Nonlinear Repair Schemes of Reed-Solomon Codes.

Roni Con
Department of Computer Science, Tel Aviv University, Israel

Itzhak Tamo
Department of Electrical Engineering-Systems, Tel Aviv University, Israel

Abstract

The problem of repairing linear codes and, in particular, Reed Solomon (RS) codes has attracted a lot of attention in recent years due to their extreme importance to distributed storage systems. In this problem, a failed code symbol (node) needs to be repaired by downloading as little information as possible from a subset of the remaining nodes. By now, there are examples of RS codes that have efficient repair schemes, and some even attain the cut-set bound. However, these schemes fall short in several aspects; they require a considerable field extension degree. They do not provide any nontrivial repair scheme over prime fields. Lastly, they are all linear repairs, i.e., the computed functions are linear over the base field. Motivated by these and by a question raised in [1] on the power of nonlinear repair schemes, we study the problem of nonlinear repair schemes of RS codes.

Our main results are the first nonlinear repair scheme of RS codes with asymptotically optimal repair bandwidth (asymptotically matching the cut-set bound). Specifically, we show that almost all 2 dimensional RS codes over prime fields (for large enough prime) are asymptotically MSR codes. This is the first example of a nonlinear repair scheme of any code and also the first example that a nonlinear repair scheme can outperform all linear ones. Moreover, we construct several RS codes over prime fields that exhibits efficient repair properties. We also show that unlike the problem of repairing RS codes over field extensions, over prime fields, one can not achieve the cut-set bound with equality. Concretely, by using ideas from additive combinatorics, we improve the cut-set bound by an additive factor, hence showing that every node must transmit more bits than the cut-set bound during a repair. Lastly, we discuss the implications of our results on repairing RS codes for leakage-resilient of Shamir’s secret sharing scheme over prime fields.

2012 ACM Subject Classification Mathematics of computing → Coding theory

Keywords and phrases Exact repair problem, Reed–Solomon codes, Cut-set bound, Regenerating codes

Digital Object Identifier 10.4230/LIPIcs.ITCS.2022.50


Funding This work was partially supported by the European Research Council (ERC grant number 852953) and by the Israel Science Foundation (ISF grant number 1030/15).

References