费马最后定理，希尔伯特方案，二十系统

数学哲学

Fermat最后定理及Hilbert方案

Daniel J. Velleman

大多数数学家都知道本世纪初出现的有关数学基础的一场争论：在逻辑主义者和直觉主义者之间的争弁以及 Hilbert 为解决这一课题而提出的方案．但是此后这争论逐渐平息，几乎没有数学家为基础问题而担忧．近来对于 Fermat 最后定理得到了证明的兴奋心情给了重新审视这个问题的机会，因为 Wiles 的证明恰是 Hilbert 希望用他的方案来验证的那类数学的良好例子．

人们经常评论道 Fermat 最后定理的陈述在概念上很简单．也许很少有人认识到它在*逻辑*上也很简单．如果在陈述它时把量词都放在前面 (即成为*前束范式*(prenex form))，那么这些量词都是全称量词，这定理可表述为：对一切正整数 x、y、z 和 n，若 n 大于 2，则 $x^n + y^n \neq z^n$．逻辑学家称这类语句为 Π_1 语句．因为这语句有这么简单的形式，它可看成是对一定的计算结局做预测：如果人们选任意正整数 x、y、z 和满足 $n > 2$ 的 n 并且计算 $x^n + y^n$ 和 z^n，结果会不等．这当然是直接执行这些计算以验证 Fermat 最后定理的任意特例．因此在某种意义下，Fermat 最后定理的内容可以用一种其他定理不能用的方式来直接观察．定理只是说进行了某种有限的计算后将可得到某些结果．[2)]

当然，该定理是对无穷多个如此的计算进行预测，所以该定理的真性 (truth) 无法通过简单地执行这些计算而得到．这就是为什么需要证明的理由，而 Wiles 给出了这样

原题：Fermat's Last Theorem and Hilbert's Program．译自：*The Mathematical Intelligencer*, Vol. 19, No. 1, 1997, pp. 64–67.

1) 我感谢 Alexander George,Taan Tone Liu, Joseph Moore 及 David Velleman 对本文的草稿提出的有益的评论 —— 作者．

2)在 Hilbert 的 "关于无穷"(见 Paul Benacerraf 和 Hilary Putnam 的 "数学的哲学：选读" 二版，剑桥．剑桥大学印刷厂．1983, pp 183–201．译自 "Über das Unendliche"(Math. Annalen 95 (1926), 161–190)) 一文中，他区分了他所说的*有穷*语句和*无穷* (或*理想*) 语句．按照 Hilbert 的说法，有穷语句是有意义的；无穷语句是无意义的，但在推导有穷语句时有用，就像虚数 i 那样有时在推导关于实数的事实时有用．他把数学描绘成具有两类公式：第一类对应于有穷语句的有意义的信息．第二类不表示任何内容，只是*我们的理论的理想结构*(160 页，原文为斜体字)．虽然 Hilbert 没有清楚地划出有穷无穷之间的分界线，看来他认为 Fermat 最后定理是有穷语句．当然该定理的每个例子是有穷语句，且定理本身可以看作是它的所有例子的简述．Hilbert 认为这样的语句是 "假设性判断"，它断言当数词符号被给定后将得到的某个事物 (194 页)．在 Fermat 最后定理的情况，四个数词符号，即 x、y、z、n 要代入数字而给定．—— 原注．

的证明，从而解决了问题.

但是 Wiles 的证明真解决了问题吗？当然，尽管许多数学家仔细检查过证明，证明仍可能有错误. 但是我考虑的不是这点. 让我们肯定 Wiles 的证明的正确性. 我的问题是，正确的数学证明的存在性就能保证定理是真的？它是否能保证如果我们继续进行计算来验证定理的特例，我们绝不会找到反例？

大多数数学家会认为这是个愚蠢的问题. 如果证明正确，定理必是真的；如果定理是真的，那么验证特例绝不会出现反例. 但是让我们对相信这点的理由作进一步的探讨. 虽然在 Fermat 最后定理的 陈述 中的概念是十分简单的，但 Wiles的证明 中包含的概念却并不这么简单. 如果 Wiles 的证明只涉及正整数，且只用到像 Peano 公理这样的关于整数的基本性质，就不容易使人对证明的可靠性有所怀疑. 但是，事实上的证明不只涉及正整数，还涉及实数、复数，这些数的集合，这些集合之间的函数，等等. 这些概念都比正整数概念复杂得多. 例如，在某种意义上说，仅仅一个实数就是无穷复杂的，因为要精确地表述它时要用无穷多位的十进位数字的展开式. 集合 $\boldsymbol{R}$ 包括不可数的无穷多个这样的无穷复杂的数. 我们真能相信具有这样复杂概念的推理真可以对只涉及正整数的计算的结果作出精确的预测吗？

验证像 Wiles 式的证明[3] 中的推理的最直接的方法是给出所有涉及的概念的谨慎的定义，然后试着去证实：当证明中的语句按这些定义来解释时，它们都可用有效的演绎逻辑规则推导出来，因此必须是真的. 因为 Fermat 最后定理的语句是 Wiles 证明中的最后的语句，这就有可能确立该定理是真的. 这就是包括 Frege, Russell 和 Whitehead 在内的逻辑主义者试图给数学提供一个基础[4] 的途径. 但是今天大多数人把逻辑主义者的方案最多看成只是部分成功的. 作为逻辑主义者研究工作的一个结果，我们可以说一切数学概念可由一个不加定义的概念 "集合" 来定义，且一切数学定理可由关于集合的一个简单的公理系统推导出来. 最广泛使用的集合论的公理系统是 Zermelo–Fraenkel 系统，通常简称 $\boldsymbol{ZF}$ 系统. 但是，关于 "集合" 这字的含义和 $\boldsymbol{ZF}$ 公理的真性的问题仍未解决. 我们必须相信所有的集合的全域的存在性，以及 $\boldsymbol{ZF}$ 公理对这个全域的真性，才能确信 Wiles 的证明是可靠的吗？[5]

有许多数学家不会愿意为了证明 Fermat 最后定理的真性而不分青红皂白地使用 $\boldsymbol{ZF}$

---

[3] 这里所谓的 "Wiles 式证明" 指的是在验证一有穷结论时用到涉及无穷语句的推理 (这些词的含义见注 2). —— 原注.

[4] 例如，见 Frege 的 "算术的基础：对数概念的一个逻辑－数学的研究"(Oxford: Blackwell, 1950, "Die Grundlagen der Arithmetik" 的一译本，2 版 (剑桥：剑桥大学印刷厂 1925–1927)).—— 原注.

[5] 由于 Wiles 的证明中使用的概念超出正整数，看来 Wiles 的证明不像能在 Peano 的公理系统 (通常简记为 $\boldsymbol{PA}$) 中进行表述. 当然它肯定能在 $\boldsymbol{ZF}$ 中表述. 但是此证明并不需要整个 $\boldsymbol{ZF}$ 系统. 它很像是可以在一个强度介于 $\boldsymbol{PA}$ 和 $\boldsymbol{ZF}$ 之间的系统中实现. 人们研究过不少这样的系统；例如，见 Solmon Fefeman 的文章 "与数学实践有关的有穷类型论" (见 Jon Barwise 编的数理逻辑手册，阿姆斯特丹，北荷兰，1977, pp. 913–971) 确定 Wiles 的证明恰好需要强度多大的公理系统是个有趣的科研项目，但据我所知，目前这项目尚未有人来做. 但是本文关心的不只是 Wiles 的证明本身，而是在一般的数学中无穷推理的使用问题，Wiles 的证明只是一个特别激动人和有趣的例子. 因此，为了本文的目的我要继续谈到 $\boldsymbol{ZF}$ 系统. —— 原注.

集论. 肯定地, Brouwer[6] 就不会愿意的, Weyl 也不会愿意[7]. 也许数学家里只有少数人知道以下事实, Lebesque 、 Borel 和 Baire 对现在人们接受的像非构造性的存在性证明[8] 这类推理的正确性提出疑问. 与这些顾虑相反, 为了捍卫像 Wiles 的这种证明, Hilbert 提出了他的基础方案[9].

Hilbert 的伟大的洞察力在于认识到可以有另外的方式去建立像 Wiles 式的证明的可靠性. 为了理解如何做到这点, 暂且不论 Wiles 的证明的可靠性, 而先来看如果找到 Fermat 最后定理的反例意味着什么. 该反例可由有穷计算得到, 而这一计算就能证明 Fermat 最后定理是假的. 这一计算和 Wiles 的证明组成了 ***ZF*** 系统中的一对矛盾. 于是, 我们只要知道 ***ZF*** 系统是协调的 (无矛盾的)—— 那么我们就能相信, 基于 Wiles 的证明, 不可能找到关于 Fermat 最后定理的反例. Hilbert 的洞察力在于认识到: 我们不需要相信 ***ZF*** 公理是真的, 甚或不需要知道它是否有意义, 就可以相信这个证明了. 我们要的只是相信公理是协调的.

事实上, 公理的协调不只是保证 ***ZF*** 系统中证明可靠性的充分条件, 也是必要条件. 如果公理是不协调的, 那么 一切 语句, 不论是真语句还是假语句都可由公理推演出来. 此时, 在 ***ZF*** 系统中 Fermat 最后定理证明的存在性不能确立起该定理的真性.

Hilbert 方案是想藉证明数学的公理系统[10] 的协调性来建立像 Wiles 的这种证明的可靠性. 这里人们可能会纳闷协调性的证明是怎么做到的. 既然 Wiles 的证明我们都不相信, 凭什么要相信协调性证明呢? 要指出协调性涉及的概念是十分简单的, 逻辑学家把证明定义为满足某种很容易检验的条件的符号安排 (Arrangements of symbols). 这概念

---

[6]Brouwer 是直觉主义的奠基人. 在他的文章 "直觉主义和形式主义"(Bull. of AMS, 20 (1913) pp. 81-96. 在 Benacerraf 和 Putnam 书中重印 (pp.77-89.)) 中, 他写道: "在有穷集领域内, 形式主义者的公理可以对直觉主义者解释得十分清楚, 后者会无保留地同意他们, 他们只是在方法上有两种不同的倾向, 而不是他们的结果不同; 但是到了无穷或超有穷集的领域就变得完全不同了, 在那里形式主义者引进了许多对直觉主义者毫无意义的概念". 作为结果, 他总结道: " 对直觉主义者无意义的广泛的研究领域, 形式主义者仍然非常感兴趣."—— 原注.

[7]见 Weyl 的 "连续统: 对分析基础的一个关键性的检验."(纽约 Dover 1987, 译自 Das Kontinuum; Kritische Untersuchungen über die Grundlagen der Analysis. 莱比锡 Veit 1918.) 在前言中 Weyl 写道: "分析的房子……很大程度上是建立在沙滩上的. 我相信我可以把这不稳固的基础换成一些永久牢固的柱子. 但是它们并不会支持当今一般人认为已有了可靠基础的一切东西. 我放弃其余的, 因为我看不到其他可能. (p 1.)—— 原注.

[8]例如 Lebesque 在给 Borel 的一封信中写道: "我相信只有在 承认 '不定义一对象而要证明它的存在性是不可能' 的条件下才可以使 (基础) 稳固". 这信是 Lebesque 、 Borel 、 Baire 和 Hadamard 等人之间交流的信件中的一部分. 这信发表于 Bulletin de la Société Mathématique de France, Vol. 33 (1905), pp. 261-273. 上面引用的英译文可参见 Gregory Moore 的书 "Zermelo 的选择公理: 它的起源、发展和影响". 纽约. Springer-Verlag 1982.—— 原注.

[9]在 "关于无穷" 一文中, Hilbert 对他的方案列举了两个目的. 第一个是很有名的: "在任何有抢救希望的地方, 我们要小心地研究富有成效的定义和演绎方法, …… 没有人能把我们赶出 Cantor 为我们创造的伊甸园." 然而, 第二个目的给我们更确切地描述了他希望完成的东西: "我们必须在整个数学中建立起这样一种推理方式, 它像通常的初等数论中使用的推理一样可信. 在那里人们不会怀疑推演的正确性而且认为矛盾和悖论是由于自己的不小心造成的."(原文 191 页).Hilbert 指的 "矛盾和悖论" 当然跟在接近世纪变更时集合论中出现的 Russell 悖论有关. —— 原注.

[10]Hilbert 脑中的公理系统, 并不正好是 ***ZF*** 系统. 但是 ***ZF*** 系统的协调性的一个证明肯定会满足 Hilbert 方案的要求的. —— 原注.

远比 Wiles 的证明中的无限复杂的实数的概念简单得多. 协调性的意思是指不存在两个这样的证明，它们分别证明相反的结论. 有理由希望只用有限的组合性质的推导而给出不存在这样的矛盾的证明，这种推理甚至能让对 Wiles 的证明有怀疑的人信服. 这正是 Hilbert 所希望做到的.

这里还可以从另外的角度来看 Hilbert 的思想. 如果可以找到所要的协调性证明，那么也就有可能给我们一个新的、概念上更简单的关于 Fermat 最后定理的证明. 这个新的证明的大部分很像 Wiles 的证明，但是对它的解释却不同. 我们将不把 Wiles 的证明看成是对复杂的概念的有意义的讨论，而是把它们看成是特定类符号的安排. 协调性证明要表明：如果 Fermat 最后定理是假的，那么这种符号的安排是不会存在的. 符号安排的展示就建立了定理的真性. 也许在数学家们看来这种证明不像 Wiles 的证明那么有趣和有益，证明中讨论的对象 —— 符号的有穷安排 —— 在概念上比 Wiles 的证明中所用的数、集、函数要简单得多. 实际上，利用 Gödel 对符号的有穷安排的配数方法，这种证明中关于符号安排的推导可以换成对自然数的推导. 因 Hilbert 方案可能已经表明，虽然在 Fermat 最后定理的证明中使用复杂的数学对象是有益的，但是有关这些对象的讨论，原则上总可以从只想使用自然数推理的证明中加以排除[11].

当然，今天我们由 Gödel 的第二不完全性定理已经知道不能找到这种协调性证明. 事实上，如果 ZF 系统是协调的，那么即使使用 ZF 的全部资源也不可能证明 ZF 系统的协调性.

这就产生了一个有趣的问题：我们是不是应该说，Wiles 所确立的并不是说 Fermat 最后定理是真的，而只是说：如果 ZF 系统是协调的，那么 Fermat 最后定理是真的[12]. 如果 Hilbert 方案成功了，那么就可以取消关于协调性的限制. 是否他的方案失败了，就意味着这限制必须保留呢？

也许可以这么想，ZF 系统的协调性已被充分圆满地建立起来了，不必为此耽心. 在本世纪大部分时间里，数学家们都用 ZF 系统进行工作，但尚未发现矛盾. 但是请记住，在 Wiles 给出他的证明之前，用直接计算的办法已经得到了 Fermat 最后定理对数百万种情况成立. 但数学界仍然感到需要一个证明，这不只是增加对定理的信心，而是要建立它的确实性. 即使我们相信 ZF 系统非常像是协调的，仍然有理由问是否 Wiles 的证明确实建立了 Fermat 最后定理的真性，或者只是定理的真性以 ZF 系统协调性为前提条件.

在集论中，把 ZF 系统的协调性作为定理的假设条件是平常的事. 例如，1963 年 Cohen 证明了连续统假设在 ZF 系统中不可证，但是他的证明要求以 ZF 系统的协调性作为假设. 他的定理通常陈述方式不是 "连续统假设在 ZF 系统中不可证明"，而是 "如果 ZF 系统是协调的，那么连续统假设是不可证明的."

---

[11] 更严格地说，如果 ZF 系统的协调性可在比如 Peano 公理系统中证明，那么在 ZF 系统中可证明的数论的任何 Π_1 语句也可以在 PA 系统中证明. 如果这是对的，我们可以说对数论的 Π_1 语句而言，ZF 是 PA 的保守扩充. —— 原注.

[12] 当然，如果可以表明 Wiles 的证明可在一个比 ZF 弱的公理系统中实现，那么这个较弱的系统的协调性需要作为假设. —— 原注.

可以肯定，在 Cohen 的证明和 Wiles 的证明之间有一个重要的不同. "***ZF*** 系统是协调的" 这个假设在 Cohen 的证明的推演中的确是用到了，但是 Wiles 的证明只用了通常的数学推演，并没有引用 ***ZF*** 系统的协调性. 只是在考虑 Wiles 的证明是否可以信赖时才想到要知道 ***ZF*** 系统是否是协调的. 对那些相信一切集合的全域是存在的，且相信 ***ZF*** 系统的公理对这个全域而言都真的人，没有理由对 Wiles 的证明有任何怀疑. 但是对那些对这全域的存在性抱有怀疑的人，这问题仍然存在： Wiles 的证明是否能使我们相信 Fermat 最后定理的反例永远也不会出现，或者只能使我们相信如果 ***ZF*** 系统是协调的，那么反例永远不会出现呢[13]?

我并不试图回答这里的这个问题. 但是我希望通过对这问题的思考，读者将会对 Hilbert 方案的意义和由于这方案的失败现在仍然不能解决的数学基础中的问题有更多的了解.

(Dan Vellemen 1976 年在 Dortmouth 学院取得学士学位， 1980 年在 Wisconsin 大学取得博士学位. 在 1983 年到 Amhers 学院工作前曾在 Texas 大学和 Toronto 大学教书. 他对逻辑，数学哲学和量子力学基础感兴趣. 他是 "如何去证明它" 一书的作者，他还和 Joe Konhauser 及 Stan Wagon 合作写了即将出版的问题集 "自行车要走向什么方向？")

(杨东屏 译　袁向东 校)

[13]考虑这问题的另一种方式是在不同的公理系统中陈述这一证明. 正如我们已观察到的那样， Wiles 的证明可在 ***ZF*** 系统中陈述，但可能在 ***PA*** 系统中不行. 因此 Fermat 最后定理在 ***ZF*** 系统中可证，但还不知道在 ***PA*** 系统中是否可证. 无论如何，语句 "如果 ***ZF*** 系统是协调的，则 Fermat 最后定理是真的" 可用数论的语言 (用 Gödel 配数法) 编码且这个编码后的语句在 ***PA*** 系统中可证. 这个证明只是我们的如何由 Fermast 最后定理的反例引出 ***ZF*** 系统的不协调性的描述的数字编码. 因此，若 Fermat 最后定理的证明可在 ***ZF*** 系统中陈述、 ***ZF*** 系统协调性的假设是不需要的，但是若证明要在 ***PA*** 系统中描述，这假设可能就是需要的. 在 Fermat 最后定理的证明中要不要 ***ZF*** 系统是协调的这个假设，取决于你要在什么系统中做这个证明. ——原注.