paper we observe 3 simple cases of reducing the quantifier expressions to the quantifier-free ones. We investigate predicates and functions defined by $\in$ predicate on the set $Z \cup 2^Z$, where Z is the set of integers. We consider predicates expressed by $\in$ predicate on the set of points of the plane and the lines lying in it. Finally, predicates expressed on the set of natural numbers by the $|$ predicate on it are also considered. Bases were found in all 3 cases.

Keywords: predicate logic, quantifier definitions