ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 39, Number 6, 2009

AUTOMORPHISM GROUPS OF THE EXTENDED QUADRATIC RESIDUE CODES OVER $\mathbf{Z}_{16}$ and $\mathbf{Z}_{32}$

CHUNG-LIN HSU, WEI LIANG KUO, STEPHEN S.-T. YAU AND YUNG YU

Dedicated to Professor Hirzebruch on the occasion of his 80th birthday.

1. Introduction. Let $\mathbf{Z}_{16}$ denote the integers modulo 16. $\mathbf{Z}_{16}$ is a ring which has $2, 4, 6, 8, 10, 12, 14$ as zero divisors. A set of n-tuples over $\mathbf{Z}_{16}$ is called a code over $\mathbf{Z}_{16}$ or a $\mathbf{Z}_{16}$-code if it is a $\mathbf{Z}_{16}$-module. Similarly one can define a $\mathbf{Z}_{32}$-code.

Linear codes are easy to understand, to encode and decode. However, in order to get the largest possible number of codewords with a fixed block size and correction capability, it is sometimes necessary to consider nonlinear codes. Some of the best known examples of nonlinear binary error-correcting codes that are better than any corresponding linear code are the Nordstrom-Robinson, Kerdock, and Preparata codes. In fact, some of these nonlinear binary codes satisfy a certain formal duality property for which a satisfactory explanation is known only in the linear code. In 1994, Hammons, Kumar, Calderbank, Sloane, and Solé [**3**] explained this formal duality by showing that the Kerdock and Preparata codes are in fact linear, if one views them over the ring of integers modulo 4 instead of the binary field and that, over this larger ring the two codes are algebraically dual. They showed a simple connection between these nonlinear codes and linear codes over $\mathbf{Z}_4$ by means of the Gray map. This generated a lot of interest on $\mathbf{Z}_4$-codes, see for example [**1, 10**]. It is a natural question to ask what happens for $\mathbf{Z}_{2^m}$-cyclic codes.

In [**2**], the authors prove that idempotent generators exist for certain $\mathbf{Z}_{q^m}$-cyclic codes. The uniqueness of an idempotent generator of any cyclic code is also proven. In fact Kanwar and López-Permouth [**5**] gave a systematic study of cyclic codes over $\mathbf{Z}_{q^m}$.

A particularly interesting family of cyclic codes is quadratic residue codes. Quadratic residue codes were first defined by Andrew Gleason.

Research partially supported by NSA grant.
Received by the editors on January 23, 2007, and in revised form on June 24, 2007.

DOI:10.1216/RMJ-2009-39-6-1947