2-modular representations of the Conway simple groups as binary codes

Bernardo Rodrigues

Department of Mathematics and Applied Mathematics
University of Pretoria
Hatfield 0028, Pretoria

Parts of this talk are from joint work with **Wolfgang Knapp**, Mathematisches Institut, Universität Tübingen, Germany

Let F be a finite field of q elements, and G be a transitive group on a finite set Ω. Then there is a G-action on Ω, namely a map $G \times \Omega \longrightarrow \Omega$, $(g, w) \mapsto w^g = gw$, satisfying $w^{gg'} = (gg')w = g(g'w)$ for all $g, g' \in G$ and all $w \in \Omega$, and that $w^1 = 1w = w$ for all $w \in \Omega$. Let $F\Omega = \{f \mid f\colon \Omega \longrightarrow F\}$, be the vector space over F with basis Ω. Extending the G-action on Ω linearly, $F\Omega$ becomes an FG-module called an FG-permutation module. We are interested in finding all G-invariant FG-submodules, i.e., codes in $F\Omega$. The elements $f \in FG$ are written in the form $f = \sum_{w\in\Omega} a_w \chi_w$ where χ_w is a characteristic function. The natural action of an element $g \in G$ is given by $g(\sum_{w\in\Omega} a_w\chi_w) = \sum_{w\in\Omega} a_w\chi_{g(w)}$. This action of G preserves the natural bilinear form defined by

$$\langle \sum_{w\in\Omega} a_w\chi_w, \sum_{w\in\Omega} b_w\chi_w\rangle = \sum_{w\in\Omega} a_w b_w.$$

There appear slightly different concepts of (linear) codes in the literature. A code over some finite field F will be a triple (V, Ω, F), where $V = F\Omega$ is a free FG-module of finite rank with basis Ω and a submodule C. By convention we call C a code having ambient space V and ambient basis Ω. F is the alphabet of the code C, the degree n of V its length, and C is an $[n, k]$-code if C is free of rank k.

In the talk we introduce and discuss an elementary tool from representation theory of finite groups for constructing linear codes invariant under a given permutation group G. The tool gives theoretical insight as well as a recipe for computations of generator matrices and weight distributions. In some interesting cases a classification of code vectors under the action of G can be obtained. As explicit examples we examine binary codes related to the 2-modular reduction of the Leech lattice and Conway groups.