Report on "PIR codes using combinatorial structures"

The thesis is a survey on Private Information Retrieval (PIR) codes and related codes such as Locally Repairable and Batch codes. The aim of the thesis was to provide a survey, covering results from [3, 7, 11, 13, 14] and explain the underlying mathematics which is mostly combinatorics.

The student starts with an introduction to combinatorial mathematics used in the thesis in Chapter 1 where objects such as projective and affine planes, arc, unitals, conics etc. are explained. The exposition uses [1] as a source and it is well-cited. The second chapter is on cryptograhic (privacy) and coding theoretic aspects. Here, several variations of PIR codes are introduced. This chapter also includes a section on the bound $P(s,k)$ which is the minimal number of servers achievable by a PIR code. The student gives the current state of the art on the bound and using computer experiments to verify the data. Chapter 3 is on constructions of PIR codes using the combinatorial ideas of the previous chapters. The student follows [3, 7] and explains the main constructions of the paper. Proofs mostly follow [3] where the student gives more detailed explanations in a few places. The final chapter is on PIR array codes which might improve $P(s,k)$ in certain instances. The student also gives definitions and examples of Batch and Locally Repairable codes following [11,13,14]. The student, also works out several examples to improve the didactical value of the exposition.

Topic of the thesis: The topic is suitable for a thesis.

Mathematical content: Mathematical content is on combinatorics and coding theory and its level is quite satisfactory.

Citations/References: Many sources are used which are cited extensively.

Student's contribution: The student gives a survey and writes programs to verify several statements, constructions and bounds.

Summary:

The use of English is good overall the thesis. A few comments on formal issues:

- (p. 5) consist - consists
- (p. 6) the Chapter 3 - delete 'the'
- (p. 9) lately - later
- A projective plane is not necessarily $\mathbb{P}^2(\mathbb{F}_q)$.
- (p. 12) In the whole proof let C be a non-degenerate conic.

Conclusion: The thesis is a nice survey on recent developments in combinatorial coding theory regarding PIR codes. Although the novelty of the thesis is small I certainly think that it deserves to be regarded as a successful thesis.