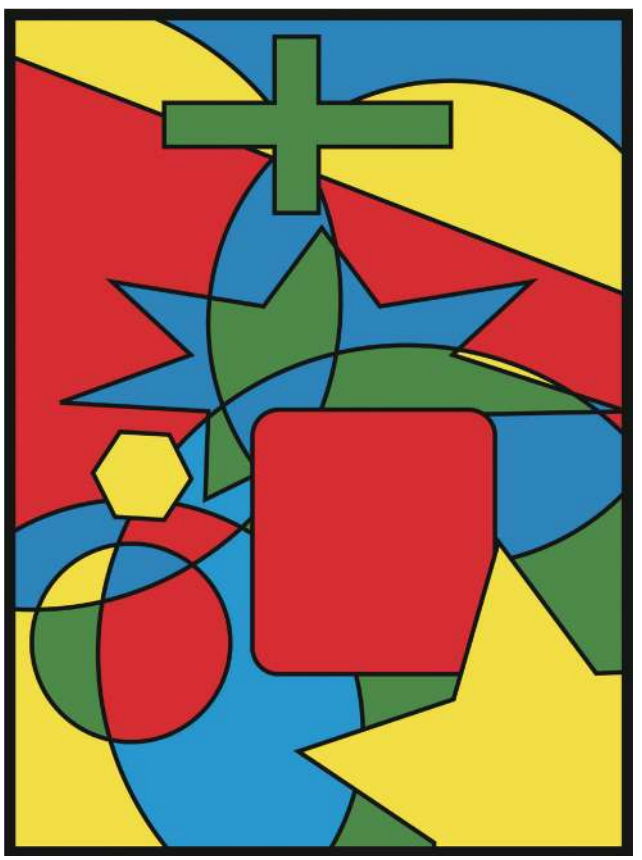
机器的光荣与人的梦想

木遥



四色定理的一个简单示范；它的计算机证明1976年被给出。

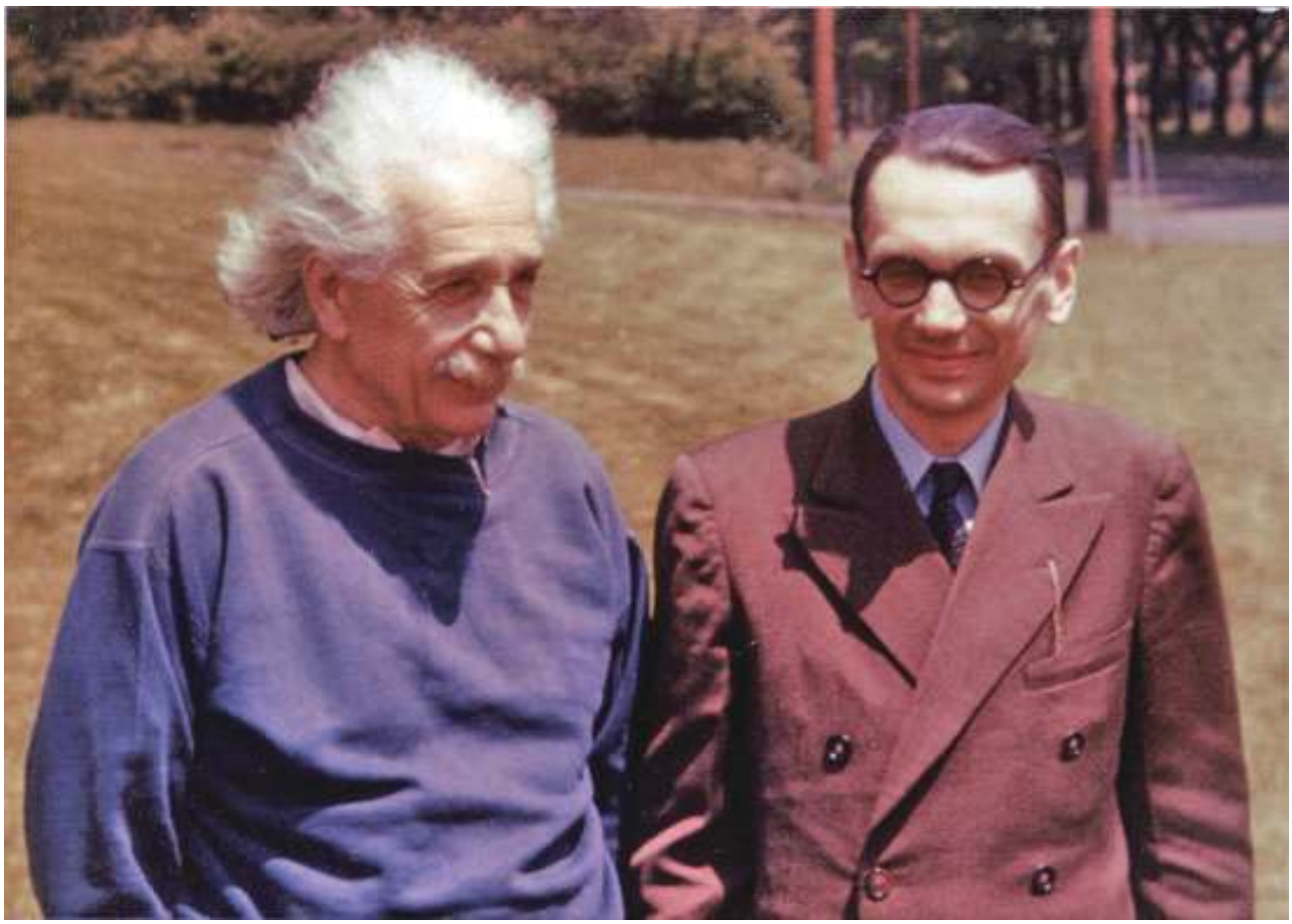
Offord 教授和我最近发现我们在《数学年鉴》中的论文存在一个蹊跷的错误。一个公式中的加号被写成了一个乘号，而后面那个命题的证明则是依赖于这个错误的公式的，因而也是无法成立的。不过，聊以自慰的是，我们最终能够确定那篇论文总的结论其实还是正确的。

——《Littlewood 文集》

如果回忆一下中学数学的两门分支课程——代数和几何，就能清楚地看到，在数学的两种最基本的推演过程——计算和证明——之间一直存在着一种巨大的差别。在初等代数问题里，一个问题的求解（例如解一个方程或者计算一个多项式乘法）是可以通过规范化的步骤顺序实现的，这使得这门课程本质上同一门按照操作手册动手的劳技课并无不同。然而，几何定理（哪怕是最基本的初中平面几何）的证明却不然，发现一个证明的过程中一定存在着那样一些“灵光一闪”的时刻，它们可遇而不可求，使得几何这门课程几乎成为本质上“不可学”的一门课程。我们都曾经面对过无从下手的证明题目而摇头叹息过，也都在阅读一个自己想不出来的证明过程时体会过那种羚羊挂角无迹可循的美感。纵然掌握了再多的定理和证明技巧，在脑海中发现完整的逻辑道路的过程仍然是一个自发而偶然的事件，反映了人类思维的某些最难于用语言刻画的能力。从某种程度上说来，这正是数学这门学科的神秘感的终极来源。

也正因为如此，计算——无论多么繁琐——本质上都是可以由机械实现的，在今天更是借助电脑的辅助成为一种相对平凡的任务。而证明才被认为是数学本质的困难所在，是人类智慧的高度结晶。阅读并验证一个证明是否正确（或者哪怕仅仅是理解它在说什么）是一项辛苦而困难的任务，只有受过训练的数学家才能够得以完成。并且，和物理、化学、生物等牵涉到真实世界的学科不同，数学定理是不能被实验所证明的，而数学家的阅读就成为本质上唯一可行的验证手段。这其实也正是今天数学界的真实运作方式：一个人写出一篇文章来宣称证明了一个定理，他的某些同行们会在特定的审议机制下阅读这篇文章并且宣布是否接受其论证。如果大家都认为证明无误，这个定理就被接纳为数学的一部分而存在下来。

这一流程的有效性已经为数学科学的茁壮生命力所证明，然而，任何人也都能看出这个过程中蕴含的极大风险：我们究竟在什么意义上能够宣称一个定理真的是正确的？其作者可能犯错，审阅者也可能犯错，我们都知道数学证明中的微小错误有时候是多么难于发现，而这些错误也许永远都不会有人知道。当然，这并不是说数学这门学问完全是空

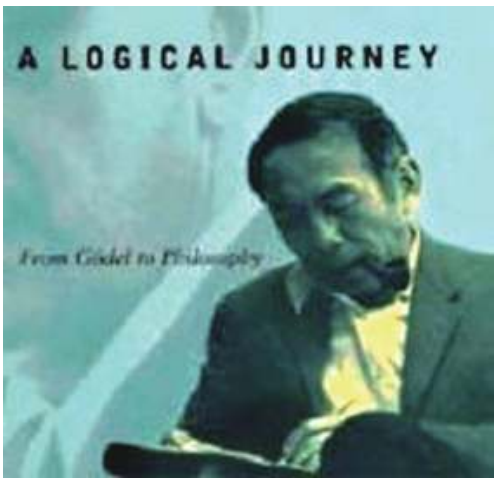


数理逻辑学的巨人哥德尔和爱因斯坦在一起

中楼阁：越是重要的定理，其阅读者也就越多，出错的概率也就越是无限趋近于零。我们不能想象一个从阿基米德时代就流传至今，被无数学生学习过的四五行的证明还会存在逻辑错误。但是即便如此，只要翻开数学史，我们还是能看到大量重要的错误由于极其偶然的原因才在事隔多年之后被人们发现的例子。

到了现代，这个问题更是严重得多，数学的复杂程度和专业化程度已经使得任何一个分支的专业人员数量同证明的普遍难度完全不成正比。这种矛盾在某些极端的例子里尖锐到了荒谬的程度：图论中的 Robertson–Seymour 定理的证明一共耗费了大约五百页的篇幅，Almgren 对几何测度论中一个定理的证明总长为 1728 页，而代数中著名的有限单群定理（确切来说这不是一个定理而是一组定理）的证明总共包含超过五百篇论文，总页数估计在一万页以上。世界上恐怕不存在任何一个人真地把这个证明从头读到尾过，遑论验证其正确性了。有限单群方面的专家之一 Aschbacher 曾经不无自嘲的说过：“一方面，当证明长度增加时，错误的概率也增加了。在有限单群分类定理的证明中出现错误的概率实际上是 1。但是另一方面，任何单个错误不能被容易地改正的概率是 0。随着时间的推移，我们将会有机会推敲证明，从而对它的信任度也必定会增加的。”

我们也希望如此，但是以严谨而著称的数学体系是以这样远远难于称为严谨的方式被建立，终究构成某种吊诡而令人心生疑虑的现实。不仅如此，这一体系在某些情况下还会完全失效，一个著名的例子是四色定理在 1976 年的证明。Appel 和 Haken 在那个证明中把所有的地图用通常的逻辑推演的方式化归为 1936 种类型，然后——这是充满争议性的一步——编写了一个电脑程序逐个验证这些类型都满足四色定理的结论，从而完成了整个证明。一个立即存在的问题是：就算前面的逻辑部分是正确的，谁能证明后面的电脑程序中没有错误？难道数学家们应当逐行阅读代码以理解其正确性么？（写过程序的人一定晓得，阅读程序代码是比阅读一个通常的逻辑证明还要痛苦的经验。）另一个时间上稍近的例子是 Hales 对开普勒堆球定理的证明。这一证明包含



著名华人数理逻辑专家王浩教授

了三百页的文本部分和四千行的代码部分，投稿至数学界最重要的杂志《数学年鉴》，杂志的编辑最终接受了这篇论文，但是指出：

“在我的经验里，还没有一篇论文曾经得到过这样的审查。审读人专门建立了一个讨论班研究这篇文章，他们检查了证明中大量的论述并且确认其正确性，这种检查常常需要耗时数个星期。……总的说来，他们并不能确认证明本身总体的正确性，而且估计永远无法做到这一点，因为他们在到达终点之前精力就耗尽了。”

至于代码部分，估计并没有被任何人认真地审阅过。

于是在一部分数学家那里，另一种可能性开始渐渐浮上水面。既然一般来说数学定理的证明及其审查是如此困难和繁琐的一件事，我们有没有可能从根本上把它转化成电脑能够承担的任务呢，就像我们已经成功地让电脑代替人类实现的大多数繁琐劳动一样？注意，这种电脑的参与并不是像上面的例子里那样仅仅负责某些验证性的工作，而是从最底层介入逻辑推演的部分，从而严格的建立整个证明过程。这种思路，一般被称为形式证明（Formal Proof），有时也称为机器证明。

两个哲学家之间的争论并不比两个会计师之间的争论更复杂，他们只需要掏出纸笔，然后对彼此说：让我们来算一算吧。

——《莱布尼茨通信》，1666

用计算的方式进行逻辑推演并不是什么新鲜想法，事实上，这是人类极为古老的梦想之一，它可以上溯到笛卡儿和莱布尼茨乃至霍布斯，甚至也许更早。霍布斯有名言曰：“推理就是计算”，不过考虑到他的数学（特别是几何）程度之糟糕，人们一向怀疑他根本不知道自己到底想说什么。莱布尼茨的观念则要清晰的多，在他看来，只要能够把一切逻辑论断用统一的语言确切地表达出来，并且采用严密的规则进行逻辑推演，那么世间的所有道理都是可以被严格推导出来的。

让我们抛开其间的哲学意涵不谈（莱布尼茨的梦想事实上已经涵盖了人类理性的全部领域），单就数学层面而言，这一框架听起来并不算特别不靠谱。从欧几里德开始，数学家们就开始着手把全部数学定理建立在公理体系之上，于是从理论上来说，任何一个数学定理的证明，确实是可以用纯粹的逻辑语言“算”出来的。这里的计算当然不是说加减乘除这样的四则运算，而是形式逻辑的基本运算，例如命题 A 为真推出命题 B 为假，诸如此类。这种运算也有其特定的“运算法则”，也就是我们平时所默认的那些形式逻辑的法则，以此为基础，一个推导就是在这些法则下的一次“计算”，而一个复杂的证明只不过是一道复杂的“计算题”而已。

事实上，经过二十世纪初那一场著名的数学革命以及随后的 ZFC 公理体系（这是今天数学界普遍承认的公理体系）的建立，这种把全部数学建立在逻辑演算之上的想法实际上并不存在理论上的障碍。实际困难在于，从人们熟悉的“人脑证明”到这种完全依赖于逻辑算符的“形式证明”之间，存在一个复杂度上的巨大鸿沟。我们在脑海中所进行的逻辑推导其实大量的依赖于人类特有的直觉想象和经验，如果要把每一环逻辑链条都清清楚楚地写下来，每一次推理都追溯到公理体系那里去，任何一个简单的证明都会变得繁琐到超乎想象的程度。我们喜欢严格性，但是这样做的代价也太大了。

然而电脑的发明改变了一切。众所周知，电脑最擅长于做的就是这种严格而繁琐的工作。把基本公理告诉电脑，把推理法则教给电脑，不就万事大吉了么？

差不多了，只剩下最后一步——非常微妙的一步。在上面的叙述里，一切传统的人脑证明都可以转化为逻辑算符的“计算”，这是对的，但是其前提是这种传统证明已经存在了，所需要的只是恰当的翻译过程而已。如何发现一个未知的证明则是一个完全崭新的挑战。我们对于人脑是如何想出一个证明的过程都不甚了了，又如何能教给电脑去自己发现一个证明？

于是人们采用了一种实用主义的策略。一方面，把人们已经知道的证明翻译给电脑，这同时也构成了对这些证明逻辑严密性的一次确认。——虽然这件事情听起来很简单，但操作起来仍然很困难。另一方面，小心翼翼的探索让电脑尝试着去自动“发现”一个证明，哪怕只是很简单的证明而已。

让我们看看半个世纪以来人们已经让电脑做到了哪些

事情：

• 1954 年，Davis 成功地让电脑证明了定理：偶数加偶数仍然等于偶数。

• 1959 年，王浩让电脑证明了罗素和怀特海的名著《数学原理》中的所有谓词逻辑定理。

• 1968 年，de Bruijn 用电脑给出了 Landau 为其女儿所写的一本关于实数的入门小册子中的全部数学定理的证明。

• 1976 年，Lenat 让电脑自发的开始探索数学世界，他的电脑从基本公理开始，自己发现了自然数、加法、乘法、素数这些词的意思，甚至还发现了算术基本定理。

• 1984 年，吴文俊发表《几何定理机器证明的基本原理》，用电脑证明了一系列平面几何中的著名定理。

• 1996 年，McCune 设法让电脑“自动”证明了布尔代数理论中的 Robbins 猜想。这里“自动”的意思是，把这个猜想输入电脑，回车之后，电脑花了八天时间给出了这个猜想的证明而没有借助人类的任何帮助。

• 2005 年，Gonthier 建立了四色定理的全部电脑化证明。这一证明和 1976 年那个证明虽然都用到了电脑，但是其意义却根本不同。1976 年的证明本质上仍然是传统证明，电脑只是起到了辅助计算的作用，而 Gonthier 的证明则是纯粹的形式证明，其每一步逻辑推导都是由电脑完成的。

到今天为止，人们已经用电脑证明了上百条重要的数学定理，甚至还曾经用电脑发现过一些猜想（这些猜想的命名恐怕会成为一个问题）。这一切还当然仅仅是个开始，人们还不曾让电脑做出过任何真正意义上的数学贡献，几乎所有被电脑证明的都是人类已经知道的事情，而且大多数都是很初等的结论。指望电脑帮我们证明哥德巴赫猜想的那一天还远远没有到来。

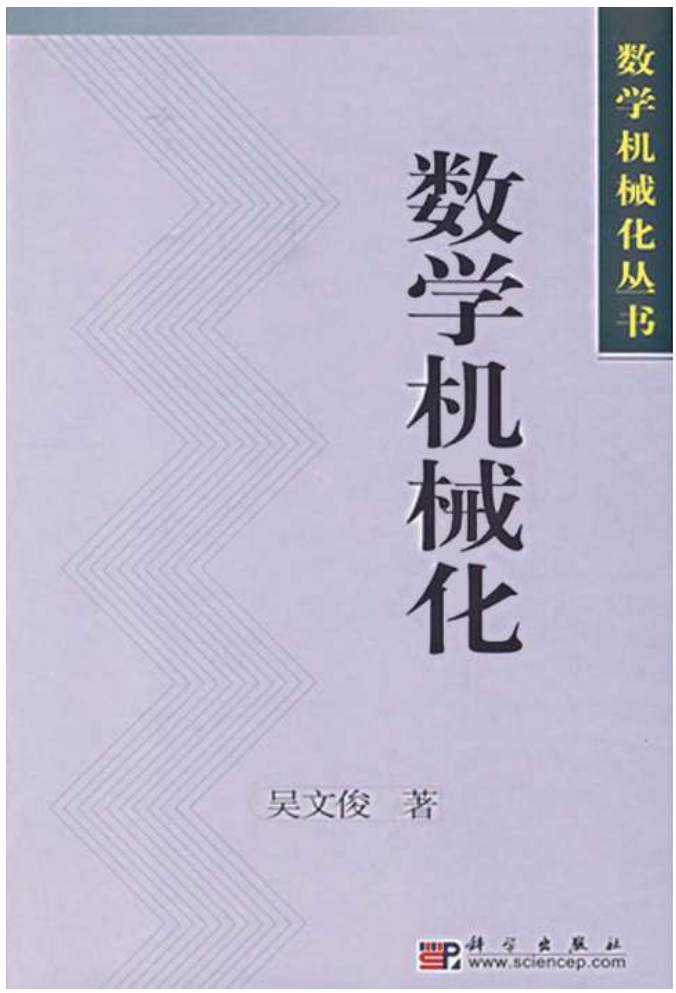
但是另一方面，任何人估计都可以看出来这条道路的远大前景。和人类相比，电脑不知疲倦和逻辑严密的优点使得其前途未可限量。电脑当然也会犯错误，但是这种错误归根结底是容易检验的——其正确性归结为这些软件内核的正确性，而内核一共也就几百行代码而已（这一点要归功于数学公理体系的简洁和精致）。一代一代数学家永远都要从零开始学习和成长，而电脑则总是建立在已有成果的肩膀上（也许应当说机箱上？），假以时日，电脑会不会成为有史以来最伟大的数学家呢？

一个好的数学证明应当像是一首诗，而这纯粹是一本电话簿！

——对 1976 年四色定理证明的一则著名评论

这条道路从第一天开始就伴随着巨大的争议和疑虑。

数学证明，正如我们在前面所提到的那样，是人类理性最光荣的成果之一。蕴藏在美丽深刻的数学定理背后的那些苦心孤诣的劳动和成功之后宛若天成的光辉，吸引了一代又一代伟大的头脑投身其中。匈牙利数学家 Erdős 曾经发明过一个术语：the Book，用以描述他心目中由上帝所拥有的那本书，在那里记载了全部美妙和精致的数学定理的证明。他曾经说过：“你可以不信仰上帝，但是你应该信仰那本书的存在。”大多数数学家是信仰的，而他们也衷心的希望自己所建立的定理和证明会出现在那本书里。



吴文俊《数学机械化》专著

如果这些定理最终都只不过是被一些代码算出来的，这种美还有什么意义？

2007 年，美国数学会通讯杂志采访了刚获得菲尔兹奖不久的陶哲轩，问题中包含了关

温家宝总理看望中国机器证明的创始人吴文俊等科学家

于形式证明的看法。陶哲轩的回答可以在很大程度上代表一般数学家对这个问题的意见：

对一个证明来说非常重要的一点在于，它应当能够被任何人清晰的理解。在这一前提下，在一个令人满意的数学证明中，计算机的作用最好只限于确认一些显而易见的事实，比如某个方程的某个孤立解或者某个宽泛条件下参数的存在性，而不是用来证明一些从人类的思维过程中闪现出来的本质上非同寻常的结论。如果计算机证明的论断在人类看来是完全直观的，那用电脑来确认一下这些结论的逻辑严密性当然没什么不好，但是基于人的阅读和理解的证明过程总是必要的。

于是这构成了某种颇为讽刺性的局面。计算机一般被认为是数学家最引以为傲的发明之一，然而当它转过头来开始侵蚀数学家的传统领地时，数学家们的首要反应便是捍卫自己的尊严。一个由计算机生成的证明在广义上来说当然也是人类智慧的产物，可是如果有朝一日，困扰人类几百年的某个著名猜想被计算机所证明，则数学家们情何以堪？

人们对形式证明的批评多半集中于它极端的繁琐和不直观。然而，既然人们已经知道如何把一个传统证明翻译为形式证明，那么把一个计算机生成的形式证明翻译回人们可以直接阅读和理解的直观证明在理论上说来也并非全然不可能。从这一点上说，形式证明和传统证明之间的鸿沟并非是不可逾越的，尽管还有很长的路要走。我们可以设想，在未来的某一天，这两种证明之间的界面变得极其友好，于是任何一个数学家都会把形式证明作为日常数学工具加以掌握，任何一本数学杂志都会要求提交的证明必须是经过计算机验证的……

而对于电脑来说真正的挑战，仍然体现在对未知证明的寻找上。如何让电脑学会迅速发现合适的证明路径，这是这一领域里最困难也最迷人的问题之一。毕竟，即便是数学家们自己往往也说不清楚那些片羽飞鸿般的灵感是怎样产生又怎样被自己捕捉到的，更不用说让电脑来模拟这一过程了。对于电脑“思考方式”的设计和研究，本身就是深刻的数学问题——从某种意义上说来，这一自我缠绕的局面不但没有构成对传统意义上的数学之美的消解，反而是它的延续。归根结底，这一领域的任何进展，都标志着人们对于“智慧思考”这一问题更深刻的理解，这已经足以令人骄傲了，不是么？

不过还是让我们暂时抛开这些遥远的设想不谈，回到形式证明的初衷之一上来：为人类已有的证明建立可靠的逻辑基础。在这一领域里活跃的若干研究小组的通力合作，已经让一个宏伟的工程颇具雏形，在这个工程里，人们试图建立一个庞大的由电脑维护的“定理库”，其中包含了人类所了解的全部数学知识，而它们的正确性完全为电脑所确认。人们所建立过的所有证明都被翻译成电脑可以理解的形式而加以保存，而人们也可以轻易的从这里查询任何已知的数学问题的答案。——同让计算机彻底取代数学家去探索未知世界相比，这一 wiki 式的设想无疑具有更高的可操作性。这一工程被称为 Q.E.D.，任何一个数学家都明白这三个字母的含义：这是拉丁文的缩写，意为“证毕”。

你可以说这是巴别塔般的梦想，也可以说这是潘多拉的盒子，你也可以像大多数数学家一样投去怀疑甚至不屑一顾的目光。但是你不能无视它的存在，因为道路已经打开，纵然迷雾重重，但是没有理由不继续走下去。

证毕。

（想象一下计算机说出这两个字的感觉…… ）