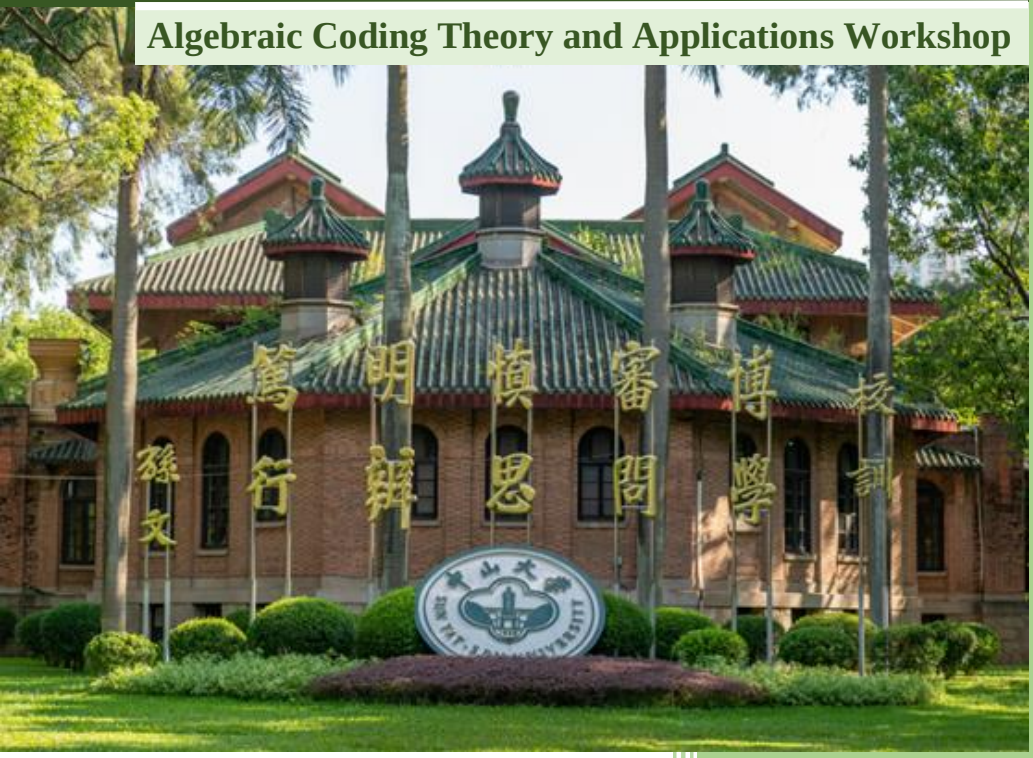
2023

代数编译码理论与应用前沿沙龙

Algebraic Coding Theory and Applications Workshop

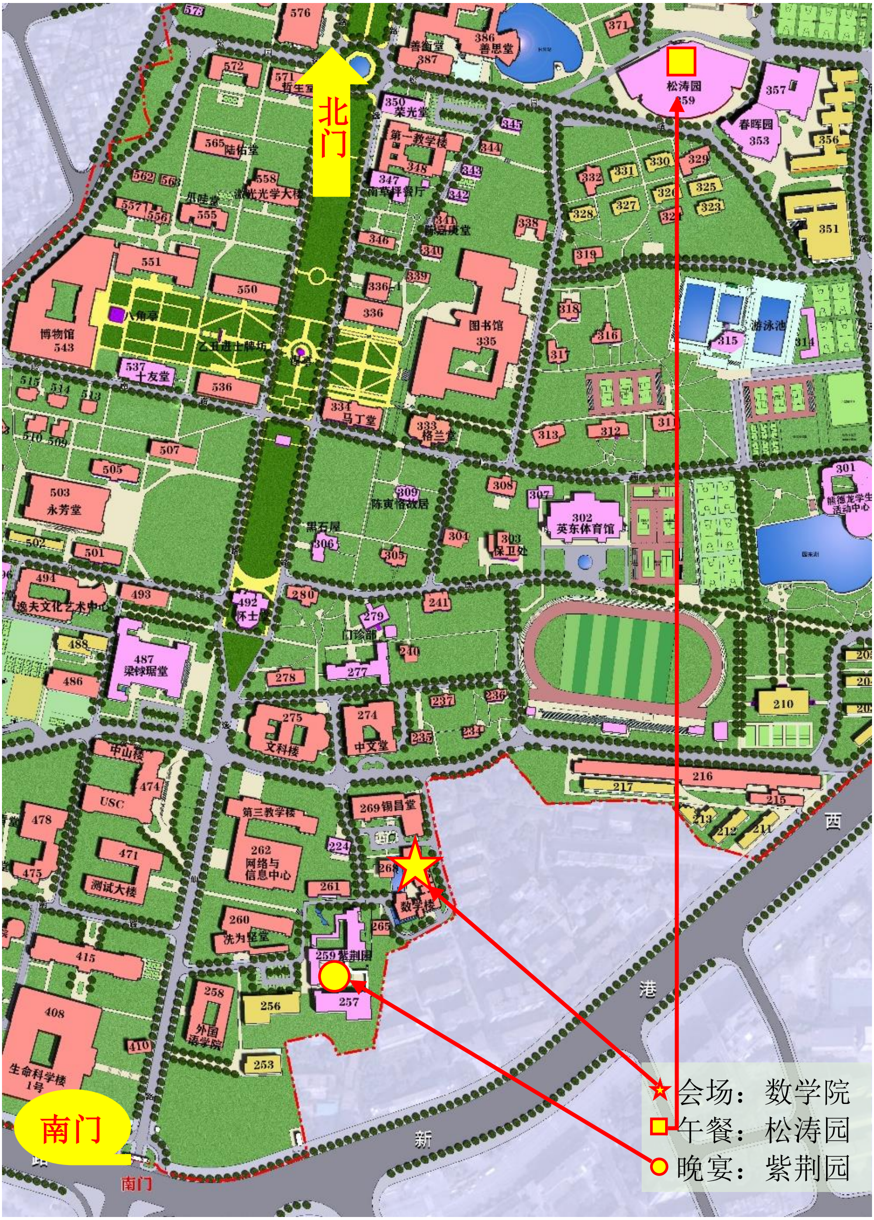


中山大学 • 中国广州

2023 年 8 月 13 日

Guangzhou Chapter

交通指引


北门
南门
松涛园
359
数学楼
259紫荆园
图书馆
335
英东体育馆
302
游泳池
博物馆
543
中山楼
测试大楼
文科楼
中文堂
269锡昌堂
第三教学楼
262
网络与
信息中心
260
冼为坚堂
外国
语学院
生命科学楼
1号
会场：数学院
午餐：松涛园
晚宴：紫荆园

会议议程

举办日期：2023 年8 月13 日，全天
会议地点：广东省广州市海珠区新港西路135号中山大学
数学院2楼多功能厅
主办单位：中山大学电子与信息工程学院
IEEE 信息论学会广州分会
会议主题：代数编译码理论与应用前沿沙龙

日程安排：

日期	时间	报告者	报告主题
上午	08:30-08:35	陈立 教授	开场
	08:35-09:25	吴英全 博士	A novel Chase Kötter -Vardy algorithm
	09:25-10:15	沈八中 教授	用人工智能技术做最大似然译码的探讨
	10:15-10:45	茶歇	合影
	10:45-11:35	邢朝平 教授	Fast Fourier transform via automorphism groups of rational function fields
	11:35-12:25	陈立 教授	Low-latency OSD of BCH codes
中午	12:30-14:30	所有人	午餐，午休
下午	14:30-15:20	张华滋 博士	New algebraic properties of polar codes
	15:20-16:10	邢炯跃 博士	Shift-sum decoding of cyclic codes
	16:10-16:40	茶歇	
	16:40-17:30	万韫琦 博士	The re-encoding transform in algebraic list decoding of algebraic-geometric codes
	17:30-18:15	受邀者	圆桌论坛
晚上	18:30-20:00	所有人	晚宴

吴英全 博士

个人简介：吴英全博士2004年毕业于美国伊利诺伊大学香槟分校电子工程专业，之后一直在硅谷从事芯片算法设计，发表过20多篇国际期刊论文并拥有40多个专利，涉及计算代数、编码理论、信号处理、数据压缩、人工智能、超大规模集成电路设计等领域。2013年吴博士和Mike Lee合伙成立了硅谷初创公司Tidal Systems，致力于开发新一代闪存控制芯片，于2015年以1.7亿美元被美光科技 (Micron) 收购。吴博士现为初创芯片设计公司Tenafe首席科学家(2018年11月创立，最新估值4亿美元)。

报告题目：A novel Chase Kötter-Vardy algorithm

报告时间：上午 8:35 – 9:25

报告摘要：In this paper, we first formulate a novel Chase Guruswami-Sudan algorithm which list corrects not only all errors among the Chase flipping symbols but also the number of errors up to the enhanced Johnson bound among remaining positions, for Reed-Solomon and q-ary BCH codes. The enhanced Johnson bound is induced by shortening the code

without those Chase flipping symbols. We next devise a novel Chase Kötter-Vardy algorithm for soft decision decoding of Reed-Solomon codes. We show that the a posteriori probabilities of two branches of one of the least unreliable symbols which undergo Chase flipping shall be merged and assigned to the correct branch out of the two (it does not matter anyway if neither is correct), based on the rationale that one of exhaustive Chase flipping patterns must hit the genie pattern among the flipped symbols. During the exhaustive trial-and-error Chase decoding, each flipping pattern is treated as the genie and thus the associated branches of each flipping symbol are assigned with the merged a posteriori probabilities while its alternative branch is amortized. The multiplicity matrix is constructed using the state-of-the-art Kötter-Vardy transformation. We show by both theoretical analysis and simulations that the proposed Chase Kötter-Vardy algorithm significantly outperforms the original Kötter-Vardy algorithm under a similar complexity. We then extend this approach to a coded Chase scheme wherein the Chase pattern set comes from a covering code. We also employ a novel preprocessing technique that enforces a zero constant term for the message polynomial, by equivalently sacrificing one parity symbol. It effectively eradicates spurious candidate bivariate polynomials by merely computing and checking their constant terms, and thus dramatically reduces the number of candidate bivariate polynomials that are actually interpolated and factorized.

沈八中 教授

个人简介：沈八中，国家特聘专家、教授，博士生导师。2017年至2020年12月任西安电子科技大学通信工程学院院长、2020年至2022年任西安电子科技大学广州研究院执行院长。2018年起担任陕西省区块链与安全计算重点实验室主任。2021年任中国通信学会工业互联网委员会委员。2022年任中国工业与应用数学学会企业合作与工业应用委员会委员。2022年任粤港澳元宇宙智库副主任。2022年被聘为全国高校人工智能大数据创新联盟元宇宙专业委员会副主任，并授予2022赋能中国元宇宙创新人物榜“元宇宙30人”。

沈八中长期从事通信领域中的信息论，信道编码，信源编码和调制理论等方面的研究和应用工作。除了在国际著名的期刊和会议上发表论文二十余篇外，他已拥有195项已发行的美国专利。沈八中博士参与制定了众多的世界标准的制定，其中包括 IEEE802，3GPP，ITU，MoCA和MPEG。他所研发设计的各类不同的通信和编码系统进入了7个国际标准，沈八中参与了世界第一片具有高阶调制及TURBO编码技术的卫星电视机顶盒芯片,其中他主持设计了TURBO码，并开

发了高速有效的硬件和软件译码技术。

沈八中目前所关心的研究方向基于现代数学的非线性通信数学理论、5G/6G无线通信和他们的垂直领域、工业互联网、信息通信网络的技术和算法、网联无人驾驶车、和财政和行政人工智能管理暨区块链、元宇宙等。

报告题目：用人工智能技术做最大似然译码的探讨

报告时间：上午 9:25 – 10:15

报告摘要：信息通信发展到今天，它的系统对信道编码 (纠错码) 的依赖性越来越迫切。为了达到未来通信的大流量、低时延、高可靠的需求，中短码长的经典纠错码，如BCH码，可能会发挥决定性的作用。但是到今天为止经典纠错码的“致命”伤是他们的软判决最大似然译码 (MLD)。自2016年起人们开始用人工智能技术来做MLD。这是否是经典纠错码在信息通信中最后的出路？我们的报告将对已经在这方面做的工作进行简单的综述和分析。然后我们将和大家一起探讨是否能用当今正红的具有创造性的“生成式人工智能”来帮助我们达到最大似然译码的结果。我们的观点是，1) 生成式人工智能的联合概率模型会非常适合纠错码的译码模型；2) 对自然语言处理 (NLP) 中序列的解决方案“自注意力”可能会帮助我们解决码字的单个元素到它所在的整个码字序列的译码关系 (这里，有序统计译码 (OSD) 与它有相似之处)。

邢朝平 教授

个人简介：邢朝平，上海交通大学讲席教授，中组部国家特聘教授。1990年在中国科学技术大学获得博士学位后留校工作，1993年获德国洪堡奖学金在Essen大学工作，其后在奥地利科学院从事研究工作。1998年加入新加坡国立大学，历任助教、终身副教授、教授。2007年始任职于新加坡南洋理工大学教授。2019年加盟上海交通大学。长期从事密码、编码、安全多方计算、代数数论等方面的研究。

报告题目：Fast Fourier Transform via automorphism groups of rational function fields

报告时间：上午 10:45 - 11:35

报告摘要：The Fast Fourier Transform (FFT) over a finite field $\mathbb{F}_q$ computes evaluations of a given polynomial of degree less than n at a specifically chosen set of n distinct evaluation points in $\mathbb{F}_q$. If q or q - 1 is a smooth number, then the divide-and-conquer approach leads to the fastest known FFT algorithms.

Depending on the type of group that the set of evaluation points forms, these algorithms are classified as multiplicative (Math of Comp. 1965) and additive (FOCS 2014) FFT algorithms. In this talk, we provide a unified framework for FFT algorithms that include both multiplicative and additive FFT algorithms as special cases, and beyond: our framework also works when $q + 1$ is smooth, while all known results require q or $q - 1$ to be smooth. For the new case where $q + 1$ is smooth (this new case was not considered before in literature as far as we know), we show that if n is a divisor of $q + 1$ that is smooth for a real $B > 0$, then our FFT needs $O(n \cdot \log n)$ arithmetic operations in $\mathbb{F}_q$. Our unified framework is a natural consequence of introducing the algebraic function fields into the study of FFT.

陈立 教授

个人介绍：陈立，中山大学电子与信息工程学院教授、博导，IEEE信息论学会广州分会主席，IEEE信息论学会理事会理事、会议委员会主席，中国电子学会信息论分会委员，中国通信学会青年工作委员会和通信理论与信号处理委员会委员，IEEE TCOM副主编等。陈立教授2008年博士毕业于英国Newcastle大学，一直系统地从事代数编译码的研究，曾在美国Notre Dame大学、德国Ulm大学和香港中文大学等多所高校访学。陈立教授于2014年获得中国首届“信息论青年新星”荣誉称号，其指导的博士生邢炯跃获得中国电子学会信息论分会2020年度优秀博士论文奖。陈立教授参与多个国际学术会议的组织工作，2018 年作为大会共同主席在广州举办了IEEE信息论研讨会(ITW)，2022年分别在深圳和佛山举办IEEE东亚信息论学校(EASIT)和IEEE/CIC中国通信国际会议 (ICCC)。2026年将在广州举办IEEE信息论年会（ISIT）。

报告题目：Low-latency OSD of BCH codes

报告时间：上午 11:35 - 12:25

报告摘要：Ordered statistics decoding (OSD) can achieve a near maximum likelihood (ML) decoding performance for BCH codes. However, Gaussian elimination (GE) that delivers the systematic generator matrix of the code has an uncompromised latency. Addressing this challenge, this talk introduces a low-latency OSD (LLOSD). Since BCH codes are binary subcodes of Reed-Solomon (RS) codes, its codeword candidates can be produced using the RS systematic generator matrix, where its entries can be generated in parallel through the Lagrange interpolation. By eliminating the non-binary codeword candidates and identifying the ML codeword, the LLOSD also has a low complexity. Decoding complexity can be further reduced by its segmented variant. This talk also shows the LLOSD can be interpreted as systematic RS encoding of a punctured BCH codeword. Such a concatenated perspective unveils the valid BCH codeword candidates are far fewer than TEPs, validating its low complexity feature. Finally, a hybrid soft decoding (HSD) that integrates the LLOSD and the algebraic Chase decoding is proposed. The latter can effectively provide extra TEPs for the LLOSD, enhancing the decoding performance. This is an effective approach for decoding longer BCH codes.

张华滋 博士

个人简介：Huazi Zhang (Senior Member, IEEE) received his Ph.D. from Institute of Information and Communication Engineering, Zhejiang University in 2013. From 2011 to 2013, he was a visiting researcher with the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, USA. From 2013 to 2014, he was a Research Fellow with the School of Computer Engineering, Nanyang Technological University, Singapore. From 2014 to 2015, he was a Research Scholar with the Department of Electrical and Computer Engineering, University of Florida, USA.

He joined Huawei Technologies Co., Ltd in 2015. Since then, he has engaged in research projects on advanced wireless communications involving channel coding and signal processing techniques, and engaged in multiple standardization activities. His current research interests are channel coding, information theory and signal processing for wireless

communications, with focus on theoretical analysis, algorithm design and hardware implementations for 5G and beyond.

报告题目：New algebraic properties of polar codes

报告时间：下午 14:30 - 15:20

报告摘要：Polar codes is a class of codes having similarities to both probabilistic codes and algebraic codes. On the one hand, the successive cancellation (SC) decoding algorithm treats polar codes as probabilistic codes. By scheduling the message passing in a particular order, SC decoding can be regarded a special case of belief propagation decoding. The SC decoding performance in AWGN channel can also be accurately obtained by probabilistic tools such as density evolution. On the other hands, polar codes share much algebraic structures with Reed-Muller codes and BCH codes. Specifically, the weight spectrum of a pre-transformed polar codes, such as polarization-adjusted convolutional (PAC) codes, is proven to improve significantly over the conventional polar codes. The increase of code distance also contributes to the coding gain for CRC-aided (CA) polar codes and parity-check (PC) polar codes. Moreover, the automorphism structures of polar codes can be exploited for an automorphism ensemble (AE) decoding, which exhibit higher parallelism and lower complexity than SC list decoding. These algebraic properties need to be further studied to improve the performance-complexity tradeoff of polar codes.

邢炯跃 博士

个人简介： Jiongyue Xing received his Ph.D. degree in Information and Communication Engineering from Sun Yat-sen University in 2020. From 2018 to 2019, he was a visiting Ph.D. student with the Institute of Communication Engineering, Ulm University, Germany. Since 2020, he has been a Researcher with Hong Kong Theory Lab, Huawei Technologies Co., Ltd. His research interests include channel coding and data communications. He received the Excellent Doctoral Dissertation Award from the Chinese Institute of Electronics Information Theory Society in 2020.

报告题目： Shift-sum decoding of cyclic codes

报告时间： 下午 15:20 – 16:10

报告摘要： Cyclic codes, including the Reed-Solomon (RS) codes and BCH codes, are widely applied for data protection due to their efficient encoding and decoding algorithms. This talk

introduces a novel shift-sum decoding method for cyclic codes, which is hardware-friendly and exhibits advanced decoding performance. It utilizes the cyclically different minimum-weight dual codewords (MWDCs) and their proper shifts to create a frequency matrix which can be considered as a reliability metric for identifying the error positions and magnitudes. A plausibility analysis is provided to reveal the rationale for its advanced error-correction capability. Several decoding algorithms based on the shift-sum operation are also presented to demonstrate its performance potential. Simulation results on RS and BCH codes show that the shift-sum based algorithms yield a competent decoding and complexity performances in comparison with the existing decoding algorithms.

万韫琦 博士

个人简介：Yunqi Wan received his Ph.D. degree in information and communication engineering from Sun Yat-sen University in 2021. Since 2022, he has been a senior engineer with the Theory Laboratory, 2012 Laboratories, Huawei Technology Company Ltd. His research interests include channel coding and data communication.

报告题目：The re-encoding transform in algebraic list decoding of algebraic geometric codes

报告时间：下午 16:40 - 17:30

报告摘要：This talk proposes the re-encoding transformed (ReT) based list decoding using the module basis reduction (BR) interpolation for algebraic geometric (AG) codes on Cab curves. The two ReT approaches are introduced to facilitate the BR interpolation. One is realized by the bivariate Lagrange polynomial.

The other is conducted by the ReT of Reed-Solomon (RS) codes based on the mathematical structure of AG codes. The ReT based BR interpolation (ReT-BR) algorithm for decoding the AG codes is further introduced. Finally, complexity of the proposed algorithm is analyzed and validated by the simulation results, demonstrating its complexity advantage over the non-ReT counterpart.

Note