Будем считать, что, если для некоторой начальной пары из состояния машины Тьюринга и символа в клетке не указано, что делать, то она заполнена произвольным образом, для определённости остановка в состоянии q_2.

C1a	**C1b**
$q_1 0 \to 0 S q_2$	$q_i 1 \to 1 R q_i$
$q_1 1 \to 1 R q_1$	$q_i 2 \to 2 R q_i$
$q_1 2 \to 2 R q_1$	$q_i 3 \to 3 R q_i$
$q_1 3 \to 3 R q_1$	$q_i \lambda \to \lambda R q_i$
$q_1 \lambda \to \lambda R q_1$	$q_i \wedge \to \wedge R q_i$, $1 \leqslant i \leqslant k+2$
$q_1 \wedge \to \wedge R q_1$	$q_1 0 \to 0 R q_4$
	$q_j 0 \to 0 R q_{j+1}$, $4 \leqslant j \leqslant k+2$
	$q_{k+3} a \to a L q_2$

C2a	**C2b**	**C3a**	**C3b**
$q_1 a \to a R q_1$, $a \neq \lambda$	$q_1 a \to a R q_1$, $a \neq \lambda$	$q_1 a \to a R q_1$, $a \neq \lambda$	$q_1 a \to a R q_1$, $a \neq \lambda$
$q_1 \lambda \to 0 R q_4$	$q_1 \lambda \to 1 R q_4$	$q_1 \lambda \to \lambda L q_4$	$q_1 \lambda \to \lambda L q_4$
$q_4 b \to \lambda S q_2$	$q_4 b \to \lambda S q_2$	$q_4 0 \to 0 S q_3$	$q_4 b \to \lambda L q_4$, $b \neq 0$
		$q_4 1 \to \lambda S q_2$	$q_4 0 \to \lambda S q_2$

♦ **C4.** (**a**)

$q_1 b \to b R q_1$, $b \neq \lambda$
$q_1 \lambda \to 0 R q_2$
$q_2 c \to \lambda S q_3$ Удлинним на 1 кортеж и вернёмся на место
$q_3 d \to d L q_3$, $d \neq *$
$q_3 * \to * S r_1$

$r_i e \to e R r_i$, $1 \leqslant i \leqslant k+2$, $e \neq 0$
$r_1 0 \to 0 R r_4$
$r_j 0 \to 0 R r_{j+1}$, $4 \leqslant j \leqslant k+2$
$r_{k+3} f \to f L r_{k+4}$
$r_{k+4} 1 \to 2 R r_{k+5}$ дошли до k-ого нуля, далее начинаем копировать единички в конец.
$r_{k+5} g \to g R r_{k+5}$, $a \neq \lambda$
$r_{k+5} \lambda \to 1 R r_{k+6}$ идём до конца, ставим единичку,
$r_{k+6} h \to \lambda S r_{k+7}$ не забывая про λ
$r_{k+7} i \to i L r_{k+7}$, $i \neq 2$ и идём
$r_{k+7} 2 \to 2 R r_{k+8}$ до последней двойки назад.
$r_{k+8} 1 \to 1 S r_{k+4}$ следующий перенос единички, если она есть, иначе
$r_{k+8} 0 \to 0 S r_{k+9}$ стирание двоек до *
$r_{k+9} 2 \to 1 L r_{k+9}$
$r_{k+9} 1 \to 1 L r_{k+9}$
$r_{k+9} 0 \to 0 L r_{k+9}$
$r_{k+9} * \to * S s_1$ когда дойдём, перейдём к выполнению той же операции с a_l

$s_i e \to e R s_i$, $1 \leqslant i \leqslant l+2$, $e \neq 0$
$s_1 0 \to 0 R s_4$
$s_j 0 \to 0 R s_{j+1}$, $4 \leqslant j \leqslant l+2$
$s_{l+3} f \to f L s_{l+4}$
$s_{l+4} 1 \to 2 R s_{l+5}$ дошли до l-ого нуля, далее начинаем копировать единички в конец.
$s_{l+5} g \to g R s_{l+5}$, $a \neq \lambda$
$s_{l+5} \lambda \to 1 R s_{l+6}$ идём до конца, ставим единичку,
$s_{l+6} h \to \lambda S s_{l+7}$ не забывая про λ
$s_{l+7} i \to i L s_{l+7}$, $i \neq 2$ и идём
$s_{l+7} 2 \to 2 R s_{l+8}$ до последней двойки назад.
$s_{l+8} 1 \to 1 S s_{l+4}$ следующий перенос единички, если она есть, иначе
$s_{l+8} 0 \to 0 S s_{l+9}$ стирание двоек до *
$s_{l+9} 2 \to 1 L s_{l+9}$
$s_{l+9} 1 \to 1 L s_{l+9}$

$s_{l+9}0 \to 0Ls_{l+9}$
$s_{l+9}* \to *Sq_2$ ещё и закончили в начале ленты

(**b**)

$q_1b \to bRq_1$, $b \neq \lambda$
$q_1\lambda \to 0Rq_2$
$q_2c \to \lambda Sq_3$ Удлинним на 1 кортеж и вернёмся на место
$q_3d \to dLq_3$, $d \neq *$
$q_3* \to *Sr_1$

$r_ie \to eRr_i$, $1 \leqslant i \leqslant k+2$, $e \neq 0$
$r_10 \to 0Rr_4$
$r_j0 \to 0Rr_{j+1}$, $4 \leqslant j \leqslant k+2$
$r_{k+3}f \to fLr_{k+4}$
$r_{k+4}1 \to 2Rr_{k+5}$ дошли до k-ого нуля, далее начинаем копировать единички в конец.
$r_{k+5}g \to gRr_{k+5}$, $g \neq \lambda$
$r_{k+5}\lambda \to 1Rr_{k+6}$ идём до конца, ставим единичку,
$r_{k+6}h \to \lambda Sr_{k+7}$ не забывая про λ
$r_{k+7}i \to iLr_{k+7}$, $i \neq 2$ и идём
$r_{k+7}2 \to 2Rr_{k+8}$ до последней двойки назад.
$r_{k+8}1 \to 1Sr_{k+4}$ следующий перенос единички, если она есть, иначе
$r_{k+8}0 \to 0Sr_{k+9}$ стирание двоек до *
$r_{k+9}2 \to 1Lr_{k+9}$
$r_{k+9}1 \to 1Lr_{k+9}$
$r_{k+9}0 \to 0Lr_{k+9}$
$r_{k+9}* \to *S\tilde{q_1}$ Таким образом, a_k скопировано в конец, мы в начале.

$\tilde{q_1}b \to bR\tilde{q_1}$, $b \neq \lambda$
$\tilde{q_1}\lambda \to 0R\tilde{q_2}$
$\tilde{q_2}c \to \lambda S\tilde{q_3}$ Удлинним на 1 кортеж и вернёмся на место
$\tilde{q_3}d \to dL\tilde{q_3}$, $d \neq *$
$\tilde{q_3}* \to *Ss_1$

$s_ie \to eRs_i$, $1 \leqslant i \leqslant l+2$, $e \neq 0$
$s_10 \to 0Rs_4$
$s_j0 \to 0Rs_{j+1}$, $4 \leqslant j \leqslant l+2$
$s_{l+3}f \to fLs_{l+4}$
$s_{l+4}1 \to 2Rs_{l+5}$ дошли до l-ого нуля, далее начинаем копировать единички в конец.
$s_{l+5}g \to gRs_{l+5}$, $a \neq \lambda$
$s_{l+5}\lambda \to 1Rs_{l+6}$ идём до конца, ставим единичку,
$s_{l+6}h \to \lambda Ss_{l+7}$ не забывая про λ
$s_{l+7}i \to iLs_{l+7}$, $i \neq 2$ и идём
$s_{l+7}2 \to 2Rs_{l+8}$ до последней двойки назад.
$s_{l+8}1 \to 1Ss_{l+4}$ следующий перенос единички, если она есть, иначе
$s_{l+8}0 \to 0Ss_{l+9}$ стирание двоек до *
$s_{l+9}2 \to 1Ls_{l+9}$
$s_{l+9}1 \to 1Ls_{l+9}$
$s_{l+9}0 \to 0Ls_{l+9}$
$s_{l+9}* \to *Sw_1$ Таким образом, a_l скопировано в конец после a_k. Остаётся перемножить два последних

$w_1b \to bRq_1$, $b \neq \lambda$
$w_1\lambda \to 0Rw_2$
$w_2c \to \lambda Lt_1$ Удлинним на 1 кортеж и не вернёмся на место. Теперь начнётся умножение...

$t_11 \to 1Lt_1$ это мы ещё в предпоследнем числе
$t_10 \to 0Lt_2$ это число закончилось. найдём единичку, заменим на троечку, прибавим

	к совсем последнему числу предпоследнее
$t_2 3 \to 3Lt_3$	мы ищем единичку в третьем с конца числе
$t_2 1 \to 3Lt_4$	либо нашли,
$t_2 0 \to 0Ru_1$	либо не нашли
$t_4 j \to jRt_4$, $j \neq 0$	выбираемся из этого числа, чтобы копировать следующее в конец
$t_4 0 \to 0Rt_5$	выбрались. Займёмся копированием предпоследнего числа
$t_5 2 \to 2Rt_5$	если не дошли до очередной единички для переноса, идём к ней
$t_5 1 \to 2Rt_6$	дошли и идём ставить в конец
$t_6 j \to jRt_6$, $j \neq \lambda$	идём к концу.
$t_6 \lambda \to 1Rt_7$	пришли. Поставили,
$t_7 j \to \lambda Lt_8$	не забыв про λ. Теперь идём за следующей единицей.
$t_8 1 \to 1Lt_8$	это мы в том же числе
$t_8 0 \to 0Lt_9$	это мы перешли в копируемое число
$t_9 1 \to 1Lt_9$	мы уверенно движемся к месту копирования, но ещё не пришли
$t_9 2 \to 2St_5$	отсюда мы начинаем опять искать единичку для копирования в предпоследнем числе
$t_5 0 \to 0Lt_{10}$	мы скопировали всё предпоследнее число.
$t_{10} 2 \to 1Lt_{10}$	пусть опять предпослелнее будут написано единичками
$t_{10} 0 \to 0Lt_2$	оно закончилось, и мы ищем следующую единичку в третьем с конца числе
$u_1 3 \to 2Ru_1$	наконец мы её не нашли, так что остаётся стереть лишнее. Начнём же!
$u_1 0 \to 2Ru_2$	закончилось третье с конца число.
$u_2 1 \to 2Ru_2$	не закончилось предпоследнее число
$u_2 0 \to 2Ru_3$	но вот и оно закончилось. Теперь надо двигать наше $a_k \cdot a_l$, стирая двойки на своём пути
$u_3 j \to jRu_3$, $j \neq \lambda$	двигаемся в конец
$u_3 \lambda \to \lambda Lu_4$	дошли. Теперь наша цель – передвигать.
$u_4 1 \to \lambda Lu_5$	взяли единицу и потащили
$u_5 1 \to 1Lu_5$	...тащим...
$u_5 2 \to 1Lu_6$	притащили и поставили. Думаем, что делать...
$u_6 2 \to 2Ru_3$	опять хотим таскать единицы...
$u_6 j \to jSv_1$, $j \neq 2$	перетаскивать больше нечего! Значит, дело сделано.
$v_1 j \to jLv_1$, $j \neq *$	идём в начало ленты, чтобы закончить там
$v_1 * \to *Sq_2$	программа завершена.

♦ **C9.** Мы начнём с моделирования одного шага машины Тьюринга. Пусть из конфигурации с кодом (p, t) рассматриваемая машина M переходит непосредственно в конфигурацию с кодом $(NextP(p,t), NextT(p,t))$. Проверим, что $NextP$ и $NextT$ – диофантовы функции.

Это утверждение нуждается в следующем уточнении. Мы определили функции $NextP$ и $NextT$ пока только в случае, когда (p, t) – код конфигурации, причём конфигурации с незаключительным состоянием. Положим

$$NextP(p,t) = 0,$$

$$NextT(p,t) = t$$

если (p, t) – код конфигурации с заключительным состоянием. Утверждение о диофантовости $NextP$ и $NextT$ следует понимать как существование диофантовых функций, ведущих себя описанным выше образом на кодах конфигураций и произвольным образом, если значения кодов отличны от кодов конфигураций.

Функции $NextP$ и $NextT$, очевидно, должны зависеть от функций A, D, Q, задающих выбор инструкций машины M. Расширим эти функции, считая, что если q_i – заключительное состояние, то $A(i, j) = j$, $D(i, j) = 5$, $Q(i, j) = 0$.

Диофантовость функции $NextT$ почти очевидна, поскольку каждый элемент кортежа с шифром $NextT(p, t)$ однозначно определяется элементами с теми же номерами кортежей с шифрами p и t. А именно, определим функцию A следующим образом:

$$A(i,j) = \begin{cases} A(i,j), & \text{если} 0 < i \leqslant v,\ 0 \leqslant j \leqslant w \\ j & \text{в противном случае} \end{cases}$$

(напомним, что v и w – это количества состояний и символов машины M). Тогда $Next$ можно определить эквивалентностью

$$t' = NextT(p,t) \Leftrightarrow \exists w\ t' = A[\beta](p,t,w),$$

где $A[\beta]$ – расширение функции A на кортежи.

Диофантовость функции $NextP$ менее очевидна, поскольку k-ый элемент кортежа с шифром $NextP(p,t)$ однозначно определяется лишь элементами с номерами $k-1$, k, $k+1$ кортежей с шифрами p и t. Функции расширять мы умеем на кортежи лишь поэлементно, однако эта трудность легко преодолима. Положим

$$p^R = p\beta, \quad p^L = p\ div\ \beta$$

$$t^R = t\beta, \quad t^L = p\ div\ \beta$$

Очевидно, что если t – шифр кортежа $(s_1,\dots,s_m,\dots,s_l)$, то t^R и t^L – шифры кортежей

$$(0,s_1,\dots,s_{m-1},\dots,s_l)$$

и

$$(s_2,\dots,s_{m+1},\dots,s_l,0).$$

(в кортежах выделены m-ые элементы). Аналогично, если p – шифр кортежа $(0,\dots,0,i,0,\dots,0)$, то p^R и p^L – шифры кортежей

$$(0,\dots,0,0,i,\dots,0)$$

$$(0,\dots,i,0,0,\dots)$$

, в которых ненулевой элемент сдвинут на одну позицию вправо или влево.

Каждый элемент кортежа с шифром $NextP(p,t)$ определяется элементами с тем же номером кортежей с шифрами p^L, p, p^R, t^L, t, t^R. Эта же зависимость, очевидно, определяется функциями D и Q. Зададим её явно, введя функция DQ следующим образом:

$$DQ(i^L,i,i^R,j^L,j,j^R) = \begin{cases} Q(i^L,j^L), & \text{если } i^L>0,\ i=i^R=0 \text{ и } D(i^L,j^L)=L \\ Q(i,j), & \text{если } i^L=0,\ i>0,\ i>0,\ i^R=0 \text{ и } D(i,j)=S \\ Q(i^R,j^R), & \text{если } i^L=i=0,\ i^R>0 \text{ и } D(i^R,j^R)=R \\ 0, & \text{в противном случае} \end{cases}$$

(к "противны случаям"относятся и случаи, когда какое-то из чисел i^L, i, i^R больше v или какое-то из чисел j^L, j, j^R больше w, ибо тогда Q и D не определены). Теперь мы можем указать диофантово представление для $NextP$:

$$p' = NextP(p,t) \Leftrightarrow \exists w\ DQ[b](pb,p,p\ div\ b,tb,t,t\ \div\ b,w)$$

♦ **C10.** Функции $NextP$, $NextT$ описывают один шаг работы рассматриваемой машины Тьюринга. Наша очередная цель – установить диофантовость трёхместных функций $AfterP$, $AfterT$, которые получаются как итерации функций $NextP$, $NetxT$:

$$AfterP(0,p,t) = p$$

$$AfterT(0,p,t) = t$$

$$AfterP(k+1,p,t) = NextP(k,AfterP(k,p,t),AfterT(k,p,t))$$

$$AfterT(k+1,p,t) = NextT(k,AfterP(k,p,t),AfterT(k,p,t))$$

Ясно, что за k шагов машина из M из конфигурации (p,t) перешла в конфигурацию (p',t'), то $p' = AfetrP(k,p,t)$, $t' = AfterT(k,p,t)$.

Рассмотрим все промежуточные конфигурации

$$(p_0,t_0),\dots,(p_k,t_k),$$

где

$$(p_0,t_0) = (p,t)$$

$$(p_{i+1},t_{i+1}) = (NextP(p_i,t_i),NextT(p_i,t_i))$$

$$(p',t') = (p_k,t_k).$$

Пусть l столь велико, что

$$p < \beta^{l-k-2}, \quad t < \beta^{l-2}$$

Это означает, что в конфигурации (p, t) не более чем $I - k - 2$ первых клеток ленты заняты символами. За k шагов работы машина M сможет заполнить не более чем k новых клеток, и потому при $i \in \{0, \ldots, k\}$

$$p_i < \beta^{l-2}, \quad t_i < \beta^{l-2}$$

в частности,

$$p' < \beta^{l-2}, \quad t' < \beta^{l-2}$$

Построим две суперконфигурации (p_L, t_L), (p_R, t_R) при помощи конкатенации конфигураций (p_i, t_i) (напомним, что диофантовость конкатенации кортежей с равными основаниями была установлена):

$$(p_L, \beta, kl) = (p_0, \beta, l) + \cdots + (p_{k-1}, \beta, l)$$
$$(t_L, \beta, kl) = (t_0, \beta, l) + \cdots + (t_{k-1}, \beta, l)$$
$$(p_R, \beta, kl) = (p_1, \beta, l) + \cdots + (p_k, \beta, l)$$
$$(t_R, \beta, kl) = (t_1, \beta, l) + \cdots + (t_k, \beta, l)$$

Суперконфигурации (p_L, t_L) и (p_R, t_R) конфигурациями не являются, поскольку кортежи с шифрами p_L и p_R содержат по k ненулевых элементов, а кортежи с шифрами t_L и t_R соответствуют лентам, на которых k клеток помечено символом «*».

Суперконфигурации соответствуют супермашине, лента которой разделена символами «*» на k участков, на каждом из которых работает своя головка в соответствии с инструкциями исходной машины M. Вместо k шагов работы машины M мы можем рассмотреть один шаг работы супермашины, при котором каждая головка независимо от других выполняет соответствующую инструкцию.

Таким образом, суперконфигурация (p_R, t_R) однозначно определяется суперконфигурацией (p_L, t_L); более того, введённые функции $NextP$ и $NextT$ без какой-либо модификации описывают работу супермашины:

$$p_R = NextP(p_L, t_L), \quad t_R = NextT(p_L, t_L)$$

Рассмотрим также суперконфигурацию (p_M, t_M), определяемую равенствами

$$(p_M, \beta, (k-1)l) = (p_1, \beta, l) + \cdots + (p_{k-1}, \beta, l)$$
$$(t_M, \beta, (k-1)l) = (t_1, \beta, l) + \cdots + (t_{k-1}, \beta, l)$$

Определения p_L, t_L можно переписать в новых обозначениях так:

$$(p_L, \beta, kl) = (p, \beta, l) + (p_M, \beta, (k-1)l)$$
$$(t_L, \beta, kl) = (t, \beta, l) + (t_M, \beta, (k-1)l)$$
$$(p_R, \beta, kl) = (p, \beta, (k-1)l) + (p', \beta, l)$$
$$(t_R, \beta, kl) = (t, \beta, (k-1)l) + (t', \beta, l)$$

Мы видели, что для любой конфигурации (p, t) и любого положительного k при любом l достаточно большом найдутся числа p_L, t_L, p_M, t_M, p_R, t_R, p', t', удовлетворяющие вышеперечисленным условиям. Покажем теперь, что выбор этих чисел однозначно определяется по k, l, p, t.

Действительно, первые l элементов кортежей (p_L, β, kl) и (t_L, β, kl) определены однозначно. Функции $NextP$ и $NextT$ были определены эквивалентностями так, что первые m элементов кортежей с шифрами $NextP(x, y)$, $NextT(x, y)$ однозначно определяются первыми $m + 1$ элементами кортежей с шифрами x, y. Таким образом, первые $l - 1$ элементыкортежей с кодами (p_R, β, kl) и (t_R, β, kl) определены однозначно. Значит однозначно определены первые $l - 1$ элементы кортежей с кодами $(p_M, \beta, (k-1)l)$, $(t_M, \beta, (k-1)l)$.

Мы видим, что однозначно определены первые $2l - 1$ элемента кортежей с кодами $(p_L, \beta.kl)$, (t_L, β, kl), следовательно, первые $2l-2$ элемента кортежей с кодами (p_R, β, kl), (t_R, β, kl), и первые $2l-2$ элеиента кортежей с кодами $(p_M, \beta, (k-1)l)$, $(t_M, \beta, (k-1)l)$.

Повторив это рассуждение достаточное число, раз, мы получим, что однозначно определены все элементы кортежей с кодами (p_L, β, kl), (t_L, β, kl), $(p_M, \beta, (k-1)l)$, $(t_M, \beta, (k-1)l)$ и все, кроме, быть может, самых последних, элементы кортежей с кодами (p_R, β, kl), (t_R, β, kl), $(p',]beta, l)$, (t', β, l). Но из вышеуказанных неравенств следует, что последние элементы кортежей с кодами (p', β, l), (t', β, l) равны нулю, и поэтому равны нулю и последние элементы кортежей с кодами (p_R, β, kl), (t_R, β, kl).

Таким образом, мы установили, что система диофантовых условий для любой конфигурации и любого положительного k при любом l достаточно большом имеет относительно p_L, t_L, p_M, t_M, p_R, t_R, p', t' ровно одно решение, и в этом единственном решении $p' = AfterP(k, p, t)$, $t' = AfterT(k, p, t)$. Отсюда мы немедленно получаем диофантовость функций $AfterP$ и $AfterT$.

♦ **C11.** Для построения требуемого диофантова уравнения нам осталось сделать небольшой шаг. Пусть $\omega_1, \ldots, \omega_z$ — номера состояни машины M, объявленных заключительными. Тогда условие

$$\exists k, r \mid [\mathbf{Elem}(After(k,p,t) = \omega_1, \beta, r) \text{ или } \ldots \text{ или } \mathbf{Elem}(After(k,p,t), \beta, r) = \omega_z]$$

Выполнено для конфигурации $\langle p, t\rangle$ в том и только в том случае, когда, начав работу в этой конфигурации, машина остановится ровно через k шагов. Это условие является диофантовым и потому может быть преобразовано в искомое диофантово уравнение.

Полученное диофантово уравнение — еще не совсем то, что нам требуется для установления диофантовости множества $\mathfrak{M}$, полуразрешаемого рассматриваемой машиной M (параметры этого уравнения — p и t, а не $a_1, \ldots, a_n$, как требуется в диофантовом представлении множества). Однако легко понять, что в начальной конфигурации $p = 1$ (машина находится в состоянии q_1, а головка расположена в крайней левой клетке) и

$$\langle t, \beta, a\rangle = \langle \varkappa, \beta, 1\rangle + \langle \mu, \beta, 1\rangle + \langle \mathbf{Repeat}(\nu, \beta, a_1), \beta, a_1\rangle + \ldots + \langle \mu, \beta, 1\rangle + \langle \mathbf{Repeat}(\nu, \beta, a_1), \beta, a_1\rangle\,,$$

где $a = a_1 + \ldots + a_n + n + 1$ — количество непустых клеток на ленте, $\varkappa$, μ и ν — номера символов «*», «0», и «1» в ленте из C10, т.е. $a_\varkappa = *$, $a_\mu = 1$. Объединяя полученное нами диофантово уравнение и выписанную строчку с тем, что $p = 1$, и считая $a_1, \ldots, a_n$ параметрами, а все остальные перменные — неизвестными, мы получаем требуемое диофантово представление $\mathfrak{M}$.

♦ **E3.** Пусть w – большое число (точное неравенство будет выписано ниже). С помощью $Equal$ мы можем перейти от кодов с основаниями b и g к новым кодам (w, s, d, e, f) и (d, e, f, w, t) того же полинома C и того же потенциального решения. Рассмотрим число

$$(1 + aw + t)^{d-1} = (1 + aw^{d^0} + x_1 w^{d^1} + \cdots + x_m w^{d^m})^{d-1} = \sum_{i_0 + \cdots + i_m < d} \binom{d-1}{i_0 \ldots i_m} a^{i_0} x_1^{i_1} \ldots x_m^{i_m} w^{i_0 d^0 + \cdots + i_m d^m}$$

Заметим, что в этой сумме все показатели степени у w различны, поэтому, если w достаточно велеко, то эта формула является шифром по основанию w некоторого кортежа, содержащего все одночлены, составляющие C, но с другимикоэффициентами. Чтобы подправить коэффициенты, умножим форулу на

$$s = \sum_{i_0 + \cdots + i_m < d} i_0! \ldots i_m! (d - 1 - i_0 - \cdots - i_m)! c_{i_0 \ldots i_m} w^{d^{m+1} - i_0 d^0 - \cdots - i_m d^m}$$

и сгруппируем вместе члены с одинаковыми степенями w:

$$(1 + aw + t)^{d-1} s = \sum_{k=0}^{2d^{m+1}-1} C_k w^k \qquad (1)$$

Здесь C_k – некоторые выражения, содержащие $C_{i_0 \ldots i_m}$, a, $x_1, \ldots, x_m$. Нетрудно видеть, что

$$C_{d^{e+1} = \sum_{i_0 + \ldots i_m < d} \binom{d-1}{i_0 \ldots i_m} i_0! \ldots i_m! (d-1-i_0-\cdots-i_m)! C_{i_0 \ldots i_m} a^{i_0} x_1^{i_1} \ldots x_m^{i_m} = (d-1)! C(a, x_1, \ldots, x_m))})$$

Таким образом, если w превосходит $C_0, \ldots, C_{2d^{m+1}-1}$, то

$$C(a, x_1, \ldots, x_m) = Elem((1 + aw + t)^{d-1} s, w, d^{e+1} + 1)/(d-1)!$$

Остаётся найти какую-нибудь явную нижнюю границу для w, гарантирующую справедливость последней формулы. Нетрудно проверить, что для этого достаточно потребовать, чтобы

$$w > (1 + a + h)^{d-1} c.$$

Определим теперь девятиместное соотношение

$Solution(a, b, c_L, c_R, d, e, f, g, h) \Leftrightarrow SCod(d, e, f, g, h) \wedge \exists s_L, s_R, t, w (w > (1+a+h)^{d-1}(c_L + c_R) \wedge Equal(c_L, b, d^{e+1} + 1, s_L, w, d^{e+1}+1) \wedge Equal(c_R, b, d^{e+1}+1, s_R, w, d^{e+1}+1) \wedge Equal(h, g, d^e+1, t, w, d^e+1) \wedge Elem((1+aw+t)^{d-1} s_L, w, d^{e+1}+1) = Elem((1 + aw + t)^{d-1} s_R, w, d^{e+1} + 1))$. Как следует из вышенаписанной формулы, $ECode(b, c_L, c_R, d, e, f) \Rightarrow \exists g, h\ SCode(d, e, f, g, h) \wedge Solution(a, b, c_L, c_R, d, e, f, g, h)) \Leftrightarrow \exists x_1, \ldots, x_m\ D_{b, c_L, c_R, d, e, f}(a, x_1, \ldots, x_m) = 0$.

Отношение $Solution(a, b, c_L, c_R, d, e, f, g, h)$, введённое нами, очевидно является диофантовым, и мы може построить диофантово уравнениее

$$U(a, b, c_L, c_R, d, e, f, g, h, y_9, \ldots, y_m) = 0,$$

задающее это отношение. Нетрудно понять, что отнеся g и h к неизвестным, мы получим требуемое универсальное уравнение.

Мы можем теперь построить для каждого n универсальный полином U_n с одним параметром-кодом и m неизвестными. Полином U_1 мы определим равенством

$$U_1(a, k, y_1, \ldots, y_m) = U^2(a, y_1, \ldots, y_m) + (k - 2^{2^6} Cantor_6(y_1, \ldots, y_6))^2.$$

Соответственно, если (b, c_L, c_R, e, d, f) — расширенный код некоторого уравнения $D(a, x_1, \ldots, x_m) = 0$, то в новой кодировке кодом уравнениябудет по определению число $2^{2^6}\mathbf{Cantor}_6(b, c_L, c_R, d, e, f)$.

При таком определенииине каждон натуральное число оказывается кодом какого-нибудь уравнения. Этот «недостаток» легко можно устранить следующим образом. Ясно, что по каждому конкретному числу k можно узнать, представимо ли оно в виде (1), где (b, c_L, c_R, d, e, f) – расширенный код какого-либо уравнения. Если k не представимо в таком виде, то будем по определению считать число k кодом уравнения

$$U_1(a, k, x_1, \ldots, x_m) = 0$$

с единственным параметром aи m неизвестными $x_1, \ldots, x_m$. Очевидно, что, каковы бы ни были значения a и k, уравнение имеет решение тогда и только тогда, когда решение имеет уравнение с кодом k независимо от того, Является ли k кодом в первоначальном смысле (1) или кодом следующего за ним уравнения.

Для $n > 1$ ниверсальный полином U_n определяется следующим образом:

$$U_n(a_1, \ldots, a_n, k, y_1, \ldots, y_m) = U_1(2^n\mathbf{Cantor}_n(a_1, \ldots, a_n, k, y_1, \ldots y_m)$$

Наконец определим универсальный полином U_n равенством

$$U_0(k, y_1, \ldots, y_m) = U_1(0, k, y_1, \ldots, y_m),$$

считая любой код уравнения на s также кодом уравнения без параметров $D(0, x_1, \ldots, x_m) = 0$.

Универсальное диофантово уравнение позволяет нам легкопостроить пример диофантова множества с недиофантовым дополнением. Существование таких множеств показывает, что мы не можем пополнить ни отрицанием, ни квантором всеобщности пополнить наш арсенал логических средств для построения диофантовых множеств (в данный момент это оъединение, пересечение, квантор существования), ибо дополнение диофантова множества, определяемого уравнением $D(a, x_1, \ldots, x_m) = 0$ задаётся формулами

$$\neg\exists x_1, \ldots, x_m\ D(a, x_1, \ldots, x_m) = 0 \qquad \text{и} \qquad \forall x_1, \ldots x_m\ D(a, x_1, \ldots, x_m) \neq 0.$$

Построение проводится по классической диагональной схеме. Рассмотрим универсальное диофантово уравнение $U_1(p, q, y_1, \ldots, y_m) = 0$ и поставим на место обоих параметров параметр-элемент a: $U_1(a, a, y_1, \ldots, y_m) = 0$. Получившееся уравнение определяет некоторое диофантово множество $\mathfrak{H}_1$ натуральных чисел. Проверим, что $\overline{\mathfrak{H}_1}$ – дополнение $\mathfrak{H}$ – не является диофантовым.

Множество $\mathfrak{H}_1$ является несколько искусственным примером. Более интересным является множество $\mathfrak{H}_0$, определяемое уравнением

$$U_0(t, y_1, \ldots, y_m) = 0.$$

Как видно из определения, $\mathfrak{H}_0$ – множество кодов диофантового уравнения (без параметра), имеющих решения. В этой терминологии десятая проблема Гильберта – вопрос с способе распознавания принадлежности данного числа a к множеству $\mathfrak{H}_0$.

Полином U_0 был определён таким образом, что решение уравнения (7) сводится к решению уравнения при $p = 0$, $q = t$. Для того, чтобы доказать, что $\overline{\mathfrak{H}_0}$ – дополнение $\mathfrak{H}_0$ – не является диофантовым. Мы установим обратную связь, а именно, покажем, что решение уравнения при произвольных значених параметров p и q сводится к решению уравнения (7) при подходящем значении t. Непосредственно в таком виде это утверждение очевидно, ибо при фиксированных значениях p и q можно взять в качестве t код уравнения (1), рассматриваемого как уравнение без параметров. Существенным для нас является то обстоятельство, что такой код может быть задан полиномом с целыми коэффициентами от p и q.

Итак, рассматриваем уравнение

$$W_{p,q}(y_1, \ldots, y_m) = 0,$$

поучившееся подстановкой конкретных значений p и q из уравнения (1). Сначала мы построим расширенный код (b, c_L, c_R, d, e, f) этого уравнения. Понятно, что d и e а следовательно и f можно взять фиксированными не зависящими от p и q.

В итоге получаем следующую связь множеств:

$$a \in \mathfrak{H}_1 \Leftrightarrow K(a, a) \in \mathfrak{H}_0$$

, где K – полином с целыми коэффициентами. Если бы дополнение первого было диофантовым, то таковым оказалось бы и дополнение второго, что не так, так что $\overline{\mathfrak{H}_0}$ не диофантово.