Ma, Liming; Xing, Chaoping

The group structures of automorphism groups of elliptic curves over finite fields and their applications to optimal locally repairable codes. (English) Zbl 07601590


Summary: Constructing optimal locally repairable codes is a challenging and interesting task and has attracted great attention in the last decade. Unlike classical MDS codes, a $q$-ary optimal locally repairable code could have length bigger than $q + 1$. In [18], a family of optimal locally repairable codes was constructed from automorphism groups of elliptic curves. The length of such a $q$-ary optimal locally repairable code can be up to $q + 2\sqrt{q}$ and the minimum distance can be linear in its length. However, the locality of this family of optimal locally repairable codes is upper bounded by 23, because there are at most 24 automorphisms of an elliptic curve fixing the point at infinity.

In this paper, we show the group structure of the automorphism group of an elliptic curve over a finite field and characterize its subgroups and abelian subgroups. Optimal locally repairable codes can be constructed from subgroups involving both translations and a nontrivial automorphism fixing the point at infinity of elliptic curves. One of the main motivations to study subgroups of the automorphism group of an elliptic curve over a finite field is to remove the constraints on locality.

MSC:

94Bxx Theory of error-correcting codes and error-detecting codes
05Bxx Designs and configurations
14Gxx Arithmetic problems in algebraic geometry; Diophantine geometry

Keywords:
locally repairable codes; elliptic curves; automorphism groups; rational points

Full Text: DOI

References:


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.