

陕西省自然科学奖提名公示材料

(2025年度)

一、项目基本情况

项目名称	代数和数论在编码和图论中的应用
主要完成人	衡子灵 周正春 王维琼 刘奋进
主要完成单位	长安大学 西南交通大学

二、提名意见（适用于提名单位）

提 名 者	陕西省教育厅	提名等级	<input type="checkbox"/> 一等奖 <input checked="" type="checkbox"/> 二等奖
<p>提名意见：</p> <p>项目《代数和数论在编码和图论中的应用》主要利用代数和数论等工具研究了编码和图论中的若干前沿科学问题。主要科学发现点包括：解决了几类混合型特征和的计算难题，并应用于序列编码设计；建立了判定线性码为极小码的充要条件；构造出传输效率高于扩展汉明码的最优二元线性码；建立了子域码基本理论并构造了一批高性能子域码；首次构造出了具有不可约特征多项式的几个无穷图类。这些原创性成果解决了编码和图论领域多个关键性问题，有力推动了代数学、图论和信息科学的交叉融合发展，在通信、压缩感知、密码学和计算机存储等领域有重要的潜在应用价值。代表性成果发表在《Journal of Algebra》、《IEEE Transactions on Information Theory》、《Finite Fields and Their Applications》、《Linear Algebra and its Applications》等国际重要期刊上。这些成果被国内外多名同行专家正面引用和高度评价，包括国际 George Boole 奖获得者、法国巴黎八大教授 Sihem Mesnager，立陶宛科学院院士、维尔纽斯大学首席研究员 Arturas Dubickas 等。经审查，该项目满足陕西省自然科学奖授奖条件。</p> <p>提名该项目为陕西省自然科学奖二等奖。</p> <p>说明：省科学技术奖一、二等奖项目，实行按等级标准提名、独立评审表决的机制。提名单者应严格依据省科学技术奖的标准条件，说明提名项目的贡献程度及等级建议。“提名一等奖”评审落选项目不再降格参评二等奖。项目组与提名单位沟通后，做出提名等级意见；提名项目提交后，提名等级建议不得变更。</p>			

三、项目简介

(一) 研究背景

编码与图论作为离散数学的核心分支，均以离散结构为研究对象，共享群、环、域等代数工具和组合计数方法。二者在信息科学中通过多种方式深度融合，共同推动了通信、数据存储和算法设计等领域的发展。随着下一代通信技术、人工智能、量子计算等新兴领域的快速发展，人类社会对信息传输可靠性、系统运行效率及复杂问题求解能力提出更高要求。在此背景下，高性能编码与图论研究具有重要的理论价值与应用前景，对于推动数学和信息科学的交叉融合发展有重要意义。为此，本项目主要基于代数和数论等工具深入研究了编码和图论中若干前沿科学问题。

(二) 主要研究内容

研究内容 1：混合型特征和及其在序列编码中的应用

混合型特征和是有限域上高斯和的推广，研究这类特征和的值有重要的理论和应用价值。20 世纪著名数学家 André Weil 在 1948 年给出了著名的 Weil 界。2014 年，挪威科学院院士 Tor Helleseth 等在顶级期刊 IEEE TIT 论文中计算了一类特殊混合型特征和的值。基于此，本项目将 Tor Helleseth 院士等论文中的混合型特征和推广到一般情形，研究了它们的精确值或模，并应用这些结果构造出了低相关序列编码。

研究内容 2：极小线性码的判定条件与构造

秘密共享是一种将秘密分割存储的密码技术，它是信息安全和数据保密中的重要手段。极小线性码可用于构造安全高效的秘密共享方案。1998 年，IEEE 会士 Alexei Ashikhmin 和 IEEE 会士 Alexander Barg 给出了“判定一个 q 元线性码是极小码”的充分但非必要条件。为此，本项目深入研究了“判定一个 q 元线性码为极小码”的充要条件，并应用该充要条件构造了若干类不满足 Ashikhmin-Barg 充分条件的极小码。

研究内容 3：高性能最优二元线性码的构造

二进制是现代通信中最常用的纠错码。构造最优二进制码是通信理论中的重要科学问题。1950 年，图灵奖获得者 R. W. Hamming 给出了历史上第一个纠错码，即二元汉明码。2004 年，加拿大工程院院士 N. C. Beaulieu 研究了扩展二元汉明码，并证明了扩展二元汉明码是达到汉明界的最优码。构造性能更好的二进制码是编码理论中的重要问题。为此，本项目基于有限几何和代数方法构造了两类高性能最优二进制码。

研究内容 4：子域码理论与高性能子域码参数研究

子域码是利用已知小维数码构造新的大维数线性码的重要方法。1998 年，国际密码研究协会 Fellow、法国巴黎八大教授 C. Carlet 等人在著名期刊 DCC 中研究了一类特殊线性码的子域码。然而，Carlet 等人没有系统研究子域码。为此，本项目系统建立了子域码基本理论并研究了若干类小维数线性码的子域码参数。

研究内容 5：具有不可约特征多项式的无穷图类构造

不可约多项式在数论、编码和密码学中有广泛应用。图特征多项式的不可约性与图的对称性、网络重构性及可控性密切相关。尽管已有研究指出大多数图的特征多项式是不可约的，但文献中尚无系统的方法来构造具有不可约特征多项式的图。为此，

本项目首次给出了具有不可约特征多项式的无穷图类的构造方法。

(三) 科学发现点与科学价值

本项目基于代数、数论等工具深入研究了上述内容，科学发现点和科学价值如下：

科学发现点 1：解决了几类混合型特征和的计算难题，并应用于序列编码设计

基于高斯和、傅里叶变换等工具研究了有限域上几类混合型特征和的精确值或模，并应用它们构造了新的渐近最优部分 Hadamard 码本，成果发表在代数学顶级期刊 Journal of Algebra 上。该成果把 Tor Helleseth 院士等的研究成果从特殊函数的情形推广到一般的弱正则 bent 函数以及扩域上二次函数的情形。此外，这几类混合型特征和可广泛应用于高性能编码和信号设计中。

科学发现点 2：建立了极小码判定的充要条件并构造了新参数极小码

建立了 q 元极小码判定的充分必要条件，并首次构造出了不满足 Ashikhmin-Barg 充分条件的非二元极小码，解决了这个有 20 年历史的重要问题，为构造新参数极小线性码以及秘密共享方案提供了重要理论基础，带动了大批学者研究极小码。该成果弥补了 IEEE 会士 Ashikhmin 和 IEEE 会士 Barg 给出的“Ashikhmin-Barg 条件”不满足必要性的缺陷。相关成果发表在顶级期刊 IEEE TIT 和权威期刊 FFA 上。

科学发现点 3：构造出传输效率高于扩展汉明码的最优二元线性码

基于有限几何工具和子域码理论在顶级期刊 IEEE TIT 论文中构造了两类新的最优二元码，其中一类的传输效率比扩展二元汉明码码率更高且它们的纠错能力相同，且该成果建立了最大弧和最优码之间的深刻联系。因二元线性码的电路实现简单，故我们构造的最优二元码有重要的潜在应用价值。

科学发现点 4：建立了子域码基本理论并构造了一批高性能子域码

建立了有限域上子域码的基本理论，包括其生成矩阵、迹表示、对偶码等。深入研究了一类 $[q+1, 2, q]$ MDS 码和若干类有限几何码的子域码。这些子域码有较大的维数和很强的纠错能力，弥补了原码维数太小的缺陷，并得到了一批新参数最优码。相关成果发表在信息理论顶级期刊 IEEE TIT 和权威期刊 FFA 上。

科学发现点 5：首次构造出了具有不可约特征多项式的几个无穷图类

基于 Eisenstein 判别法和域扩张理论，首次提出三种具有不可约特征多项式的无穷图类的构造方法。三种方法覆盖不同图结构，为后续研究提供多样化实例，建立了图的结构性质与多项式代数性质的直接关联。成果发表在线性代数权威期刊 LAA 上。

(四) 发表论文、同行引用及评价

本项目发表论文 53 篇 (SCI 论文 43 篇)，包括代数学顶级期刊 JA 论文 1 篇、CCF 推荐 A 类期刊 IEEE TIT 论文 6 篇、代数编码权威期刊 DCC 和 FFA 论文共 10 篇、代数组合权威期刊 JAC 论文 1 篇、线性代数权威期刊 LAA 论文 6 篇、离散数学权威期刊 DM 论文 4 篇。5 篇代表性论文他引 113 次，1 篇入选 ESI 高被引，正面评价这些成果的专家包括 George Boole 奖获得者、巴黎八大教授 Sihem Mesnager，立陶宛科学院院士、维尔纽斯大学首席研究员 Artūras Dubickas，IEEE Fellow、西南交通大学教授唐小虎，暨南大学教授陈豪，浙江大学教授冯涛等。

四、客观评价

根据 WOS 核心合集统计结果, 5 篇代表性论文被他引 113 次, 1 篇论文入选 ESI 前 1%高被引论文。多位著名专家在顶级期刊或知名数学文摘期刊高度评价我们的成果。

(一) 科学发现点 1 的客观评价:

- 国际组合及其应用协会 Kirkman 奖获得者、DCC 编委、浙江大学教授冯涛在《Mathematical Reviews》(MR4633696) 中评价如下: “The proofs are technical and involve complicated calculations using Gauss sums. The authors then present five constructions of partial Hadamard codebooks with alphabet size p , which generalize the results in [S. Hong et al., IEEE Trans. Inform. Theory 60 (2014), no. 6, 3698 - 3705; MR3215336]. ...Those codebooks have applications in the construction of deterministic sensing matrices with small coherence.”
- 印度泰兹普尔大学教授 Dhiren Kumar Basnet 在《Zentralblatt MATH》(Zbl 07741950) 中正面评论了本成果。评论如下: “...In this article, the absolute values or explicit values of them are determined under certain conditions with the help of Gaussian sums.... the constructed codebooks are equivalent to nearly equiangular tight frames and have nice application in compressed sensing matrices.”

(二) 科学发现点 2 的客观评价:

代表性论文 2 被他引 77 次, 入选 ESI 前 1%高被引论文。代表性评价如下:

- 第一届国际 George Boole 奖获得者、IEEE 信息论法国分会主席、法国巴黎八大教授 Sihem Mesnager 及其合作者在代表性引文 1 中评价如下: “Ding, Heng, and Zhou presented a necessary and sufficient condition for linear codes over finite fields to be minimal. These significant advances motivated several authors to investigate constructions of minimal codes further satisfying the new condition and particularly to violate the Ashikhmin-Barg condition.”
- 国际组合及其应用协会 Kirkman 奖获得者、浙江大学教授冯涛及其合作者在代表性引文 2 中肯定我们的成果如下: “A sufficient and necessary condition was given by Heng et al.”。
- 保加利亚科学院的 N. L. Manev 在《Mathematical Reviews》(MR3857591) 也肯定了该成果, 评论如下: “In this paper a sufficient and necessary condition for a linear code over a finite field to be minimal is proved.”

(三) 科学发现点 3 的客观评价:

- 菲律宾大学迪里曼分校 Romar dela Cruz 教授在《Mathematical Reviews》(MR4158620) 中评论如下: “This work presents two new classes of binary linear codes whose minimum distances are optimal with respect to the sphere-packing bound.... It is shown in the paper that these codes have better information

rates than the extended binary Hamming codes.”

- IEEE Fellow、西南交通大学教授唐小虎及其合作者在代表性引文 3 中评论如下：
“Some linear codes with good parameters have been constructed by using different mathematical objects such as cryptographic functions [9], [10], [12], [22], [36], [42], [43], [53], combinatorial t-designs [10], [15], (almost) difference sets [7], [19], [52], simplicial complexes (also called down-sets) [6], [24], [26], [48], [49], posets [25] and maximal arcs [20].”
（[20]即为代表作 3）
- 我国著名教授屈龙江及其合作者在代表性引文 4 中对其评论如下：“Recently, Heng, Ding and Wang [24] considered the binary subfield code of C D and obtained a class of distance-optimal binary codes.”
- 暨南大学教授陈豪及其合作者在代表性引文 5 中正面引用了该成果，具体如下：
“Distance-optimal codes with minimum distance four and six were constructed in [9], [13], [14], and [29]. There are only few distance-optimal codes with minimum distance six reported in the literature, see [13], [28, Theorem 9] and [2, Corollary 5].”（这里[13]即为代表作 3）

（四）科学发现点 4 的客观评价：

- 国际 George Boole 奖获得者、IEEE 信息论法国分会主席、法国巴黎八大 Sihem Mesnager 教授及其合作者在代表性引文 6 中肯定了我们在子域码方面的贡献，评论如下：“The subfield codes of some optimal codes or very good codes over F_{q^m} have been studied in several references, for example ... and maximum distance separable (MDS) codes in [31], [32], [33], and [51]. Most of the resultant subfield codes have good parameters and few weights”。
- 韩国建国大学著名教授 Jong Yoon Hyun 及其合作者在代表性引文 7 中评价如下：
“In [15], Ding and Heng constructed several families of optimal trace codes from $[q+1, 2, q]_q$, which are both MDS codes and simplex codes.”

（五）科学发现点 5 的客观评价：

- 立陶宛科学院院士、维尔纽斯大学首席研究员 Artūras Dubickas 在组合数学顶级期刊《Combinatorica》中肯定了代表性论文 5 在图的特征值方面的贡献，具体评论如下：“The eigenvalues of a graph contain important information about the properties of the graph itself; see [2 - 4, 10] for some basic information on this and, e. g., [9, 12 - 14] for some recent work”。
- 法国里昂大学教授 Fabien Vignes-Tourneret 在《Zentralblatt MATH》(Zbl 1479.05166)中评论如下：“This article proposes three methods of construction of families of graphs with irreducible characteristic polynomials over Q ”。

五、代表性论文专著目录
(不超过 8 条, 其中代表性论文不超过 5 篇, 代表性专著不超过 3 部)

序号	论文专著名称	刊名	作者	年卷 页码 (xx 年 xx 卷 xx 页)	发表时间 (年月日)	通讯作者 (含共同)	第一作者 (含共同)	国内作者	他引总次数	检索数据库	知识产权是否归国内所有
1	Hybrid character sums and near-optimal partial Hadamard codebooks	Journal of Algebra	Ziling Heng, Fuling Chen	2023 年 634 卷 790-831 页	2023 年 06 月 17 日	Ziling Heng	Ziling Heng	衡子灵, 陈辅灵	0	SCI	是
2	Minimal linear codes over finite fields	Finite Fields and Their Applications	Ziling Heng, Cunsheng Ding, Zhengchun Zhou	2018 年 54 卷 176-196 页	2018 年 08 月 23 日	Zhen gchu n Zhou	Ziling Heng	衡子灵, 丁存生, 周正春	77	SCI	是
3	Optimal binary linear codes from maximal arcs	IEEE Transactions on Information Theory	Ziling Heng, Cunsheng Ding, Weiqiong Wang	2020 年 66 卷 5387-5394 页	2020 年 08 月 18 日		Ziling Heng	衡子灵, 丁存生, 王维琼	22	SCI	是
4	The Subfield Codes of Some $[q+1, 2, q]$ MDS Codes	IEEE Transactions on Information Theory	Ziling Heng, Cunsheng Ding	2022 年 68 卷 3643-3656 页	2022 年 05 月 20 日	Ziling Heng	Ziling Heng	衡子灵, 丁存生	12	SCI	是
5	Note on graphs with irreducible characteristic polynomials	Linear Algebra and its Applications	Qian Yu, Fenjin Liu, Hao Zhang, Ziling Heng	2021 年 629 卷 72-86 页	2021 年 07 月 24 日	Fenjin Liu	Qian Yu	于倩, 刘奋进, 张浩, 衡子灵	2	SCI	是
合 计									113		
补充说明(视情填写): 代表性论文 3 中没有标注通讯作者。											

按照指南要求填写(P34)。

六、主要完成人情况表

姓 名	衡子灵	排 名	1
行政职务	无		
技术职称	教授		
工作单位	长安大学		
完成单位	长安大学		
对本项目主要学术贡献： 衡子灵对本项目所列的科学发现点 1，2，3，4，5 等五项科学发现均作出了重要贡献，包括混合型特征和的计算及其在序列编码中的应用、判定线性码为极小码充要条件的证明和极小码的构造、基于最大弧的最优码的参数研究、MDS 码子域码参数的研究以及不可约多项式在图论中的应用等。衡子灵是代表作 1-4 的第一作者、代表作 5 的第四作者。			

姓 名	周正春	排 名	2
行政职务	西南交通大学信息科学与技术学院副院长		
技术职称	教授		
工作单位	西南交通大学		
完成单位	西南交通大学		
对本项目主要学术贡献： 周正春是科学发现点 2 的主要完成人之一，对提出判定 q 元线性码为极小码的充要条件作出了重要贡献，是代表性论文 2 研究思路的提出者之一。他是代表性论文 2 的通讯作者。			

姓 名	王维琼	排 名	3
行政职务	无		
技术职称	教授		
工作单位	长安大学		

完成单位	长安大学
<p>对本项目主要学术贡献：</p> <p>王维琼是科学发现点 3 的重要参与者，对该发现点中第一类最优码参数的计算提供了思路。她是代表性论文 3 的作者之一。</p>	

姓 名	刘奋进	排 名	4
行政职务	长安大学理学院统计系系主任		
技术职称	副教授		
工作单位	长安大学		
完成单位	长安大学		
对本项目主要学术贡献： 刘奋进是科学发现点 5 的主要完成人，提出了三种具有不可约特征多项式无穷图类的构造方法，是该发现点主要研究思路的提出者。他是代表性论文 5 的通讯作者。			

七、主要完成单位情况表

单位名称	长安大学
对本项目主要学术贡献： 长安大学是代表性论文 1-5 的第一单位，即为科学发现点 1-5 的主要完成单位。	

单位名称	西南交通大学
对本项目主要学术贡献： 西南交通大学是代表性论文 2 的通讯单位，为科学发现点 2 的主要完成单位之一。	

八、完成人合作关系说明

- 衡子灵和周正春在代表性论文 2 中合作研究了判定线性码为极小码的充要条件和极小码的构造；
- 衡子灵和王维琼在代表性论文 3 中合作研究了基于最大弧的两类最优二源码构造；
- 刘奋进和衡子灵在代表性论文 5 中合作研究了具有不可约特征多项式的几个无穷图类；
- 衡子灵、王维琼、刘奋进共同获得了 2025 年陕西高等学校科学技术研究优秀成果二等奖。

完成人合作关系情况汇总表

序号	合作方式	合作者/项目排名	合作起始时间	合作完成时间	合作成果	证明材料
1	论文合著	衡子灵(1), 周正春(2)	2017 年 8 月	2018 年 8 月	合作代表性论文 2 《Minimal linear codes over finite fields》	代表性论文 2
2	论文合著	衡子灵(1), 王维琼(3)	2019 年 1 月	2020 年 1 月	合作代表性论文 3 《Optimal Binary Linear Codes From Maximal Arcs》	代表性论文 3
3	论文合著	衡子灵(1), 刘奋进(4)	2020 年 7 月	2021 年 7 月	合作代表性论文 5 《Note on graphs with irreducible characteristic polynomials》	代表性论文 5
4	共同获奖	衡子灵(1), 王维琼(3), 刘奋进(4)	2013 年 1 月	2025 年 7 月	共同获得 2025 年陕西高等学校科学技术研究优秀成果二等奖	获奖证书

