中国科学 : 数学　2021 年　第 51 卷　第 10 期 : 1461 ∼ 1462
SCIENTIA SINICA　Mathematica

冯克勤先生简介

冯克勤先生 1941 年 10 月 16 日出生于河北省宁河县 (今属天津). 1959 年从天津一中考入中国科学技术大学应用数学和计算技术系, 1962 年大三下学期进入华罗庚先生开设的数论和代数专门化, 1964 年成为华罗庚先生的研究生, 研究方向是数论. 1968 年研究生毕业后分配到太原钢铁公司工作, 1973 年调回中国科学技术大学数学系任教, 期间参加了曾肯成先生领导的代数编码和密码学研究小组. 1979–1981 年分别在威斯康星大学、马里兰大学和普林斯顿大学访问学习代数数论. 之后他同万哲先先生在北京组织密码和编码讨论班以及代数数论讨论班, 为通信和国防事业服务. 这些经历成为他一生研究代数数论、代数编码和密码学的最重要契机. 1985 年起被中国科学技术大学聘为教授, 1986 年成为博士生导师. 1988–1993 年担任数学系主任, 1993–2000 年担任中国科学技术大学副校长, 其中 1996–2000 年兼任中国科学技术大学研究生院 (北京) 常务副院长, 1998–1999 年兼任中国科学院信息安全国家重点实验室主任. 2000 年调入清华大学数学科学系, 并于 2000–2003 年担任系主任.

冯克勤先生曾任国务院学位委员会学科评议组成员, 国家教委高校教育指导委员会副主任和工科数学教育指导分委员会主任, 中国数学会常务理事, 2002 年国际数学家大会组织委员会成员. 冯克勤先生曾任南开大学陈省身数学研究所、中国科学院晨兴数学中心、北京大学北京国际数学研究中心、中国科学院信息安全国家重点实验室等重要学术机构学术委员会和指导委员会委员, 是 2003–2006 年清华大学与法国巴黎十一大算术代数几何合作项目的中方负责人, 曾任《中国科学》《科学通报》《数学学报》《数学年刊》《代数集刊》和 International Journal of Number Theory 等学术期刊编委.

冯克勤先生的学术研究非常宽泛, 他的主要成果集中在分圆单位的独立性研究、同余数的研究、图论及其在数论上的应用、量子纠错码和量子信息数学理论、具有密码学性质的布尔函数等方面.

20 世纪 70 年代, 在华罗庚先生和王元先生的指导下, 裴定一先生和冯克勤先生开始研究分圆单位独立性, 计算出分圆单位群的秩. 冯克勤先生将结果推广到了任意阿贝尔域情形, 后来又进一步移植到函数域情形. 这些工作, 是我国学者在国内完成的代数数论领域最早的一些研究工作, 被收入 Washington 著名教材 Introduction to Cyclotomic Fields (GTM 82) 和 Narkiewicz 的专著 The Story of Algebraic Numbers in the First Half of the 20th Century (Springer 2019). 同期, 他在组合设计和图论领域发表了多篇重要研究文章, 特别是 1979 年与李乔在《应用数学学报》发表的中文论文《论图的最大特征根》, 是代数图论研究领域十分重要的文献, 仅 2001 年后的 SCI 他引就有近百次. 冯克勤和李文卿 1996 年的论文 “Spectra of hypergraphs and applications” 研究超图伴随矩阵特征值, 是 Ramanujan 双图重要研究文献, 被 Marcus-Spielman-Srivastava 2015 年 Annals of Mathematics 文章、Valette 1996/97 年 Bourbaki 报告和 Finite Fields (Shparlinski 1999)、Spectral Graph Theory (Chung-Graham 1997)、Discrete Groups, Expanding Graphs and Invariant Measures (Lubotzky 2010)、Handbook of Finite Fields (Mullen-Panario 2013) 和 Mathematical Methods in Electromagnetism: Linear Theory and Applications (Michel 1996) 等著名专著引用. 自 20 世纪 90 年代开始, 冯克勤开创性地利用图论方法研究同余数问题, 独立并与合作者一起决定了多个系列的非同余数, 并验证对应的椭圆曲线 BSD 猜想成立. 他的方法激发了国内学者对于同余数和椭圆曲线的深入研究, 最终发展到田野在同余数问题上国际瞩目的突破性工作.

1995 年以前, 人们普遍认为解决量子通信的纠错问题比数字通信要困难得多. 1995 年 Sloane 和 Shor 构造了第一个量子纠错码, 由此, 国际上有关学者发展构造量子纠错码的第一个有效方法: 加性码方法. 冯克勤先生在国内率先开始量子码研究, 给出量子码的完全不同刻画. 由此他和林杉、邢朝平等首先给出了一类非加性码的构造, 其性能比加性码更优. 这一刻画还可以将经典编码中的代数几何码的许多结果应用到量子编码中, 得到大量新的量子码. 这个结果的出现, 令国际同行备感意外, 将国际量子码的研究向前大大地推进了一步. 除量子编码工作外, 冯克勤等还利用数学理论系统地构造了多系统纠缠态, 而在此前国际上只有几个零星的例子.

布尔函数被用来构造流密码的密钥, 是流密码研究最基础最核心的内容. 为了抵抗不断发展的攻击方式, 布尔函数需要具有良好的统计相关性、大的非线性度和大的代数免疫度等. 满足这些性质的布尔函数的构造是密码学一个挑战性问题. 2008 年以前人们没有找到同时具有理想的非线性度和代数免疫度的布尔函数. 2008 年 Carlet 和冯克勤在密码学三大顶级会议之一的亚密会上给出了这样的函数, 这是密码学领域的突破性进展, 该类函数也被称为 Carlet-Feng 函数. 著名密码学家 Mesnager 在专著 Bent Functions (Springer 2016) 第二章详细介绍了 Carlet-Feng 的结果, 美国数学会 Math Review 在 “Feature Review” 中用大量篇幅也介绍了这一成果.

由于冯克勤先生在代数数论、代数编码理论、组合学与图论、密码学和信息安全及量子通信等方面取得的多项重大研究成果, 他获得了一系列荣誉: 1988 年获中国科学院科技进步奖二等奖, 1989 年获国家自然科学三等奖, 1990/91 年获陈省身数学奖, 1991 年被评为国家教育委员会全国教育系统劳动模范, 1992 年被评为中国科学院有突出贡献的中青年专家.

在潜心学术研究的同时, 冯克勤先生还积极投身于知识的普及和传播, 先后撰写专著 2 本, 编写数学教材 9 种, 译书 4 部, 撰写普及读物 7 部, 其中教材《近世代数》(与李尚志、查建国合著)、《交换代数》和《代数数论》等在国内深受学生好评. 主编的丛书《走向数学》(湖南教育出版社) 获 1992 年中国图书评论学会二等奖, 协助主编的丛书《中学生数学视野》(湖南教育出版社) 获 2001 年中国教育学会特等奖.

除此之外, 冯克勤先生还非常注重人才培养, 在数论、算术几何、密码和编码等领域共培养硕士 23 人、博士 17 人、博士后若干, 多名学生都是相关领域的中坚力量. 作为 2003 年设立的清华大学与法国科学院 Fontaine 院士合作培养高水平学生项目的中方负责人, 他领导的项目培养出了多位新一代青年数论、代数和代数几何学家. 多年来他还负责组织南开代数几何年、中法算术几何和自守表示暑期班和国际会议、全国数论 (和代数几何) 会议、有限域及其应用国际会议、组合学编码和密码国际会议、中韩编码会议等, 为促进国内数论、编码和密码学界的交流、加强和国际同行的密切联系作出了卓越贡献. 退休以后, 他仍然每年奔波各地, 为全国组合、编码和密码研究生暑期学校、西部地区教育进修班等授课, 与年轻人一起合作研究, 指导和帮助年轻学者尽快走上高水平的学术研究道路.

冯克勤先生是中国代数数论和算术代数几何研究的开拓者, 是近 30 年来我国代数数论和数论应用研究的主要领导人之一, 在代数数论、代数编码理论、组合学与图论、密码学和信息安全、量子通信等方面均取得了多项重大研究成果. 他一生勤勉耕耘, 发表论文 140 余篇. 年逾古稀后仍保持论文的高产高质, 发表论文近 40 篇, 且大多发表在专业顶级学术期刊上. 2019 年接连荣获中国数学会华罗庚数学奖、中国密码学会杰出贡献奖和中国电子学会信息论分会信息论终身成就奖.

在冯克勤先生 80 华诞之际, 我们特组织此专辑表达对冯先生崇高的敬意和真诚的祝福, 衷心祝愿冯先生平安、健康、快乐、长寿!

葛力明、欧阳毅、田野、邢朝平、徐飞