第22卷第4期 数学进展 Vol.22, No.4
1993年8月 ADVANCES IN MATHEMATICS Aug., 1993

Jones在Hilbert第十问题及其相关课题上的工作

——为Jones教授访华而作*

孙智伟

(南京大学数学系，南京，210008，江苏)

摘要 本文是有关Hilbert第十问题近代成果(特别是James P. Jones教授的工作)的综述报告。它由六个部分组成：1. Hilbert第十问题；2. 9未知数定理；3. 通用不定方程；4. 不定方程前缀量词分类；5. Diophantine表示；6. Hilbert第十问题的应用。文中还提到了作者的一些新结果，例如$\exists^{11}$ over $\mathbf{Z}$不可判定。

关键词 Hilbert第十问题；Diophantine方程；Diophantine表示；不可判定性；计算复杂性

James P. Jones是一位国际上著名的不定方程复杂性方面的专家。他于1968年在Washington大学获得数学博士学位，之后便到加拿大的Calgary大学任教，1982年晋升为教授。

Jones教授从1966年开始发表学术论文或专著，他的大部分工作都直接或间接地与Hilbert第十问题有关(参看[1]—[23])。目前在Hilbert第十问题及其相关课题上，Jones教授已是位著名的国际学术带头人。鉴于他的工作意义重大且极具代表性，而我国又缺少介绍Hilbert第十问题新进展的文章(关于Hilbert第十问题的否定解决，莫绍揆[24,25]和胡久稔[26]都作过介绍)，作者不揣浅陋，冒昧撰写此文，借Jones教授访华之机，让国内同行进一步了解有关Hilbert第十问题及其相关课题的最新成果。

1 Hilbert第十问题

在1900年的国际数学家大会上，D.Hilbert提出了著名的23个数学问题，其中第十问题要求找出一个可用以判定任一(整系数)多项式方程$P(x_1,\cdots,x_n)=0$是否有整数解的算法。

显然$P(x_1,\cdots,x_n)=0$有整数解当且仅当$\prod P(\pm x_1,\pm x_2,\cdots,\pm x_n)=0$有自然数(非负整数)解，这儿求积运算$\prod$过所有可能的正负号配置。另一方面，$P(x_1,\cdots,x_n)=0$有自然数解当且仅当$P(x_1^2+y_1^2+z_1^2+t_1^2,\cdots,x_n^2+y_n^2+z_n^2+t_n^2)=0$有整数解(根据数论中的Lagrange

收稿日期：1990-05-21，修改稿：1991-06-10。
* 国家自然科学基金资助项目。

定理，每个自然数都是四个整数的平方和）。可见 Hilbert 第十问题等价于寻找可用以判定多项式方程是否有自然数解的算法。

递归论诞生后算法的概念明确了，Church 论题断言可计算函数类就是部分递归函数类、Turing 可计算函数类（后两者已被证明是一致的）.如果存在（全的）递归函数 f 使得

$$R(a_1,\cdots,a_m)\Longleftrightarrow \exists x_1\cdots\exists x_n[f(a_1,\cdots,a_m,x_1,\cdots,x_n)=0],$$

则说 m 元关系 R 是递归可枚举(recursively enumerable)关系（r.e.关系)(在本文中若无特别声明，变元均在自然数集 N 中取值。）一元递归可枚举关系称为递归可枚举集(r.e.集)，熟知 r.e.集就是空集或者一元递归函数的值域。由于存在非递归的 r.e.集（例如 K），为否定解决 Hilbert 第十问题，我们只需证明

定理1 每个 r.e.关系 $A(a_1,\cdots,a_m)$ 均可表成下形

$$A(a_1,\cdots,a_m)\Longleftrightarrow \exists x_1,\cdots,x_n[P(a_1,\cdots,a_m,x_1,\cdots,x_n)=0]。\qquad (1)$$

这儿 $P(a_1,\cdots,a_m,x_1,\cdots,x_n)$ 为整系数多项式。对任给的 r.e.关系 A 有多项式 P 使(1)对所有 $a_1,\cdots,a_m$ 均成立。（变元 $a_1,\cdots,a_m$ 称为参数，$x_1,\cdots,x_n$ 叫做未知数。）

如果 Hilbert 第十问题（递归）可解，即存在所要求的那种（递归）算法，则由定理 1 知每个 r.e.关系都是递归的，而这与事实不符。

可用(1)那种形式定义的关系 $A(a_1,\cdots,a_m)$ 叫做 Diophantine 关系。集 A 为 Diophantine 集指 "$a\in A$" 为 Diophantine 关系。为方便起见以后把 "Diophantine" 省写成 "D"，如此便有 D-集、D-关系、D-方程、D-表示、D-可定义性之类的术语了。由定理 1 知每个 r.e.关系均为 D-关系，而另一方面 D-关系显然是 r.e.关系，故定理 1 蕴含着 r.e.性和 D 性的吻合一致。

下面我们将勾划出定理 1 的最现代也最简洁的证明，它基本上是 Jones 和 Ju. V.Matijasevič 的杰作(参看[22])。

最初对 Hilbert 第十问题的解决分两步走。1961年 M.Davis, H. Putnam 和 J. Robinson 迈出了重要的第一步（参看[27]），他们证明了指数形式的定理 1，即其中的 $P(a_1,\cdots,a_m,x_1,\cdots,x_n)$ 是形如 $ca_1^{\beta_1}\cdots a_k^{\beta_k}$（$c$ 为整数，每个 a_i、β_i 是正整数或者变元 $a_1,\cdots,a_m,x_1,\cdots,x_n$ 之一）的项的和.（依这种形式，定理 1 可解释为每个 r.e.关系都是指数 D 的。）最后一步（也是最关键的一步）由 Matijasevič 在1970年完成（参看[28]），他证明了指数关系是 D-关系，这样就完成了定理 1 的证明从而否定解决了 Hilbert 第十问题，为证明指数关系的 D 性，Matijasevič 利用了 Fibonacci 数列$\{F_n\}$($F_0=0,F_1=1,F_{n+2}=F_n+F_{n+1}$)的若干整除性质，其后不久大家都习惯使用 Pell 方程的解序列。

Pell 方程的一般形式是

$$x^2-dy^2=1\ (d\notin\square,\ \square\text{表示全体平方数构成的集合})。\qquad (2)$$

依数论上一条熟知的定理，对每个 $d\notin\square$ 不定方程(2)有无穷多组解。实际使用时仅需考虑 $d=a^2-1$ 情形的 Pell 方程。显然

$$x^2-(a^2-1)y^2=1\ (a>0)\qquad (3)$$

有平凡解 $(x,y)=(a,1)$。定义 $X_a(n)$、$Y_a(n)$ 如下：

$$X_a(0)=1, X_a(1)=a,\ X_a(n+2)=2aX_a(n+1)-X_a(n);$$
$$Y_a(0)=0, Y_a(1)=1,\ Y_a(n+2)=2aY_a(n+1)-Y_a(n).$$

可以证明序列$\{X_a(n)\}$和$\{Y_a(n)\}$($a>0$)有下列性质(请参看[22],[24],[26]以及 Davis[29]、Matijasevič 与 Robinson[30]等文献)。

性质1 (Diophantine 特征) 自然数对(x,y)为(3)的解当且仅当有 n 使得 $x=X_a(n), y=Y_a(n)$。

性质2(单调性) $X_1(n)=1, Y_1(n)=n$。$a>1$时 $X_a(n)$和 $Y_a(n)$是 n的严格递增函数。

性质3(倍角公式) $X_a(2n)=2X_a^2(n)-1,\ Y_a(2n)=2X_a(n)Y_a(n)$。

性质4(同余规则) $Y_a(n)\equiv Y_b(n) \pmod{a-b}$,特别地 $Y_a(n)\equiv Y_1(n)=n \pmod{a-1}$。

性质5(第一降级引理) $Y_a^2(n)\mid Y_a(m)\Longleftrightarrow nY_a(n)\mid m$。

性质6(第二降级引理) 设 $a>1, n>0$,则

$$Y_a(k)\equiv\pm Y_a(m) \pmod{X_a(n)}\Longleftrightarrow k\equiv\pm m \pmod{2n}.$$

由上述性质我们可以得到

引理1 设 $A>1, B>0$,则 $C=Y_A(B)$当且仅当有自然数 D,E,F,G,H,I 使得如下的(i)—(ix)成立:

(i) $D^2-(A^2-1)C^2=1$, (ii) $F^2-(A^2-1)E^2=1$, (iii) $I^2-(G^2-1)H^2=1$, (iv) $2C^2\mid E$ 且 $E\neq 0$, (v) $G\equiv A \pmod F$, (vi) $G\equiv 1 \pmod{2C}$, (vii) $H\equiv C \pmod F$, (viii) $H\equiv B \pmod{2C}$, (ix) $B\leqslant C$。

证 (⇐)设有自然数 D,E,F,G,H,I 满足(i)—(ix),依(i)、(ii)、(iii)存在(自然数)p,q,r 使得(注意利用性质 1)

$$D=X_A(p), C=Y_A(p);\ F=X_A(q), E=Y_A(q);\ I=X_G(r), H=Y_G(r).$$

显然 $C=Y_A(p)\geqslant p(\geqslant 0)$(由性质2),由(ix)有 $C\geqslant B(>0)$。若证得 $B\equiv r\equiv\pm p \pmod{2C}$,则必 $B=p, C=Y_A(B)$。(不然将有 $B\neq p, 0<B+p<2C, B\not\equiv\pm p \pmod{2C}$。)由 (iv) 知 $Y_A^2(p)\mid Y_A(q)$,利用性质 5 即得 $pY_A(p)\mid q$ 从而 $C\mid q$。依(vi)、(viii)及同余规则我们有

$$B\equiv H=Y_G(r)\equiv Y_1(r)=r \pmod{2C}.$$

由(v)、(vii)利用同余规则可得

$$Y_A(r)\equiv Y_G(r)=H\equiv C=Y_A(p) \pmod{X_A(q)}.$$

考虑到 $A>1, q>0$(因为 $E\neq 0$),利用性质 6 即得 $r\equiv\pm p \pmod{2q}$。而 $C\mid q$,故 $r\equiv\pm p \pmod{2C}$,因此

$$B\equiv r\equiv\pm p \pmod{2C}.$$

如上所言现在可得 $B=p, C=Y_A(B)$。

(⇒)假定 $C=Y_A(B)$,令 $D=X_A(B)$,则(i)、(ix)已成立。($C\geqslant B$ 可由性质 2 得到。)令 $q=BY_A(B), F=X_A(2q), E=Y_A(2q)$,则(ii)成立。依性质 5,$Y_A^2(B)\mid Y_A(BY_A(B))$,即 $C^2\mid Y_A(q)$。由倍角公式 $2X_A(q)Y_A(q)=Y_A(2q)=E$,故 $2C^2\mid E$。又 $B>0, q>0, E>0$,故(iv)成立。令 $G=A+F^2(F^2-A)$(注意 $F^2=1+(A^2-1)E^2\geqslant 1+(A^2-1)\geqslant A$),则(v)成立。依(ii)、(iv),$F^2\equiv 1 \pmod E$ 从而 $F^2\equiv 1 \pmod{2C}$。于是 $G\equiv A+1\cdot(1-A)=1 \pmod{2C}$,(vi)成立。令 $I=X_G(B), H=Y_G(B)$,则(iii)成立。使用同余规则得

$$H=Y_G(B)\equiv B(\mathrm{mod}\,G-1),\qquad H=Y_G(B)\equiv Y_A(B)=C(\mathrm{mod}\,G-A),$$
$$H\equiv B(\mathrm{mod}2C),\qquad H\equiv C(\mathrm{mod}\,F),$$

可见(vii)、(viii)也成立。

综上，引理1获证。

关于序列$\{X_a(n)\}$、$\{Y_a(n)\}(a>0)$，我们还需要

性质7[22,30] $n>1$时$(2a-1)^n\leqslant Y_a(n+1)<(2a)^n$。

性质8[29] $X_a(n)-(a-k)Y_a(n)\equiv k^n(\mathrm{mod}\,2ak-k^2-1)$。

值得指出，性质8是J.Robinson在1952年首先获得的(参看[31])。

引理2 设$n>0,k>1,a\geqslant Y_k(n+1)$,则$k^n=\mathrm{rem}(X_a(n)-(a-k)Y_a(n),2ak-k^2-1)$。($\mathrm{rem}(x,y)$表示$x$被除以$y$后所得的余数。)

证 依性质7我们有

$$k\leqslant k^n<(2k-1)^n\leqslant Y_k(n+1)\leqslant a$$
$$<ak+(k+1)k-k^2-1\leqslant ak+ak-k^2-1=2ak-k^2-1,$$

由此利用性质8即得欲证。

现在由引理1、2可以看出指数关系$m=k^n$是D的。事实上，$n>0$且$k>1$时$m=k^n$当且仅当有（自然数）a使得

$$a=Y_k(n+1),\quad m<2ak-k^2-1,$$
$$m\equiv X_a(n)-(a-k)Y_a(n)\,(\mathrm{mod}\,2ak-k^2-1).$$

(注意$x=X_a(n)$当且仅当有y使得$y=Y_a(n)$并且$x^2-(a^2-1)y^2=1$。)

引理3 设$u>2^n$，则$\binom{n}{k}=\mathrm{rem}\left(\lfloor\frac{(u+1)^n}{u^k}\rfloor,u\right)$。(本文用$\lfloor\alpha\rfloor$和$\lceil\alpha\rceil$分别表示不超过$\alpha$的最大整数、不小于$\alpha$的最小整数。)

该引理的证明并不难，但要注意使用二项式定理，详情可见[22]、[29]。

依引理3，$m=\binom{n}{k}$当且仅当有（自然数）u,x,y使得

$$(u+1)^n=yu^{k+1}+mu^k+x,\quad 2^n<u,x<u^k\text{且}m<u.$$

由此利用指数关系的D性，我们得到$m=\binom{n}{k}$为D-关系。

E.Lucas早在1878年就证明过组合数有如下的

性质9[22] 设p为素数，$r=\sum_{i=0}^{n}r_ip^i(0\leqslant r_i<p)$，$s=\sum_{i=0}^{n}s_ip^i(0\leqslant s_i<p)$，则

$$\binom{s}{r}\equiv\binom{s_0}{r_0}\binom{s_1}{r_1}\cdots\binom{s_n}{r_n}\ (\mathrm{mod}\,p).$$

任给自然数r和s，如果r的每个二进位数字均不超过s的相应二进位的数字，我们就说r被s所遮掩并记之为$r\leqslant s$。显然$\leqslant$是个半序关系，而且$r\leqslant s\Rightarrow r\leqslant s$。遮掩关系$\leqslant$还是个$D$-关系，因为我们有

引理4 $r\leqslant s\Longleftrightarrow\binom{s}{r}\equiv 1(\mathrm{mod}\,2)$。

证 在性质 9 中取 $p=2$ 并注意

$$\binom{0}{0}=\binom{1}{0}=\binom{1}{1}=1,\quad \binom{0}{1}=0.$$

如前所述，r.e.关系与 r.e.集的定义牵涉到递归函数。关于递归函数(完全可计算函数)的概念，我们使用等价于 Turing 机的一种机器模型——记录器 (register machine)。

记录器是这样的一种机器，它具有一个有穷程序和有穷多个分开的可访问的记录（或存贮）单元 $R1,R2,\cdots,Rr$。记录单元的个数没有上界（但要有穷），每个记录单元可记录一个任意大的自然数。一组记录单元，譬如说 $R1,\cdots,Rk(k<r)$，将被设计成输出单元；还有一组记录单元，譬如说 $R1,\cdots,Rm(m<r)$将被用作输入单元。这样做是为了处理 k 元函数值是 m 元组的情形。（通过使用一一对应的配对函数组，每个自然数均可看成是有顺序的 m 个自然数的编码。）对于一元函数来说 k 等于 1，通常 m 也都是 1，因此 $R1$ 常被当作输入-输出单元。

记录器的有穷程序是逐行列出的（以 $L1,L2,\cdots,Ll$ 来标记）的一组指令。(若不发生转移就依次执行。) 为能计算全体递归函数，只需假定记录器具有加 1、减 1 以及转移之功能。为避免从 0 减去 1，Minsky 规定只有在判出非零后才允许减 1，他的减 1 指令要求如下两行

$$Li \text{ IF } Rj=0,\text{GOTO } Lk,$$

$$L(i+1) \text{ ELSE } Rj\leftarrow Rj-1.$$

我们将假定我们的记录器具有以下几种基本指令（实际程序中均（象 Minsky 那样）避免出现从 0 减去 1）：

指　令	解　释
Li GOTO Lk	(无条件) 转移至 Lk 行
Li IF $Rj>0$ GOTO Lk	条件转移至 Lk 行
Li $Rj\leftarrow Rj+1$	记录单元 Rj 内容增 1
Li $Rj\leftarrow Rj-1$	记录单元 Rj 内容减 1。

可以证明（参看 Minsky [32]），这种记录器（完全）可计算函数即是 Turing 机（完全）可计算函数，反之亦然。因此递归函数与记录器完全可计算函数实际上是一回事。

下面考虑记录器工作的算术化。假设记录器 M 计算全函数 $y=f(x)$，它有 r 个记录单元和 l 条基本指令。通过使用 GOTO 语句，我们不妨假定 $l>0$。(若 $l=0$ 可让指令 $L1$ 为 GOTO $L2$。) 我们还可假定只有一条停机指令且在程序的最后，其标号为 $L(l+1)$。考虑到只有增 1 指令才能增大记录单元的内容，在计算过程中记录单元 Rj 在时刻 t (第 t 步) 所记录之数 $r_{j,t}$ 不会超过 $x+t$。根据在时刻 t 是否执行指令 Lj，我们让 $l_{j,t}$ 取值 1 或 0。

假定 s 步后值 $y=f(x)$ 由 M 获得。显然有（自然数）Q 使得

$$2(x+s)<Q,\ (4)\qquad l+1<Q,\ (5)\qquad Q \text{ pow } 2.\ (6)$$

(Q pow 2 表示 Q 为 2 的幂次。)考虑到 $0\leqslant r_{j,t}\leqslant x+t\leqslant x+s<\frac{Q}{2}<Q$，我们可用 Q 进表示的数 $r_{j,s}r_{j,s-1}\cdots r_{j,0}=\sum_{t=0}^{s}r_{j,t}Q^t$ 来展示各个计算时刻 Rj 的内容，现以 R_j 表示这样的数。

由于$0\leqslant l_{i,t}<2\leqslant Q$，我们又可用$L_i=\sum_{t=0}^{s}l_{i,t}Q^t$（$Q$进表示为$l_{i,s}l_{i,s-1}\cdots l_{i,0}$，其第$t$位（从右数从零计数）数字是$l_{i,t}$）来描述计算过程中指令$Li$的执行情况．此外，数$I=\sum_{t=0}^{s}Q^t$可用下式来刻画：

$$1+(Q-1)I=Q^{s+1}. \tag{7}$$

如果$Q=2^n$，$a_t=\sum_{i=0}^{n-1}a_{t,i}2^i\ (0\leqslant a_{t,i}<2)\ (t=0,\cdots,s)$，则$\sum_{t=0}^{s}a_tQ^t$（其$Q$进表示为$a_s\cdots a_t\cdots a_0$）等于$\sum_{t=0}^{s}\sum_{i=0}^{n-1}a_{t,i}2^{tn+i}$，其二进表示为

$$\underbrace{a_{s,n-1}\cdots a_{s,0}}_{a_s\text{的}(n\text{位})\text{二进表示}}\cdots\cdots\underbrace{a_{t,n-1}\cdots a_{t,0}}_{a_t\text{的}(n\text{位})\text{二进表示}}\cdots\cdots\underbrace{a_{0,n-1}\cdots a_{0,0}}_{a_0\text{的}(n\text{位})\text{二进表示}}.$$

正是由于这一事实，R_j的形如$\sum_{t=0}^{s}r_{t,t}Q^t\left(0\leqslant r_{j,t}<\frac{Q}{2}\right)$的表示可用条件

$$R_j\leqslant\left(\frac{Q}{2}-1\right)I\qquad(j=1,\cdots,r) \tag{8}$$

来刻画．$\left(\text{注意}\left(\frac{Q}{2}-1\right)I=\sum_{t=0}^{s}\left(\frac{Q}{2}-1\right)Q^t\text{，若 }Q=2^n\text{ 则}\frac{Q}{2}-1=2^{n-1}-1\text{ 的}(n\text{ 位})\text{二进表示为}\underbrace{01\cdots11}_{n-1\text{个}}.\right)$记录器的确定性以及$L_i$的形如$\sum_{t=0}^{s}l_{i,t}Q^t\ (0\leqslant l_{i,t}\leqslant1)$的表示可用条件

$$I=\sum_{i=1}^{l+1}L_i \tag{9}$$

和

$$L_i\leqslant I\ \ (i=1,\cdots,l+1) \tag{10}$$

来保证．事实上，条件(10)保证了$l_{i,t}$只取0，1值（注意$I=\sum_{t=0}^{s}Q^t$，1的(n位)二进表示为$\underbrace{0\cdots01}_{n-1\text{个}}$）；依条件(9)

$$\sum_{t=0}^{s}\left(\sum_{i=1}^{l+1}l_{i,t}\right)Q^t=\sum_{i=1}^{l+1}L_i=\sum_{t=0}^{s}Q^t,$$

由于$\sum_{i=1}^{l+1}l_{i,t}\leqslant l+1<Q$我们必有$\sum_{i=1}^{l+1}l_{i,t}=1$，这和条件(10)一起表明在每个计算时刻$t(\leqslant s)$恰有一条指令在被执行．

记录器一工作就执行指令$L1$(即$L1$在时刻0被执行，$l_{1,0}=1$)，这可用

$$1\leqslant L_1 \tag{11}$$

来描述．(注意使用前述的关于Q进制数二进表示的基本事实．)s步后停机可表述为

$$L_{l+1}=Q^s \tag{12}$$

$$(l_{l+1,s}=1,\ l_{l+1,s-1}=\cdots=l_{l+1,0}=0).$$

GOTO语句Li GOTO Lk可如下刻画：

$$QL_i\leqslant L_k. \tag{13}$$

为理解这一点请注意 $Q>l+1\geqslant 2$，$Q=2^n(n>1)$时$\sum_{t=0}^{s}l_{k,t}Q^t$和$Q\left(\sum_{t=0}^{s}l_{i,t}Q^t\right)$的二进表示分别为

$$l_{k,s}\underbrace{0\cdots0}_{n-1个}l_{k,s-1}\cdots\cdots\underbrace{0\cdots0}_{n-1个}l_{k,t+1}\cdots\cdots\underbrace{0\cdots0}_{n-1个}l_{k,1}\underbrace{0\cdots0}_{n-1个}l_{k,0},$$

$$l_{i,s}\underbrace{0\cdots0}_{n-1个}l_{i,s-1}0\cdots0l_{i,s-2}\cdots\cdots\underbrace{0\cdots0}_{n-1个}l_{i,t}\cdots\cdots\underbrace{0\cdots0}_{n-1个}l_{i,0}\underbrace{0\cdots00}_{n-1个}.$$

$Q\left(\sum_{t=0}^{s}l_{i,t}Q^t\right)\leqslant\sum_{t=0}^{s}l_{k,t}Q^t$ 意味着 $l_{i,s}=0$(在最后时刻 s 不执行非停机指令 Li)而且 $l_{i,t}=1\Rightarrow l_{k,t+1}=1$（若在时刻 t 执行 Li，在时刻 $t+1$ 就执行 Lk)。

条件转移指令 Li IF $Rj>0$ GOTO Lk 可如下描述（假定 $k\neq i+1$，$k=i+1$ 时指令 Li 相当于 GOTO $L(i+1)$从而不必使用条件转移指令)：

$$QL_i\leqslant L_k+L_{i+1}\quad 且\quad QL_i\leqslant L_k+QI-2R_j。\tag{14}$$

前一式保证执行完 Li 后将转至 Lk 或 $L(i+1)$。事实上由于 $k\neq i+1$，$l_{k,t}$ 与 $l_{i+1,t}$ 不同时为1，于是 $0\leqslant l_{k,t}+l_{i+1,t}\leqslant 1$ $(t=0,\cdots,s)$。类似于无条件 GOTO语句的处理情况，(14)的前一式意味着 $l_{i,s}=0$（在最后时刻 s 不执行非停机指令 Li）而且

$$l_{i,t}=1\Rightarrow l_{k,t+1}+l_{i+1,t+1}=1$$

（若在某时刻执行 Li，在下一时刻就执行 Lk 或 $L(i+1)$)。(14)的后一式用以决定究竟执行 Lk 还是 $L(i+1)$(依 Rj 内容是否大于0而定)。事实上，由于 $0\leqslant 2r_{j,t}<Q$，$I=\sum_{t=0}^{s}Q^t$，$Q=2^n(n>1)$时 QI 和 $2\left(\sum_{t=0}^{s}r_{j,t}Q^t\right)$的二进表示分别为

$$\underset{第n(s+1)二进位}{\uparrow}\qquad\underset{第n(t+1)二进位}{\uparrow}$$

$$10\cdots01\cdots\cdots0\cdots010\cdots01\cdots\cdots0\cdots010\cdots00,$$

$$\underbrace{*\cdots*0}_{2r_{j,s}的}\cdots\cdots\underbrace{*\cdots*0}_{2r_{j,t+1}的}\ \underbrace{*\cdots*0}_{2r_{j,t}的}\cdots\cdots\underbrace{*\cdots*0}_{2r_{j,1}的}\underbrace{*\cdots*0}_{2r_{j,0}的}.$$

(n位)二进表示 (n位)二进表示 (n位)二进表示 (n位)二进表示 (n位)二进表示

由此可看出，$QI-2\sum_{t=0}^{s}r_{j,t}Q^t$ 的第 $n(t+1)$二进位(从右数从零计数)数字为0当且仅当$r_{j,t}>0$。$Q\left(\sum_{t=0}^{s}l_{i,t}Q^t\right)\leqslant\sum_{t=0}^{s}l_{k,t}Q^t+QI-2\sum_{t=0}^{s}r_{j,t}Q^t$表明 $l_{i,t}=1$ 时 $S=QI-2\sum_{t=0}^{s}r_{j,t}Q^t$ 和 $\sum_{t=0}^{s}l_{k,t}Q^t$ 相加后的第 $n(t+1)$(二进)位数字为1。注意 $l_{i,t}=1$ 时 $l_{k,t}=0$。(若 $k=i$，则因 s 步后要停机故必 $r_{j,t}=0$，从而指令 Li 可换为无条件转移指令 GOTO $L(i+1)$。) 如果 S 的第 nt 位数字是0，则由于 $\sum_{t=0}^{s}l_{k,t}Q^t$ 的第 nt 位数字 $l_{k,t}$ 也是0，二进形式的 S 与 $\sum_{t=0}^{s}l_{k,t}Q^t$ 相加时在第 nt 位处不需向第 $nt+1$ 位进位；假若 S 的第 nt 位数字是1，则 $t>0$，$r_{j,t-1}=0$，从

而S的第$nt-1$位数字是0，而$\sum_{t=0}^{s}l_{k,t}Q^t$的第nt位数字是$l_{k,t}=0$，第$nt-1$位数字也是0，故二进表示的S与$\sum_{t=0}^{s}l_{k,t}Q^t$相加时在第$nt-1$位处不需向第nt位进位，在第nt位处不需向第$nt+1$位进位。正因为二进形式的S与$\sum_{t=0}^{s}l_{k,t}Q^t$相加时在第nt位处不需向第$nt+1$位进位，而且二进表示的$\sum_{t=0}^{s}l_{k,t}Q^t$的第$nt+1,nt+2,\cdots,nt+n-1$位数字都是0，二进形式的S与$\sum_{t=0}^{s}l_{k,t}Q^t$相加时在第$nt+n-1$位处不需向第$n(t+1)$位进位，从而$S+\sum_{t=0}^{s}l_{k,t}Q^t$的第$n(t+1)$二进位数字为1当且仅当$S$的第$n(t+1)$二进位数字与$l_{k,t+1}$一个为0、一个为1。因此(14)的后一式意味着$l_{i,t}=1$时

$$l_{k,t+1}=1\Longleftrightarrow S\text{的第}n(t+1)\text{二进位数字为}0\Longleftrightarrow r_{j,t}>0.$$

(执行Li时若Rj内容大于零下一步就执行Lk(否则依(14)的前一式将执行Lk和$L(i+1)$二者中的另一个——$L(i+1)$。)

顺便指出，对于下形的指令Li IF $Rj=0$ GOTO $Lk(k\neq i+1)$(Rj内容大于零时执行下一条指令$L(i+1)$，否则执行Lk)，(类似于非零条件转移指令的情形)我们可用下式来描述(注意把(14)中的L_k与L_{i+1}换位)：

$$QL_i\leqslant L_{i+1}+L_k\quad\text{且}\quad QL_i\leqslant L_{i+1}+QI-2R_j.$$

形如Li $Rj\leftarrow Rj\pm1$的指令执行完后应执行下一条指令，故它与

$$QL_i\leqslant L_{i+1}\tag{15}$$

(GOTO $L(i+1)$)相对应(Rj的内容依指令增1或减1)。

我们还需要记录方程以保证每个记录单元Rj在时刻t的内容等于相应数R_j的第t个Q进位数字。

$$R_j+\begin{cases}yQ^{s+1} & \text{若 } j=1\\ 0 & \text{若 } j>1\end{cases}=QR_j+\sum_k QL_k-\sum_i QL_i+\begin{cases}x\text{若}j=1\\ 0\text{若}j>1\end{cases}\quad(j=1,2,\cdots,r).\tag{16}$$

其中求和号$\sum_k$过所有Lk为$Rj\leftarrow Rj+1$的那些k，$\sum_i$过所有Li为$Rj\leftarrow Rj-1$的那些i。$R1$的记录方程与其它的有所不同，因为(对于一元函数)$R1$是输入-输出单元。在时刻$t=0$，$R1$的内容为x；而在时刻s其记录内容为$y=f(x)$。在这两个时刻其余记录单元内容为零。

现在不难看出，$y=f(x)$当且仅当存在(自然数)$s,Q,I,R_1,\cdots,R_r,L_1,\cdots,L_{l+1}$使得(4)—(16)成立。利用指数关系和遮掩关系$\leqslant$的$D$性，我们又可进一步找到(整系数)多项式$P$使得

$$y=f(x)\Longleftrightarrow\exists x_1\cdots\exists x_n[P(y,x,x_1,\cdots,x_n)=0].$$

任给非空的m元r.e.关系A，(依递归论的知识)集合$\{\langle a_1,\cdots,a_m\rangle:A(a_1,\cdots,a_m)\text{成立}\}$为r.e.集，从而是某个一元递归函数$f$的值域，于是

$$A(a_1,\cdots,a_m)\Longleftrightarrow\exists x(f(x)=\langle a_1,\cdots,a_m\rangle),$$

这儿$\langle a_1,\cdots,a_m\rangle = pg(\cdots(pg(pg(a_1,a_2),a_3)\cdots,a_m)$为有穷序列$a_1,\cdots,a_m$的编码. 其中配对合函数$pg(x,y)=(x+y)^2+x$,相应的配对左、右函数为$Kx=x\dot{-}[\sqrt{x}]^2$,$Lx=\lfloor\sqrt{x}\rfloor\dot{-}Kx$(参看[24]). 考虑到$f$是记录器完全可计算的,而且$\langle a_1,\cdots,a_m\rangle$是$a_1,\cdots,a_m$的多项式,必存在多项式$P$使得

$$A(a_1,\cdots,a_m)\Longleftrightarrow\exists x(f(x)=\langle a_1,\cdots,a_m\rangle)$$
$$\Longleftrightarrow\exists x\exists x_1\cdots\exists x_n[P(a_1,\cdots,a_m,x,x_1,\cdots,x_n)=0].$$

对于m元的空关系A,$A(a_1,\cdots,a_m)$恒不成立,于是

$$A(a_1,\cdots,a_m)\Longleftrightarrow\exists x(a_1^2+\cdots+a_m^2+x^2+1=0).$$

综上,定理1获证.

不可判定性是个否定性结果,但Hilbert第十问题的解决也有不少正面的推论. 下面我们给出一个比较奇特的函数表示定理(参见[22]).

定理2 设f为一元递归函数,则有整系数多项式Q使得对任何(自然数)x,y都成立

$$f(x)=y\Longleftrightarrow\exists x_0,\cdots,x_n[Q(x,x_0,\cdots,x_n)=y].$$

证 设多项式P D-定义了r.e.关系"$f(x)=y$",我们有

$$f(x)=y\Longleftrightarrow\exists x_1,\cdots,x_n[P(x,y,x_1,\cdots,x_n)=0]$$
$$\Longleftrightarrow\exists x_0,x_1,\cdots,x_n[1-P^2(x,x_0,x_1,\cdots,x_n)>0\wedge x_0=y]$$
$$\Longleftrightarrow\exists x_0,x_1,\cdots,x_n[(x_0+1)(1-P^2(P^2(x,x_0,x_1,\cdots,x_n))=y+1]$$
$$\Longleftrightarrow\exists x_0,x_1,\cdots,x_n[Q(x,x_0,x_1,\cdots,x_n)=y],$$

这儿$Q(x,x_0,x_1,\cdots,x_n)=(x_0+1)(1-P^2(x,x_0,x_1,\cdots,x_n))-1$是整系数多项式.

定理2告诉我们,从某种意义上说任何一元递归函数都相当于一个多项式.

2 9未知数定理

我们知道,全体一元部分递归函数可能行地枚举出来:$\varphi_0,\varphi_1,\varphi_2,\cdots$. 令$W_i=\mathrm{Dom}\,\varphi_i$(即$W_i$为$\varphi_i$的定义域),则$W_0,W_1,W_2,\cdots$给出了全体r.e.集,特别地非递归的$K=\{x:\varphi_x(x)$有定义$\}$也在其中.

依定理1存在多项式P使得

$$x\in K\Longleftrightarrow\exists x_1,\cdots,x_\nu[P(x,x_1,\cdots,x_\nu)=0].$$

考虑到K的非递归性,我们知道有ν使得不存在可判定ν个未知数的(整系数)多项式不定方程是否有(自然数)解的算法. 1970年夏天在一次国际会议上Matijasevič宣布说ν可小于200,不久J.Robinson指出ν可取为35,之后两人合作把ν值降到24,1971年底ν被降为14,1973年他们又把ν值降到13(参看[30]).

1975年Matijasevič[33]进一步宣称ν可取为9(注意$\nu=1$是不可能的),其出发点仍是[30]中的编码思想. 然而文[33]相当简略,连证明的完整提纲都没有. 1982年Jones发表了文[11],第一次给出9未知数定理艰深而完整的证明.

定理3 (9未知数定理) 不存在可判定9个未知数的(整系数)多项式不定方程是否有自然数解的算法.

在9未知数定理的证明中,下述几个引理是比较关键的.

引理5[11] 设 b pow 2，多项式 $P(z_0,\cdots,z_\nu)$ 的次数 $\delta\geqslant 4$，且 $P(x,0,\cdots,0)$ 恒大于 0，则

$$\exists z_0,\cdots,z_\nu[z_0<b\wedge\cdots\wedge z_\nu<b\wedge P(z_0,\cdots,z_\nu)=0\wedge z_0=x] \tag{17}$$

成立当且仅当存在正整数 g 使得

$$x<b,\ g<2bB^{(\delta+1)^\nu},\ \tau_2(g,M)=0,\ \tau_2(2E_0,(B-2)B^{(\delta+1)^{\nu+1}})=0.$$

设整数 $P_{i_0,\cdots,i_\nu}$ 由

$$\delta!P(z_0,z_1,\cdots,z_\nu)=\sum_{i_0+\cdots+i_\nu\leqslant\delta}\frac{\delta!}{i_0!\cdots i_\nu!(\delta-i_0-\cdots-i_\nu)!}P_{i_0,\cdots,i_\nu}z_0^{i_0}\cdots z_\nu^{i_\nu} \tag{18}$$

所确定，上述的 B,M,E_0 如下给出：

$$B=\beta b^\delta, \tag{19}$$

β 满足 β pow 2 和 $\beta>2(\nu+2)^\delta\max\limits_{i_0+\cdots+i_\nu\leqslant\delta}|P_{i_0,\cdots,i_\nu}|$；

$$M=\sum_{j=0}^{(\delta+1)^\nu}m_jB^j, \tag{20}$$

这儿

$$m_j=\begin{cases}B-b & \text{若}j\in\{\delta+1,(\delta+1)^2,\cdots,(\delta+1)^\nu\},\\ B-1 & \text{此外；}\end{cases}$$

$$E_0=c^\delta\sum_{i_0+\cdots+i_\nu\leqslant\delta}P_{i_0,\cdots,i_\nu}B^{(\delta+1)^{\nu+1}-i_0-i_1(\delta+1)-\cdots-i_\nu(\delta+1)^\nu}+\sum_{i=0}^{(2\delta+1)(\delta+1)^\nu}\frac{B}{2}B^i, \tag{21}$$

此处 $c=1+xB+g$。记号 $\tau_2(S,T)$ 表示二进制形式的 S,T 相加时需向前进位的位的个数（显然 a 的二进表示中 1 的个数 $\sigma(a)=\tau_2(a,a)$。）

我们指出，E_0 表达式中的 c 实际上就是 $1+\sum\limits_{i=0}^{\nu}z_iB^{(\delta+1)^i}$ $(0\leqslant z_i<b)$。

引理6[11] 设 N pow 2，$0\leqslant S,T<N$，$R=S(N^2-N)+(T+1)(N^2-1)$，则

$$\tau_2(S,T)=0\Longleftrightarrow N^2\left|\binom{2R}{R}\right.$$

引理7（[11]中的引理 2.25） 假定 $R\geqslant 8$，$N\geqslant 8$，$R\geqslant b$，$N\geqslant b>0$，则

$$N^2\left|\binom{2R}{R}\right.\ \text{且}\ \ b\ \text{pow}\ 2,$$

当且仅当存在正整数 h,s,w,ϕ 使得

$$(P^2-1)K^2+1\in\square,\ \left(\frac{C}{K}-Y\right)^2<\frac{1}{4},$$

$$C=Y_A(B),\ 3WC\equiv 2(W^2-1)\pmod{4A-5},$$

这儿

$$W=bw,\ Y=N^2s,\ A=RY(N^2w+1),\ B=2R+1,$$
$$C=2R+1+\phi,\ P=2R^2Y^2N^2w,\ K=R+1+h(P-1).$$

引理8[11,30] 设 $A>1$，$1<B\leqslant C$，$2B\leqslant C$ 或 $2\nmid B$，则 $C=Y_A(B)$ 成立当且仅当有正整

数 i, j 使得

$$DFI\in\square \quad 且 \quad F\mid H-C,$$

其中 $$D=(A^2-1)C^2+1,\ E=iJDC^2\ (J\text{为任一正整数}),$$

$$F=(A^2-1)E^2+1,\ G=A+F(CD+1-A),$$

$$H=B+jC,\ I=(G^2-1)H^2+1.$$

我们知道 $Y_A(0)=0$, $Y_A(1)=1$, $Y_A(n+2)=2AY_A(n+1)-Y_A(n)$。令

$$\psi_A(0)=0,\ \psi_A(1)=1,\ \psi_A(n+2)=A\psi_A(n+1)-\psi_A(n)\ (n=0,1,2,\cdots),$$

则 $Y_A(n)=\psi_{2A}(n)$。关于 $C=\psi_A(B)$ 的 D-表示，读者可参看[34]（作者在[34]中还考虑了整变元情形）。

引理9[30]（关系组合定理） 任给自然数 k，必存在(整系数)多项式 M_k 使得对任何整数 $A_1,\cdots,A_k$, $B(\neq 0)$, C, D 条件

$$A_1\in\square,\cdots,A_k\in\square,\ B\mid C,\ D>0$$

全成立当且仅当有自然数 n 满足

$$M_k(A_1,\cdots,A_k;B,C,D,n)=0.$$

事实上 M_k 可如下给出：

$$M_k(A_1,\cdots,A_k,B,C,D,n)$$

$$=\prod(B^2n+C^2-B^2(2D-1)(C^2+W^k\pm\sqrt{A_1}\pm\sqrt{A_2}W\pm\cdots\pm\sqrt{A_k}W^{k-1})),$$

其中 $W=1+\sum_{i=1}^{k}A_i^2$，求积号$\prod$过所有可能的正负号配置。

Jones[11] 首次成功地揭示出9未知数定理证明的全部技术性细节，对此 Matijasević 在为 MR 做评论时给予了高度的评价。

对于整变元情形，S.P.Tung[35] 证明了不存在可判定含27个未知数的多项式不定方程是否有整数解的算法，最近孙智伟成功地把27换成了11(参看[34]、[36])。

3 通用不定方程

设 $W_0,W_1,\cdots$ 是全体 r.e. 集的能行枚举（依递归论的知识这样的枚举是存在的），于是关系 $x\in W_n$ 为 r.e. 关系，依定理1存在整系数多项式 U 使得

$$x\in W_n\Longleftrightarrow\exists x_1,\cdots,x_\nu[U(x,n,x_1,\cdots,x_\nu)=0].$$

考虑到 $W_0,W_1,\cdots$ 恰好给出了全体 r.e. 集，方程

$$U(x,n,x_1,\cdots,x_\nu)=0 \tag{22}$$

称为通用不定方程(x,n 作为参数)。如果通用方程(22)以 $x_1,\cdots,x_\nu$ 为未知数而其次数为 δ，我们就说 (ν,δ) 为通用对。

如上所言，通用不定方程是存在的。如何着手去构造它呢？1971年 N.K.Kosovskiĭ[37] 给出了第一个通用方程，但它的写出依赖于一个明确的通用对 (ν,δ)，而那时还不知道任何具体的通用对。

Jones 最初研究通用方程是基于字问题的，而这常常导致要占据数页纸的不定方程。1975 年 Jones[6] 成功地构造出了仅占十行的通用方程，其出发点是 J.Robinson 所发现的枚举(多项式)不定方程的办法，构造过程中还使用了改进的有界量词定理和如下的引理10。

引理10[5,30] (指数级引理) 设 $J\geqslant 2$，则

$$J^3(J+2)(r+1)^2+1\in\square\Longrightarrow r\geqslant J^{J^{J^2}}+J-1.$$

反过来，任给正整数 J 和 m，必有(自然数) r 满足

$$^{m}(J+2)(r+1)^2+1\in\square \quad 且 \quad m\mid r+1.$$

1982年Jones[11] 又有所突破，他仅用寥寥七行写出了一个通用不定方程，还证明了如下的

定理4 下列有序对(未知数个数，次数)是通用对：

$(9,1.6\times10^{45})$, $(10,8.6\times10^{44})$, $(11,4.6\times10^{44})$, $(12,1.3\times10^{44})$,
$(13,6.6\times10^{43})$, $(14,2.0\times10^{5})$, $(19,2668)$, $(21,96)$,
$(24,36)$, $(25,28)$, $(26,24)$, $(28,20)$,
$(29,16)$, $(32,12)$, $(38,8)$, $(58,4)$.

[注意通用对(ν,δ)中的δ可为 4 (如$\nu=58,\delta=4$)，ν可为 9 (如$\nu=9,\delta=1.6\times10^{45}$)。]

如果不用(ν,δ)来作为复杂性度量而考虑算术操作(加减法和乘法)的次数 o，那么依 Jones[11] 通用方程的 o 可取为100。([11]中的定理 5 给出了这个结果的证明论形式。)

4 不定方程前缀量词分类

为方便起见，我们采用一些简单的记号，例如$\forall\ \forall\ \exists$(或$\forall^2\exists$)表示所有形如

$$\forall x_1\forall x_2\exists x_3[P(x_1,x_2,x_3)=0]\quad (P\text{为整系数多项式})$$

的公式所构成的类。根据定理 1 我们知道对足够大的 n 值，$\exists^n$(即$\underbrace{\exists\cdots\exists}_{n\text{个}}$)不可判定。9 未未知数定理表明 $\exists^9$ 不可判定。由于

$$\forall x_1\cdots\forall x_9\exists y[P^2(x_1,\cdots,x_9)=1+y]$$
$$\Longleftrightarrow\ \neg\ \exists x_1\cdots\exists x_9[P(x_1,\cdots,x_9)=0],$$

$\forall^9\exists$也不可判定。

关于(多项式)不定方程前缀量词分类，Matijasevič[38] 作了最初的尝试，他证明了$\exists^3\forall\exists$, $\exists^2\forall\exists^2$, $\exists\forall\exists^3$, $\exists^2\forall^2\exists$, $\exists\forall\exists\forall\exists$, $\exists\forall^2\exists^2$和$\exists\forall^3\exists$都是不可判定的。1972 年他又证明了$\exists\forall\exists^2$不可判定(参看[39])。1974年 Matijasevič 和Robinson 合作证明了$\exists^2\forall\exists$的不可解性，1975年他俩合作的重要论文[30]又蕴涵了$\forall^2\exists^2$不可判定。1981年 Jones[9] 进一步证明了

定理5 $\forall\exists$可判定；$\exists\forall^2\exists$, $\forall\exists^3$和$\forall\exists\forall\exists$不可判定。

值得指出，Jones在证明$\forall\exists$可判定时利用了Th.Skolem的一条代数定理。

Jones[11] 对(多项式)不定方程前缀量词作了细致而完整的分类，现列出如下：

(Ⅰ)$\forall$受限的情形

可判定：$\exists$, $\forall$；

不可判定：$\exists\forall\exists^2, \exists^2\forall\exists, \exists\forall^2\exists, \exists^9$；

尚未解决：$\exists\forall\exists, \exists^2, \exists^3, \exists^4, \exists^5, \exists^6, \exists^7, \exists^8$。

(Ⅱ)$\forall$不受限的情形

可判定：$\exists, \forall, \forall\exists$；

不可判定：$\exists\forall\exists^2, \exists^2\forall\exists, \exists\forall^2\exists, \exists^9, \forall^9\exists, \forall^2\exists^2, \forall\exists\forall\exists, \forall\exists^3$；

尚未解决：$\exists\forall\exists, \exists^2, \exists^3, \exists^4, \exists^5, \exists^6, \exists^7, \exists^8, \forall\exists^2, \forall^2\exists, \forall^3\exists, \forall^4\exists, \forall^5\exists, \forall^6\exists, \forall^7\exists, \forall^8\exists$。

1986年Jones与H.Levitz和A.J.Wilkie合作对以2为底的指数不定方程(等号两边都是由自然数和变元通过加、乘以及2的幂次运算而得)前缀量词也作了完整的分类，他们的结果如下(参看[17])：

A $\forall$受限的情形

可判定：$\forall, \forall^2, \forall^3, \exists, \exists\forall, \exists\forall^2, \forall\exists, \forall^2\exists, \forall\exists\forall$；

不可判定：$\exists^3, \exists\forall\exists$；

尚未解决：$\exists^2$。

B $\forall$不受限的情形

可判定：$\forall, \forall^2, \forall^3, \exists, \exists\forall, \exists\forall^2$；

不可判定：$\exists^3, \exists\forall\exists, \forall^2\exists, \forall\exists^2$；

尚未解决：$\exists^2, \forall\exists$。

前缀量词分类中的不可判定性结果都是通过证明每个r.e.集均可表成相应形状而获得的。文献[6]、[14]、[39]给出了不少一般r.e.集的算术表示。

关于整变元情形的(多项式)不定方程前缀量词分类，S.P.Tung在[40]中已做了些工作，例如他证明了$\forall^n\exists$是co-NP完全的(从而是可判定的)；孙智伟最近已基本完成这方面的研究，例如他证明了$\exists^{11}, \forall^{10}\exists^2, \forall^9\exists^3, \forall\exists^6, \forall^2\exists^4, \forall^2\exists\forall^2\exists^2, \forall\exists\forall\exists^3, \forall\exists\forall^3\exists^2, \exists\forall^5\exists^2, \exists^2\forall^3\exists^2, \exists^2\forall\exists^3$($\forall$也可受限)，$\exists\forall^4\exists^2$($\forall$受限)$\exists^2\forall^2\exists^2$($\forall$受限)，$\exists\forall\exists^4$($\forall$也可受限)，$\exists\forall\exists\forall\exists^2$($\forall$受限)都是不可判定的(over $\mathbf{Z}$)。

5 Diophantine表示

定理1表明每个r.e.集都是D-集，每个r.e.关系(特别地递归关系)都有其D-表示。但要明确地并且尽可能简单地给出一些有趣的r.e.关系的D-表示却不是一件容易的事，这里不仅需要细致、耐心，还需要高超的技巧和深邃的洞察。在一些具体关系、集合的D-表示方面，Jones教授的工作在国际上是首屈一指的。

1976年Jones与D.Sato,H.Wada和D.Wiens合作证明了素数集等同于一个有26个(自然数)变元的25次多项式的正值集合，这个在[5]中仅占五行的素数表示多项式还可用一个有12个变元的多项式来代替(次数相对来说就变大了，由25升为13697)。1977年Matijasevič[41]进一步指出素数表示多项式可仅有10个变元(次数为15905)，Jones在对[41]作翻译时又把次数从15905降到11281。数论中的Wolstenholme定理断言$p>3$为素数时

$$\binom{2p-1}{p}\equiv 1 \pmod{p^3} \text{亦即} \binom{2p}{p}\equiv 2 \pmod{2p^3},$$

Jones 教授猜想它的逆命题也是正确的(参看[Guy[42]]). 在Jones猜想之下，孙智伟[43,44]证明了仅用7个(自然数)未知量就可给出素数集的 Diophantine 表示，从而素数集是某个8元(整系数)多项式的非负值域(变元取值自然数). [请读者注意，数论中已经证明不存在整系数多项式 P 使得 P 的值域恰为素数集(P 中变元取值自然数或整数).]

众所周知，1970年Matijasevič通过证明 $y = F_{2x}$ 为 D-关系来最终否定解决 Hilbert 第十问题. 1975年Jones[3]证明了 Fibonacci 数恰与多项式

$$-x^4y - 2x^3y^2 + x^2y^3 + 2xy^4 - y^5 + 2y$$

的非负值相吻合(变元 x,y 取值自然数)而且Fibonacci 数集F不可能恰好是某个多项式的值域. 1988年Jones[21]又进一步证明了

定理6 (i)Fibonacci 数集F是单重 D-可定义的，事实上有四次(整系数)多项式 $P(x,y)$ 使得

$$y\in \mathbf{F}\Longleftrightarrow \exists\, !\, x[P(x,y)=0].$$

(ii)F恰为下列多项式 $Q(x,y)$ 的非负值集：

$$Q(x,y) = -x^6 - 5x^5y - 7y^4y^2 + x^3y^2 + 7x^2y^4 + xy^5 - 2y^6 + x^2 + 3xy + 2y^2 + x + 2y.$$

不仅如此，任给Fibonacci数 F_n 恰有唯一的 x,y 使得 $Q(x,y)=F_n$，这样的 x,y 又都是 Fibonacci 数.

定理的前一部分告诉我们F是一元单重 D-可定义的，后一部分则表明F有二元单重自身 D-表示. Jones[21]问 F 有无一元单重自身 D-表示，即是否有多项式 R 使得

$$a\in \mathbf{F}\Longleftrightarrow \exists\, x[R(a,x)=0],$$

并且 $a\in$ F 时所存在的 x 是唯一的而且是个 Fibonacci 数？这个问题迄今尚未解决，但孙智伟最近指出(参见[45])对于 $m=0,2,3,4,\cdots$ 集合

$$U_m=\{u_n^{(m)}:\ n=0,1,\cdots\}\qquad (u_0^{(m)}=0,u_1^{(m)}=1,u_{n+2}^{(m)}=mu_{n+1}^{(m)}+u_n^{(m)})$$

都有一元单重自身 D-表示(注意 $\mathbf{F}=U_1$.)

Fibonacci数列 $\{F_n\}$ 的对偶是所谓的Lucas序列 $\{L_n\}$ ($L_0=2,L_1=1,L_{n+2}=L_{n+1}+L_n$)，在[4]中Jones仔细研究了 Lucas 数的 D-表示.

在指数关系的 D-表示方面，Jones[7]实现了 J.Robinson 的一个想法，给出了仅用5个(自然数)未知量来 D-定义指数关系的新办法.(孙智伟的文[43]中也有类似的方法.)在[7]中Jones明确写出了Fermat 素数(形如 $2^{2^n}+1$ 的素数)、Mersenne 素数(2^p-1 形素数)以及偶完全数(满足 $\sum_{d\mid n}1=2n$ 的数 n 叫完全数)的表示多项式. 孙智伟[44]仅用7个未知数就分别给出了 $Y=\binom{PX}{QX}$ ($P>Q>0$ 为常数)、X pow 2和 $Z=C_X$(Z 为第 X 个Catalan数 $\frac{1}{X+1}\binom{2X}{X}$) 的Diophantine表示.

著名的Fermat大定理断言对任何(自然数) $n>3$ 方程

$$x^n+y^n=z^n$$

无正整数解. 在[46]中孙智伟构造了一个 220 次的整系数多项式 $P(n,a,b,c,w,x,y,z,m)$，

Fermat大定理对奇指数$n>3$不真当且仅当存在(任意大的)正整数a,b,c,w,x,y,z,m使得

$$P(n-2,a,b,c,w,x,y,z,m)=0.$$

顺便指出，Fermat大定理与Fibonacci数列有意想不到的联系(参看孙智宏、孙智伟的文[47])。

6 Hilbert第十问题的应用

Hilbert第十问题的否定解决带来了不少重要的副产品，以下就其应用给出数例。

Kalmar初等函数类是从本原函数(零函数、后继函数、射影函数)和$x+y$,$x\dot{-}y$($x\geqslant y$时$x\dot{-}y=x-y$，$x<y$时$x\dot{-}y=0$)出发利用迭置与有界和$\left(\sum_{i<n}\right)$、有界积$\left(\prod_{i<n}\right)$所作出的最小函数类，它与Grzegorczyk[48]的ε^3吻合一致。根据孙智伟[49]的文章，它也是包含本原函数、$ct(x|y)$(x整除y的特征函数)、$\max(x,y)$和2^x且对迭置与有界μ算子$rti\ (\text{即}\mu_{i<n})$封闭的最小函数类。以下用K与KF分别表示Kalmar初等关系(特征函数为Kalmar函数的关系)类和Kalmar初等函数类。

1953年Grzegorczyk[48]提出能否找到KF的有穷基底。(函数类的基底是这个类的一个子类，由其中的函数和本原函数通过迭置可产生出这个类中的一切函数。)1964年D.Rödding[50]成功地确立了KF有穷基底的存在性，1980年S.S.Marchenkov[51]利用关于Hilbert第十问题的结果给出了K和KF的比较简单的有穷基底。(K的基底指由K中关系的特征函数所构成的函数类的基底。)1982年Jones和Matijasević[14]改进了Marchenkov的结果，证明了$\{x+y,x\dot{-}y,\lfloor x/y\rfloor,\lfloor\sqrt{x}\rfloor,2^x\}$是$K$的有穷基底。最近Jones[10]进一步证明了

定理7 函数$x+y,x\dot{-}y,\lfloor x/y\rfloor,2^x$组成Kalmar初等关系类$K$的基底；函数$x+y,\lfloor x/y\rfloor,2^x,\varphi(x,y)$构成Kalmar初等函数类$KF$的基底，其中$\varphi(x,y)$指$y$写成$x$进制时从右数首次出现数字0的位数(为使$\varphi$为全函数，$\varphi(0,y)$和$\varphi(1,y)$都定义成0)。

以上考虑的是Kalmar函数类与Kalmar关系类，下面再来考虑Turing机多项式时间内可计算函数类PF与非确定型Turing机多项式时间内可计算函数类NPF。

首先要注意，第1节中描述的记录器不可能在多项式时间$P(|x|)$(P为多项式，$|x|=\lceil\log_2(x+1)\rceil$为$x$的二进长度)之内(即运行步数$s\leqslant P(|x|)$)进行加、乘法。为获得多项式时间等价于Turing机器的记录器，我们只需再允许两种新指令(参见[16])：

$$Ln\quad Ri\leftarrow Ri+Rj,$$
$$Lp\quad Rj\leftarrow\lceil Rj/2\rceil.$$

关于它们的合用性及算术化(指数D-方程的刻画)，读者可参看[16]。

对于复杂性类NP，Adleman和Manders[52,53]首次获得了NP的有界Diophantine特征。根据Karp等人的工作我们只需在上面给出的记录器基础上增添如下不确定指令

$$Ln\quad \text{BRANCH}(Li,Lj)\qquad(\text{转移到}Li\text{或者}Lj),$$

就可得到不确定记录器，它是多项式时间等价于非确定型Turing机的。(依第1节，上一条指令可用$QL_n\leqslant L_i+L_j$来刻画。)1984年Jones和Matijasević[16]证明了集A属于NP当且仅当A可表成下形：

$$x\in A\Longleftrightarrow\exists x_0,\cdots,x_n[|x_0|\leqslant P(|x|)\wedge\cdots\wedge|x_n|\leqslant P(|x|)\wedge F(x,x_0,\cdots,x_n)=G(x,x_0,\cdots,x_n)],$$

其中 P 为多项式，$F(x,x_0,\cdots,x_n)$和$G(x,x_0,\cdots,x_n)$由$x,x_0,\cdots,x_n$经加、乘、“且”而得.

通常的P类、NP类都是针对关系(谓词、集合)而言的，若针对函数来讲我们就有复杂性类PF、NPF.(注意P与PF不同，例如函数2^x不属于PF，但关系$y=2^x$属于P.)大家可能认为$PF=NPF$仅仅是$P=NP$的重新表述，如果确实如此那就应有$P=NP\Longleftrightarrow P=NP\cap\text{co-}NP$，因为Jones[18]证明了$PF=NPF$当且仅当$P=NP\cap\text{co-}NP$.在[22]中Jones和Matijasević注意到Hilbert第十问题在有界算术中的否定解决将意味着$NP=\text{co-}NP$.

函数类PF是有有穷基底的，这在1970年就被A.A.Muchinik所证明.1988年Jones和Matijasević[20]明确地构造了一个二元函数$H(x,y)$，使得仅由它就可组成PF的基底.函数类NPF介于PF与KF之间，确切地$PF\subseteq NPF\subseteq KF$(参看[20])，但$NPF$是否有有穷基底在目前还是个未解决问题.

关于Diophantine复杂性的其它结果，读者可参考[54]、[55]、[56].

下面我们提一下Hilbert第十问题在双人游戏方面的应用.在这儿所涉及的游戏中甲乙两人轮流选取自然数$x_1,x_2,\cdots$.游戏形式如下：甲选定x_1，乙选定x_2，甲选定$x_3,\cdots$，乙选定x_l(若l为奇数则甲选定x_l).选定x_l的一方获胜当且仅当$f(x_1,\cdots,x_l)=0$，这儿f是个预先给出的数论函数.

von Neumann和Zermelo的一条定理表明在上述类型游戏中总有一方具有取胜策略，然而这样的取胜策略未必是能行可计算的(亦即其选择函数未必是递归的).1957年M.O.-Rabin[57]证明了存在三元递归函数f使得在上述游戏中甲乙双方均无可计算的取胜策略.1982年Jones[12]利用不定方程前缀量词分类方面的结果(参看[9])证明了存在整系数多项式$f(x_1,\cdots,x_6)$使得在相应的游戏中任何一方均无可计算的取胜策略.最近Jones[23]指出对于多项式

$$f(x_1,x_2,x_3,x_4)=x_1x_3x_4+x_3x_4^2-x_3^2x_4-x_1x_2-x_2x_4+x_2x_3$$

在相应的游戏(这次变元x_i取值正整数)中甲乙双方都无多项式时间内可计算的取胜策略.

后记

Hilbert第十问题及其相关课题上的研究成果很多，限于篇幅本文不可能面面俱到.为补此不足，建议有兴趣的读者参看文献[58]—[76].

致谢 本文是受莫绍揆教授和吕义忠副教授的委托而写的，他们给予作者极大的指导、鼓励并提供了许多重要的资料.Jones教授本人也给作者寄来了宝贵的第一手资料，在此一并致谢.

参考文献

1 Jones J P. Recursive undecidability——an exposition. *Amer. Math. Monthly*, 1974, 81: 724—738. MR 50#9568.

2 Jones J P. A formula for the nth prime number. *Canad. Math. Bull.*, 1975, 18: 433—434.

3 Jones J P. Diophantine representation of the Fibonacci numbers. *Fibonacci Quart.*, 1975,

13: 84—88. MR 52#3035.

4 Jones J P. Diophantine representation of the Lucas numbers. *Fibonacci Quart.*, 1976, 14: 134. MR 53#2818.

5 Jones J P, Sato D, Wada H and Wiens D. Diophantine representation of the set of prime numbers. *Amer. Math. Monthly*, 1976, 83: 449—464. MR 54#2615.

6 Jones J P. Three universal representations of recursively enumerable sets. *J. Symbolic Logic*, 1978, 43: 335—351. MR 58#16226.

7 Jones J P. Diophantine representation of Mersenne and Fermat primes. *Acta Arith.*, 1979, 35: 209—221. MR 81a:10020.

8 Jones J P. Undecidable diophantine equations. *Bull. Amer. Math. Soc.*, 1980, 3: 859—862. MR 81k:10094.

9 Jones J P. Classification of quantifier prefixes over Diophantine equations. *Z. Math. Logik Grundlag. Math.*, 1981, 27: 403—410. MR 83a:03037.

10 Jones J P. Huber-Dyson V and Shepherdson J C. Some Diophantine forms of Gödel's theorem. *Arch. Math. Logik Grundlag.*, 1982, 22: 51—60. MR 83k:03073.

11 Jones J P. Universal Diophantine equation. *J. Symbolic Logic*, 1982, 47: 543—571. MR 84e:10070.

12 Jones J P. Some undecidable determined games. *Internatl. J. Game Theory*, 1982, 11: 63—70. MR 84b:90107.

13 Jones J P and Matijasevič Ju V. A new representation for the symmetric binomial coefficient and its applications. *Ann. Sci. Math. Québec*, 1982, 6: 81—97, 223. MR 84g:03060.

14 Jones J P and Matijasevič Ju V. Exponential Diophantine representation of recursively enumerable sets. *Proc. of the Herbrand sympos.* (Marseilles, 1981), 159—177, Stud. Logic Foundations Math., 107, North-Holland, Amsterdam-New York, 1982. MR 85i:03138.

15 Jones J P and Matijasevič Ju V. Direct translation of register machines into exponential Diophantine equations, in: Lutz Priese (Ed.). Fachbereich Mathematik-Informatik, Univ. Gesamthochschule, Paderborn, Germany, 1983, 117—130.

16 Jones J P and Matijasevič Ju V. Register machine proof of the theorem on exponential Diophantine representation of enumerable sets. *J. Symbolic Logic*, 1984, 49: 818—829. MR 85i:03139.

17 Jones J P, Levitz H and Wilkie A J. Classification of quantifier prefixes over exponential Diophantine equations. *Z. Math. Logik Grundlag. Math.*, 1986, 32: 399—406. MR 88d:03064.

18 Jones J P. Elementary properties of the class of nondeterministic polynomial time computable functions. Proc. of the Semester on Mathematical Problems in Computation Theory(1985), Banach Centre Publications, Polish Academy of Sciences, Warszawa, 1988, 21: 277—283.

19 Jones J P. Basis for the Kalmar elementary functions, in: R. A. Mollin(Ed.). Number Theory and Applications, Kluwer Acad. Pub., Dordrecht, Netherlands, 1989, 435—444.

20 Jones J P and Matijasevič Ju V. Basis for the polynomial time computable functions, Proc. of the 1st Conference of the Canadian Number Theory Association (Banff, 1988), de Gruyter, Berlin, 1990, 255—270. MR93d: 03046.

21 Jones J P. Diophantine representation of Fibonacci numbers over natural numbers. Proc. of the 3rd International Conference on Fibonacci Numbers and Their

Applications (Pisa, 1988), Kluwer Academic Publishers, Dordrecht, Netherlands, 1988, 197—201. MR 92f: 11027

22 Jones J P and Matijasevič Ju V. Proof of recursive unsolvability of Hilbert's tenth problem. Amer.Math.Monthly., 1991,98(8): 689—709,MR2i: 03050.

23 Jones J P. Computational complexity of computing winning strategies in polynomial games. 南京大学学报数学半年刊, 1991, 8 (1): 1—5. MR 93a:03039.

24 莫绍揆，递归论。科学出版社，北京，1987.

25 莫绍揆。从Hilbert第十问题谈起——介绍数理逻辑的两个有名结果。数理化信息(2)，辽宁教育出版社，1986.

26 胡久稔。希尔伯特第十问题。辽宁教育出版社，沈阳，1987.

27 Davis M, Putnam H and Robinson J. The decision problem for exponential diophantine equations. *Ann. of Math.*, 1961, 74(2): 425—436. MR 24#A3061.

28 Matijasevič Ju V. Enumerable sets are diophantine. Dokl. *Akad. Nauk SSSR*, 1970, 191: 279—282; English translation with addendum, *Soviet Math.*; Doklady, 1970, 11: 354—357. MR 41#3390.

29 Davis M. Hilberts's tenth problem is unsolvable. *Amer. Math. Monthly*, 1973, 80: 233—269. MR 47#6465.

30 Matijasevič Ju V and Robinson J. Reduction of an arbitrary diophantine equation to one in 13 unknowns. *Acta Arith.*, 1975, 27: 521—553. MR 52#8033.

31 Robinson J. Existential definability in arithmetic. *Trans. Amer. Math. Soc.*, 1952, 72: 437—449. MR 14, 4.

32 Minsky M. Computation: Finite and Infinite Machines. Prentice-Hall, Englewood Cliffs, New Jersey, 1967. MR 50#9050.

33 Matijasevič Ju V. Some purely mathematical results inspired by mathematical logic,in: Logic, foundations of mathematics and computability theory (London, Ont., 1975), Reidel, Dordrecht, 1977, Part I, 121—127. MR 58#5508.

34 孙智伟。Diophantine表示中未知数的精减。中国科学，A辑，1991，(10)：1030—1040.

35 Tung Shih-Ping. On weak number theories. *Japan. J. Math.* (N.S.), 1985, 11: 203—232. MR 88m: 03088.

36 Sun Zhiwei (孙智伟). A new relation-combining theorem and its application. *Z. Math. Logik Grundlag. Math.*, 1992, 38: 209—212.

37 Kosovskič N K. On diophantine representation of the sequence of solutions of Pell's equation. Zap. Naučn. Sem. *Leningrad Otdel. Mat. Inst.* Steklov. (LOMI), 1971, 20: 49—59, 283; English translation: *J. Soviet Math.*, 1973, 1: 28—35.MR45#226.

38 Matijasevič Ju V. On recursively unsolvability of Hilbert's tenth problem, in: Logic, methodology and philosophy of science, IV(Bucharest, 1971) (Studies in Logic and Foundations of Math., vol. 74), North-Holland, Amsterdam, 1973, 89—110. MR 57#5711.

39 Matijasevič Ju V. Arithmetic representations of enumerable sets with a small number of quantifiers. Zap. Naučn. Sem. *Leningrad Otdel. Mat. Inst. Steklov* (LOMI), 1972, 32: 77—84; translated in *J. Soviet Math.*, 1976, 6: 410—416. MR 49#8835.

40 Tung Shihping. Computational complexities of Diophantine equations with parameters. *J. Algorithms*, 1987, 8: 324—336. MR 88m: 03063.

41 Matijasevič Ju V. Primes are enumerated by a polynomial in 10 variables. Zap. Naučn. Sem. Leningrad Otdel. Mat. Inst. Steklov. (LOMI), 1977, 68: 62—82, 144—145; translated in J. Soviet Math., 1981, 15: 33—44. MR 58#21534.

42 Guy R K. Unsolved problems in number theory. Springer-Verlag, New York, 1981, B31.MR 83k:10002.

43 孙智伟。关于Hilbert第十问题的注记——Lucas序列。指数函数和素数集的丢番图表示。第一次逻辑学术交流会论文集(扬州，1989)，138。

44 孙智伟。与 $\binom{PX}{QX}$ 有关的一些Diophantine表示，"双B"代数和计算机逻辑论文集（沈百英主编）。上海交通大学出版社，1991，131—138。

45 Sun Zhiwei (孙智伟). Singlefold Diophantine representation of the sequence $u_0=0$, $u_1=1$, $u_{n+2}=mu_{n+1}+u_n$. 数理和应用逻辑文集（张锦文主编）北京大学出版社，1992，97—101。

46 孙智伟.有关 Hilbert 第十问题的进一步结果，南京大学博士论文，1992.

47 Sun Zhihong (孙智宏) and Sun Zhiwei (孙智伟). Fibonacci numbers and Fermat's last theorem. *Acta Arith.*, 1992, 60(4): 371—388.

48 Grzegorczyk A. Some classes of recursive functions, Rozprawy Matematyczne. 1953, 4: 1—44. MR 15, 66.

49 孙智伟。关于递归函数的若干结果。南京大学学报数学半年刊，1987，4(2)：196—206。MR 89f: 03034。

50 Rödding D. Uber die eliminierbarket von definitionschemata in der theorie der rekursiven funktionen. *Z. Math. Logik Grundlag. Math.*, 1964, 10: 315—330. MR30#18

51 Marchenkov S S. On a certain basis with respect to composition for the class of Kalmar elementary functions. *Mat. Zametki*, 1980, 27: 321—332, 492. MR 81e: 03039.

52 Adleman L and Manders K. Computational complexity of decision procedures for polynomials. 16th Annual Symposium on Foundations of Computer Science (Berkeley, Calif., 1975), IEEE Comput. Soc., Long Beach, Calif., 1975, 169—177. MR 57#264.

53 Adleman L and Manders K. Diophantine complexity. 17th Annual Symposium on Foundations of Computer Science (Houston, Tex., 1976), IEEE Comput. Soc., Long Beach, Calif., 1976, 81—88. MR 56#7314.

54 Kent C F and Hodgson B R. An arithmetical characterization of NP. *Theoret. Comput. Sci.*, 1982, 21: 255—267. MR 84k: 03110.

55 Hodgson B R and Kent C F. A normal form for arithmetical representation of NP-sets. *J. Comput. System Sci.*, 1983, 27: 378—388. MR 85m: 68011.

56 Matijasevič Ju V. Diophantine complexity. Zap. Nauchn. Sem. *Leningrad Otdel. Mat. Inst. Steklov.* (LOMI), 1988, 174: Teor. Slozhn. Vychisl. 3, 122—131, 181—182. MR 90f: 03078.

57 Rabin M O. Effective computability of winning strategies, in: Contributions to the Theory of Games (Ed. by M. Dresher et al.). *Ann. Math. Studies*, 1957, 39: 147—157. MR 20, 263.

58 Davis M, Matijasevič Ju V and Robinson J. Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution, in: Mathematical Developments Arising from Hilbert Problems (Proc. Sympos. Pure Math., vol. 28). *Amer. Math. Soc.*, Providence, R.I., 1976, 323—378. MR 55#5522.

59 Denef J. Hilbert's tenth problem for quadratic rings. *Proc. Amer. Math. Soc.*, 1975, 48: 214—220. MR 50#12961.

60 Carstens H G. The theorem of Matijasevič is provable in Peano's arithmetic by finitely many axioms. *Logique et Anal.* (*N.S.*), 1977, 20: no. 77—78, 116—121. MR 58#27400.

61 Denef J and Lipshitz L. Diophantine sets over some rings of algebraic integers. *J. London Math. Soc.*, 1978, 18(2): 385—391. MR 81a: 12030.

62 Denef J. The Diophantine problem for polynomial rings and fields of rational functions. *Trans. Amer. Math. Soc.*, 1978, 242: 391—399. MR58#10809.

63 Koppel M. Some decidable Diophantine problems: positive solution to a problem of Davis, Matijasevič and Robinson. *Proc. Amer. Math. Soc.* 1979, 77: 319—323. MR 81a: 10069.

64 Dimitracopoulos C. Matijasevič's theorem and fragments of arithmetic. Ph. D. Thesis, Manchester Univ., 1980.

65 Anick D J. Diophantine equations, Hilbert series,and undecidable spaces. *Ann. of Math.*, 1985, 122(2): 87—112. MR 87b: 55008.

66 Delzell C N. Note on quantifier prefixes over Diophantine equations. *Z. Math. Logik Grundlag. Math.*, 1986, 32: 395—397. MR 88e: 03062; Correction to "Note on quantifier prefixes over Diophantine equations", *Z. Math. Logik Grundlag. Math.*, 1988, 34: 283—286.MR 89b: 03072.

67 Tung Shihping. Definability on formulas with a single quantifier. *Z. Math. Logik Grundlag. Math.*, 1988, 34: 105—108. MR 89e: 03048.

68 Pheidas T. Hilbert's tenth problem for a class of rings of algebraic integers. *Proc. Amer. Math. Soc.*, 1988, 104: 611—620. MR90b,12002.

69 Román L. Ultradiophantine categories. *Z. Math. Logik Grundlag. Math.*, 1988, 34: 289—295.MR90d: 03139.

70 Kim K H and Roush F W. Problems equivalent to rational Diophantine solvability. *J. Algebra*, 1989, 124: 493—505. MR 90i: 03048.

71 Denef J and Lipshitz L. Decision problems for differential equations. *J. Symbolic Logic*, 1989, 54: 941—950. MR 91b: 03074. MR92b: 11018.

72 Shapiro H and Shlapentokh A. General Diophantine relations between algebraic number fields. *Comm. Pure Appl. Math.*, 1989, 42: 1113—1122.

73 Kaye R. Diophantine induction. *Ann. Pure Appl. Logic*, 1990, 46: 1—40. MR91f: 03117.

74 Tung Shihping. Decidable fragments of field theories. *J. Symbolic Logic*, 1990, 55: 1007—1018.MR91g: 03023.MR92e: 11145.

75 Pheidas T. Hilbert's tenth problem for fields of rational functions over finite fields. *Invent. Math.*, 1991, 103: 1—8. MR92e: 11145.

76 Tung Shih-ping. Arithmetic definability by formulas with two quantifiers. *J.Symbolic* Logic, 1992,57(1):1—11.MR93c:03041.

Jones' Work on Hilbert's Tenth Problem and Related Topics

Dedicated to Prof. Jones for his Visiting China

Sun Zhiwei

(*Department of Mathematics, Nanjing University, Nanjing*, 210008, *Jiangsu*, P.R.C.)

Abstract This paper is a survey of modern results on Hilbert's tenth problem (especially the work of Prof. James P. Jones). It consists of six sections: 1. Hilbert's tenth problem; 2. The nine unknowns theorem; 3. Universal Diophantine equations; 4. Classification of quantifier prefixes over Diophantine equations; 5. Diophantine representations; 6. Applications of Hilbert's tenth problem. Some new results due to the author, such as the undecidability of $\exists^{11}$ over Z, are also mentioned in the survey.

Key words Hilbert's tenth problem; Diophantine equation; Diophantine representation; undecidability