深圳北理莫斯科大學

УНИВЕРСИТЕТ МГУ–ППИ В ШЭНЬЧЖЭНЕ

SHENZHEN MSU-BIT UNIVERSITY

2021年代数几何码研讨会（Ⅱ）

Workshop in Algebraic Geometry Codes（II）， 2021

会议手册

深圳北理莫斯科大学
УНИВЕРСИТЕТ МГУ-ППИ В ШЭНЬЧЖЭНЕ
SHENZHEN MSU-BIT UNIVERSITY

时间：12/11-12/16

Zoom会议号：396 431 7007　密码：579229

（注：6天同一会议号及密码）

<table>
<tr><td colspan="4">12月11号
会议地点：2教313</td></tr>
<tr><td colspan="4">早餐（一号食堂二楼）7：00-8：30</td></tr>
<tr><td colspan="4">8:30-8:50 开幕式致辞
南方科技大学 张继平院士；深圳北理莫斯科大学 朱迪俭书记；
清华大学 冯克勤教授；深圳北理莫斯科大学 张晔教授.
8:50-9:10　合影(湖边背景墙)</td></tr>
<tr><td>时间</td><td>主持人</td><td>报告人</td><td>报告题目</td></tr>
<tr><td>9:10-9:55</td><td rowspan="4">冯克勤</td><td>邢朝平</td><td>Progress Report on the Project of Algebraic Geometry Codes</td></tr>
<tr><td>9:55-10:40</td><td>马立明</td><td>An Introduction to Algebraic Geometry Codes-(I)</td></tr>
<tr><td>10:40-11:05</td><td colspan="2">自由讨论</td></tr>
<tr><td>11:05-11:50</td><td>马立明</td><td>An Introduction to Algebraic Geometry Codes-(II)</td></tr>
<tr><td colspan="4">午餐（湖滨食堂二楼）</td></tr>
</table>

14:30-17:30	自由讨论交流（2教313、主楼301&336, 有茶歇）		
晚宴（奥林宾馆）			
12月12号 会议时间：9:00-17:30 会议地点：2教313			
早餐（一号食堂二楼）7：00-9：00			
时间	主持人	报告人	报告题目
9:00-9:45	邢朝平	上官冲	Combinatorial List-Decoding of Reed-Solomon Codes
9:45-10:30		Masahito Hayashi	Secure list decoding and its application to bit-string commitment
10:30-11:00		自由讨论	
11:00-11:45		胡创强	Drinfeld Modular Curves Arising from T-Torsion Trees and Their Applications in AG Codes
午餐（湖滨食堂二楼）			
14:30-17:30	自由讨论交流（2教313、主楼301&336, 有茶歇）		
晚餐（湖滨食堂二楼）			
12月13号 会议时间：9:00-17:30 会议地点：2教313			

<table>
<tr><td colspan="4">早餐（一号食堂二楼）7：00-9：00</td></tr>
<tr><td>时间</td><td>主持人</td><td>报告人</td><td>报告题目</td></tr>
<tr><td>9:00-9:45</td><td rowspan="4">向青</td><td>张子涵</td><td>A Survey on the Decoding of Algebraic-Geometry Codes-(I)</td></tr>
<tr><td>9:45-10:30</td><td>张子涵</td><td>A Survey on the Decoding of Algebraic-Geometry Codes-(II)</td></tr>
<tr><td>10:30-11:00</td><td colspan="2">自由讨论</td></tr>
<tr><td>11:00-11:45</td><td>彭帆</td><td>Decoding Algebraic Geometry Codes up to $\frac{d^*-1}{2}$</td></tr>
<tr><td colspan="4">午餐（湖滨食堂二楼）</td></tr>
<tr><td>14:30-17:30</td><td colspan="3">自由讨论交流（2教313、主楼301&336, 有茶歇）</td></tr>
<tr><td colspan="4">晚餐（湖滨食堂二楼）</td></tr>
<tr><td colspan="4">12月14号
会议时间：9:00-17:30
会议地点： 2教313，主楼301&336</td></tr>
<tr><td colspan="4">自由讨论交流</td></tr>
<tr><td colspan="4">12月15号
会议时间：9:00-17:30
会议地点： 2教313</td></tr>
</table>

<table>
<tr><td colspan="4">早餐（一号食堂二楼）7：00-9：00</td></tr>
<tr><td>时间</td><td>主持人</td><td>报告人</td><td>报告题目</td></tr>
<tr><td>9:00-9:45</td><td rowspan="4">李才恒</td><td>韩永祥</td><td>Update Bandwidth for Distributed Storage</td></tr>
<tr><td>9:45-10:30</td><td>曹喜望</td><td>Constructions of Optimal Binary Locally Recoverable Codes via a General Construction of Linear Codes</td></tr>
<tr><td>10:30-11:00</td><td colspan="2">自由讨论</td></tr>
<tr><td>11:00-11:45</td><td>刘姝</td><td>Maximally Recoverable Local Reconstruction Codes from Subspace Direct Sum Systems</td></tr>
<tr><td colspan="4">午餐（湖滨食堂二楼）</td></tr>
<tr><td>14:30-17:30</td><td colspan="3">自由讨论交流（2教313、主楼301&336, 有茶歇）</td></tr>
<tr><td colspan="4">晚餐（湖滨食堂二楼）</td></tr>
<tr><td colspan="4">12月16号
会议时间：9:00-17:30
会议地点： 2教313</td></tr>
<tr><td colspan="4">早餐（一号食堂二楼）7：00-9：00</td></tr>
<tr><td>时间</td><td>主持人</td><td>报告人</td><td>报告题目</td></tr>
<tr><td>9:00-9:45</td><td>曹喜望</td><td>袁晨</td><td>On the Complexity of Arithmetic Secret Sharing</td></tr>
</table>

9:45-10:30		王琦	On the size distribution of Levenshtein balls with radius one
10:30-11:00		自由讨论	
11:00-11:45		肖东亮	一种改进的代数几何码构造算法研究
午餐（湖滨食堂二楼）			
14:30-17:30	自由讨论交流（2教313、主楼301&336, 有茶歇）		
晚餐（湖滨食堂二楼）			
12月17号			
早餐（一号食堂二楼）7：00-9：00			

报告摘要

Constructions of Optimal Binary Locally Recoverable Codes via a General Construction of Linear Codes

曹喜望

（南京航空航天大学，南京）

Locally recoverable codes play a crucial role in distributed storage systems. Many studies have only focused on the constructions of optimal locally recoverable codes with regard to the Singleton bound. In this talk, we will introduce some new frameworks for constructing optimal binary locally recoverable codes meeting the alphabet dependent bound. Using a general framework for linear codes associated to a set, we provide a new approach to constructing binary locally recoverable codes with locality 2. We turn the problem of designing optimal binary locally recoverable codes into constructing a suitable set. Several constructions of optimal binary locally recoverable codes are proposed by this new method. Finally, we propose constructions of optimal binary locally recoverable codes with locality 2 and locality parameters ((r,δ)) by Griesmer codes.

Update Bandwidth for Distributed Storage

韩永祥

（电子科技大学（深圳）高等研究院，深圳）

In this talk, we consider the update bandwidth in distributed storage systems~(DSSs). The update bandwidth, which measures the transmission efficiency of the update process in DSSs, is defined as the average amount of data symbols transferred in the network when the data symbols stored in a node are updated. This

talk contains the following contributions. First, we establish the closed-form expression of the minimum update bandwidth attainable by irregular array codes. Second, after defining a class of irregular array codes, called Minimum Update Bandwidth~(MUB) codes, which achieve the minimum update bandwidth of irregular array codes, we determine the smallest code redundancy attainable by MUB codes. Third, the code parameters, with which the minimum code redundancy of irregular array codes and the smallest code redundancy of MUB codes can be equal, are identified, which allows us to define MR-MUB codes as a class of irregular array codes that simultaneously achieve the minimum code redundancy and the minimum update bandwidth. Last, we establish a lower bound of the update complexity of MR-MUB codes, which can be used to prove that the minimum update complexity of irregular array codes may not be achieved by MR-MUB codes.

Secure list decoding and its application to bit-string commitment

Masahito Hayashi

（南方科技大学量子科学与工程研究院，深圳）

We propose a new concept of secure list decoding, which is related to bit-string commitment. While the conventional list decoding requires that the list contains the transmitted message, secure list decoding requires the following additional security conditions to work as a modification of bit-string commitment. The first additional security condition is the receiver's uncertainty for the transmitted message, which is stronger than the impossibility of the correct decoding, even though the transmitted message is contained in the list.

The other additional security condition is the impossibility for the sender to estimate another element of the decoded list except for the transmitted message. The first condition is evaluated by the equivocation rate. The asymptotic property is

evaluated by three parameters, the rates of the message and list sizes, and the equivocation rate. We derive the capacity region of this problem. We show that the combination of hash function and secure list decoding yields the conventional bit-string commitment. Our results hold even when the input and output systems are general probability spaces including continuous systems. When the input system is a general probability space, we formulate the abilities of the honest sender and the dishonest sender in a different way.

Full paper version of this talk is available from https://arxiv.org/abs/2103.11548.

Drinfeld Modular Curves Arising from T-Torsion Trees and Their Applications in AG Codes

胡创强

（北京雁栖湖应用数学研究院，北京）

Drinfeld modular curves are used to construct sequences of curves with many rational points over any non-prime field. The specific structure of Drinfeld modular curve plays an important role in the field of coding. Indeed, constructing a linear error correction code with a sufficiently long code length is a fundamental problem in coding theory. In the 1980s, V.D.Goppa used the algebraic curve over finite fields to construct a special linear error correction code, which is now called the algebraic geometry code. The parameters (code length, dimension, minimum Hamming distance) of this type of linear code mainly depend on the geometric properties of the corresponding algebraic curve, namely, the number of rational points and genus. It is proved theoretically that there is a family of asymptotically optimal linear error-correction codes whose parameters attain the Drinfeld–Vladut bound. Surprisingly, in 1982, Tsfasman, Vladut¸, and Zink proved the existence of an asymptotically optimal long linear code with relative parameters which exceeds the Gilbert–

Varshamov bound within a certain range. This work shows a vital link between Ihara's quantity and the realm of coding theory. In practical applications, we need to know the explicit construction of such algebraic geometry codes, and it boils down to finding a family of asymptotically good function field sequences (called tower) which are measured by the Ihara's constant. In 2000, based on his procedure for constructing explicit towers of modular curves, Elkies deduced explicit equations of rank-2 Drinfeld modular curves which coincide with the asymptotically optimal towers of curves constructed by Garcia and Stichtenoth. In 2015, Bassa, Beelen, Garcia, and Stichtenoth constructed a celebrated (recursive and good) tower (BBGS tower for short) of curves and outlined a modular interpretation of the defining equations. In this talk, we aim to construct a sequence of Drinfeld modular curves which are organized in an elegant manner — a hierarchical topology tree which we call the T-torsion tree. We believe that our novel approach by the T-torsion tree not only promotes the classic torsion sequence structure, but also further integrates the internal connections of different torsion structures.

Maximally Recoverable Local Reconstruction Codes from Subspace Direct Sum Systems

刘姝

（电子科技大学，成都）

Maximally recoverable local reconstruction codes (MR LRCs for short) have received great attention in the last few years. Various constructions have been proposed in literatures. The main focus of this topic is to construct MR LRCs over small fields. An $(N=nr,r,h,\Gd)$-MR LRC is a linear code over finite field $\F_\ell$ of length N, whose codeword symbols are partitioned into n local groups each of size r. Each local group can repair any $\Gd$ erasure errors and

there are further h global parity checks to provide fault tolerance from more global erasure patterns.

MR LRCs deployed in practice have a small number of global parities such as $h=O(1)$. In this parameter setting, all previous constructions require the field size $\ell =\Omega_h (N^{h-1-o(1)})$. It remains challenging to improve this bound. In this paper, via subspace direct sum systems, we present a construction of MR LRC with the field size $\ell= O(N^{h-2+\frac1{h-1}-o(1)})$. In particular, for the most interesting cases where $h=2,3$, we improve previous constructions by either reducing field size or removing constraints. In addition, we also offer some constructions of MR LRCs for larger global parity h that have field size incomparable with known upper bounds. The main techniques used in this paper is through subspace direct sum systems that we introduce. Interestingly, subspace direct sum systems are actually equivalent to $\F_q$-linear codes over extension fields. Based on various constructions of subspace direct sum systems, we are able to construct several classes of MR LRCs.

An Introduction to Algebraic Geometry Codes

马立明

（中国科学技术大学，合肥）

In this talk, I will present a brief introduction to algebraic geometry codes. The discovery of algebraic geometry codes by Goppa has greatly stimulated research in both coding theory and number theory. The major breakthrough of Goppa's algebraic geometric codes is that they improved the long-standing benchmark bound, the Gilbert-Varshamov bound (GV bound for short).

In this talk, I will introduce the basic concepts and theory of algebraic function fields over finite fields in the first part, various constructions of algebraic geometry

codes in the section part, and asymptotic construction of algebraic geometry codes exceeding the GV bound in the third part. In particular, I will focus on the asymptotic constructions of algebraic geometry codes exceeding the GV bound or Tafasman-Vladut-Zink bound.

Decoding Algebraic Geometry Codes up to $\frac{d^*-1}{2}$

彭帆

（广西师范大学，桂林）

Feng-Rao 在1993年提出通用的多数决议译码算法，是第一个可纠正 $\frac{d^*-1}{2}$ 个错误的译码算法复杂度为$O(n^3)$. 而相对简单的Berlekamp-Welch算法可以纠正 $\frac{d^*-1-g}{2}$ 个错误. 1999年Guruswami-Sudan应用带重数对带权重的高阶二元多项式插值并求根，将BW算法推广到代数几何的list-decoding. 借鉴Guruswami-Sudan 译码的插值部分，我们提出了一个可以纠正 $\frac{d^*-1}{2}$ 个错误的通用代数几何码译码算法. 再应用多项式格(Lattices on polynomial rings)上的快速基约化(base reduction)算法，可将Hermitian码的译码复杂度降低到$O(cn^{\frac{5}{3}})$.

Combinatorial List-Decoding of Reed-Solomon Codes

上官冲

（山东大学，青岛）

The notion of list-decoding was introduced independently by Elias and Wozencraft in the 1950s. It is a generalization of the unique decoding model typically considered in coding theory, where given a received word the decoder

might output a list of possible codewords, instead of a unique one. This allows for handling a greater number of errors than that allowed by unique decoding.

The number of errors that can be handled by a given code in list-decoding is measured by its list-decoding radius. It is well-known that the list-decoding radius of any given code lies between the Johnson bound and the list-decoding capacity. It is also well-known that random codes achieve list-decoding capacity with high probability. However, until recently, it had been a longstanding open question that whether Reed-Solomon codes can be list-decoded beyond the Johnson radius. In this talk, we will survey the known results on the list-decoding radius of Reed-Solomon codes, and show how polynomial method and graph theory come into play in the recent study of this topic.

On the size distribution of Levenshtein balls with radius one

王琦

（南方科技大学，深圳）

The fixed length Levenshtein (FLL) distance between two words $\mathbf{x, y} \in \mathbb{Z}_m^n$ is the smallest integer t such that the word $\mathbf{x}$ ca n be transferred to $\mathbf{y}$ by t insertions and t deletions. The size of a ball in FLL metric is a fundamental but challenging problem. Very recently, Bar-Lev, Etzion, and Yaakobi found the explicit expressions for the minimum, maximum and average sizes of FLL balls with radius one. In this talk, we will further prove that the size of the FLL ball with radius one is highly concentrated around its mean by Azuma's inequality.

一种改进的代数几何码构造算法研究

肖东亮

（中国农业大学，北京）

基于伴随式计算差错位置多项式的译码算法提出了一种改进方法，达到了代数几何码的设计纠错能力，通过仿真测试，与当前主流编码技术LDPC码和Polar码进行了比较，以软判决译码算法为代表的LDPC码在低信噪比环境下具有优势，而由于代数几何码良好的距离特性将在高信噪比条件下纠错性能超过LDPC码，降低了误码平底。针对低信噪比环境的要求，提出了代数几何码和LDPC码级联方案，性能提升显著。根据随机共振机理，还提出了一种加扰算法。

Progress Report on the Project of Algebraic Geometry Codes

邢朝平

（上海交通大学，上海）

In this talk, we will first survey some results on Reed-Solomon codes as well as algebraic geometry codes. We will then report some of our recent progresses on constructions of algebraic geometry codes and decoding of algebraic geometry codes. Finally, some possible research goals on algebraic geometry codes are proposed.

On the Complexity of Arithmetic Secret Sharing

袁晨

（上海交通大学，上海）

Since the mid 2000s, asymptotically-good strongly-multiplicative linear (ramp) secret sharing schemes over a fixed finite field have turned out as a central theoretical primitive in numerous constant-communication-rate results in multi-party cryptographic scenarios, and, surprisingly, in two-party cryptography as well.

Known constructions of this most powerful class of arithmetic secret sharing schemes all rely heavily on algebraic geometry (AG), i.e., on dedicated AG codes based on asymptotically good towers of algebraic function fields defined over finite fields. It is a well-known open question since the first (explicit) constructions of such schemes appeared in CRYPTO 2006 whether the use of "heavy machinery" can be avoided here. i.e., the question is whether the mere existence of such schemes can also be proved by "elementary" techniques only (say, from classical algebraic coding theory), even disregarding effective construction. So far, there is no progress.

In this talk, we show the theoretical result that, (1) no matter whether this open question has an affirmative answer or not, these schemes can be constructed explicitly by elementary algorithms defined in terms of basic algebraic coding theory. This pertains to all relevant operations associated to such schemes, including, notably, the generation of an instance for a given number of players n, as well as error correction in the presence of corrupt shares. We further show that (2) the algorithms are quasi-linear time (in n); this is (asymptotically) significantly more efficient than the known constructions. That said, the analysis of the mere termination of these algorithms does still rely on algebraic geometry, in the sense that it requires blackbox application of suitable existence results for these schemes. This is a joint work with Ronald Cramer and Chaoping Xing.

A Survey on the Decoding of Algebraic-Geometry Codes

张子涵

（上海交通大学，上海）

In this talk, we give an overview on the development of decoding Algebraic-Geometry codes. We will give a brief introductions on several major decoding algorithms including Berlekamp-Welch type algorithm, Feng-Rao's majority voting algorithm, Berlekamp-Massey type algorithm, power decoding algorithm and Guruswami-Sudan type list decoding algorithm etc. Meanwhile, we will give the computational complexity of those aforementioned algorithms and conclude the best-known ones as well.