Codes and arrays from cocycles

GARRY HUGHES

This thesis applies the two-dimensional cohomology of finite groups and the theory of cocycles to two areas: combinatorics and error correcting codes.

In the first case, it is shown that several combinatorial objects defined on groups: semi-regular central relative difference sets, sequences with certain auto-correlation properties and cocyclic generalized Hadamard matrices can all be thought of as being equivalent to a single underlying concept, namely, a *base sequence*. Using this equivalence we can move from one of these objects to another, and so use whichever formulation is most useful. This gives a unified way of studying the combinatorial properties of extension groups in both the splitting and, more difficult, non-splitting cases. General results proven about base sequences imply corresponding results about the equivalent combinatorial objects. We apply this in two cases, generalized perfect binary arrays and perfect quaternary arrays and show, for example, that these objects are equivalent to Hadamard matrices of a specific easy to describe form. We also prove, using cohomology and generalized perfect binary arrays, that in studying the existence of abelian non-splitting semi-regular difference sets (relative to order two subgroups) we can assume the groups in question have a simple "canonical" form. We also show that a perfect quaternary array is explicitly equivalent to a particular type of generalized perfect binary array.

In the theory of error correcting codes, cohomology allows us to give an isomorphism between a group ring code and the direct sum of other group ring codes that have been "twisted" by cocycles. This is a known result in certain cases (for example in the abelian case it is a generalized Chinese Remainder Theorem) but our approach gives the isomorphism explicitly in terms of multiplication by a Vandermonde matrix.

We use the isomorphism to construct new codes from known "smaller" codes. For example, over a field of odd characteristic, we have a $u+v \mid u-v$ code construction which has a distance estimated no worse than the well known $u \mid u+v$ construction. It has an advantage over that construction, however, because when given a cyclic code

Received 16th October, 2000
Thesis submitted to RMIT University, February 2000. Degree approved, May 2000. Supervisor: Professor K.J. Horadam.

https://doi.org/10.1017/S0004972700019420 Published online by Cambridge University Press

and a nega-cyclic code (of the same length) it will produce a cyclic code of twice the length. By combining known MDS cyclic and nega-cyclic codes we obtain new cyclic codes, some of which are also optimal linear codes. More generally the isomorphism gives a "Vandermonde" construction and from this other new cyclic codes are obtained.

As well as this constructive use, the isomorphism also provides a decomposition of a larger code into "smaller" codes in such a way that many properties of the larger code are inherited by the new codes. This idea is used to prove the non-existence of self-dual group ring codes in the case when the group is the direct product of a 2-group and a group of odd order, and the ring is either $GF(q)$, with q odd, or $\mathbb{Z}_t$ with t odd and not a square. So, there can be no self-dual abelian codes (and, in particular, no self-dual cyclic codes) over these rings. This result also holds in fields where self-duality is defined in terms of an Hermitian inner product.

CMR-DSTO
Department of Defence
Locked Bag 5076
Kingston ACT 2604
Australia

https://doi.org/10.1017/S0004972700019420 Published online by Cambridge University Press