# Additive Reed-Muller Codes[1]

Jaume Pujol and Josep Rifà
Dept. Informàtica
Universitat Autònoma de Barcelona
08193 Bellaterra, Spain
Email jpujol@ccd.uab.es

*Abstract* — **We construct a new class of additive codes of type $Z_2^{k_1} \oplus Z_4^{k_2}$. These codes have a binary non-linear structure, but it is possible to give a description of them as additive subgroups of $Z_2^{k_1} \oplus Z_4^{k_2}$.**

**In this paper a generalization of linear Reed-Muller codes is obtained.**

## I. Preliminaries

Let $\mathbf{F}^n$ be a vector space of dimension $n$ over the Galois field $GF(2)$. We denote by $Z_2^n$ the additive group of $\mathbf{F}^n$. A subset $C$ of $\mathbf{F}^n$ is a binary code of length $n$. We shall assume, unless stated otherwise, that $\mathbf{0} \in C$, where $C \subset \mathbf{F}^n$ is a binary code.

By a *quaternary code* $C$ of length $k$ we shall mean an additive subgroup of $Z_4^k$. The notions of Hamming weight and *dual code*, $\mathcal{C}^\perp$, are defined in [1]

Let $\mathcal{C}$ be an additive subgroup of the $Z$-module $\mathbf{R} = Z_2^{k_1} \oplus Z_4^{k_2}$. We will say that $\mathcal{C}$ is an *additive code* over $\mathbf{R}$.

In [3] we introduced a new class of perfect single-error-correcting additive but non-linear binary codes:

Let ${}^lH$ and $H^r$ two matrices constructed in the following way: ${}^lH$ is the parity check matrix of the Hamming code of length $n = 2^m - 1$, $(m \geq 3)$. $H^r$ is the matrix obtained from ${}^lH$ by adding a first column all zero. We define $\mathcal{H} = \Phi^{-1}({}^lH|H^r)$ where $\mathbf{R} = Z_2^n \oplus Z_4^{(n+1)/2}$ and $\Phi$ identifies $\mathbf{R}$ to $\mathbf{F}^{2n+1}$.

Let $\mathcal{C}$ be the additive code over $\mathbf{R}$ generated by $\mathcal{H}$. In [3] we have shown the following theorem:

**Theorem 1** *For $n = 2^m - 1$, $(m \geq 3)$, $C_\perp = \Phi(\mathcal{C}^\perp)$ is a perfect single-error-correcting non-linear, but additive, code of length $2n + 1$.*

The code $\mathcal{C}^\perp$ will be denoted by $\mathcal{AH}_n$ $(n = 2^m - 1,\ m \geq 3)$ and $C_\perp$ by $AH_n$. Let $\overline{\mathcal{AH}_n}$ be the extended code of $\mathcal{AH}_n$ obtained by adding a binary parity check symbol to $\mathcal{AH}_n$ (see [3]).

## II. Additive Reed-Muller codes

Let $k_1 = 2^{m-1}$, $k_2 = 2^{m-2}$, $m \geq 2$. We will identify $\mathbf{F}^{2^m}$ to $\mathbf{R} = Z_2^{k_1} \oplus Z_4^{k_2}$. For every $r$ $(0 \leq r \leq m)$ we define the *Additive Reed-Muller* code $\mathcal{ARM}(r, m)$ of order $r$ in the following way:

1. $\mathcal{ARM}(0, m) = \{0 \cdots 0, 1 \cdots 1 | 2 \cdots 2\}$, $\mathcal{ARM}(m, m) = \mathbf{R}$
2. $\mathcal{ARM}(r, m) = \{(u|u + v) | u \in \mathcal{ARM}(r, m-1),\ v \in \mathcal{ARM}(r-1, m-1)\}$, $r < m$ where $u + v$ denotes the addition in $\mathbf{R}$.

**Proposition 2** *For every $0 \leq r \leq m$, $\mathcal{ARM}(r, m)$ is an additive subgroup of $\mathbf{R}$ and $\Phi(\mathcal{ARM}(r, m)) = ARM(r, m)$ is a binary additive code of $\mathbf{F}^{2^m}$.*

As in the linear case we can find a generator matrix for the code $\mathcal{ARM}(r, m)$:

**Lemma 3** *If $G(r, m)$ is a generator matrix for $\mathcal{ARM}(r, m)$ then*

$$G(r, m) = \begin{pmatrix} G(r, m-1) & G(r, m-1) \\ 0 & G(r-1, m-1) \end{pmatrix}$$

**Proposition 4** *The additive Reed-Muller code $\mathcal{ARM}(r, m)$ of order $r$ has the following properties:*

1. *Minimum distance $d = 2^{m-r}$*
2. *If $k = \sum_{i=0}^{r} \binom{m}{i}$ then $|\mathcal{ARM}(r, m)| = 2^k$*
3. *There exists a coordinate permutation $\sigma_r$ such that $\sigma_r(\mathcal{ARM}(r-1, m)) \subset \mathcal{ARM}(r, m)$, $r > 0$*

**Proposition 5** *For $r < m$ there exists a code equivalent to $\mathcal{ARM}(r, m)$ such that its dual code is $\mathcal{ARM}(m - r - 1, m)$.*

As in the linear case we can see that the family of additive Reed-Muller codes contains the family of extended perfect codes introduced in [3] (see theorem 1).

**Proposition 6** *$\mathcal{ARM}(1, m)$ is the dual code of $\overline{\mathcal{AH}_n}$ with $n = 2^m - 1$, $m \geq 3$.*

From theorem 1 and proposition 6 we obtain,

**Corollary 7** *The extended code of the additive perfect binary code $AH_n$, $(n = 2^m - 1,\ m \geq 3)$ is equivalent to the binary additive code $ARM(m - 2, m)$.*

A question arises at this point. Under which conditions $ARM(r, m)$, $(m \geq 2)$ is a linear binary code? Next proposition partially answers this question.

**Proposition 8** *The binary additive Reed-Muller Code $ARM(r, m)$ $(m \geq 2)$ of length $2^m$ is linear for $r = 0, 1, m-1, m$ and non-linear for $r = m - 2$ $(m > 3)$.*

## References

[1] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Solé. The $Z_4$-linearity of kerdock, preparata, goethals and related codes. *IEEE Transaction on Information Theory*, 40:301–319, 1994.

[2] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland Publishing Company, 1977.

[3] J. Rifà and J. Pujol. Translation invariant propelinear codes. To appear in IEEE Transaction on Information Theory, 1997.

[1]This work was partially supported by Spanish CICYT Grant No. TIC94-0331