Construction of Additive Reed-Muller Codes*

J. Pujol, J. Rifà, and L. Ronquillo

Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain.

Abstract. The well known Plotkin construction is, in the current paper, generalized and used to yield new families of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, whose length, dimension as well as minimum distance are studied. These new constructions enable us to obtain families of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes such that, under the Gray map, the corresponding binary codes have the same parameters and properties as the usual binary linear Reed-Muller codes. Moreover, the first family is the usual binary linear Reed-Muller family.

Key Words: $\mathbb{Z}_2\mathbb{Z}_4$-Additive codes, Plotkin construction, Reed-Muller codes, $\mathbb{Z}_2\mathbb{Z}_4$-linear codes.

1 Introduction

The aim of our paper is to obtain a generalization of the Plotkin construction which gave rise to families of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes such that, after the Gray map, the corresponding $\mathbb{Z}_2\mathbb{Z}_4$-linear codes had the same parameters and properties as the family of binary linear *RM* codes. Even more, we want the corresponding codes with parameters $(r, m) = (1, m)$ and $(r, m) = (m-2, m)$ to be, respectively, any one of the non-equivalent $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard and $\mathbb{Z}_2\mathbb{Z}_4$-linear 1-perfect codes.

2 Constructions of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes

In general, any non-empty subgroup $\mathcal{C}$ of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is a $\mathbb{Z}_2\mathbb{Z}_4$-*additive code*, where $\mathbb{Z}_2^\alpha$ denotes the set of all binary vectors of length α and $\mathbb{Z}_4^\beta$ is the set of all β-tuples in $\mathbb{Z}_4$.

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code, and let $C = \Phi(\mathcal{C})$, where $\Phi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \longrightarrow \mathbb{Z}_2^n$ is given by the map $\Phi(u_1, \dots, u_\alpha | v_1, \dots, v_\beta) = (u_1, \dots, u_\alpha | \phi(v_1), \dots, \phi(v_\beta))$ where $\phi(0) = (0, 0)$, $\phi(1) = (0, 1)$, $\phi(2) = (1, 1)$, and $\phi(3) = (1, 0)$ is the usual Gray map from $\mathbb{Z}_4$ onto $\mathbb{Z}_2^2$.

Since the Gray map is distance preserving, the Hamming distance of a $\mathbb{Z}_2\mathbb{Z}_4$-linear code C coincides with the Lee distance computed on the $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C} = \phi^{-1}(C)$.

* This work has been partially supported by the Spanish MICINN Grants MTM2006-03250, TSI2006-14005-C02-01, PCI2006-A7-0616 and also by the *Comissionat per a Universitats i Recerca de la Generalitat de Catalunya* under grant FI2008.

A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is also isomorphic to an abelian structure like $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Therefore, $\mathcal{C}$ has $|\mathcal{C}| = 2^\gamma 4^\delta$ codewords and, moreover, $2^{\gamma+\delta}$ of them are of order two. We call such code $\mathcal{C}$ a $\mathbb{Z}_2\mathbb{Z}_4$*-additive code of type* $(\alpha, \beta; \gamma, \delta)$ and its binary image $C = \Phi(\mathcal{C})$ is a $\mathbb{Z}_2\mathbb{Z}_4$*-linear code of type* $(\alpha, \beta; \gamma, \delta)$.

Although $\mathcal{C}$ may not have a basis, it is important and appropriate to define a generator matrix for $\mathcal{C}$ as:

$$\mathcal{G} = \begin{pmatrix} B_2 | Q_2 \\ \hline B_4 | Q_4 \end{pmatrix}, \qquad (1)$$

where B_2 and B_4 are binary matrices of size $\gamma \times \alpha$ and $\delta \times \alpha$, respectively; Q_2 is a $\gamma \times \beta$-quaternary matrix which contains order two row vectors; and Q_4 is a $\delta \times \beta$-quaternary matrix with order four row vectors.

2.1 Plotkin construction

In this section we show that the well known Plotkin construction can be generalized to $\mathbb{Z}_2\mathbb{Z}_4$-additive codes.

Definition 1 (Plotkin Construction) *Let $\mathcal{X}$ and $\mathcal{Y}$ be any two $\mathbb{Z}_2\mathbb{Z}_4$-additive codes of types $(\alpha, \beta; \gamma_\mathcal{X}, \delta_\mathcal{X})$, $(\alpha, \beta; \gamma_\mathcal{Y}, \delta_\mathcal{Y})$ and minimum distances $d_\mathcal{X}$, $d_\mathcal{Y}$, respectively. If $\mathcal{G}_\mathcal{X}$ and $\mathcal{G}_\mathcal{Y}$ are the generator matrices of $\mathcal{X}$ and $\mathcal{Y}$, then the matrix*

$$\mathcal{G}_P = \begin{pmatrix} \mathcal{G}_\mathcal{X} & \mathcal{G}_\mathcal{X} \\ 0 & \mathcal{G}_\mathcal{Y} \end{pmatrix}$$

is the generator matrix of a new $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$.

Proposition 2 *Code $\mathcal{C}$ defined above is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(2\alpha, 2\beta; \gamma, \delta)$, where $\gamma = \gamma_\mathcal{X} + \gamma_\mathcal{Y}$, $\delta = \delta_\mathcal{X} + \delta_\mathcal{Y}$, binary length $n = 2\alpha + 4\beta$, size $2^{\gamma+2\delta}$ and minimum distance $d = \min\{2d_\mathcal{X}, d_\mathcal{Y}\}$.*

2.2 BA-Plotkin construction

Applying two Plotkin constructions, one after another, but slightly changing the submatrices in the generator matrix, we obtain a new construction with interesting properties with regard to the minimum distance of the generated code. We call this new construction *BA-Plotkin construction.*

Given a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ with generator matrix $\mathcal{G}$ we denote, respectively, by $\mathcal{G}[b_2]$, $\mathcal{G}[q_2]$, $\mathcal{G}[b_4]$ and $\mathcal{G}[q_4]$ the four submatrices B_2, Q_2, B_4, Q_4 of $\mathcal{G}$ defined in (1); and by $\mathcal{G}[b]$ and $\mathcal{G}[q]$ the submatrices of $\mathcal{G}$, $\begin{pmatrix} B_2 | \\ \hline B_4 | \end{pmatrix}$, $\begin{pmatrix} | Q_2 \\ \hline | Q_4 \end{pmatrix}$, respectively.

Definition 3 (BA-Plotkin Construction) *Let $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ be any three $\mathbb{Z}_2\mathbb{Z}_4$-additive codes of types $(\alpha, \beta; \gamma_\mathcal{X}, \delta_\mathcal{X})$, $(\alpha, \beta; \gamma_\mathcal{Y}, \delta_\mathcal{Y})$, $(\alpha, \beta; \gamma_\mathcal{Z}, \delta_\mathcal{Z})$ and minimum distances $d_\mathcal{X}$, $d_\mathcal{Y}$, $d_\mathcal{Z}$, respectively. Let $\mathcal{G}_\mathcal{X}$, $\mathcal{G}_\mathcal{Y}$ and $\mathcal{G}_\mathcal{Z}$ be the generator matrices* *of the* $\mathbb{Z}_2\mathbb{Z}_4$*-additive codes* $\mathcal{X}$*,* $\mathcal{Y}$ *and* $\mathcal{Z}$*, respectively. We define a new code* $\mathcal{C}$ *as the* $\mathbb{Z}_2\mathbb{Z}_4$*-additive code generated by*

$$\mathcal{G}_{BA} = \left(\begin{array}{cc|cccccc} \mathcal{G}_\mathcal{X}[b] & \mathcal{G}_\mathcal{X}[b] & 2\mathcal{G}_\mathcal{X}[b] & \mathcal{G}_\mathcal{X}[q] & \mathcal{G}_\mathcal{X}[q] & \mathcal{G}_\mathcal{X}[q] & \mathcal{G}_\mathcal{X}[q] \\ 0 & \mathcal{G}_\mathcal{Y}[b_2] & \mathcal{G}_\mathcal{Y}[b_2] & 0 & 2\mathcal{G}'_\mathcal{Y}[q_2] & \mathcal{G}'_\mathcal{Y}[q_2] & 3\mathcal{G}'_\mathcal{Y}[q_2] \\ 0 & \mathcal{G}_\mathcal{Y}[b_4] & \mathcal{G}_\mathcal{Y}[b_4] & 0 & \mathcal{G}_\mathcal{Y}[q_4] & 2\mathcal{G}_\mathcal{Y}[q_4] & 3\mathcal{G}_\mathcal{Y}[q_4] \\ \mathcal{G}_\mathcal{Y}[b_4] & \mathcal{G}_\mathcal{Y}[b_4] & 0 & 0 & 0 & \mathcal{G}_\mathcal{Y}[q_4] & \mathcal{G}_\mathcal{Y}[q_4] \\ 0 & \mathcal{G}_\mathcal{Z}[b] & 0 & 0 & 0 & 0 & \mathcal{G}_\mathcal{Z}[q] \end{array}\right),$$

where $\mathcal{G}'_\mathcal{Y}[q_2]$ *is the matrix obtained from* $\mathcal{G}_\mathcal{Y}[q_2]$ *after switching twos by ones in its* $\gamma_\mathcal{Y}$ *rows of order two, and considering the ones from the third column of the construction as ones in the quaternary ring* $\mathbb{Z}_4$*.*

Proposition 4 *Code* $\mathcal{C}$ *defined above is a* $\mathbb{Z}_2\mathbb{Z}_4$*-additive code of type* $(2\alpha, \alpha + 4\beta; \gamma, \delta)$ *where* $\gamma = \gamma_\mathcal{X} + \gamma_\mathcal{Z}$*,* $\delta = \delta_\mathcal{X} + \gamma_\mathcal{Y} + 2\delta_\mathcal{Y} + \delta_\mathcal{Z}$*, binary length* $n = 4\alpha + 8\beta$*, size* $2^{\gamma+2\delta}$ *and minimum distance* $d = \min\{4d_\mathcal{X}, 2d_\mathcal{Y}, d_\mathcal{Z}\}$*.*

3 Additive Reed-Muller codes

We will refer to $\mathbb{Z}_2\mathbb{Z}_4$-additive Reed-Muller codes as $\mathcal{ARM}$. Just as there is only one RM family in the binary case, in the $\mathbb{Z}_2\mathbb{Z}_4$-additive case there are $\lfloor \frac{m+2}{2} \rfloor$ families for each value of m. Each one of these families will contain any of the $\lfloor \frac{m+2}{2} \rfloor$ non-isomorphic $\mathbb{Z}_2\mathbb{Z}_4$-linear extended perfect codes which are known to exist for any m [3].
We will identify each family $\mathcal{ARM}_s(r,m)$ by a subindex $s \in \{0, \dots, \lfloor \frac{m}{2} \rfloor\}$.

3.1 The families of $\mathcal{ARM}(r, 1)$ and $\mathcal{ARM}(r, 2)$ codes

We start by considering the case $m = 1$, that is the case of codes of binary length $n = 2^1$. The $\mathbb{Z}_2\mathbb{Z}_4$-additive Reed-Muller code $\mathcal{ARM}(0,1)$ is the repetition code, of type $(2,0;1,0)$ and which only has one nonzero codeword (the vector with only two binary coordinates of value 1). The code $\mathcal{ARM}(1,1)$ is the whole space $\mathbb{Z}_2^2$, thus a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(2,0;2,0)$. Both codes $\mathcal{ARM}(0,1)$ and $\mathcal{ARM}(1,1)$ are binary codes with the same parameters and properties as the corresponding binary $RM(r,1)$ codes (see [8]). We will refer to them as $\mathcal{ARM}_0(0,1)$ and $\mathcal{ARM}_0(1,1)$, respectively.

The generator matrix of $\mathcal{ARM}_0(0,1)$ is $\mathcal{G}_0(0,1) = \begin{pmatrix} 1 & 1 \end{pmatrix}$ and the generator matrix of $\mathcal{ARM}_0(1,1)$ is $\mathcal{G}_0(1,1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

For $m = 2$ we have two families, $s = 0$ and $s = 1$, of additive Reed-Muller codes of binary length $n = 2^2$. The family $\mathcal{ARM}_0(r,2)$ consists of binary codes obtained from applying the Plotkin construction defined in Proposition 2 to the family $\mathcal{ARM}_0(r,1)$. For $s = 1$, we define $\mathcal{ARM}_1(0,2)$, $\mathcal{ARM}_1(1,2)$ and $\mathcal{ARM}_1(2,2)$ as the codes with generator matrices $\mathcal{G}_1(0,2) = \left(\begin{array}{cc|c} 1 & 1 & 2 \end{array}\right)$, $\mathcal{G}_1(1,2) = \left(\begin{array}{cc|c} 1 & 1 & 2 \\ \hline 0 & 1 & 1 \end{array}\right)$ and $\mathcal{G}_1(2,2) = \left(\begin{array}{cc|c} 1 & 1 & 2 \\ 0 & 1 & 0 \\ \hline 0 & 1 & 1 \end{array}\right)$, respectively.

3.2 Plotkin and BA-Plotkin constructions

Take the family $\mathcal{ARM}_s$ and let $\mathcal{ARM}_s(r, m-1)$, $\mathcal{ARM}_s(r-1, m-1)$ and $\mathcal{ARM}_s(r-2, m-1)$, $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$, be three consecutive codes with parameters $(\alpha, \beta; \gamma', \delta')$, $(\alpha, \beta; \gamma'', \delta'')$ and $(\alpha, \beta; \gamma''', \delta''')$; binary length $n = 2^{m-1}$; minimum distances 2^{m-r-1}, 2^{m-r} and 2^{m-r+1}; and generator matrices $\mathcal{G}_s(r, m-1)$, $\mathcal{G}_s(r-1, m-1)$ and $\mathcal{G}_s(r-2, m-1)$, respectively. By using Proposition 2 and Proposition 4 we can prove the following results:

Theorem 5 *For any r and $m \geq 2$, $0 < r < m$, code $\mathcal{ARM}_s(r, m)$ obtained by applying the Plotkin construction from Definition 1 on codes $\mathcal{ARM}_s(r, m-1)$ and $\mathcal{ARM}_s(r-1, m-1)$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type (2α, 2β; γ, δ), where $\gamma = \gamma' + \gamma''$ and $\delta = \delta' + \delta''$; binary length $n = 2^m$; size 2^k codewords, where $k = \sum_{i=0}^{r} \binom{m}{i}$; minimum distance 2^{m-r} and $\mathcal{ARM}_s(r-1, m) \subset \mathcal{ARM}_s(r, m)$.*

We consider $\mathcal{ARM}_s(0, m)$ to be the repetition code with only one nonzero codeword (the vector with 2α ones and 2β twos) and $\mathcal{ARM}_s(m, m)$ be the whole space $\mathbb{Z}_2^{2\alpha} \times \mathbb{Z}_4^{2\beta}$.

Theorem 6 *For any r and $m \geq 3$, $0 < r < m$, $s > 0$, use the BA-Plotkin construction from Definition 3, where generator matrices $\mathcal{G}_\mathcal{X}$, $\mathcal{G}_\mathcal{Y}$, $\mathcal{G}_\mathcal{Z}$ stand for $\mathcal{G}_s(r, m-1)$, $\mathcal{G}_s(r-1, m-1)$ and $\mathcal{G}_s(r-2, m-1)$, respectively, to obtain a new $\mathbb{Z}_2\mathbb{Z}_4$-additive $\mathcal{ARM}_{s+1}(r, m+1)$ code of type (2α, $\alpha + 4\beta$; γ, δ), where $\gamma = \gamma' + \gamma'''$, $\delta = \delta' + \gamma'' + 2\delta'' + \delta'''$; binary length $n = 2^{m+1}$; 2^k codewords, where $k = \sum_{i=0}^{r} \binom{m+1}{i}$, minimum distance 2^{m-r+1} and, moreover, $\mathcal{ARM}_{s+1}(r-1, m+1) \subset \mathcal{ARM}_{s+1}(r, m+1)$.*

To be coherent with all notations, code $\mathcal{ARM}_{s+1}(-1, m+1)$ is defined as the all zero codeword code, code $\mathcal{ARM}_{s+1}(0, m+1)$ is defined as the repetition code with only one nonzero codeword (the vector with 2α ones and $\alpha + 4\beta$ twos), whereas codes $\mathcal{ARM}_{s+1}(m, m+1)$ and $\mathcal{ARM}_{s+1}(m+1, m+1)$ are defined as the even Lee weight code and the whole space $\mathbb{Z}_2^{2\alpha} \times \mathbb{Z}_4^{\alpha+4\beta}$, respectively.

Using both Theorem 5 and Theorem 6 we can now construct all $\mathcal{ARM}_s(r, m)$ codes for $m > 2$. Once applied the Gray map, all these codes give rise to binary codes with the same parameters and properties as the *RM* codes. Moreover, when $m = 2$ or $m = 3$, they also have the same codewords.

References

1. J. Borges, J. Rifà, A characterization of 1-perfect additive codes. *IEEE Trans. Inform. Theory*, 45(5): 1688-1697, 1999.
2. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes.* North-Holland Publishing Company, 1977.