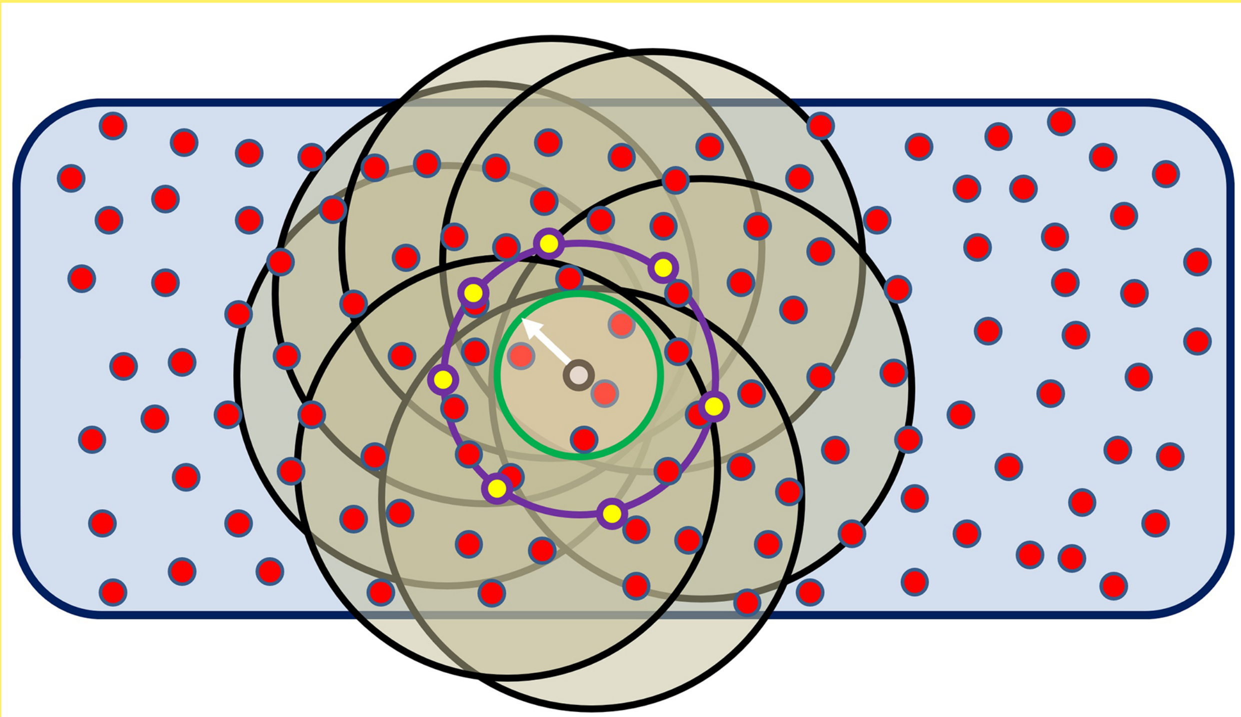
Colloquium on Combinatorial Designs

2021.10.17 8:30-12:00

https://meeting.tencent.com/dm/wFJUi8NHPzQc

ID: 867 299 433



Invited Speakers

Yiwei Zhang Private proximity retrieval and its connections with covering designs

Chong Shanggan Combinatorial list-decoding of Reed-Solomon codes

Weijun Fang Improved bounds and optimal constructions of locally repairable codes

Organisers: Tao Feng, Xiande Zhang, Yue Zhou

Colloquium on Combinatorial Designs

Organized by Tao Feng, Xiande Zhang and Yue Zhou

October 17, 2021

Information

Our 5th colloquium will be held via Tencent Voov meeting on 17th October from 08:30 to 12:00. It consists of three invited talks, each of which will take around 1 hour. There will be a 5-minutes break between every two talks.

ID:867 299 433

https://meeting.tencent.com/dm/wFJUi8NHPzQc

Contents

Information **iii**

Abstracts **1**

Private proximity retrieval and its connections with covering designs (*Yiwei Zhang*) . . . 1

Combinatorial list-decoding of Reed-Solomon codes (*Chong Shangguan*) . . 1

Improved Bounds and Optimal Constructions of Locally Repairable Codes (*Weijun Fang*) . . . 2

Abstracts

Private proximity retrieval and its connections with covering designs

17 October
8:30am

Yiwei Zhang

Shandong University, China

Proximity retrieval allows a user to search into a database for files which are similar to his or her sample file. By the trivial approach of uploading the exact sample, the user's privacy is completely revealed. In order to partly protect the privacy of the user, we introduce a private proximity retrieval scheme, when the database is stored on several servers. We analyze the tradeoff between the privacy level and the number of servers required. We will show that such schemes are closely related to covering designs. In some sense, the schemes are covering designs with additional 'covering' constraints. This is a joint work with Tuvi Etzion and Eitan Yaakobi.

Combinatorial list-decoding of Reed-Solomon codes

17 October
9:30am

Chong Shangguan

Shandong University, China

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 introduce our recent progress.

---

17 October
10:30am

Improved Bounds and Optimal Constructions of Locally Repairable Codes

Weijun Fang
Shandong University, China

Locally repairable codes (LRCs) as a new coding scheme have given more rise to the system performance and attracted a lot of interest in the theoretical research in coding theory. In this talk, we first of all derive an improved and general upper bound on the code length of Singleton-optimal LRCs with minimum distanced$= 5, 6$, some known constructions are shown to exactly achieve our new bound, which verifies its tightness. Moreover, we obtain a complete characterization for Singleton-optimal LRCs with $r = 2$ and $d = 6$. Such characterization has established an important connection between the existence of Singleton-optimal LRCs and that of a special subset of lines of finite projective plane $PG(2, q)$, thus provides a methodology for constructing LRCs with longer length based on any advance on finite projective plane $PG(2, q)$. Furthermore, we employ the well-known line-point incidence matrix and Johnson bounds for constant weight codes to derive tighter upper bounds on the code length. To the best of our knowledge, this is the best bound on the code length of optimal $(n, k, 6; 2)$-LRCs until now.
