|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | 成 绩 |  |
|  |  |  | 评阅人 |  |

**复 旦 大 学**

**研 究 生 课 程 论 文**

|  |  |
| --- | --- |
| 论文题目： |  |
| 修读课程： | 自然辩证法概论(MAST610022) |
| 选课学期： | 2021-2022第1学期 |
| 选课学生： | 陈淇奥（21210160025） |
| 完成日期： | 2021.11.1 |

1. 数学与科学技术的关系

为什么我要选择数学，数学与科学技术是什么关系呢？我认为，科学技术是数学的某种外化形式。“科学是一种系统性的知识体系，它积累和组织并可以检验关于宇宙的解释和预测”[9]，它扎根于数学：在进行推理时，我们隐含地在使用一套形式推理系统；在进行假设时，我们需要借助一些数学上的结果来支持假设的过程；在检验时，对于实验学科，我们需要统计学的知识去计算结论的置信度，而对于理论学科，我们则需要使用深刻的数学结论证明我们的假设。技术则是科学的产物，它来自于被应用于实际问题的科学知识。

科技的一个最典型的例子是计算机，它既是科学的（计算机科学）也是理论的（计算机软件），在这里我想论述一下计算机的一些方面与数学的关系。

首先我们可以考虑一下，计算机是如何影响我们这个时代的？我们普通人使用计算机或是手机时[[1]](#footnote-1)，我们有两个目的：生产与娱乐。借助处理器庞大的计算能力以及构筑在其上的各类生产力软件（比如word，photoshop），我们得以完成一些任务，进行一些生产活动；而我们的娱乐活动，则依赖于视频、音乐与文字，而它们最主要的传播工具，就是计算机，借助计算机，我们才能较方便地获取这些东西。

归根结底，我们在利用他人写好的程序来达成我们的目的，而程序，则由各式各样的算法组成。算法是什么？算法就是给定一些输入，程序在接受这些输入后，返回一些输出。例如对于无处不在的推荐算法来说，它的输入就是某个特定用户在平时使用计算机或手机时的一些特征，在经过一系列运算后，返回这个用户可能感兴趣的一些结果。更抽象地说，我们几乎可以认为一个具体的算法就是一个“可计算”[[2]](#footnote-2)的函数，它的参数是我们的输入，它的值就是我们的输出。再进一步，我们要如何来判断什么样的结果是好的，什么样的结果是坏的？也就是说，我们需要一个参数来刻画我们的结果，并且我们就需要证明，我们的结果对应的参数在某个好的区间上。为此，我们需要不同的数学命题与数学定理来定量地刻画我们想要的性质与我们计算的方式之间的关系，并最终证明我们写出来的算法确实能做我们想要做的事情。因此本质上，算法就是数学，计算来自于数学。

1. 数学与社会的关系

数学问题、数学定理会影响我们的社会吗？答案是显然的，它们构成了我们对于自然世界的认识。进一步，一个自然的问题就是，它又会多大程度地影响我们的社会呢？

首先我们应该注意到它对我们世界观的可能作用，一个例子是有名的连续统假设，它是希尔伯特第一问题，说的是：

不存在一个基数绝对大于可数集而绝对小于实数集的集合。

抛开内容不谈，对于我们普通人来说，给我们一个问题，我们总是会认为，这要么是正确，要么是错误的，虽然我们证明不出来，但总会有人能将它证明出来。在这个问题解决之前，我们对于数学总是抱有一种二元论的观点，正如希尔伯特所言：“我们必须知道，我们终将知道”。但哥德尔[7]跟科恩[8]证明了，连续统假设独立于ZFC[[3]](#footnote-3)，也就是说，我们既不能证明它正确，也不能证明它错误，于是我们证明了它的真假与否并不可知。

第一眼看去，这种独立性离我们似乎很远，在我们的日常生活中，对与错的确定性是那么的强烈，以致于对于任何“常见”的数学命题，大量证明带来的刻板印象会让我们觉得，它要么错误，要么正确。但是Shelah[5]对于Whitehead问题的证明说明，独立性就在我们的身边。Whitehead问题问的是：对于任何阿贝尔群，如果阿贝尔群的正合序列分裂，那么自由吗？看起来，这似乎只是抽象代数书本中的一道课后习题，但是Shelah的结果说明，这个问题独立于ZFC。这从侧面印证了，有很多东西，它既不真，也不假。而对于这些特殊的对象，我们可以假设它真，也可以假设它假，这是集合论的一个常见思路。

因此，超越二元论的物体是实实在在存在的，并且是可以被证明的，而不是那些虚无缥渺的、需要讨论的一些概念。

另外一点我想讨论的，是当今时代、当今社会对于“做得快、做得好”的追求，这等价于说是对更高生产力的追求。但这里有一个问题，对于任何问题，我们总是能找到更好的解决方法吗?

对于这个观点，我们首先可以考虑一个正则函数（normal function），它是单调递增的，即我们可以将它看作是我们生产力增长的一个函数。我们可以证明，任何一个正则函数都有一个不动点，即到某一点时，我们无法再利用它进行增长。

另一个例子与我们的生活更相近的例子是P对NP问题，它是克雷数学研究所高额悬赏的七个千禧年难题之一。在算法理论的发展过程中，我们会倾向于认为能够在多项式时间内能够被解决的问题是快的，记作P，而那些我们能够在多项式时间内验证答案的问题是慢，记作NP，这两个概念是如此广泛以致于很多基本的问题都与它们有关，例如以下的NP完全问题：

* 找到一个最符合一系列DNA片段的DNA序列[2]。
* 在一些特定环境中找到纳什均衡[3]。
* 判断一个数学陈述是否短的证明[4]。

显然P是属于NP的，那么一个自然的问题是，NP是否属于P，也就是说P是否等于NP。计算机科学家与数学家倾向于认为它们不相等，因为目前种种迹象表明它们不相等，只是我们还缺乏相应的技术去证明，但这要求我们去承认有一些问题是本质上困难的，我们并不能有效地解决它们。而如果它们相等，用Fortnow的话说，“互联网将会变成历史的脚注”[1]，首先与我们息息相关的公钥加密手段不再安全，但同时，我们能够快速地解决大多数的运筹学问题，举例来说，我们可以以最优的方式根据不同的条件安排各种运输手段（飞机，火车等），同时制造业也能够通过新的算法提高它们的工作效率，减少浪费。

以上的例子说明，虽然数学定理或是数学命题看起来与我们的生活很远，却能够确确实实地改变我们的观念，改变我们的思想，改变我们的生活。

1. 通过数学而进步

数学可以引领社会的发展吗？答案是肯定的，或者说是毋庸置疑的。

首先最重要的一点是，数学告诉我们，什么是可以做的，什么是不能做的，什么是我们能做得快的，什么是我们不可能做得快的，并且这些抽象的性质是可以被刻画并且是可以被证明出来的。在这一层面上，数学似乎是对人类能力的一种抽象，它刻画了我们能力的边界。比如，Hales[6]对Kepler猜想的证明说明，当你把同样的小球丢到一个箱子中，你最多只能装满约74%的区域。一个问题的下界一旦被证明，它的直接结果就是让我们放弃找到更好结果的可能性，而去进行更现实的研究。

同时，数学也会问，我们可以做得更好吗？更好意味着在某些问题上，我们可以得到更精确的结果，或是能够更快地得到想要的结果。无论如何，一旦我们这些问题与现实的联系，那么我们的现实就彻彻底底地改变了。

最后，数学的进步带来的是我们对于自然世界的更加清晰的认识，它反映的是时代的进步。这就像是一个对圆盘进行划分的过程，在每一步我们都进行某种划分，于是这个圆盘就被划分地越来越细了。

1. 参考文献

[1] Fortnow L. The status of the P versus NP problem[J]. Communications of the ACM, 2009, 52(9): 78-86.

[2] Gusfield D. Algorithms on stings, trees, and sequences: Computer science and computational biology[J]. Acm Sigact News, 1997, 28(4): 41-60.

[3] Conitzer V, Sandholm T. New complexity results about Nash equilibria[J]. Games and Economic Behavior, 2008, 63(2): 621-641.

[4] Cook S A. The complexity of theorem-proving procedures[C]//Proceedings of the third annual ACM symposium on Theory of computing. 1971: 151-158.

[5] Shelah S. Infinite abelian groups, Whitehead problem and some constructions[J]. Israel Journal of Mathematics, 1974, 18(3): 243-256.

[6] Hales T C. A proof of the Kepler conjecture[J]. Annals of mathematics, 2005, 162(3): 1065-1185.

[7] Gödel K. The consistency of the axiom of choice and of the generalized continuum-hypothesis[J]. Proceedings of the National Academy of Sciences of the United States of America, 1938, 24(12): 556.

[8] Cohen, P. The independence of the continuum hypothesis I[J]. Proceedings of the U.S. National Academy of Sciemces, 1963，50: 1143–48.

[9] Wilson E O. Consilience: The unity of knowledge[M]. Vintage, 1999.

1. 计算机与手机本质上没有什么区别，因此之后我们只会使用计算机来称呼这一系列类似的机器。 [↑](#footnote-ref-1)
2. 通俗的说就是一台计算机可以计算的函数，但是在数学中我们有更严谨的定义来刻画什么是可计算的，什么是不可计算的。 [↑](#footnote-ref-2)
3. ZFC是大多数人所使用的公理集合论，也是几乎所有的数学发生的地方。 [↑](#footnote-ref-3)