Augmented Reed-Muller Codes of High Rate and Erasure Repair

Hiram H. López
Department of Mathematics and Statistics
Cleveland State University
Cleveland, Ohio 44115
Email: h.lopezvaldez@csuohio.edu

Gretchen L. Matthews
Department of Mathematics
Virginia Tech
Blacksburg, VA 24061
Email: gmatthews@vt.edu

Daniel Valvo
Department of Mathematics
Virginia Tech
Blacksburg, VA 24061
Email: vdaniel1@vt.edu

***Abstract*—We present two families of augmented Reed-Muller (ARM) codes, which are evaluation codes obtained by adding specific vectors to a Reed-Muller code. We develop exact repair schemes for single erasures for these ARM codes. When a dimension and a base field are fixed, we give examples where ARM codes provide a lower bandwidth in comparison with Reed-Solomon codes. We analyze the asymptotical behavior when ARM codes achieve the maximum rate.**

I. Introduction

Distributed storage systems operate by storing a data file over multiple storage nodes. Ideally, the system is set up so if one node fails, the information on that node can be recovered with the information stored on the remaining nodes. A scheme to exactly recover a failed node is known as an *exact repair scheme*. Particular types of systems known as erasure-coded distributed storage systems distribute the data in accordance with an erasure code, where the the data file is encoded as a codeword and each node stores a symbol. With this setup, it is clear that recovering a failed node exactly is equivalent to fixing an erasure in the codeword [3], [4].

Recently, much work has been done on developing efficient repair schemes for erasure-coded distributed storage systems based on evaluation codes. Notably, Guruwarmi and Wooters developed a foundational scheme (GW-scheme) to efficiently repair a single erasure in a Reed-Solomon (RS) code in [6], and this work was extended by Chen and Zhang in [1] to efficiently repair Reed-Muller (RM) codes. These schemes gain their advantage by employing the concept of subsymbols. Rather than transmit a certain number of remaining symbols from a codeword to recover an erasure, Guruswarmi and Wooters opted to transmit subsymbols, but from more coordinates. In this context, every symbol is represented by several subsymbols. With the right subsymbols in an appropriate set-up, these new schemes require less information than standard approaches to repair.

Both RS and RM codes are evaluation codes that employ polynomials with restricted degrees. Using such a set of polynomials allows for easily definable codes, but there is no reason to expect this set will yield the highest rate or most efficiently repairable codes. *Monomial-Cartesian codes* [9] are evaluation codes that allow for more finely-tuned polynomial sets. We can develop *augmented Reed-Muller (ARM) codes* via monomial-Cartesian codes, which are evaluation codes obtained when certain vectors are added to a RM code so that the dimension is increased and a linear exact repair scheme can still be implemented. In this paper, we introduce two families of ARM codes and develop associated exact repair schemes.

The GW-scheme repairs a RS code provided the code satisfies a restriction on the dimension. Hence, there are codes and parameters for which the GW-scheme does not apply. In this paper, we fill some of those gaps using ARM codes. When a dimension and a base field are fixed, there are instances where ARM codes provide a lower bandwidth in comparison with RS codes, and a lower bandwidth in terms of bits versus Hermitian codes.

A. Preliminaries

Let q be a power of a prime p and $K = \mathbb{F}_{q^t}$ a field extension of degree $t = [K : \mathbb{F}_q]$ of $\mathbb{F}_q$. The *field trace* can be defined as the polynomial $\mathrm{Tr}_{K/\mathbb{F}_q}(x) \in K[x]$ given by

$$\mathrm{Tr}_{K/\mathbb{F}_q}(x) = x^{q^{t-1}} + \cdots + x^{q^0}.$$

For the sake of convenience, we will often refer to $\mathrm{Tr}_{K/\mathbb{F}_q}(x)$ as simply $\mathrm{Tr}(x)$ when the extension being used is obvious from context. Importantly, the field trace $\mathrm{Tr}(x)$ always outputs an element of $\mathbb{F}_q$. Additionally, $\mathrm{Tr}(x)$ is an $\mathbb{F}_q$-linear map, treating the field K as a vector space over $\mathbb{F}_q$. One can also verify that $p(x) := \frac{\mathrm{Tr}(zx)}{x} = z^{q^{t-1}} x^{q^{t-1}-1} + \cdots + z^{q^0}$ satisfies $p(0) = z$ for $z \in K$. Another useful property is found in the next remark.

Remark 1.1. *Let $B = \{z_1, \ldots, z_t\}$ be a basis of K over $\mathbb{F}_q$. Then there exists a basis $B' = \{z'_1, \ldots, z'_t\}$ of K over $\mathbb{F}_q$, such that $Tr(z_i z'_j) = \delta_{ij}$. In this case, B and B' are called dual bases. For $\alpha \in K$,*

$$\alpha = \sum_{i=1}^{t} Tr(\alpha z_i) z'_i.$$

Thus, determining α is equivalent to finding $Tr(\alpha z_i)$ for all $i \in [t] := \{1, \ldots, t\}$ [11].

The work of Hiram H. López was supported in part by the AMS–Simons Travel Grant. The work of Gretchen L. Matthews was supported in part by NSF under Grant DMS-1855136 and in part by the Commonwealth Cyber Initiative. (Corresponding author: Hiram H. López.)

Let C be an $[n,k]$-linear code over K. The elements of K are called *symbols* and the elements of $\mathbb{F}_q$ are called *subsymbols*. Note that every entry of each vector $c \in C$ can be represented using t subsymbols, because K is a degree t extension of $\mathbb{F}_q$. In terms of distributed storage systems, the code C is saved over n different storage nodes, one for each coordinate. When one of the storage nodes fails or is erased, an *exact repair scheme* is an algorithm that is able to recover the information of the erased node in terms of the rest of the storage nodes. The *repair bandwidth* b is the number of subsymbols that the scheme algorithm needs to download to recover the erased entry. Observe that a vector $c \in K^n$ is composed of nt subsymbols, so the number $\frac{b}{nt}$ can be seen as the fraction of the codeword that is needed by the exact repair scheme to recover the erased symbol.

By Reed-Muller codes, we mean the evaluation codes obtained when polynomials in m variables up to certain total degree $k \in \mathbb{Z}_{\geq 0}$ are evaluated at all the points of K^m. In this work, we are interested in two new families of codes that are obtained when certain polynomials in m variables are evaluated on all the points of K^m. Reed-Muller codes and these two families of evaluation codes are particular cases of monomial-Cartesian codes [9], whose definition is the following. Let $R = K[x_1, \ldots, x_m]$ be the set of m-variate polynomials over K. For a point $\boldsymbol{a} = (a_1, \ldots, a_m) \in \mathbb{Z}_{\geq 0}^m$, we use $\boldsymbol{x^a}$ to denote the monomial $x_1^{a_1} \cdots x_m^{a_m} \in R$. Given a set $\mathcal{A} \subseteq \mathbb{Z}_{\geq 0}^m$, let $\mathcal{L}(\mathcal{A}) = \mathrm{Span}_K\{\boldsymbol{x^a} \ : \ \boldsymbol{a} \in \mathcal{A}\}$ be the set of K-linear combinations of monomials with exponents in $\mathcal{A}$.

Definition 1.2. Let $\mathcal{S} = \{P_1, \ldots, P_n\} \subseteq K^m$ be a Cartesian set and $\mathcal{A} \subset \mathbb{Z}_{\geq 0}^m$ a finite set. The *monomial-Cartesian code* associated to $\mathcal{S}$ and $\mathcal{A}$ is given by

$$\mathcal{C}(\mathcal{S}, \mathcal{A}) = \{\mathrm{ev}_{\mathcal{S}}(f) \ : \ f \in \mathcal{L}(\mathcal{A})\} \subseteq K^n,$$

where $\mathrm{ev}_{\mathcal{S}}(f) = (f(P_1), \ldots, f(P_n))$.

Remark 1.3. *Assume $\mathcal{S} = S_1 \times \cdots \times S_m$, where $S_i \subseteq K$. When $\mathcal{A} \subseteq \prod_{i=1}^m \{0, \ldots, |S_i| - 1\}$, the function $ev_{\mathcal{S}} \colon \mathcal{L}(\mathcal{A}) \to K^n$ given by $ev_{\mathcal{S}}(f) = (f(P_1), \ldots, f(P_n))$ is injective. Thus, for the monomial-Cartesian code $\mathcal{C}(\mathcal{S}, \mathcal{A})$, the length is $|\mathcal{S}|$, the dimension is $\dim_K \mathcal{C}(\mathcal{S}, \mathcal{A}) = |\mathcal{A}|$, and the rate is $\frac{|\mathcal{A}|}{|\mathcal{S}|}$.*

Definition 1.4. The *Reed-Muller code* (RM code) is given by

$$\mathrm{RM}(K^m, k) = \mathcal{C}(K^m, \mathcal{A}_{RM}(k)),$$

where $\mathcal{A}_{RM}(k) = \{\boldsymbol{a} \in \mathbb{Z}_{\geq 0}^m \ : \ a_i \leq |K| - 1, \sum_{i=1}^m a_i \leq k\}$.

The dual of $\mathcal{C}(\mathcal{S}, \mathcal{A})$, denoted by $\mathcal{C}(\mathcal{S}, \mathcal{A})^\perp$, is the set of all $\alpha \in K^n$ such that $\alpha \cdot \beta = 0$ for all $\beta \in \mathcal{C}(\mathcal{S}, \mathcal{A})$, where $\alpha \cdot \beta$ is the ordinary inner product in K^n. The dual code $\mathcal{C}(\mathcal{S}, \mathcal{A})^\perp$ was previously studied in [9] in terms of the vanishing ideal of $\mathcal{S}$ and in [10] in terms of the indicator functions of $\mathcal{S}$. The dual code $\mathrm{RM}(K^m, k)^\perp$ has been extensively studied in the literature. See for instance [1], [2], [7].

II. Repairing augmented Reed-Muller code 1

We define now a family of ARM codes. Then we describe a scheme to repair an erasure inspired by Guruswarmi and Wooters's work in [6] for Reed-Solomon codes and later extended in [1] by Chen and Zhang for generalized Reed-Muller codes.

Definition 2.1. The *augmented Reed-Muller code 1* (ARM1 code) is defined by

$$\mathrm{ARM1}(K^m, k) = \mathcal{C}(K^m, \mathcal{A}_1(k)),$$

where $\mathcal{A}_1(k) = \{0, \ldots, |K| - 1\}^m \setminus \{k+1, \ldots, |K| - 1\}^m$.

Remark 2.2. *As $\mathcal{A}_{RM}(k) \subset \mathcal{A}_1(k)$, we clearly obtain $RM(K^m, k) \subset ARM1(K^m, k)$, hence the name augmented Reed-Muller code 1 is appropriate.*

The following proposition will be relevant to develop the exact repair scheme for $\mathrm{ARM1}(K^m, k)$.

Proposition 2.3. *Take $k < |K|$. The dimension and the dual of the augmented Reed-Muller code 1 are given by*

(a) $\dim ARM1(K^m, k) = q^{tm} - (q^t - k - 1)^m$, *and*
(b) $ARM1(K^m, k)^\perp = \mathcal{C}(K^m, \mathcal{A}_1^\perp(k))$,
where $\mathcal{A}_1^\perp(k) = \{0, \ldots, |K| - k - 2\}^m$.

Proof. As $\mathcal{A}_1(k)$ is contained in $\{0, \ldots, |K| - 1\}^m$, by Remark 1.3 we have that $\dim_K \mathrm{ARM1}(K^m, k) = |\mathcal{A}_1(k)| = |\{0, \ldots, |K| - 1\}^m \setminus \{k+1, \ldots, |K| - 1\}^m| = q^{tm} - (q^t - k - 1)^m$. Observe that $a \in \mathcal{A}_1^c$ if and only if $(|K| - 1, \ldots, |K| - 1) - a \in \mathcal{A}_1^\perp(k)$. Thus the result about the dual follows from [10, Theorem 7.8]. □

Example 2.4. Take $K = \mathbb{F}_7$. The code $\mathrm{ARM1}(K^2, 2)$ is generated by the vectors $\mathrm{ev}_{K^2}(M)$, where M is a monomial whose exponent is a point in Figure 1(a). The dual $\mathrm{ARM1}(K^2, 2)^\perp$ is generated by the vectors $\mathrm{ev}_{K^2}(M)$, where M is a monomial whose exponent is a point in Figure 1(b).

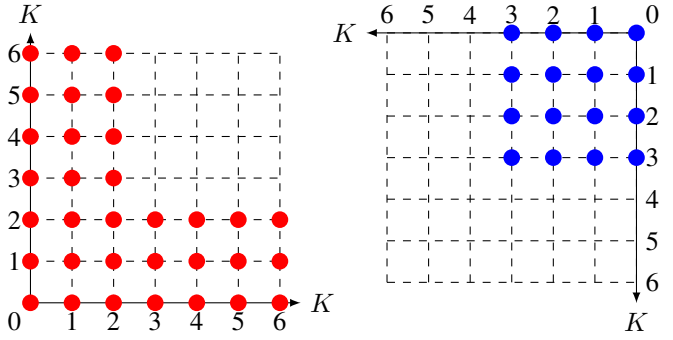

Fig. 1: The $\mathrm{ARM1}(K^2, 2)$ code in Example 2.4 with $K = \mathbb{F}_7$ is generated by the vectors $\mathrm{ev}_{K^2}(M)$, where M is a monomial whose exponent corresponds to a point in (a). $\mathrm{ARM1}(K^2, 2)^\perp$ is generated by the vectors $\mathrm{ev}_{K^2}(M)$, where M is a monomial whose exponent corresponds to a point in (b).

Compare this to Figure 2, which shows the monomials that define $\mathrm{RM}(K^2, 2)$ and $\mathrm{RM}(K^2, 2)^\perp$. Notice, by the definition, the monomial diagram for any Reed-Muller code will restrict the allowable monomials under some diagonal. This excludes many monomials along or near the edges, resulting in codes with lower dimensions and rates. Hence the reason ARM1 codes have higher rates than their associated Reed-Muller codes.

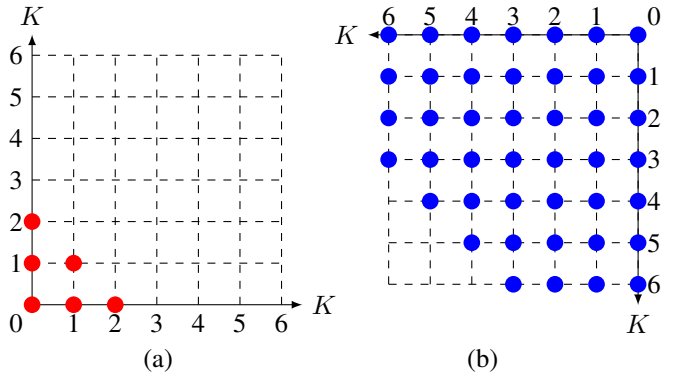

Fig. 2: The code $\mathrm{RM}(K^2, 2)$ in Example 2.4 with $K = \mathbb{F}_7$ is generated by the vectors $\mathrm{ev}_{K^2}(M)$, where M is a monomial whose exponent corresponds to a point in (a). The dual $\mathrm{RM}(K^2, 2)^\perp$ is generated by the vectors $\mathrm{ev}_{K^2}(M)$, where M is a monomial whose exponent corresponds to a point in (b).

Theorem 2.5. *Assume $k < q^t - q^{t-1}$. There exists an exact repair scheme for ARM1(K^m, k) with bandwidth*

$$b = t|K|^m - (t-1)(|K|-1)^m - t.$$

Proof. Let $P^* = (\alpha_1^*, \ldots, \alpha_m^*) \in K^m$ and assume that the entry $f(P^*)$ of the codeword $(f(P_1), \ldots, f(P_n)) \in \mathrm{ARM1}(K^m, k)$ is erased. Let $\{z_1, \ldots, z_t\}$ be a basis for K over $\mathbb{F}_q$. For $i \in [t]$, define the following polynomials

$$p_i(\boldsymbol{x}) = \frac{\mathrm{Tr}(z_i(x_1 - \alpha_1^*)\cdots(x_m - \alpha_m^*))}{(x_1 - \alpha_1^*)\cdots(x_m - \alpha_m^*)}.$$

By Proposition 2.3, the dual $\mathrm{ARM1}(K^m, k)^\perp$ is given by $\mathcal{C}(K^m, \{0, \ldots, |K| - k - 2\}^m)$. We have that $k < q^t - q^{t-1}$, then $|K| - k - 2 \geq |K| - q^t + q^{t-1} + 1 - 2 = q^{t-1} - 1$. As $\deg_{x_j} p_i(\boldsymbol{x}) \leq q^{t-1} - 1$ and the monomials that appear on each $p_i(\boldsymbol{x})$ are of the form $x_1^{a_1} \ldots x_m^{a_m}$ where $0 \leq a_i < q^{t-1}$, we obtain that every polynomial $p_i(\boldsymbol{x})$ defines an element in $\mathrm{ARM1}(K^m, k)^\perp$. Therefore, we obtain the t equations

$$p_i(P^*)f(P^*) = -\sum_{P \in K^m \setminus \{P^*\}} p_i(P)f(P), \quad i \in [t].$$

Define the following two sets:

$$\Gamma_1 = \{(\alpha_1, \ldots, \alpha_m) \in K^m \,|\, \alpha_i = \alpha_i^* \text{ some } i\} \setminus \{P^*\},$$
$$\Gamma_2 = \{(\alpha_1, \ldots, \alpha_m) \in K^m \,|\, \alpha_i \neq \alpha_i^* \text{ for all } i\}.$$

Observe $p_i(P) = z_i$ for all $P \in \Gamma_1$. Thus, for $i \in [t]$,

$$z_i f(P^*) = -\sum_{P \in \Gamma_1} z_i f(P) - \sum_{P \in \Gamma_2} \frac{\mathrm{Tr}(z_i \prod_{i=1}^m (\alpha_i - \alpha_i^*))f(P)}{\prod_{i=1}^m (\alpha_i - \alpha_i^*)}.$$

Applying the trace function to both sides, by the linearity of the trace function we obtain

$$\mathrm{Tr}\left(z_i f(P^*)\right) = -\sum_{P \in \Gamma_1} \mathrm{Tr}\left(z_i f(P)\right) - \sum_{P \in \Gamma_2} \mathrm{Tr}(z_i \prod_{i=1}^m (\alpha_i - \alpha_i^*)) \mathrm{Tr}\left(\frac{f(P)}{\prod_{i=1}^m (\alpha_i - \alpha_i^*)}\right).$$

As a consequence, the t independent traces $\mathrm{Tr}\left(z_i f\left(P^*\right)\right), i \in [t]$, of $f(P^*)$ can be determined by downloading the following.

- The symbol $f(P)$, which is equivalent to the t subsymbols $\mathrm{Tr}\left(z_1 f(P)\right), \ldots, \mathrm{Tr}\left(z_t f(P)\right)$, for $P \in \Gamma_1$.
- The subsymbol $\mathrm{Tr}\left(\frac{f(P)}{\prod_{i=1}^m (\alpha_i - \alpha_i^*)}\right)$ for $P \in \Gamma_2$.

Thus, by Remark 1.1 the erased symbol $f(P^*)$ can be recovered from its t independent traces by downloading $t|\Gamma_1| + |\Gamma_2|$ subsymbols. Note, $|\Gamma_2| = (|K| - 1)^m$ and $|\Gamma_1| = |K^m \setminus \Gamma_2 \cup \{P^*\}| = |K|^m - (|K| - 1)^m - 1$. Hence, the bandwidth becomes $b = t|K|^m - (t-1)(|K| - 1)^m - t$, as desired. □

III. Repairing Augmented Reed-Muller code 2

We now define a second family of augmented Reed-Muller codes and provide an associated exact repair scheme. Note that this exact repair scheme has a greater bandwidth, but importantly the rate is improved with respect to the family defined in Section II.

Definition 3.1. The *augmented Reed-Muller code 2* (ARM2-code) is defined as

$$\mathrm{ARM2}(K^m, k) = \mathcal{C}(K^m, \mathcal{A}_2(k)),$$

where $\mathcal{A}_2(k) = \{0, \ldots, |K| - 1\}^m \setminus \bigcup_{i=1}^m L_i$ and

$$L_i = \{\boldsymbol{a} \in K^m \,:\, k{+}1 \leq a_i \leq |K|{-}1\,,\; a_j = |K|{-}1 \;\forall j \neq i\}$$

Proposition 3.2. *Take $k < |K|$. The dimension and the dual of the augmented Reed-Muller code 2 are given by*

(a) $\dim$ *ARM2*$(K^m, k) = q^{tm} - m(q^t - k - 2) - 1$, *and*
(b) *ARM2*$(K^m, k)^\perp = \mathcal{C}\left(K^m, \mathcal{A}_2^\perp(k)\right)$,

where $\mathcal{A}_2^\perp(k) = \bigcup_{i=1}^m L_i'$ and

$$L_i' = \{\boldsymbol{a} \in K^m \,:\, 0 \leq a_i \leq |K|{-}k{-}2\;,\; a_j = 0 \;\forall j \neq i\}.$$

Proof. The set $\mathcal{A}_2(k)$ is contained in $\{0, \ldots, |K| - 1\}^m$. By Remark 1.3 we have that $\dim_K \mathrm{ARM2}(K^m, k) = |\mathcal{A}_2(k)| = |\{0, \ldots, |K| - 1\}^m \setminus \bigcup_{i=1}^m L_i| = q^{tm} - |\bigcup_{i=1}^m L_i|$. As $\bigcap_{i=1}^m L_i = \{a\}$, where $a = (|K| - 1, \ldots, |K| - 1)$, and $(L_i \setminus \{a\}) \bigcap (L_j \setminus \{a\}) = \emptyset$ for all $i \neq j$, then $|\bigcup_{i=1}^m L_i| = \sum_{i=1}^m |L_i \setminus \{a\}| + 1 = m(|K| - k - 2) + 1$. Thus $\dim \mathrm{ARM1}(K^m, k) = q^{tm} - m(q^t - k - 2) - 1$. Observe that $b \in \mathcal{A}_2^c$ if and only if $(|K| - 1, \ldots, |K| - 1) - b \in \mathcal{A}_2^\perp(k)$. Thus the result follows from [10, Theorem 7.8]. □

Example 3.3. Take $K = \mathbb{F}_7$. The code $\mathrm{ARM2}(K^2, 2)$ is generated by the vectors $\mathrm{ev}_{K^2}(M)$, where M is a monomial whose exponent is a point in Figure 1(a). The dual $\mathrm{ARM2}(K^2, 2)^\perp$ is generated by the vectors $\mathrm{ev}_{K^2}(M)$, where M is a monomial whose exponent is a point in Figure 1(b).

Theorem 3.4. *Assume $k < q^t - q^{t-1}, t > m$ and $(m, p) = 1$. There exists a repair scheme algorithm for ARM2(K^m, k) with bandwidth $b = t|K|^m - (t - m)(|K| - 1)^m - t$.*

Proof. Let $P^* = (\alpha_1^*, \ldots, \alpha_m^*)$ be an element in K^m and assume that the entry $f(P^*)$ is missing in the codeword $(f(P_1), \ldots, f(P_n)) \in \mathrm{ARM2}(K^m, k)$. Let $\{z_1, \ldots, z_t\}$ be a basis for K over $\mathbb{F}_q$. For $i \in [t]$, define the following polynomials:

$$p_i(\boldsymbol{x}) = \sum_{j=1}^m \frac{\mathrm{Tr}(z_i(x_j - \alpha_j^*))}{x_j - \alpha_j^*}.$$

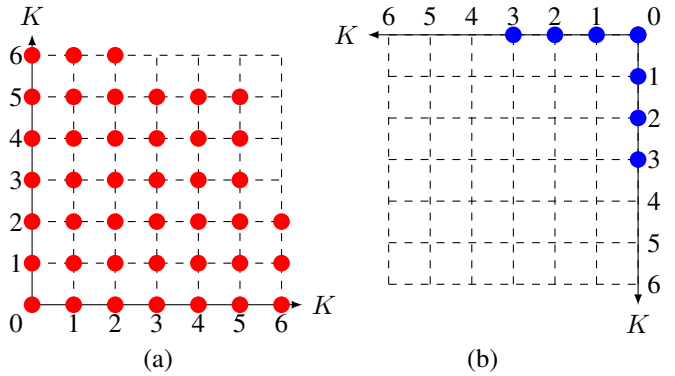

Fig. 3: The code ARM2$(K^2, 2)$ in Example 3.3 with $K = \mathbb{F}_7$ is generated by the vectors $\mathrm{ev}_{K^2}(M)$, where M is a monomial whose exponent corresponds to a point in (a). The dual ARM2$(K^2, 2)^\perp$ is generated by the vectors $\mathrm{ev}_{K^2}(M)$, where M is a monomial whose exponent corresponds to a point in (b).

By Proposition 3.2, the dual ARM2$(K^m, k)^\perp$ is given by $\mathcal{C}\left(K^m, \mathcal{A}_2^\perp(k)\right)$, where $\mathcal{A}_2^\perp(k) = \bigcup_{i=1}^m L_i'$ and $L_i' = \{\boldsymbol{a} \in K^m \ : \ 0 \leq a_i \leq |K|-k-2 \ , \ a_j = 0 \ \forall j \neq i\}$. We have that $k < q^t - q^{t-1}$. Then $|K| - k - 2 \geq |K| - q^t + q^{t-1} + 1 - 2 = q^{t-1} - 1$. As $\deg_{x_j} p_i(\boldsymbol{x}) \leq q^{t-1} - 1$ and the monomials that appear on each $p_i(\boldsymbol{x})$ are of the form $x_j^{a_j}$ where $0 \leq a_j < q^{t-1}$ and $1 \leq j \leq m$, we obtain that every polynomial $p_i(\boldsymbol{x})$ define an element in ARM2$(K^m, k)^\perp$. Therefore, we obtain the following t equations

$$p_i(P^*)f(P^*) = -\sum_{P \in K^m \setminus \{P^*\}} p_i(P)f(P), \quad i \in [t].$$

Define Γ_1 and Γ_2 as in the proof of Theorem 2.5. Observe that if $P \in \Gamma_1$, then there exist an integer $\ell_P \geq 1$ and an element β_P in $\mathbb{F}_q$ such that $p_i(P) = (\ell_P)z_i + \beta_P$. Actually ℓ_P is the number of entries where P and P^* coincide, in other words, $\ell = m - d_H(P, P^*)$, where $d_H(P, P^*)$ represents the Hamming distance. Even more, $p_i(P^*) = mz_i$, hence why it is relevant that $(m, p) = 1$. Thus, applying the trace and by the linearity of the trace function we obtain that for $i \in [t]$

$$\begin{aligned} &m\mathrm{Tr}\left(z_i f(P^*)\right) = \\ &-\sum_{P \in \Gamma_1} \mathrm{Tr}\left(\left[(\ell_P)z_i + \beta_P\right] f(P)\right) \\ &-\sum_{P \in \Gamma_2} \sum_{j=1}^{m} \mathrm{Tr}(z_i(\alpha_j - \alpha_j^*))\mathrm{Tr}\left(\frac{f(P)}{\alpha_j - \alpha_j^*}\right). \end{aligned}$$

As a consequence, the t independent traces $\mathrm{Tr}\left(z_i f\left(P^*\right)\right)$, $i \in [t]$, of $f(P^*)$ can be determined by downloading the whole symbol $f(P)$, for $P \in \Gamma_1$, and the m subsymbols $\mathrm{Tr}\left(\frac{f(P)}{\alpha_1 - \alpha_1^*}\right), \ldots, \mathrm{Tr}\left(\frac{f(P)}{\alpha_m - \alpha_m^*}\right)$ from each $f(P)$, where $P \in \Gamma_2$. Thus, by Remark 1.1 the erased symbol $f(P^*)$ can be recovered from its t independent traces by downloading $t|\Gamma_1| + m|\Gamma_2| = t|K|^m - (t-m)(|K|-1)^m - t$ subsymbols. □

There are important comments about the repair polynomials $p_i(\boldsymbol{x})$ defined in the proofs of Theorems 2.5 and 3.4. **(a)** While the proofs of Theorems 2.5 and 3.4 are similar in spirit, both are important because each shows the behavior of $p_i(\boldsymbol{x})$ and their impact on the computation of the bandwidths. **(b)** Every ARM code has the property that the $p_i(\boldsymbol{x})$'s define an element in its dual. Trivial modifications in the $p_i(\boldsymbol{x})$'s can give an even larger family of ARM codes. For instance, in the $p_i(\boldsymbol{x})$'s of the proof of the Theorem 3.4, instead of the sum from $j = 1$ to m, we may have the sum from $j = 1$ to ℓ, with $1 \leq \ell < m$. This would allows to define ARM2$'(K^m, k)$ using $\mathcal{A}_2'(k) = \{0, \ldots, |K| - 1\}^m \setminus \bigcup_{i=1}^{\ell} L_i$ as in Definition 3.1. However, a difference between ARM2(K^m, k) and ARM2$'(K^m, k)$ is that the minimum distance of ARM2$'(K^m, k)$ is lower that of ARM2$'(K^m, k)$ by [5, Proposition 4].

IV. Results

The Reed-Solomon code with evaluation set K and dimension k is denoted by RS(K, k). Table I shows the length, dimension, bandwidth and restrictions on the exact repair schemes that we have discussed in previous sections for the RS, RM, ARM1 and ARM2 codes.

We first compare the GW-scheme and the scheme developed for the ARM1 codes (ARM1-scheme) in Theorem 2.5 when the dimension and the base field $\mathbb{F}_q$ are the same. Assume m divides t and $t = mt^*$. The GW-scheme and the ARM1-scheme repair the codes RS$(\mathbb{F}_{q^t}, k)$ and ARM1$(\mathbb{F}_{q^{t^*}}^m, k)$ when the dimensions are at most $q^t - q^{t-1}$ and $q^t - q^{t-m}$, respectively. An advantage of the ARM1$(\mathbb{F}_{q^{t^*}}^m, k)$ comes when a code with dimension k^* between $q^t - q^{t-1}$ and $q^t - q^{t-m}$ is required. The restriction on the dimension of the GW-scheme implies that to employ an RS code, it must utilize an alphabet of size q^{t+1} to achieve dimension k^*. However, as the dimension of the code ARM1$(\mathbb{F}_{q^{t^*}}^m, k)$ can be up to $q^t - q^{t-m}$, there are values between $q^t - q^{t-1}$ and q^t where we can still use ARM1$(\mathbb{F}_{q^{t^*}}^m, k)$, whose bandwidth can be lower. We show this in the following example.

Code	Length	Dimension	Bandwidth	Restrictions
RS(K, k)	q^t	k	$q^t - 1$	$k < q^t - q^{t-1}$ by [6, Theorem 1]
RM(K^m, k)	q^{mt}	$\binom{m+k}{k}$	$(q^t - 1)(t - \lfloor \log_q(q^t - k - 1) \rfloor)$	$k < q^t - 1$ by [1, Theorem III.1]
ARM1(K^m, k)	q^{mt}	$q^{tm} - (q^t - k - 1)^m$	$tq^{tm} - (t-1)(q^t - 1)^m - t$	$k < q^t - q^{t-1}$ by Theorem 2.5
ARM2(K^m, k)	q^{mt}	$q^{tm} - m(q^t - k - 2) - 1$	$tq^{tm} - (t-m)(q^t - 1)^m - t$	$k < q^t - q^{t-1}, m < t, (m, p) = 1$ by Theorem 3.4

TABLE I: For each code we consider the associated linear exact repair scheme over $\mathbb{F}_q$, with $K = GF(q^t)$ a field extension of degree t of $\mathbb{F}_q$.

Example 4.1. Assume that a code of dimension $k^* = 648$ over a field of characteristic 3 is required. Observe that $3^6 - 3^5 = 486 < k^* < 3^6 = 729$. Over the field of size 3^6, there is a Reed-Solomon code with dimension 648, but the GW-scheme is not applicable. Indeed, the requirement that the dimension is at most $n - q^{t-1} = 486$ is not satisfied. To resolve this, a larger field such as one of size $3^7 = 2187$ may be used. Given that the GW-scheme requires the dimension to be at most $n - q^{t-1}$, the RS code's length must then be bounded below by $648 + q^{t-1} = 1377$, meaning the bandwidth is at least 1376. The code ARM1$(\mathbb{F}_{3^3}^2, 17)$ has dimension k^* and bandwidth 837. As a consequence we obtain the following. Using RS codes and the GW-scheme, we obtain a code over F_{2187}, length 1377, bandwidth 1376 and dimension 648. Using ARM1 and the ARM1-scheme, we obtain a code over F_{27}, length 729, bandwidth 837 and dimension 648.

Example 4.2. The code ARM1$(\mathbb{F}_{2^3}^3, 3)$ has length 512 and dimension 448. The bandwidth in bits is 847, whereas the Hermitian code of the same rate in [8, Example 14] requires (3)(511)=1533 bits for repair. In addition, the ARM1$(\mathbb{F}_{2^3}^3, 3)$ code is over $\mathbb{F}_8$, while the Hermitian code is over $\mathbb{F}_{64}$. An RS code of the same length and dimension requires a field of size at least 512 and 1533 bits for repair.

By Table I, the ARM codes will have greater repair bandwidths than the RM codes when q increases. However, the expression makes it difficult to immediately determine the massive rate improvement gained by implementing the ARM codes. Figure 4 graphs the rate versus the repair bandwidth of the exact repair schemes of RM$(\mathbb{F}_{5^4}^3, k)$, ARM1$(\mathbb{F}_{5^4}^3, k)$, and ARM2$(\mathbb{F}_{5^4}^3, k)$, for all values of k that satisfy the restriction in Table I. The same figure demonstrates that RM codes admit repair schemes with much lower bandwidths than the ARM. However, it also reveals that the ARM codes have significantly higher rates, increasing from at most 0.2 to more than 0.99.

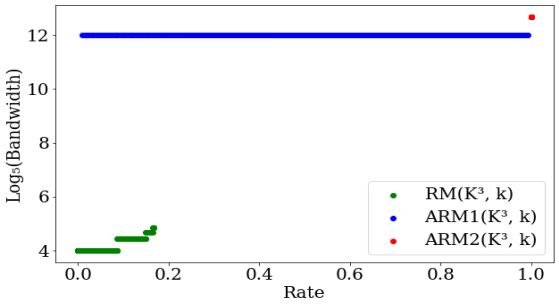

Fig. 4: Rate versus the repair bandwidth of the exact repair schemes of RM$(\mathbb{F}_{5^4}^3, k)$, ARM1$(\mathbb{F}_{5^4}^3, k)$, and ARM2$(\mathbb{F}_{5^4}^3, k)$, for all values of k that satisfy the restriction in Table I.

Example 4.3. By Table I, the maximum k for RM$(\mathbb{F}_{2^7}^5, k)$, ARM1$(\mathbb{F}_{2^7}^5, k)$ and ARM2$(\mathbb{F}_{2^7}^5, k)$ are 126, 63 and 63, respectively. The code RM$(\mathbb{F}_{2^7}^5, 126)$ has rate 0.009002376 and bandwidth 889. The code ARM1$(\mathbb{F}_{2^7}^5, 62)$ has rate 0.96975 and bandwidth 4.229×10^{10}. The code ARM2$(\mathbb{F}_{2^7}^5, k)$ has rate 0.999999991 and bandwidth 1.744×10^{11}.

A. Maximum rates and asymptotical behavior

Focusing on the improved rate, here we study the asymptotic behavior of the rate and $\frac{b}{nt}$. The maximum k for which RM(K^m, k) admits the repair scheme given in [1, Theorem III.1] is $k^* = q^t - 2$. In this case, by Table I $\dim_K \mathrm{RM}(K^m, k^*) = \binom{m+q^t-2}{q^t-2}$ and b^* = bandwidth at $k^* = (q^t-1)t$. Thus $\lim_{t\to\infty} \frac{\dim_K \mathrm{RM}(K^m,k^*)}{n} = \lim_{t\to\infty} \frac{\binom{m+q^t-2}{q^t-2}}{q^{tm}} \leq \lim_{t\to\infty} \frac{\left(\frac{e(m+q^t-2)}{q^t-2}\right)^m}{q^{tm}} = 0$, and $\lim_{t\to\infty} \frac{b^*}{nt} = \lim_{t\to\infty} \frac{(q^t-1)t}{tq^{tm}} = 0$.

The maximum k for which ARM1(K^m, k) admits the repair scheme given in Theorem 2.5 is $k^* = q^t - q^{t-1} - 1$. In this case, by Table I, $\dim_K \mathrm{ARM1}(K^m, k^*) = q^{tm} - q^{(t-1)m}$ and bandwidth $b^* = tq^{tm} - (t-1)(q^t-1)^m - t$. Thus $\lim_{t\to\infty} \frac{\dim_K \mathrm{ARM1}(K^m,k^*)}{n} = \lim_{t\to\infty} \frac{q^{tm}-q^{(t-1)m}}{q^{tm}} = 1 - \frac{1}{q^m}$, and $\lim_{t\to\infty} \frac{b^*}{nt} = \lim_{t\to\infty} \frac{tq^{tm}-(t-1)(q^t-1)^m-t}{tq^{tm}} = 0$.

The maximum k for which ARM2(K^m, k) admits the repair scheme given in Theorem 3.4 is $k^* = q^t - q^{t-1} - 1$. In this case, by Table I $\dim_K \mathrm{ARM2}(K^m, k^*) = q^{tm} - m(q^{t-1}-1) - 1$ and b^* = bandwidth at $k^* = tq^{tm} - (t-m)(q^t-1)^m - t$. Thus $\lim_{t\to\infty} \frac{\dim_K \mathrm{ARM2}(K^m,k^*)}{n} = \lim_{t\to\infty} \frac{q^{tm}-m(q^{t-1}-1)-1}{q^{tm}} = \lim_{t\to\infty} \frac{q^{tm}-mq^{t-1}+m-1}{q^{tm}} = 1$, and $\lim_{t\to\infty} \frac{b^*}{nt} = \lim_{t\to\infty} \frac{tq^{tm}-(t-m)(q^t-1)^m-t}{tq^{tm}} = \lim_{t\to\infty} 1 - (1-\frac{m}{t})(1-\frac{1}{q^t})^m - \frac{1}{q^{tm}} = 1 - 1 - 0 = 0$. By previous paragraphs, as t increases, the relative bandwidth advantage of the RM codes lessens, while the rate advantage of the ARM codes intensifies, as summarized in Table II.

Code	Dimension	$\lim_{t\to\infty}$ Rate	$\lim_{t\to\infty} \frac{b}{nt}$
RM(K^m, max)	$\binom{m+q^t-2}{q^t-2}$	0	0
ARM1(K^m, max)	$q^{tm} - q^{(t-1)m}$	$1 - 1/q^m$	0
ARM2(K^m, max)	$q^{tm} - m(q^{t-1}-1) - 1$	1	0

TABLE II: Asymptotic behavior of the codes RM, ARM1 and ARM2, when each achieves the maximum dimension so the repair schemes given in [1, Theorem III.1], Theorem 2.5 and Theorem 3.4 can be applied.

As expected, the augmented Reed-Muller codes, which were designed to maximize the rate of the code, have a higher repair bandwidth as well, due to the trade-off between the rate of a code and the bandwidth of its associated repair scheme.

V. Conclusion

In this paper, we defined two new families of augmented Reed-Muller codes and described erasure repair schemes for each of them. We demonstrated that when a dimension and a base field are fixed, there are some instances where augmented Reed-Muller codes provide a better bandwidth than Reed-Solomon codes, and a better bandwidth in terms of bits than Hermitian codes. We analyzed the asymptotical behavior when Reed-Muller and augmented Reed-Muller codes achieve the maximum rate.

REFERENCES

[1] T. Chen and X. Zhang, Repairing Generalized Reed-Muller Codes, https://arxiv.org/pdf/1906.10310.pdf.

[2] P. Delsarte, J. M. Goethals and F. J. Mac Williams, On generalized Reed-Muller codes and their relatives, Information and control, **16** (1970), no. 5, 403–442.

[3] A. Dimakis, P. Godfrey, Y. Wu, M. Wainwright and K. Ramchandran, Network coding for distributed storage systems, IEEE Transactions on Information Theory, **56** (2010), no. 9, 4539–4551.

[4] A. Dimakis, K. Ramchandran, Y. Wu and C. Suh, A survey on network codes for distributed storage, Proceedings of the IEEE, **99** (2011), no. 3, 476–489.

[5] O. Geil and C. Thomsen, Weighted Reed-Muller codes revisited, Designs Codes and Cryptography, **66** (2013), 195–220. https://doi.org/10.1007/s10623-012-9680-8

[6] V. Guruswami and M. Wootters, Repairing Reed-Solomon Codes, IEEE Transactions on Information Theory, **63** (2017), no. 9, 5684–5698.

[7] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003.

[8] L. Jin, Y. Luo and C. Xing, Repairing Algebraic Geometry Codes, IEEE Transactions on Information Theory, **64** (2018), no. 2, 900–908.

[9] H. H. López, G. L. Matthews and I. Soprunov, Monomial-Cartesian codes and their duals, with applications to LCD codes, quantum codes, and locally recoverable codes, Designs Codes and Cryptography, **88** (2020), 1673–1685.

[10] H. H. López, I. Soprunov and R. H. Villarreal, The dual of an evaluation code, Designs Codes and Cryptography, (2021), https://doi.org/10.1007/s10623-021-00872-w.

[11] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press (1994), https://doi.org/10.1017/CBO9781139172769.