

A Complete Classification of Partial-MDS (Maximally Recoverable) Codes Correcting one Additional Erasure

Anna-Lena Horlemann-Trautmann

University of St. Gallen, Switzerland

June 7th, 2017

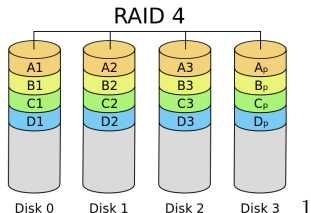
Fq13, Italy

Joint work with Alessandro Neri.

What are PMDS and MR codes?

- PMDS = partial MDS
- MR = maximally recoverable
- special classes of locally repairable codes
 - $\implies [n, k]$ block codes where we only need $\ell < k$ correct coordinates to recover an erased coordinate
- used for (distributed) storage systems

Application in RAID (redundant array of inexpensive disks):



- data is encoded in $[n, k]$ -MDS code
- data is written horizontally, one symbol per disk
- storage system can tolerate $n - k$ disk failures

¹<https://commons.wikimedia.org/w/index.php?curid=1509166>

Generalizations:

- write storage system as an $m \times n$ array, where each row is a codeword and each column represents a disk
- encode data in a locally repairable code such that groups of columns form locality groups

a_1	a_2	$\dots$	a_h	a_{h+1}	$\dots$	a_{2h}	$\dots$	a_{n-h+1}	$\dots$	a_n
b_1	b_2	$\dots$	b_h	b_{h+1}	$\dots$	b_{2h}	$\dots$	b_{n-h+1}	$\dots$	b_n
		$\vdots$			$\vdots$		$\vdots$		$\vdots$	
m_1	m_2	$\dots$	m_h	m_{h+1}	$\dots$	m_{2h}	$\dots$	m_{n-h+1}	$\dots$	m_n



locality group



locality group



locality group

a_1	a_2	$\dots$	a_h	a_{h+1}	$\dots$	a_{2h}	$\dots$	a_{n-h+1}	$\dots$	a_n
b_1	b_2	$\dots$	b_h	b_{h+1}	$\dots$	b_{2h}	$\dots$	b_{n-h+1}	$\dots$	b_n
		$\vdots$			$\vdots$		$\vdots$		$\vdots$	
m_1	m_2	$\dots$	m_h	m_{h+1}	$\dots$	m_{2h}	$\dots$	m_{n-h+1}	$\dots$	m_n

$\underbrace{\hspace{10em}}$
locality group

$\underbrace{\hspace{10em}}$
locality group

$\underbrace{\hspace{10em}}$
locality group

- each block has locality ℓ
 $\implies$ each block can correct $h - \ell$ erasures (due to server failures)
- s additional erasures anywhere should be correctable
 $\implies$ this happens e.g. in SSD storage systems due to leakage
- we can also allow the locality groups to have different sizes

- 1 Introduction
- 2 PMDS and MR Codes
- 3 PMDS Codes for $s = 1$
- 4 Bounds on Field Size
- 5 Conclusions

Definition

A code is called *maximally recoverable (MR)* for a given configuration, if any erasure pattern that is information theoretically correctable is correctable.

We consider a distributed storage system with locality ℓ and m disjoint locality groups, where the i -th group can correct any r_i erasures ($\implies$ block length $r_i + \ell$).

Definition

Let $\ell, m, r_1, \dots, r_m \in \mathbb{N}$. Define $n := \sum_{i=1}^m (\ell + r_i)$ and let $C \subseteq \mathbb{F}_q^n$ be a linear code of dimension $k < n$ with generator matrix

$$G = (B_1 \mid \cdots \mid B_m) \in \mathbb{F}_q^{k \times n}.$$

such that $B_i \in \mathbb{F}_q^{k \times (\ell + r_i)}$. Then C is a $[n, k, \ell; r_1, \dots, r_m]$ -*partial-MDS (PMDS) code* if

- for $i \in \{1, \dots, m\}$ the row space of B_i is a $[r_i + \ell, \ell, r_i + 1]$ -MDS code, and
- for any r_i erasures in the i -th block ($i = 1, \dots, m$), the remaining code (after puncturing the coordinates of the erasures) is MDS.

ℓ is the locality of the code (fixed for all blocks).

Lemma

A $[n, k, \ell; r_1, \dots, r_m]$ -PMDS code can correct any r_i erasures in the i -th block (simultaneously) plus $s := m\ell - k$ additional erasures anywhere in the code.

Lemma

A $[n, k, \ell; r_1, \dots, r_m]$ -PMDS code can correct any r_i erasures in the i -th block (simultaneously) plus $s := m\ell - k$ additional erasures anywhere in the code.

Lemma

If $k = \ell$, then a code is a $[n, k, \ell; r_1, \dots, r_m]$ -PMDS code if and only if it is a $[n, k]$ -MDS code.

This includes the case $m = 1$, since this automatically implies $k = \ell$.

Lemma

A $[n, k, \ell; r_1, \dots, r_m]$ -PMDS code can correct any r_i erasures in the i -th block (simultaneously) plus $s := m\ell - k$ additional erasures anywhere in the code.

Lemma

If $k = \ell$, then a code is a $[n, k, \ell; r_1, \dots, r_m]$ -PMDS code if and only if it is a $[n, k]$ -MDS code.

This includes the case $m = 1$, since this automatically implies $k = \ell$.

Theorem

A $[n, k, \ell; r_1, \dots, r_m]$ -PMDS code is maximally recoverable.

Related results:

- [Chen-Huang-Li '07]: MR codes exist for any configuration if the field size is large enough ($q > \binom{n-1}{k-1}$).
- [Blaum-Hafner-Hetzler '13]: Some constructions for PMDS codes with $r = 1, 2$ or $s = 1$ ($q \in O(mn)$).
- [Gopalan-Huang-Jenkins-Yekhanin '14]: Some constructions for PMDS codes with $r = 1$ ($q \in O(2^n)$).
- [Chen-Shum-Yu-Sung '15]: PMDS construction with $s = 1$ ($q \geq n/m$).
- [Calis-Kayouglou '16]: PMDS-construction for all parameters based on MRD and MDS codes (q^{n-mr}).

- 1 Introduction
- 2 PMDS and MR Codes
- 3 PMDS Codes for $s = 1$
- 4 Bounds on Field Size
- 5 Conclusions

Theorem

For any integers $m \geq 2$ and $\ell, r_1, \dots, r_m \geq 1$, the following generator matrix generates a $[n, k, \ell; r_1, \dots, r_m]$ -PMDS code of length $n = m\ell + \sum r_i$, dimension $k = m\ell - 1$ and locality ℓ over $\mathbb{F}_q$:

$$G = \left(\begin{array}{cccc|c} B_1 & 0 & \dots & 0 & M \\ 0 & B_2 & \dots & 0 & M \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & B_{m-1} & M \\ \hline 0 & 0 & \dots & 0 & A \end{array} \right)$$

where $[\dots]$

Theorem

[...]

$$B_i = [I_\ell \mid *] \in \mathbb{F}_q^{\ell \times (\ell + r_i)}, A = [I_{\ell-1} \mid 1 \mid *] \in \mathbb{F}_q^{(\ell-1) \times (\ell + r_m)},$$

$$M = [0_{\ell \times \ell-1} \mid 1 \mid (\star \cdots \star)(1 \dots 1)^\top] \in \mathbb{F}_q^{\ell \times (\ell + r_m)}$$

such that, for $i = 1, \dots, m-1$, the matrices

$$\widehat{B}_i = [B_i \mid 1],$$

are generator matrices of an $[\ell + r_i + 1, \ell, r_i + 2]$ -MDS code and

$$\widehat{A} = \left(\begin{array}{c|c} 1 & M_{(\ell)} \\ \hline 0 & A \end{array} \right)$$

is a generator matrix of an $[\ell + r_m + 1, \ell, r_m + 2]$ -MDS code.

Lemma

An MDS code always has an equivalent code with a generator matrix of the form B_i, A, M from before.

Corollary

For any integers $m \geq 2$ and $\ell, r_1, \dots, r_m \geq 1$ there exists an $[n, k = m\ell - 1, \ell; r_1, \dots, r_m]$ -PMDS code over any field $\mathbb{F}_q$ with $q \geq \max_i \{r_i\} + \ell$.

Lemma

An MDS code always has an equivalent code with a generator matrix of the form B_i, A, M from before.

Corollary

For any integers $m \geq 2$ and $\ell, r_1, \dots, r_m \geq 1$ there exists an $[n, k = m\ell - 1, \ell; r_1, \dots, r_m]$ -PMDS code over any field $\mathbb{F}_q$ with $q \geq \max_i \{r_i\} + \ell$.

- For $\max_i \{r_i\} + \ell = 2^b + 1, \ell \in \{3, 2^b - 1\}$, we can decrease the field size to $q \geq 2^b = \max_i \{r_i\} + \ell - 1$.
- For $\ell = 1$, we can decrease the field size to $q \geq 2$.

Example: $[n, k, \ell; r_1, r_2] = [6, 3, 2; 1, 1]$ -PMDS over $\mathbb{F}_3$

$$G = \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 2 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 & 1 & 2 \end{array} \right)$$

- 1 erasure per block
 (each block is MDS)
- plus 1 additional erasure anywhere
 (any two columns from 1st and 2nd block each are MDS)

The other way around:

Theorem

For any $m, \ell \geq 2$ and $r_1, \dots, r_m \geq 1$, a code of length $n = m\ell + \sum r_i$, dimension $k = \ell m - 1$ and locality ℓ over $\mathbb{F}_q$ is a PMDS code if and only if it has a generator matrix of the form:

$$G = \left(\begin{array}{cccc|c} B_1 & 0 & \dots & 0 & M_1 \\ 0 & B_2 & \dots & 0 & M_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & B_{m-1} & M_{m-1} \\ \hline 0 & 0 & \dots & 0 & A \end{array} \right) \quad (1)$$

where $[\dots]$

Theorem

$$B_i = [I_\ell \mid *] \in \mathbb{F}_q^{\ell \times (\ell + r_i)}, A = [I_{\ell-1} \mid *^{(A)}] \in \mathbb{F}_q^{(\ell-1) \times (\ell + r_m)},$$

$$M = [0_{\ell \times \ell-1} \mid *_{\ell \times 1}^{(M)} \mid (\star \cdots \star)(1 \dots 1)^\top] \in \mathbb{F}_q^{\ell \times (\ell + r_m)}$$

such that, for $i = 1, \dots, m-1$, the matrices

$$\hat{B}_i = [B_i \mid *_{\ell \times 1}^{(M)}],$$

are generator matrices of an $[\ell + r_i + 1, \ell, r_i + 2]$ -MDS code and

$$\hat{A} = \left(\begin{array}{ccccc|c} 1 & 0 & \dots & 0 & 1 & \star \cdots \star \\ 0 & 1 & \dots & 0 & 1 & \\ \vdots & & \ddots & & \vdots & \\ 0 & 0 & \dots & 1 & 1 & *^{(A)} \end{array} \right)$$

is a generator matrix of an $[\ell + r_m + 1, \ell, r_m + 2]$ -MDS code.

- 1 Introduction
- 2 PMDS and MR Codes
- 3 PMDS Codes for $s = 1$
- 4 Bounds on Field Size
- 5 Conclusions

Remember: A $[n, k, \ell; r_1, \dots, r_m]$ -PMDS code can correct any r_i erasures in the i -th block (simultaneously) plus $s := m\ell - k$ additional erasures anywhere in the code.

Theorem

$[n, m\ell - 1, \ell; r_1, \dots, r_m]$ -PMDS code exist over $\mathbb{F}_q$ if

$$q \geq \max_i \{r_i\} + \ell.$$

Remember: A $[n, k, \ell; r_1, \dots, r_m]$ -PMDS code can correct any r_i erasures in the i -th block (simultaneously) plus $s := m\ell - k$ additional erasures anywhere in the code.

Theorem

$[n, m\ell - 1, \ell; r_1, \dots, r_m]$ -PMDS code exist over $\mathbb{F}_q$ if

$$q \geq \max_i \{r_i\} + \ell.$$

If the MDS conjecture is true, then the statement is an **if and only if** statement.

Except if

- $\ell = 3$ or $\ell = 2^b - 1$ and $\max_i \{r_i\} + \ell = 2^b + 1$, then we can decrease field size to $\max_i \{r_i\} + \ell - 1 = 2^b$.
- $\ell = 1$, then it exists over any finite field.

Comparisons:

- Our construction: field size

$$q \geq \max_i \{r_i\} + \ell$$

- If we treat each locality block separately, we can use a $[r_i + \ell + 1, \ell]$ -MDS code, which exists with field size $q \geq \max_i \{r_i\} + \ell$. But then the length of the whole code increases by m .

Comparisons:

- Our construction: field size

$$q \geq \max_i \{r_i\} + \ell$$

- If we treat each locality block separately, we can use a $[r_i + \ell + 1, \ell]$ -MDS code, which exists with field size $q \geq \max_i \{r_i\} + \ell$. But then the length of the whole code increases by m .
- Other PMDS constructions:
 - MR bound: $q \geq \binom{n-1}{k-1}$
 - MRD based: $q \geq 2^{n-rm}$

- 1 Introduction
- 2 PMDS and MR Codes
- 3 PMDS Codes for $s = 1$
- 4 Bounds on Field Size
- 5 Conclusions

Conclusions and Outlook

- We generalize the definition of PMDS codes to locality blocks of various length.
- These codes are maximally recoverable (MR).

Conclusions and Outlook

- We generalize the definition of PMDS codes to locality blocks of various length.
- These codes are maximally recoverable (MR).
- We give generalized construction for $s = 1$ with field size $q \geq \max_i \{r_i + \ell\}$
→ in special cases $q \geq \max_i \{r_i + \ell - 1\}$.

Conclusions and Outlook

- We generalize the definition of PMDS codes to locality blocks of various length.
- These codes are maximally recoverable (MR).
- We give generalized construction for $s = 1$ with field size $q \geq \max_i \{r_i + \ell\}$
→ in special cases $q \geq \max_i \{r_i + \ell - 1\}$.
- We show that all PMDS codes with $s = 1$ are of this form.
⇒ Bound on field size is necessary.

Conclusions and Outlook

- We generalize the definition of PMDS codes to locality blocks of various length.
- These codes are maximally recoverable (MR).
- We give generalized construction for $s = 1$ with field size $q \geq \max_i \{r_i + \ell\}$
→ in special cases $q \geq \max_i \{r_i + \ell - 1\}$.
- We show that all PMDS codes with $s = 1$ are of this form.
⇒ Bound on field size is necessary.
- Generalization to $s > 1$ gets complicated.

Conclusions and Outlook

- We generalize the definition of PMDS codes to locality blocks of various length.
- These codes are maximally recoverable (MR).
- We give generalized construction for $s = 1$ with field size $q \geq \max_i \{r_i + \ell\}$
→ in special cases $q \geq \max_i \{r_i + \ell - 1\}$.
- We show that all PMDS codes with $s = 1$ are of this form.
⇒ Bound on field size is necessary.
- Generalization to $s > 1$ gets complicated.

Thank you for your attention!
Questions? – Comments?

