Constructions of High-Rate MSR Codes over Small Fields

Netanel Raviv       Natalia Silberstein       Tuvi Etzion
June 24, 2015

Abstract

Three constructions of minimum storage regenerating (MSR) codes are presented. The first two constructions provide access-optimal MSR codes, with two and three parities, respectively, which attain the sub-packetization bound for access-optimal codes. The third construction provides larger MSR codes with three parities, which are not access-optimal, and do not necessarily attain the sub-packetization bound.

In addition to a minimum storage in a node, these codes have the following two important properties: first, given storage $\ell$ in each node, the entire stored data can be recovered from any $2 \log \ell$ (any $3 \log \ell$) for 2 parity nodes (for 3 parity nodes, respectively); second, for the first two constructions, a helper node accesses the minimum number of its symbols for repair of a failed node (access-optimality). The goal of this paper is to provide a construction of such optimal codes over the smallest possible finite fields. The generator matrix of these codes is based on perfect matchings of complete graphs and hypergraphs, and on a rational canonical form of matrices. The field size required for our construction is significantly smaller when compared to previously known codes.

1 Introduction

Regenerating codes are a family of erasure codes proposed by Dimakis et al.\cite{Dimakis2010} to store data in distributed storage systems (DSSs) in order to reduce the amount of data (repair bandwidth) downloaded during repair of a failed node. An $(n, k, \ell, d, \beta, B)_q$ regenerating code $C$, for $k \leq d \leq n - 1$, $\beta \leq \ell$, is used to store a file of size $B$ in a DSS across a network of $n$ nodes, where each node of the system stores $\ell$ symbols from $\mathbb{F}_q$, a finite field with $q$ elements, such that the stored file can be recovered by downloading the data from any set of $k$ nodes. When a single node fails, a newcomer node which substitutes the failed node, contacts any set of $d$ nodes, called helper nodes, and downloads $\beta$ symbols from each helper node to reconstruct the data stored in the failed node. This process is called a node repair process and the parameter $d$ is called the repair degree. There are two general methods of node repairs: functional repair and exact repair. Functional repair ensures that when a node repair process is completed, the system is equivalent to the original one, i.e., the stored file can be recovered from any $k$ nodes. However, the newcomer node may contain a different data from what was stored

This research was supported in part by the Israeli Science Foundation (ISF), Jerusalem, Israel, under Grant 10/12.
The work of Netanel Raviv is part of his Ph.D. thesis performed at the Technion.
The work of Natalia Silberstein was supported in part by the Fine fellowship.
The authors are with the Department of Computer Science, Technion, Haifa 32000, Israel.
e-mail: \{netanel, natalys, etzion\}@cs.technion.ac.il.
in the failed node. Exact repair requires that the newcomer node will store exactly the same data as was stored in the failed node. Usually, exact repair is required for systematic nodes (nodes that contain the actual data), while the parity nodes can be functionally repaired.

Based on a min-cut analysis of the information flow graph which represents a DSS, Dimakis et al. [4] presented an upper bound on the size of a file that can be stored using a regenerating code under functional repairs:

\[
B \leq \sum_{i=1}^{k} \min\{(d - i + 1)\beta, \ell\}.
\] (1)

Given the values of \(B, n, k, d\), this bound provides a tradeoff between the number \(\ell\) of stored symbols in a node and the repair bandwidth \(\beta d\). One of the extremal points on this tradeoff is referred to as minimum storage regenerating (MSR) point, and a code that attains it, namely, minimum storage regenerating (MSR) code satisfies [4]

\[
(\ell, \beta d) = \left(\frac{B}{k}, \frac{Bd}{k(d - k + 1)}\right).
\] (2)

Another extremal point on this tradeoff is referred to as minimum bandwidth regenerating (MBR) point, and a code that attains it, namely, minimum bandwidth regenerating (MBR) code satisfies [4]

\[
(\ell, \beta d) = \left(\frac{2Bd}{2kd - k^2 + k}, \frac{2Bd}{2kd - k^2 + k}\right).
\]

Constructions of exact MSR and MBR codes (codes which support exact repairs) can be found in [10, 11, 12, 13, 14, 15, 16] and references therein. MSR codes are in particular MDS array codes [2, 3].

In this paper we focus on MSR codes which provide exact minimum repair bandwidth of systematic nodes and have additional properties listed below.

1. **Maximum repair degree** \(d = n - 1\): this enables to minimize the repair bandwidth among all MSR codes. Namely, such MSR codes satisfy \((\ell, \beta d) = \left(\frac{B}{k}, \frac{B(n-1)}{k(n-k)}\right)\) [4].

2. **High rate** \(\frac{k}{n}\): in particular the number of parity nodes \(r = n - k\) is \(r = 2\) or \(r = 3\) (see e.g. [10, 15, 16] for previously known constructions of such MSR codes).

3. **Optimal access**: the number of symbols accessed in a helper node is minimal and equals to the number \(\beta\) of symbols transmitted during node repair. (See [1, 17] for bounds and constructions of access-optimal codes.)

4. **Optimal sub-packetization factor**: for an \((n, k, \ell, d, \beta, B)\) regenerating code, the number of stored symbols \(\ell\) in a node is also called the sub-packetization factor of the code. Low-rate \((\frac{k}{n} \leq \frac{1}{2}, \text{i.e., } r_n \geq \frac{1}{2})\) MSR codes with \(d = n - 1\), where \(\ell\) is linear in \(r\) were constructed in [11]. However, in the known high-rate \((\frac{k}{n} > \frac{1}{2})\) MSR codes \(\ell\) is exponential in \(k\) [10, 15]. Moreover, it was proved in [17] that for an access-optimal code, given a fixed sub-packetization factor \(\ell\) and \(r\) parity nodes, the largest number \(k\) of systematic nodes is

\[
k = r \log_r \ell,
\] (3)
in other words, the required sub-packetization factor is \(r^\frac{k}{n}\).
5. **Small finite field**: construction of access-optimal MSR codes with $r = 2$ and optimal sub-packetization over a finite field of size $1 + 2 \log \ell$ is presented in [15]. For general $r$, codes with sub-packetization factor $\ell = r^m$ and $k = rm$, over $\mathbb{F}_q$, where $q \geq k^{r-1}r^{m-1} + 1$ were presented in [15] and codes for $q \geq \binom{r}{k}r^{m+1}$ were presented in [10]. Note that for $r = 3$ the field size is at least $m^2 3^{m+1} + 1$ in [15] and at least $(3m+3)3^{m+1}$ in [10].

We propose a construction of access-optimal MSR codes with optimal sub-packetization factor $\ell = r^m$, $k = rm$, for $r = 2$ and $r = 3$, over any finite field $\mathbb{F}_q$ such that $q \geq m + 1$ and $q \geq 6m + 1$, respectively. Moreover, for $r = 3$, if $q$ is a power of 2 then the field size can be reduced to $q \geq 3m + 1$.

For $r = 3$ and $\ell = 3^m$ the following table illustrates the comparison between the lower bounds on the field size $q$ of our construction and the construction from [15].

| $m$ | the lower bound on $q$ in [15] | the lower bound on $q$ in our codes |
|-----|-------------------------------|-------------------------------------|
| 1   | 10                            | 4                                  |
| 2   | 109                           | 13                                 |
| 3   | 730                           | 16                                 |
| 4   | 3889                          | 16                                 |
| 5   | 18226                         | 16                                 |

For $r = 2$, a construction which achieves $k = (r + 1)m = 3m$ and requires $q \geq 2m + 1$, is presented [15]. Note that this construction does not contain a subcode that achieves $k = 2m$ and requires $q \geq m + 1$. In addition, a construction for $r = 2$ which achieves $k = rm = 2m$ and requires $q \geq m + 1$ is presented in [7]. This construction requires $q$ to be even, does not provide the optimal access property, and provides a different property called *optimal update*.

The construction for $r = 2$ is given in Section 3 (with proofs) and for $r = 3$ in Section 4 (proofs will be provided in the next version of this paper). Additional construction for $r = 3$, which does not have the access-optimal property, is given without proofs is Section 5. This construction achieves $k = (r + 1)m = 4m$ and requires a field size which is larger than the one required in Section 4, yet still linear in $m$. The latter is comparable to [15] in terms of the parameter $k$, but it is explicit, and may be defined over exponentially smaller fields. The techniques from Section 5 can be used for $r = 2$, but the resulting codes do not seem to supersede the code from [15] in any aspect, and hence they were not included in this paper.

The next section contains three subsections in which the techniques and underlying ideas of Sections 3, 4, and 5 are discussed. Section 2.1 contains some necessary mathematical background, Section 2.2 describes the underlying algebraic problem, and Section 2.3 explains the outline for all constructions.

## 2 Preliminaries

### 2.1 Mathematical Background and Notations

The constructions in Section 3 and Section 4 extensively use several standard linear-algebraic notions. For the sake of completeness, we include below a short introduction about these necessary notions. Some of the given background is not directly used in the constructions, but may greatly assist the reader with understanding our techniques, and their underlying reasoning.

For a prime power $q$, $\mathbb{F}_q^*$ is the set $\mathbb{F}_q \setminus \{0\}$, $\mathbb{F}_q^\ell$ is a vector space of dimension $\ell$ over $\mathbb{F}_q$, and $\mathbb{F}_q^\ell \times \ell$ is the set of all $\ell \times \ell$ matrices with entries in $\mathbb{F}_q$. It is widely known that a matrix $M \in \mathbb{F}_q^\ell \times \ell$ admits *eigenvectors* and *eigenvalues* [9, Section VII.7]. If $v \in \mathbb{F}_q^\ell$ and $vM = \lambda v$ for some $\lambda \in \mathbb{F}_q$, then
$v$ is called a left eigenvector for the eigenvalue $\lambda$. The linear span of all eigenvectors for a certain eigenvalue $\lambda$ is a subspace of $\mathbb{F}_q^{\ell}$, and it is called an eigenspace of $M$.

For a subspace $S$ of $\mathbb{F}_q^{\ell}$, let $SM \triangleq \{sM \mid s \in S\}$. The set $SM$, called the shift of $S$ by $M$, is obviously a subspace of $\mathbb{F}_q^{\ell}$, and if $M$ is invertible then $\dim S = \dim(SM)$. A subspace $S$ which satisfies $SM = S$ is called an invariant subspace of $M$ [8, Section XI.4]. Clearly, an eigenspace of $M$ is also an invariant subspace of $M$, but not necessarily vice versa.

For a polynomial $p(x) \in \mathbb{F}_q[x]$ such that $p(x) = \sum_{i=0}^{d} p_i x^i$, let $p(M) \triangleq \sum_{i=0}^{d} p_i M^i$. The characteristic polynomial of $M$ is the determinant of $M - xI$ [9, Section IX.5], where $I$ is the $\ell \times \ell$ identity matrix. The famous Cayley-Hamilton Theorem [9, Section IX.6, Theorem 14] states that if $c(x)$ is the characteristic polynomial of $M$, then $c(M) = 0$. Furthermore, there exists a unique monic polynomial $m(x) \in \mathbb{F}_q[x]$, of minimum degree, such that $m(M) = 0$. The polynomial $m(x)$, called the minimal polynomial of $M$, divides the characteristic polynomial $c(x)$ of $M$, and its roots are the eigenvalues of $M$.

If $P \in \mathbb{F}_q^{\ell \times \ell}$ is an invertible matrix, then the matrices $P^{-1}MP$ and $M$ are called similar matrices, and the matrix $P$ is called a change matrix, (or a change-of-basis matrix) [9, Section VII.7]. It is easily verified that if $e_0, \ldots, e_{\ell-1}$ is the standard basis of $\mathbb{F}_q^{\ell}$, and $p_0, \ldots, p_{\ell-1}$ are the rows of $P$, then $P^{-1}MP$ acts on $p_0, \ldots, p_{\ell-1}$ exactly as $M$ acts on $e_0, \ldots, e_{\ell-1}$. That is, if

$$
\left( \sum_{i=0}^{\ell-1} \mu_i e_i \right) M = \sum_{i=0}^{\ell-1} \delta_i e_i
$$

for some coefficients $(\mu_i)_{i=0}^{\ell-1}$ and $(\delta_i)_{i=0}^{\ell-1}$, then

$$
\left( \sum_{i=0}^{\ell-1} \mu_i p_i \right) (P^{-1}MP) = \sum_{i=0}^{\ell-1} \delta_i p_i.
$$

As a result of this fact, we have that similar matrices share the same eigenvalues, but not necessarily the same eigenvectors. In addition, similar matrices also share the same minimal polynomial [9, Section IX.7].

Determining matrix similarity is possible by converting given matrices to one of several canonical forms. One such canonical form, which does not always exist, is the diagonal form. If a matrix $M$ is similar to a diagonal matrix then $M$ is called a diagonalizable matrix. It is well known that $M$ is diagonalizable if and only if there exists a basis of $\mathbb{F}_q^{\ell}$ in which all vectors are eigenvectors of $M$ [9, Section VII.8, Theorem 19], and two matrices with the same diagonal form are similar.

Determining matrix similarity for matrices which are not necessarily diagonalizable is a corollary of the so-called decomposition theorem [9, Section XI.4, Theorem 8], which is one of the profoundest results in linear algebra. This theorem states that any matrix $M$ is similar to a block diagonal matrix, whose blocks are companion matrices of certain factors of the characteristic polynomial. The polynomials corresponding to these companion matrices may be ordered such that any polynomial is a multiple of the next, and the first one is the minimal polynomial of $M$. This block diagonal matrix is called the rational canonical form (rational form, in short) of $M$, and any matrix $N$ is similar to $M$ if and only if the share the same rational form.

Several graph theoretic notions are also used in this paper. For any positive integer $r$, the $r$-uniform hypergraph is a hypergraph whose edges are sets of size $r$ of nodes (a graph if $r = 2$). A matching in a hypergraph is a set of mutually disjoint edges. A perfect matching is a matching

---

* A companion matrix of a polynomial $p(x)$ is a $\deg p \times \deg p$ matrix consisting of 1’s in the main sub-diagonal, the additive inverses of the coefficients of $p$ in the rightmost column, and 0 elsewhere.
which covers the entire vertex set. The complete $r$-uniform hypergraph $K^r_\ell$ on $\ell$ nodes is the $r$-uniform hypergraph which consists of all possible edges. For convenience, we identify the $\ell$ nodes of $K_\ell$ with $e_0, \ldots, e_{\ell-1}$, the unit vectors of length $\ell$, and denote $K_\ell$ for $K^2_\ell$.

In what follows, for a set of vectors $T$ we denote its $F_q$-linear span by $\langle T \rangle$ and for subspaces $U$ an $V$, let $U + V \triangleq \{u + v \mid u \in U, v \in V\}$. For a matrix $N$ we denote its left image by $\text{Im}(N) \triangleq \{vN \mid v \in F_q^\ell\}$ and its row span by $\langle N \rangle$.

2.2 The Subspace Condition

In many real-world applications, a distributed storage system is required to have a systematic part, i.e., certain nodes in the system should store an uncoded part of the data. Such nodes are called systematic nodes, and they allow instant access to their stored data. An efficient repair algorithm for a failed systematic node is vital. In this paper, we devise an MSR code which allows a minimum repair bandwidth for a failed systematic node.

This problem was previously studied by [5, 6, 15, 17], where it was shown to be equivalent to a purely algebraic condition called the subspace condition. In this subsection we describe this condition, and explain why codes which satisfy it are sufficient for minimum repair bandwidth for a failed systematic node. We refer the interested reader to [15] for a proof that the subspace condition is also necessary. A more general formulation of the subspace condition, which is irrelevant in our context, may also be found in [15].

As mentioned in the Introduction, MSR codes are in particular MDS array codes. In an MSR code with $k$ systematic nodes, $r$ parity nodes, and sub-packetization $\ell$, a file $f \in F_{k\ell}^q$ is partitioned into $k$ parts of length $\ell$ each, denoted by $f = (C_1, \ldots, C_k)$. The file $f$ is multiplied by a generator block matrix of the form

$$
\begin{pmatrix}
I \\
\vdots \\
I \\
A_1 & \cdots & A_k \\
\vdots & \ddots & \vdots \\
A_1^{r-1} & \cdots & A_k^{r-1}
\end{pmatrix}
$$

(4)

where $I$ is the $\ell \times \ell$ identity matrix, and $A_1, \ldots, A_k$ are invertible matrices which will be defined in the sequel. The resulting codeword is partitioned into $k + r$ columns of length $\ell$ each, denoted $(C_1, \ldots, C_k, C_{k+1}, \ldots, C_{k+r})$, where for all $j \in [r]$,

$$
C_{k+j} = \sum_{i=1}^k A_i^{j-1}C_i.
$$

Each column $C_i$ is stored in a different storage node, where the first $k$ nodes are the systematic ones and the remaining $r$ nodes are called parity nodes.

Upon a failure of a systematic node $m \in [k]$, storing $C_m$, it is required to repair it by downloading a minimal amount of data. According to [2], since $n = k + r$ and $d = n - 1$, we have that the

[15, 17] used the term “subspace property”.

Note that this specific form (4) is a special case of a generator matrix of an MSR code. For a general form of a generator matrix of an MSR codes, see [15].
minimum bandwidth in this scenario is
\[
\frac{B}{k} \cdot \frac{d}{d-k+1} = \frac{k\ell}{k} \cdot \frac{k+r-1}{r} = \frac{\ell}{r}(k+r-1).
\] (5)

That is, each of the remaining \(k+r-1\) nodes should contribute \(1/r\) of its stored data. Sufficient conditions for this minimum repair bandwidth are as follows.

**Definition 1. (The Subspace Condition, [17, Section II]** Let \(\ell\) and \(r\) be integers such that \(r\) divides \(\ell\). A set of pairs \((A_i, S_i)\)\(_{i=1}^{k}\), where for all \(i\), \(A_i\) is an invertible \(\ell \times \ell\) matrix and \(S_i\) is an \(\ell/r\)-subspace of \(\mathbb{F}_q^\ell\), satisfies the subspace condition if the following properties hold.

The **independence property**: for all \(i \in [k]\), \(S_i + S_i A_i + S_i A_i^2 + \ldots + S_i A_i^{r-1} = \mathbb{F}_q^\ell\).

The **invariance property**: for all \(i, j \in [k], i \neq j\), \(S_i A_j = S_i\).

The **nonsingular property**: Every square block submatrix of the following block matrix is invertible.

\[
\begin{pmatrix}
I & A_1 & \cdots & A_1^{r-1} \\
\vdots & \vdots & \ddots & \vdots \\
I & A_k & \cdots & A_k^{r-1}
\end{pmatrix}
\]

If a subspace \(S\) satisfies the invariance property for a matrix \(A\), then \(S\) is an **invariant subspace** of \(A\) (see Section 2.1). If a subspace \(S'\) satisfies the independence property for \(A\), then \(S'\) is an **independent subspace** of \(A\). Notice that the nonsingular property must hold for the code to be an MDS array code [2, 3], regardless of any applications in distributed storage.

**Theorem 1.** If the set \((A_i, S_i)\)\(_{i=1}^{k}\) satisfies the subspace condition for given \(\ell\) and \(r\), then the code whose generator matrix is given in (4) is an MSR code which allows a minimum repair bandwidth for any systematic node.

The subspaces \((S_i)\)\(_{i=1}^{k}\) in this theorem are used in the repair process. To repair a systematic node \(i\), the remaining nodes project their data on \(S_i\) and send it to the newcomer. For additional details see [5, 6, 15, 17].

A set of the form \((A_i, S_i)\)\(_{i=1}^{k}\) is called an \((A, S)\)-set. Since the subspace condition is necessary and sufficient for our purpose, this paper will focus solely on the construction of \((A, S)\)-sets which satisfy it.

### 2.3 Our Techniques

Our constructions strongly rely on the properties of a matrix \(A\), to whom the matrices in our \((A, S)\)-set are similar using certain change matrices. These change matrices are defined according to a set of matchings in the \(r\)-uniform hypergraph. In this subsection the matrix \(A\) is described, its properties are discussed, and the use of matchings for the definition of the change matrices is explained.

The matrix \(A\) and the change matrices will be described with respect to a construction with \(r\) parities, for a general \(r\). In the following sections, the special cases of \(r = 2\) and \(r = 3\) will be discussed in detail.
For a given number of parities $r$ and an integer $m$, the matrix $A$ is an $r^m \times r^m$ block diagonal matrix whose constituent blocks are the $r \times r$ companion matrix of $x^r - 1$. That is, the companion matrix $C$ of the polynomial $x^r - 1$ is

$$C \triangleq \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 1 & \cdots & 0 & 0 \\ 0 & \ddots & \ddots & \ddots \\ 0 & \cdots & 0 & 1 \end{pmatrix},$$

and the matrix $A$ is

$$A \triangleq \begin{pmatrix} C & \cdots & \cdots \\ \cdots & \ddots & \cdots \\ \cdots & \cdots & C \end{pmatrix}.$$  \hfill (7)

In order for $A$ to have as many eigenspaces as possible, we operate over a field $\mathbb{F}_q$, where $r | q - 1$. This assumption about $q$ provides the existence of all roots of unity $1, \gamma_1, \ldots, \gamma_{r-1}$ of order $r$ in the field $\mathbb{F}_q$ (using the well-known Sylow theorems [9, Section XII.5]). Since $1, \gamma_1, \ldots, \gamma_{r-1} \in \mathbb{F}_q$, it is readily verified that the eigenvalues of $A$ are $1, \gamma_1, \ldots, \gamma_{r-1} \in \mathbb{F}_q$, since they are the roots of the minimal polynomial $x^r - 1$ of $A$. We note that for the special case of $r = 2$ (Section 3), we use an additional technique which allows to operate with any $q \geq m + 1$, without requiring that $2 | q - 1$.

In what follows we present the structure of the eigenspaces of $A$, and the eigenspaces of matrices which are similar to $A$.

**Lemma 1.** The matrix $C \in \mathbb{F}_q^{r \times r}$, \hfill (6)

is a diagonalizable matrix whose set of linearly independent eigenvectors is $\{(1, \ldots, 1)\} \cup \{(1, \gamma_i, \gamma_i^2, \ldots, \gamma_i^{r-1})\}_{i=1}^{r-1}$. Furthermore, the subspace $S = \langle e_0 \rangle$ is an independent subspace of $C$.

**Proof.** It is readily verified that the matrix $C$ performs the cyclic permutation $\pi = (r, r - 1, \ldots, 1)$ on the entries of the vector it operates on. Hence, $(1, \ldots, 1)$ is an eigenvector for the eigenvalue 1. In addition, for any $i \in [r - 1]$, we have that

$$(1, \gamma_i, \gamma_i^2, \ldots, \gamma_i^{r-1})C = (\gamma_i, \gamma_i^2, \ldots, \gamma_i^{r-1}, 1) = \gamma_i(1, \gamma_i, \gamma_i^2, \ldots, \gamma_i^{r-1}),$$

and thus the vector $(1, \gamma_i, \gamma_i^2, \ldots, \gamma_i^{r-1})$ is an eigenvector which corresponds to the eigenvalue $\gamma_i$. These eigenvectors form an $r \times r$ Vandermonde matrix, and hence they are linearly independent and $C$ is diagonalizable.

Since the matrix $C$ preforms the permutation $\pi$ on the input vector, it follows that $e_0C = e_{r-1}$, and $e_jC = e_{j-1}$ for all $j \in [r - 1]$. Hence, $S + SC + \ldots + SC^{r-1} = \mathbb{F}_q^r$, and $S$ is an independent subspace. \hfill \square

The structure of the eigenspaces and eigenvalues of $A$ is a simple corollary of Lemma [1].

**Corollary 1.** The matrix $A$ is diagonalizable, and the linearly independent vectors of $A$ are as follows.

---

\[^{1}\text{A permutation } \sigma \text{ is denoted by } \sigma = (i_0, i_1, \ldots, i_{r-1}) \text{ if it preforms } \sigma(i_j) = i_{(j+1) \text{mod } r} \text{ for all } j \in \{0, \ldots, r-1\}.\]
1. For the eigenvalue 1, the linearly independent eigenvectors are
\[
(1, \ldots, 1, 0, \ldots, 0, \ldots, 0) \\
(0, \ldots, 0, 1, \ldots, 1, \ldots, 0) \\
\vdots \\
(0, \ldots, 0, 0, \ldots, 0, \ldots, 1, \ldots, 1)
\]

2. For the eigenvalue $\gamma_i$, $i \in [r-1]$, the linearly independent eigenvectors are
\[
(1, \gamma_i, \ldots, \gamma_i^{r-1}, 0, 0, \ldots, 0) \\
(0, 0, \ldots, 0, 1, \gamma_i, \gamma_i^{r-1}, \ldots, 0, \ldots, 0) \\
\vdots \\
(0, 0, \ldots, 0, 0, 1, \gamma_i, \gamma_i^{r-1})
\]

In addition, if $S = (e_0, e_r, e_{2r}, \ldots, e_{\ell-r})$ then $S + SA + SA^2 + \ldots + SA^{r-1} = \mathbb{F}_q^\ell$.

The matrices in our construction are similar to the matrix $A$. The following lemma, that is based on a well-known algebraic fact, presents the eigenvalues and eigenvectors of a matrix which is similar to $A$.

**Lemma 2.** If $P \in \mathbb{F}_q^{\ell \times \ell}$ is an invertible matrix whose rows are $p_0, \ldots, p_{\ell-1}$, and $B \triangleq P^{-1}AP$, then $B$ is diagonalizable, with the following eigenspaces,

A1. For the eigenvalue 1, a basis of the eigenspace is $\left\{ \sum_{j=0}^{r-1} p_{ir+j} \mid i \in \{0, \ldots, \ell/r - 1\} \right\}$.

A2. For the eigenvalue $\gamma_i$, a basis of the eigenspace is $\left\{ \sum_{j=0}^{r-1} \gamma_i^j p_{ir+j} \mid i \in \{0, \ldots, \ell/r - 1\} \right\}$.

In addition, the subspace $T \triangleq \langle p_0, p_r, p_{2r}, \ldots, p_{\ell-r} \rangle$ satisfies $T + TB + TB^2 + \ldots + TB^{r-1} = \mathbb{F}_q^\ell$.

**Proof.** Notice that the vectors in A1 and A2 are given by multiplying the eigenvectors of $A$ (see Corollary [1]) by the matrix $P$. If $v$ is an eigenvector of $A$ which corresponds to an eigenvalue $\lambda$ then,

\[(vP)B = (vP)P^{-1}AP = vAP = \lambda vP\]

and hence $vP$ is an eigenvector of $B$.

Notice that the subspace $T$ may be written as $T = \langle e_0P, e_rP, \ldots, e_{\ell-r}P \rangle = \langle e_0, e_r, \ldots, e_{\ell-r} \rangle P = SP$, where $S = \langle e_0, e_r, e_{2r}, \ldots, e_{\ell-r} \rangle$. Hence, it follows from Corollary [1] that,

\[
T + TB + TB^2 + \ldots + TB^{r-1} = SP + SPB + SPB^2 + \ldots + SPB^{r-1} = SP + SAP + SA^2P + \ldots + SA^{r-1}P = (S + SA + SA^2 + \ldots + SA^{r-1})P = \mathbb{F}_q^\ell P = \mathbb{F}_q^\ell
\]

The change matrices which induce the similarity to $A$ are defined using perfect colored matchings in the complete $r$-uniform hypergraph (matchings, in short). Although the specific choice of these change matrices varies from one construction to another, the general idea behind the use of matchings is roughly identical, and will be explained in the remainder of this subsection.
Definition 2. A perfect colored matching (matching, in short) is a perfect matching in the \( r \)-uniform hypergraph, whose edges are colored in \( r \) colors such that no edge contains two nodes of the same color.

We denote a matching by \( \mathcal{M} = (M^{(0)}, \ldots, M^{(r-1)}) \), where each \( M^{(i)} \) is an ordered color set, and if \( M^{(i)} = (m_0^{(i)}, \ldots, m_{\ell/r-1}^{(i)}) \) for each \( i \in \{0, \ldots, r-1\} \), then the edges of \( \mathcal{M} \) are

\[
\left\{ \{m^{(0)}_j, m^{(1)}_j, \ldots, m^{(r-1)}_j\} \right\}_{j=0}^{\ell/r-1}.
\]

For example, for \( r = 2 \), a matching is denoted by \( \mathcal{M} = (M, M') \) (we use \( M \) and \( M' \) instead of \( M^{(0)} \) and \( M^{(1)} \) for convenience), where \( M = (m_0, \ldots, m_{\ell/2-1}) \), \( M' = (m'_0, \ldots, m'_{\ell/2-1}) \), and the edges of \( \mathcal{M} \) are \( \left\{ \{m_i, m'_i\} \right\}_{i=0}^{\ell/2-1} \).

Each matching will be used for the construction of \( r \) (or \( r+1 \) in Section 5) change matrices in the \((\mathcal{A}, S)\)-set. Each \( \ell \times \ell \) change matrix is constructed using constituent \( r \times \ell \) blocks. Each such block is a function of a single edge in the matching. That is, if the matching is \( \mathcal{M} = (M^{(0)}, \ldots, M^{(r-1)}) \), then \( r \) matrices in the \((\mathcal{A}, S)\)-set are constructed as \( A_i = P_i^{-1}AP_i \), where

\[
P_i = \begin{pmatrix}
\text{An } r \times \ell \text{ submatrix based on }
m_0^{(0)}, m_0^{(1)}, \ldots, m_0^{(r-1)} \\
\text{An } r \times \ell \text{ submatrix based on }
m_1^{(0)}, m_1^{(1)}, \ldots, m_1^{(r-1)} \\
\vdots \\
\text{An } r \times \ell \text{ submatrix based on }
m_{\ell/r-1}^{(0)}, m_{\ell/r-1}^{(1)}, \ldots, m_{\ell/r-1}^{(r-1)}
\end{pmatrix}.
\]

Recall that the vertices of the \( r \)-uniform hypergraph \( K^r_\ell \) are identified by the \( \ell \) unit vectors \( e_0, \ldots, e_{\ell-1} \). In all subsequent constructions, the subspaces in the \((\mathcal{A}, S)\)-set are defined using the color sets from the matchings, i.e., if \( \mathcal{M} = (M^{(0)}, \ldots, M^{(r-1)}) \) is a matching, then we define \( r+1 \) subspaces of dimension \( \ell/r \) as follows

\[
\forall i \in \{0, \ldots, r-1\}, \ S_{M^{(i)}} \triangleq \left\langle M^{(i)} \right\rangle \\
S_{M^*} \triangleq \left\langle \left\{ m^{(0)}_i + m^{(1)}_i + \cdots + m^{(r-1)}_i \right\}_{i=0}^{\ell/r-1} \right\rangle.
\]

That is, each subspace \( S_{M^{(i)}} \) is the span of the color set \( M^{(i)} \), and the additional subspace \( S_{M^*} \) is the span of the sums of each edge in \( \mathcal{M} \). To enlarge the \((\mathcal{A}, S)\)-set, different matchings can be used, as long as they satisfy the following simple condition.

Definition 3. Two matchings \( \mathcal{X} = (X^{(0)}, \ldots, X^{(r-1)}) \) and \( \mathcal{Y} = (Y^{(0)}, \ldots, Y^{(r-1)}) \) satisfy the pairing condition if any edge in \( \mathcal{X} \) is monochromatic in \( \mathcal{Y} \), and vice versa.

Subspaces which correspond to distinct matchings \( \mathcal{X} = (X^{(0)}, \ldots, X^{(r-1)}) \) and \( \mathcal{Y} = (Y^{(0)}, \ldots, Y^{(r-1)}) \), that satisfy the pairing condition, have a very useful property. This property is a corollary of the following lemma.
Lemma 3. If \( D \in \{X^{(0)}, \ldots, X^{(r-1)}\} \) and \( E \in \{Y^{(0)}, \ldots, Y^{(r-1)}\} \) then \(|D \cap E| = \ell/r^2\).

Proof. Since \( \mathcal{X} \) and \( \mathcal{Y} \) satisfy the pairing condition, \( D \) can be written as a union of edges from \( \mathcal{Y} \), that is, \( D = \bigcup_{i=0}^{\ell/r^2-1}\{y_i^{(0)}, y_i^{(1)}, \ldots, y_i^{(r-1)}\} \). Hence, \( D \) contains exactly \( \ell/r^2 \) elements of \( E \). \( \square \)

As a result, we have the following.

Lemma 4. If \( U \in \{S_{X^{(0)}}, S_{X^{(1)}}, \ldots, S_{X^{(r-1)}}, S_{X^*}\} \) and \( V \in \{S_{Y^{(0)}}, S_{Y^{(1)}}, \ldots, S_{Y^{(r-1)}}, S_{Y^*}\} \), then \( \dim(U \cap V) = \ell/r^2 \).

In the sequel we use a large set of matchings in which every two matchings satisfy the pairing condition. To satisfy the nonsingular property (Definition 1), each matrix is multiplied by a properly chosen field constant. The constructions of the \((\mathcal{A}, \mathcal{S})\)-sets, which follow the general outline described in this subsection, are discussed in detail in the following sections.

3 Construction of an MSR Code with Two Parities

3.1 Two Parities Code from One Matching

Recall that the vertices of the complete graph \( K_\ell \) are identified by all unit vectors \( e_0, \ldots, e_{\ell-1} \) of length \( \ell \), \( \ell = 2^m \) for some integer \( m \), and a matching \( \mathcal{M} = (M, M') \) is a set of \( \ell/2 \) vertex-disjoint edges of \( K_\ell \). Such a matching will provide an \((\mathcal{A}, \mathcal{S})\)-set of size 2, satisfying the subspace condition. The construction of this \((\mathcal{A}, \mathcal{S})\)-set also relies on the following \( \ell \times \ell \) matrices, which resemble the matrix in (7). For \( \lambda \in \mathbb{F}_q^\ast \), consider the following two \( \ell/2 \times \ell/2 \) matrices

\[
A^+(\lambda) \triangleq \begin{pmatrix}
0 & \lambda & 0 & 0 & \cdots & 0 & 0 \\
\lambda & 0 & 0 & 0 & \cdots & 0 & 0 \\
0 & 0 & 0 & \lambda & \cdots & 0 & 0 \\
0 & 0 & \lambda & 0 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 0 & \lambda \\
0 & 0 & 0 & 0 & \cdots & \lambda & 0
\end{pmatrix}, \quad A^-(\lambda) \triangleq -A^+(\lambda),
\]

and let \( A(\lambda) \) be the following \( \ell \times \ell \) block diagonal matrix

\[
A(\lambda) \triangleq \begin{pmatrix}
A^+(\lambda) & 0 \\
0 & A^-(\lambda)
\end{pmatrix}.
\]  \( (9) \)

The matrix \( A(\lambda) \) possesses several useful properties, which are essential in our construction. These useful properties follow from the fact that the minimal polynomial of \( A(\lambda) \) is \( x^2 - \lambda^2 \). This form of the minimal polynomial shows that the matrix \( A(\lambda) \) acts as a transposition on the vectors of \( \mathbb{F}_q^{\ell/2} \) which are not eigenvectors, up to a multiplication by \( \lambda \). That is, all vectors which are not eigenvectors may be partitioned to pairs \((u, v)\) such that \( uA = v \) and \( vA = \lambda^2 u \), as proved in Lemma 5 which follows. In addition, for field with even characteristic, the matrix \( A(\lambda) \) is non-diagonalizable. To the best of our knowledge, this constitutes the first construction of an \((\mathcal{A}, \mathcal{S})\)-set satisfying the subspace condition whose matrices are non-diagonalizable. Notice that the multiplication of a vector \( v \) by the matrix \( A(\lambda) \) switches between entries \( 2t \) and \( 2t + 1 \) of \( v \) for all \( t \in \{0, \ldots, \ell/2 - 1\} \), and multiplies all entries by either \( \lambda \) or \( -\lambda \) according to \( t \leq \ell/4 - 1 \) or \( t > \ell/4 - 1 \). This fact is demonstrated in the following lemma.
Lemma 5. If $P \in \mathbb{F}_q^{\ell \times \ell}$ is an invertible matrix whose rows are $p_0, \ldots, p_{\ell-1}$, and $B \triangleq P^{-1} A(\lambda) P$ for some $\lambda \in \mathbb{F}_q^*$, then for all $t \in \{0, \ldots, \ell/2 - 1\}$

$$p_{2t} B = \begin{cases} 
\lambda p_{2t+1} & \text{if } t \leq \ell/4 - 1 \\
-\lambda p_{2t+1} & \text{if } t > \ell/4 - 1
\end{cases}, \quad p_{2t+1} B = \begin{cases} 
\lambda p_{2t} & \text{if } t \leq \ell/4 - 1 \\
-\lambda p_{2t} & \text{if } t > \ell/4 - 1
\end{cases}.$$ 

Furthermore, the vectors $p_{2t+1} + p_{2t}$ and $p_{2t+1} - p_{2t}$ are eigenvectors of $B$.

Proof. By (9), for all $t \in \{0, \ldots, \ell/2 - 1\}$ we have that

$$e_{2t} A(\lambda) = \begin{cases} 
\lambda e_{2t+1} & \text{if } t \leq \ell/4 - 1 \\
-\lambda e_{2t+1} & \text{if } t > \ell/4 - 1
\end{cases}, \quad e_{2t+1} A(\lambda) = \begin{cases} 
\lambda e_{2t} & \text{if } t \leq \ell/4 - 1 \\
-\lambda e_{2t} & \text{if } t > \ell/4 - 1
\end{cases}.$$ 

In addition, since $PP^{-1} = I$, it follows that $p_i P^{-1} = e_i$ for all $i \in \{0, \ldots, \ell - 1\}$. Therefore, for all $t \in \{0, \ldots, \ell/2 - 1\}$

$$p_{2t} B = p_{2t} P^{-1} A(\lambda) P = e_{2t} A(\lambda) P = \pm \lambda e_{2t+1} P = \pm \lambda p_{2t+1}, \quad (10)$$

$$p_{2t+1} B = p_{2t+1} P^{-1} A(\lambda) P = e_{2t+1} A(\lambda) P = \pm \lambda e_{2t} P = \pm \lambda p_{2t}, \quad (11)$$

where the $\pm$ sign distinguishes between the cases $t \leq \ell/4 - 1$ and $t > \ell/4 - 1$. To see that $p_{2t+1} + p_{2t}$ and $p_{2t+1} - p_{2t}$ are eigenvectors of $B$, notice that by adding and substracting $\{10\}$ and $\{11\}$, we have that

$$\langle p_{2t+1} + p_{2t} \rangle B = \pm \lambda \langle p_{2t+1} + p_{2t} \rangle \quad (12)$$

$$\langle p_{2t+1} - p_{2t} \rangle B = \mp \lambda \langle p_{2t+1} - p_{2t} \rangle. \quad (13)$$

Given a matching $\mathcal{M} = (M, M')$, it is easily verified that the following two matrices are invertible. Recall that $m_i, m'_i$ are vertices in the complete graph, which are identified by unit vectors of length $\ell$.

$$P_M \triangleq \begin{pmatrix} 
m_0 & m'_0 - m_0 \\
m_1 & m'_1 - m_1 \\
\vdots & \vdots \\
m_{\ell/2-1} & m'_{\ell/2-1} - m_{\ell/2-1}
\end{pmatrix}, \quad P_{M'} \triangleq \begin{pmatrix} 
m'_0 & m_0 + m'_0 \\
m'_1 & m_1 + m'_1 \\
\vdots & \vdots \\
m'_{\ell/2-1} & m_{\ell/2-1} + m'_{\ell/2-1}
\end{pmatrix}$$

Definition 4. Given a matching $\mathcal{M} = (M, M')$, let

$$A_M(\lambda) \triangleq P_M^{-1} \cdot A(\lambda) \cdot P_M; \quad S_M \triangleq \langle M \rangle = \{ m_i \}_{i=0}^{\ell/2-1}$$

$$A_{M'}(\lambda) \triangleq P_{M'}^{-1} \cdot A(\lambda) \cdot P_{M'}; \quad S_{M'} \triangleq \langle M' \rangle = \{ m'_i \}_{i=0}^{\ell/2-1}.$$ 

(14)
As an immediate consequence of Lemma 5 and Definition 4, we have the following.

**Corollary 2.** For every \( i \in \{0, \ldots, \ell/4 - 1\} \),

\[
\begin{align*}
m_i A_M(\lambda) &= \begin{cases} 
\lambda(m'_i - m_i) & \text{if } i \leq \ell/4 - 1 \\
-\lambda(m'_i - m_i) & \text{if } i > \ell/4 - 1
\end{cases}, \\
m'_i A_M(\lambda) &= \begin{cases} 
\lambda(m_i + m'_i) & \text{if } i \leq \ell/4 - 1 \\
-\lambda(m_i + m'_i) & \text{if } i > \ell/4 - 1
\end{cases},
\end{align*}
\]

and,

- For \( i \leq \ell/4 - 1 \),
  - \( m'_i \) is an eigenvector of \( A_M(\lambda) \) which corresponds to the eigenvalue \( \lambda \).
  - \( m_i \) is an eigenvector of \( A_M(\lambda) \) which corresponds to the eigenvalue \( -\lambda \).

- For \( i > \ell/4 - 1 \),
  - \( m'_i \) is an eigenvector of \( A_M(\lambda) \) which corresponds to the eigenvalue \( -\lambda \).
  - \( m_i \) is an eigenvector of \( A_M(\lambda) \) which corresponds to the eigenvalue \( \lambda \).

A matching \( \mathcal{M} \) provides an \((\mathcal{A}, \mathcal{S})\)-set of size two as follows.

**Lemma 6.** If \( \mathcal{M} = (M, M') \) is a matching, then \( \{(A_M(\lambda), S_M), (A_{M'}(\lambda), S_{M'})\} \) satisfies the subspace condition.

**Proof.** For convenience of notation, and since \( \lambda \) does not play a role in the current proof, let \( A_M \) and \( A_{M'} \) denote \( A_M(\lambda) \) and \( A_{M'}(\lambda) \), respectively. We show that all four properties of the subspace condition are satisfied.

To prove the independence property, notice that by Corollary 2

\[
\begin{align*}
S_M A_M &= \left\langle \{m'_i - m_i\}_{i=0}^{\ell/2-1} \right\rangle, \\
S_M A_{M'} &= \left\langle \{m_i + m'_i\}_{i=0}^{\ell/2-1} \right\rangle,
\end{align*}
\]

and thus, \( S_M A_M + S_M = S_M A_{M'} + S_{M'} = \mathbb{F}_q^\ell \).

To prove the invariance property, notice that by Corollary 2 \( S_M \) (resp. \( S_{M'} \)) is a span of eigenvectors of \( A_{M'} \) (resp. \( A_M \)) and hence it is \( A_{M'} \) (resp. \( A_M \)) invariant.

To prove the nonsingular property, first notice that \( A_M, A_{M'} \) are invertible since they are defined as a product of invertible matrices, and thus every \( 1 \times 1 \) submatrix is invertible. Second, notice that

\[
\begin{pmatrix}
I \\
A_M & A_{M'}
\end{pmatrix}
\]

is invertible if and only if \( A_M - A_{M'} \) is invertible. Since \( M \cup M' \) is a basis of \( \mathbb{F}_q^\ell \), to show that \( A_M - A_{M'} \) is invertible it suffices to show that its image contains \( M \cup M' \).

Let \( i \in \{0, \ldots, \ell/2 - 1\} \), and notice that by Corollary 2 if \( i \leq \ell/4 - 1 \) then

\[
\begin{align*}
\lambda^{-1} m_i (A_M - A_{M'}) &= \lambda^{-1} (m_i A_M - m_i A_{M'}) \\
&= \lambda^{-1} (\lambda(m'_i - m_i) + \lambda m_i) = m'_i \\
-\lambda^{-1} m'_i (A_M - A_{M'}) &= -\lambda^{-1} (m'_i A_M - m'_i A_{M'}) \\
&= -\lambda^{-1} (\lambda m'_i - \lambda(m_i + m'_i)) = m_i.
\end{align*}
\]

\footnote{Note that it does not comply with the definition of an eigenspace, since it contains vectors that correspond to distinct eigenvalues.}
On the other hand, if \( i > \ell/4 + 1 \),
\[
-\lambda^{-1}m_i(A_M - A_{M'}) = -\lambda^{-1}(m_iA_M - m_iA_{M'}) = -\lambda^{-1}(-\lambda(m'_i - m_i) - \lambda m_i) = m'_i
\]
\[
\lambda^{-1}m'_i(A_M - A_{M'}) = \lambda^{-1}(m'_iA_M - m_iA_{M'}) = \lambda^{-1}(-\lambda m'_i + \lambda(m'_i + m_i)) = m'_i.
\]
Therefore, for all \( i \in \{0, \ldots, \ell/2 - 1\} \), the vectors \( m_i \) and \( m'_i \) are in \( \text{Im}(A_M - A_{M'}) \), which implies that \( A_M - A_{M'} \) is of full rank. \( \square \)

From Lemma 6 it is evident that any pair \((M, \lambda)\) of a matching \( M = (M, M') \) and a nonzero field element \( \lambda \) provides an \((A, S)\)-set of size two. In Section 3.2 we discuss the required relation between two such pairs \((X, \lambda_x), (Y, \lambda_y)\) that allow the corresponding \((A, S)\)-sets to be united without compromising the subspace condition.

### 3.2 Two Parities Code from Two Matchings

To construct larger \((A, S)\)-sets, we analyse the required relations between two distinct pairs \((X, \lambda_x), (Y, \lambda_y)\) that allow the construction of an \((A, S)\)-set of size four. In Lemma 7, which follows, we show that there exists three sufficient conditions that \((X, \lambda_x), (Y, \lambda_y)\) should satisfy for this purpose. The first condition states that \( \lambda_x \) and \( \lambda_y \) must be distinct. The second condition, called the pairing condition, appears in Definition 3. The third condition, which is a more subtle one and will only be relevant in fields with odd characteristic, is that the vertices of certain edges from \( X \) fall into distinct halves defined by the order of \( Y \), and vice versa.

Clearly, a set \( \{(X_i, \lambda_i)\}_{i=1}^t \) such that any two pairs satisfy all of the above conditions, will provide an \((A, S)\)-set of size \( 2t \). In the sequel we provide such a set of size \( m \) over \( \mathbb{F}_q \), for any \( m \in \mathbb{N} \) and any \( q \geq m + 1 \). This set will yield an \((A, S)\)-set of size \( 2m \) for \( q \geq m + 1 \), which consists of matrices of size \( 2^m \times 2^m \).

**Lemma 7.** If \( X = (X, X'), Y = (Y, Y') \) are matchings and \( \lambda_x, \lambda_y \) are nonzero field elements such that

\( A1. \lambda_x \neq \lambda_y. \)

\( A2. \ X \) and \( Y \) satisfy the pairing condition.

\( A3. \) If \( \lambda_x = -\lambda_y \), then for all \( i \in \{0, \ldots, \ell/2 - 1\} \),

- if \( (x_i, x'_i) = (y_j, y_t) \) then \( i \leq \ell/4 - 1, \ j \leq \ell/4 - 1, \) and \( t > \ell/4 - 1 \), and
- if \( (x_i, x'_i) = (y'_j, y'_t) \) then \( i > \ell/4 - 1, \ j \leq \ell/4 - 1, \) and \( t > \ell/4 - 1 \).

then the \((A, S)\)-set
\[
\{(A_X(\lambda_x), S_X), (A_X'(\lambda_x), S_X'), (A_Y(\lambda_y), S_Y), (A_Y'(\lambda_y), S_Y')\}
\]
satisfies the subspace condition.
The independence property follows directly from Lemma 6, as well as the non-singularity of any $1 \times 1$ submatrix in the nonsingular property. To prove the invariance property, notice that the cases
\[
S_X A_X' = S_X \quad \quad S_Y A_Y' = S_Y
\]
follow from Lemma 3 as well. We prove now that $S_X A_Y = S_X$, and the rest of the cases follow by symmetry.

Since $S_X = \langle x_0, \ldots, x_{\ell/2-1} \rangle$, a necessary and sufficient condition for $S_X A_Y = S_X$ is that $x_i A_Y \in S_X$ for every $i \in \{0, \ldots, \ell/2 - 1\}$. Let $x_i \in S_X$ for some $i \in \{0, \ldots, \ell/2 - 1\}$. Since $X$ and $Y$ are matchings over the same vertex set, we have that either $x_i \in Y$ or $x_i \in Y'$. If $x_i \in Y'$, i.e., $x_i = y'_j$ for some $j \in \{0, \ldots, \ell/2 - 1\}$, then by Corollary 2 and by the definition of $A_Y$ (14), we have that $y'_j$ is an eigenvector of $A_Y$. Therefore,
\[
S_X A_Y = y'_j A_Y = \pm \lambda y_j' = \pm \lambda y x_i \in S_X.
\]
On the other hand, if $x_i \in Y$, i.e., $x_i = y_j$ for some $j \in \{0, \ldots, \ell/2 - 1\}$, then by Corollary 2
\[
x_i A_Y = y_j A_Y = \pm \lambda y (y_j' - y_j) = \pm \lambda y_j' \mp \lambda y_j = \pm \lambda y_j' \mp \lambda y x_i. \quad (16)
\]
According to A2 (the pairing condition), we have that if $y_j \in X$, then $y_j' \in X$ as well. Therefore (16) is a sum of two vectors in $S_X$, which implies that $x_i A_Y \in S_X$.

To prove the nonsingular property, we show that $X \cup X' \subseteq \text{Im}(A_X - A_Y)$, and the rest of the cases follow by symmetry. Since $X \cup X'$ is a basis of $\mathbb{F}_q^{\ell}$, it will follow that $\text{rank}(A_X - A_Y) = \ell$ as required. We split the proof to two cases as follows.

Case 1. $\lambda_x \neq -\lambda_y$ (and thus $\lambda_x \neq \pm \lambda_y$ by A1). If $i \in \{0, \ldots, \ell/2 - 1\}$, then by A2, we have that either $(x_i, x_i') = (y_j, y_t)$ or $(x_i, x_i') = (y'_j, y'_t)$ for some distinct $j, t \in \{0, \ldots, \ell/2 - 1\}$. If $(x_i, x_i') = (y'_j, y'_t)$, then simple calculations that follow from Corollary 2 show that
\[
x_i(A_X - A_Y) = \begin{cases} 
\lambda x x_i' - (\lambda x + \lambda y) x_i & \text{if } i \leq \ell/4 - 1, j \leq \ell/4 - 1 \\
\lambda x x_i' - (\lambda x - \lambda y) x_i & \text{if } i \leq \ell/4 - 1, j > \ell/4 - 1 \\
-\lambda x x_i' + (\lambda x - \lambda y) x_i & \text{if } j \leq \ell/4 - 1, j \leq \ell/4 - 1 \\
-\lambda x x_i' + (\lambda x + \lambda y) x_i & \text{if } j > \ell/4 - 1, j > \ell/4 - 1 
\end{cases} \quad (17)
\]
\[
x_i'(A_X - A_Y) = \begin{cases} 
(\lambda x - \lambda y) x_i' & \text{if } i \leq \ell/4 - 1, t \leq \ell/4 - 1 \\
(\lambda x + \lambda y) x_i' & \text{if } i \leq \ell/4 - 1, t > \ell/4 - 1 \\
-(\lambda x + \lambda y) x_i' & \text{if } j \leq \ell/4 - 1, t \leq \ell/4 - 1 \\
-(\lambda x - \lambda y) x_i' & \text{if } j > \ell/4 - 1, t > \ell/4 - 1.
\end{cases} \quad (18)
\]
Since $\lambda_x \neq \pm \lambda_y$, it follows by (18) that $x_i' \in \text{Im}(A_X - A_Y)$, which also implies by (17) that
Case 2. Let \( x_i \in \text{Im}(A_X - A_Y) \). If \((x_i, x_i') = (y_j, y_t)\), then similar calculations show that

\[
x_i(A_X - A_Y) = \begin{cases} 
\lambda x x_i' - (\lambda x - \lambda y)x_i - \lambda y y_j' & \text{if } i \leq \ell/4 - 1, j \leq \ell/4 - 1 \\
\lambda x x_i' - (\lambda x + \lambda y)x_i + \lambda y y_j' & \text{if } i \leq \ell/4 - 1, j > \ell/4 - 1 \\
-\lambda x x_i' + (\lambda x + \lambda y)x_i - \lambda y y_j' & \text{if } i > \ell/4 - 1, j \leq \ell/4 - 1 \\
-\lambda x x_i' + (\lambda x - \lambda y)x_i + \lambda y y_j' & \text{if } i > \ell/4 - 1, j > \ell/4 - 1 
\end{cases}
\]

(19)

\[
x_i'(A_X - A_Y) = \begin{cases} 
(\lambda x + \lambda y)x_i' - \lambda y y_t' & \text{if } i \leq \ell/4 - 1, t \leq \ell/4 - 1 \\
(\lambda y - \lambda x)x_i' + \lambda y y_t' & \text{if } i \leq \ell/4 - 1, t > \ell/4 - 1 \\
- (\lambda x - \lambda y)x_i' - \lambda y y_t' & \text{if } i > \ell/4 - 1, t \leq \ell/4 - 1 \\
- (\lambda x + \lambda y)x_i' + \lambda y y_t' & \text{if } i > \ell/4 - 1, t > \ell/4 - 1 
\end{cases}
\]

(20)

Now, notice that since \( x_i = y_j \) we have that \( y_j \in X \). By A2, we also have that \( y_j' \in X \), and hence \( y_j' = x_s \) for some \( s \in \{0, \ldots, \ell/2 - 1\} \). We have shown earlier that if \( x_s = y_j' \) then \( x_s = y_j' \in \text{Im}(A_X - A_Y) \). Similarly, since \( x_i' = y_t \), we have that \( y_t' \in X' \), i.e., \( y_t' = x_r' \) for some \( r \in \{0, \ldots, \ell/2 - 1\} \). This implies that \( x_r, x_r' \in Y' \) by the pairing condition, and thus, \( x_i' = y_t' \in \text{Im}(A_X - A_Y) \).

Since \( y_t' \in \text{Im}(A_X - A_Y) \), and since \( \lambda_x \neq \pm \lambda_y \), it follows from (20) that \( x_i' \in \text{Im}(A_X - A_Y) \). Therefore, by (19), and since \( y_j' \in \text{Im}(A_X - A_Y) \) and \( \lambda_x \neq \pm \lambda_y \), it follows that \( x_i \in \text{Im}(A_X - A_Y) \) as well.

Case 2. \( \lambda_x = -\lambda_y \) (and thus we have to consider A3). The pairing condition implies that either \((x_i, x_i') = (y_j, y_t)\) or \((x_i, x_i') = (y_j', y_t')\) for some distinct \( j, t \in \{0, \ldots, \ell/2 - 1\} \). However, by A3, most of the cases in (17), (18), (19), (20) are impossible. Hence, if \((x_i, x_i') = (y_j', y_t')\) then \( i > \ell/4 - 1, j \leq \ell/4 - 1, \) and \( t > \ell/4 - 1 \), and thus

\[
x_i(A_X - A_Y) = -\lambda x x_i' + (\lambda x - \lambda y)x_i \\
x_i'(A_X - A_Y) = (\lambda y - \lambda x)x_i'.
\]

Since \( \lambda_x \neq \lambda_y \), we have that \( x_i, x_i' \in \text{Im}(A_X - A_Y) \). If \((x_i, x_i') = (y_j, y_t)\) then \( i \leq \ell/4 - 1, j \leq \ell/4 - 1, \) and \( t > \ell/4 - 1 \), and thus

\[
x_i(A_X - A_Y) = \lambda x x_i' + (\lambda y - \lambda x)x_i - \lambda y y_j' \\
x_i'(A_X - A_Y) = (\lambda x - \lambda y)x_i' + \lambda y y_t'.
\]

As in Case 1, we can prove that \( y_j', y_t' \in \text{Im}(A_X - A_Y) \), and get that since \( \lambda_x \neq \lambda_y \), we have that \( x_i, x_i' \in \text{Im}(A_X - A_Y) \).

\[ \square \]

By Lemma 7 we have that two matchings \( \mathcal{X}, \mathcal{Y} \) and two corresponding field elements \( \lambda_x, \lambda_y \) that meet the requirements A1-A3, provide an \((\mathcal{A}, \mathcal{S})\)-set of size four. Therefore, a construction of a large set of pairs \((\mathcal{X}_i, \lambda_i)\), such that any two pairs satisfy A1-A3, is required for a construction of a large \((\mathcal{A}, \mathcal{S})\)-set which satisfies the subspace condition.

### 3.3 Construction of Matchings for Two Parities

In the sequel we construct a set \( \{(\mathcal{X}_i, \lambda_i)\}_{i=0}^{n-1} \) whose elements satisfy the requirements of Lemma 7 in pairs. For convenience we identify vertex \( e_i \) of \( K_\ell \) with the integer \( i \) in its binary representation. We will use the following standard notion of a boolean cube.
Definition 5. Given a sequence of distinct integers \( i_1, \ldots, i_k \) in \( \{0, \ldots, m - 1\} \) and a sequence of boolean values \( b_1, \ldots, b_k \), the boolean cube \( C(\{(i_j, b_j)\}_{j=1}^k) \) is the set of all \( m \)-bit vectors over \( \{0, 1\} \) that have \( b_j \) in entry \( i_j \) for all \( j = 1, \ldots, k \). That is,
\[
C(\{(i_j, b_j)\}_{j=1}^k) \triangleq \{ x \in \{0, 1\}^m \mid \text{for all } j \in [k], \ x_{i_j} = b_j \}.
\]

For convenience, we consider the elements in such a boolean cube as ordered according to the lexicographic order (see Example 1 below), that is, we consider a boolean cube as a sequence rather than a set.

Example 1. If \( m = 4 \) then the boolean cube \( C(\{(1,1), (2,1)\}) \) is the set \( \{v_1, v_2, v_3, v_4\} \) such that \( (v_1, v_2, v_3, v_4) = (0110, 0111, 1110, 1111) \).

We begin by defining a set of matchings that meets the pairing condition.

Definition 6. For any \( m \in \mathbb{N} \), define \( m \) matchings \( \mathcal{X}_i = (X_i, X_i') \) \( \forall i = 0, \ldots, m-1 \) as follows
\[
\mathcal{X}_0 : \begin{cases}
X_0 = C(\{(0,0),(1,0)\}) \circ C(\{(0,0),(1,1)\}) \\
X'_0 = C(\{(0,0),(1,0)\}) \circ C(\{(0,1),(1,1)\})
\end{cases}
\]
\[
\mathcal{X}_1 : \begin{cases}
X_1 = C(\{(0,0),(1,0)\}) \circ C(\{(0,1),(1,0)\}) \\
X'_1 = C(\{(0,0),(1,1)\}) \circ C(\{(0,1),(1,1)\})
\end{cases}
\]
\[
\mathcal{X}_2 : \begin{cases}
X_2 = C(\{(2,0),(3,0)\}) \circ C(\{(2,1),(3,1)\}) \\
X'_2 = C(\{(2,1),(3,0)\}) \circ C(\{(2,1),(3,1)\})
\end{cases}
\]
\[
\mathcal{X}_3 : \begin{cases}
X_3 = C(\{(2,0),(3,0)\}) \circ C(\{(2,1),(3,0)\}) \\
X'_3 = C(\{(2,0),(3,1)\}) \circ C(\{(2,1),(3,1)\})
\end{cases}
\]

which implies that
\[
\begin{align*}
\mathcal{X}_0 : & \begin{cases}
X_0 = \{0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111\} \\
X'_0 = \{1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111\}
\end{cases} \\
\mathcal{X}_1 : & \begin{cases}
X_1 = \{0000, 0001, 0010, 0011, 1000, 1001, 1010, 1011\} \\
X'_1 = \{0100, 0101, 0110, 0111, 1100, 1101, 1110, 1111\}
\end{cases} \\
\mathcal{X}_2 : & \begin{cases}
X_2 = \{0000, 0100, 1000, 1100, 0001, 0101, 1001, 1101\} \\
X'_2 = \{0010, 0110, 1010, 1110, 0011, 0111, 1111, 1111\}
\end{cases} \\
\mathcal{X}_3 : & \begin{cases}
X_3 = \{0000, 0100, 1000, 1100, 0010, 0110, 1010, 1110\} \\
X'_3 = \{0011, 0101, 1011, 1111, 0111, 1011, 1111, 1111\}
\end{cases}
\end{align*}
\]
where the characters in bold indicate the fixed entries in each boolean cube.

Since the pairing condition (Definition 3) is independent of the choice of a field element for every matching, we first show that the matchings from Definition 6 meet the pairing condition. The choice of field element for each matching, which satisfies A1 and A3 of Lemma 7, will be done in the sequel.

**Lemma 8.** Every two distinct matchings \( X_i, X_j \) from Definition 6 satisfy the pairing condition.

**Proof.** Denote the elements of the matchings \( X_i, X_j \) as

\[
X_i = \{x_{i,0}, \ldots, x_{i,\ell/2-1}\} \\
X_i' = \{x_{i,0}', \ldots, x_{i,\ell/2-1}'\} \\
X_j = \{x_{j,0}, \ldots, x_{j,\ell/2-1}\} \\
X_j' = \{x_{j,0}', \ldots, x_{j,\ell/2-1}'\}.
\]

According to Definition 6 it is evident that in every edge \((x_{i,t}, x_{i,t}') \in X_i\), the \(i\)-th entry of \(x_{i,t}\) is 0, the \(i\)-th entry of \(x_{i,t}'\) is 1, and the rest of the entries are identical. Similarly, in every edge \((x_{j,t}, x_{j,t}') \in X_j\), the \(j\)-th entry of \(x_{j,t}\) is 0, the \(j\)-th entry of \(x_{j,t}'\) is 1, and the rest of the entries are identical. Therefore, for every edge \((x_{i,t}, x_{i,t}') \in X_i\) if the \(j\)-th entry of both \(x_{i,t}\) and \(x_{i,t}'\) is 0, then \(x_{i,t}, x_{i,t}' \in X_j\), and if it is 1, then \(x_{i,t}, x_{i,t}' \in X_j'\). Therefore, \(X_j\) is a union of edges from \(X_i\). The proof that \(X_i\) is a union of edges from \(X_j\) is similar. \(\blacksquare\)

We now turn to choose a proper nonzero field element for every matching from Definition 6. This choice must comply with requirements A1 and A3 of Lemma 7. Note that if \(q\) is even, then A3 follows from A1. Hence, in these fields the choice of field elements is straightforward.

**Lemma 9.** If \(q \geq m+1\) is a power of two, then by arbitrarily assigning pairwise distinct elements from \(\mathbb{F}_q^*\) to the \(m\) matchings from Definition 6, the resulting \((A,S)\)-set satisfies A1-A3 from Lemma 7.

**Proof.** Since the assigned elements are distinct, every two matchings satisfy property A1 of Lemma 7. According to Lemma 8 every two matchings satisfy the pairing condition (A2) as well. Since \(q\) is even, property A3 is implied from property A1. \(\blacksquare\)

If \(q\) is odd, more care is needed for the mapping of nonzero field elements to the matchings. We do this by assigning the field elements \(\lambda\) and \(-\lambda\) to two adjacent matchings \(X_{2t}, X_{2t+1}\).

**Lemma 10.** If \(q \geq m+1\) is a power of an odd prime, then by arbitrarily assigning pairwise distinct elements from \(\mathbb{F}_q^*\) to the \(m\) matchings from Definition 6 such that \(X_{2t}, X_{2t+1}\) are mapped to additive inverses \(\lambda, -\lambda\) for every \(t \in \{0, \ldots, \left\lfloor \frac{m}{2} \right\rfloor - 1\}\), the resulting \((A,S)\)-set satisfies A1-A3 from Lemma 7.

**Proof.** For every two distinct matchings, requirement A1 of Lemma 7 is trivially satisfied, and requirement A2 is satisfied by Lemma 8. To prove A3, let \(X_i, X_j\) be matchings that are mapped to additive inverses \(\lambda_i = -\lambda_j\). By the definition of the mapping, it follows w.l.o.g that \(i = 2t\) and \(j = 2t+1\) for some \(t \in \{0, \ldots, \left\lfloor \frac{m}{2} \right\rfloor - 1\}\).

Let \((x_{2t,s}, x_{2t,s}')\) be an edge in \(X_{2t}\), and thus the \((2t)\)-th bit of \(x_{2t,s}\) is 0 and the \((2t)\)-th bit of \(x_{2t,s}'\) is 1. To prove A3, we must show that

\[
\begin{align*}
&\text{if } (x_{2t,s}, x_{2t,s}') = (x_{2t+1,u}, x_{2t+1,r}) & s \leq \ell/4 - 1, & u \leq \ell/4 - 1, & r > \ell/4 - 1, & \text{and} \\
&\text{if } (x_{2t,s}, x_{2t,s}') = (x_{2t+1,u}', x_{2t+1,r}') & s > \ell/4 - 1, & u \leq \ell/4 - 1, & r > \ell/4 - 1.
\end{align*}
\]
If \((x_{2t,s}, x'_{2t,s}) = (x_{2t+1,u}, x_{2t+1,r})\) for some \(u, r \in \{0, \ldots, \ell/2 - 1\}\), it follows that the \((2t)\)-th bit of \(x_{2t+1,s}\) and \(x'_{2t+1,s}\) is 0. Therefore

\[
x_{2t,s} = x_{2t+1,u} \in C(\{(2t, 0), (2t + 1, 0)\})
\]
\[
x'_{2t,s} = x_{2t+1,r} \in C(\{(2t, 1), (2t + 1, 0)\}),
\]

and hence, by the definition of \(X_{2t+1}\) (Definition 3), it follows that \(u \leq \ell/4 - 1\) and \(r > \ell/4 - 1\). In addition, by the definition of \(X_{2t}\) it follows that \(s \leq \ell/4 - 1\).

If \((x_{2t,s}, x'_{2t,s}) = (x'_{2t+1,u}, x'_{2t+1,r})\) for some \(u, r \in \{0, \ldots, \ell/2 - 1\}\), it follows that the \((2t)\)-th bit of \(x_{2t+1,s}\) and \(x'_{2t+1,s}\) is 1. Therefore

\[
x_{2t,s} = x'_{2t+1,u} \in C(\{(2t, 0), (2t + 1, 1)\})
\]
\[
x'_{2t,s} = x'_{2t+1,r} \in C(\{(2t, 1), (2t + 1, 1)\}),
\]

and hence, by the definition of \(X_{2t+1}\), it follows that \(u \leq \ell/4 - 1\) and \(r > \ell/4 - 1\). In addition, by the definition of \(X_{2t}\) it follows that \(s > \ell/4 - 1\).

The main construction of this section is summarized in the following theorem.

**Theorem 2.** If \(m\) is a positive integer and \(q \geq m+1\) is a prime power, then there exists an explicitly defined \((A, S)\)-set \(\mathbb{C}\) of size \(2m\) and \(2^m \times 2^m\) matrices over \(\mathbb{F}_q\), which satisfies the subspace condition.

**Proof.** Let \(\{X_i = (X_i, X'_i)\}_{i=0}^{m-1}\) be the set of matchings from Definition 6 which by Lemma 8 satisfies the pairing condition (Definition 3). If \(q\) is even, let \(\lambda_0, \ldots, \lambda_{m-1}\) be distinct elements in \(\mathbb{F}_q^*\), and let

\[
\mathbb{C} \triangleq \bigcup_{i=0}^{m-1} \{(A_{X_i}(\lambda_i), S_{X_i}), (A_{X'_i}(\lambda_i), S_{X'_i})\}, \tag{21}
\]

where \((A_{X_i}(\lambda_i), S_{X_i}), (A_{X'_i}(\lambda_i), S_{X'_i})\) were defined in Lemma 6. Since conditions A1-A3 of Lemma 7 are met with respect to every two matchings and their respective field elements, it follows that \(\mathbb{C}\) satisfies the subspace condition.

If \(q\) is odd, let \(\lambda_0, \ldots, \lambda_{m-1}\) be distinct elements in \(\mathbb{F}_q^*\) such that \(\lambda_{2t} = -\lambda_{2t+1}\) for every \(t \in \{0, \ldots, \lfloor \frac{m}{2} \rfloor - 1\}\). Define \(\mathbb{C}\) in the same manner as in (21). Conditions A1 and A2 are satisfied as in the case of an even \(q\). Condition A3 is satisfied by Lemma 10 and therefore \(\mathbb{C}\) satisfies the subspace condition in this case as well.

\[
\square
\]

### 4 Construction of an MSR Code with Three Parities

In this section we construct MSR codes with three parities using the framework mentioned in Subsection 2.3. The size of the matrices is \(\ell \times \ell\), where \(\ell = 3^m\) for some integer \(m\). This construction requires that all three roots of unity of order three lie in the base field (which implies the necessary condition \(3|q - 1\)). If \(q\) is odd we require that \(q \geq 6m + 1\) and if \(q\) is even we require that \(q \geq 3m + 1\). As the roots of unity of order three play an important role in this section, recall the following properties of these roots, some of which can be generalized for every set of roots of unity of any order.

**Lemma 11.** If \(q\) is a prime power such that \(3|q - 1\), then \(\mathbb{F}_q\) contains three distinct roots of unity of order three \(1, \gamma_1, \gamma_2\), which satisfy \(1 + \gamma_1 + \gamma_2 = 0, \gamma_1^2 = \gamma_2, \text{ and } \gamma_2^{-1} = \gamma_1\).
From now on we assume that \(3|q - 1\), and \(1, \gamma_1, \gamma_2\) are the three roots of unity of order three. Notice that this necessary condition rules out the possibility of using fields with characteristic 3.

For three parities, proving the nonsingular property becomes slightly more involved, since we must show that the following conditions are satisfied.

**Conditions for the nonsingular property:** (three parities)

1. For all \(i \in [k]\), \(A_i\) is invertible.

2. For all \(i, j \in [k], i \neq j\), the matrix \(\begin{pmatrix} I & I \\ A_i & A_j \end{pmatrix}\) is invertible.

3. For all \(i, j \in [k], i \neq j\), the matrix \(\begin{pmatrix} I & I \\ A_i^2 & A_j^2 \end{pmatrix}\) is invertible.

4. For all \(i, j \in [k], i \neq j\), the matrix \(\begin{pmatrix} A_i & A_j \\ A_i^2 & A_j^2 \end{pmatrix}\) is invertible.

5. For all distinct \(i, j, t \in [k]\), the matrix \(\begin{pmatrix} I & I & I \\ A_i & A_j & A_t \\ A_i^2 & A_j^2 & A_t^2 \end{pmatrix}\) must be invertible.

However, assuming that Condition 1 is satisfied, we have that Condition 4 follows from Condition 2 using block-row operations\(\parallel\). That is, by multiplying the left column of the matrix in Condition 4 by \(A_i^{-1}\) and multiplying the right column by \(A_j^{-1}\), we get the exact same matrix as in Condition 2.

### 4.1 Three Parities from One Matching

Recall that in Section 3, every matching \(\mathcal{M}\) (Definition 2) provided an \((\mathcal{A}, S)\)-set \((A_M, S_M), (A_{M'}, S_{M'})\), where \(S_M\) is an eigenspace of \(A_{M'}\) and \(S_{M'}\) is an eigenspace of \(A_M\). Later on, we added together \((\mathcal{A}, S)\)-sets which were defined by different matchings satisfying the pairing condition (Definition 3). For three parities, we consider the natural generalization of matchings in the complete 3-uniform hypergraph.

Similarly to Section 3, this construction will rely on \(\ell \times \ell\) matrices whose minimal polynomial is \(x^3 - \lambda^3\) for some \(\lambda \in \mathbb{F}_q^*\). All the matrices in the \((\mathcal{A}, S)\)-set will be similar to the matrix \(A\) (7), which for \(r = 3\) takes the form of

\[
A \triangleq \begin{pmatrix}
0 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0
\end{pmatrix}.
\tag{22}
\]

\(\parallel\)The three standard block operations are interchanging two block rows (columns), multiplying a block row (column) from the left (right) by a non-singular matrix, and multiplying a block row (column) by a matrix from the left (right) and adding it to another row.
According to Corollary \ref{cor1} we have the following lemma.

**Lemma 12.** The matrix $A$ \eqref{A_matrix} is diagonalizable, with the following eigenspaces,

1. For the eigenvalue $\lambda$, a basis of the eigenspace is
   $$
   \{(1, 1, 1, 0, 0, 0, \ldots, 0, 0, 0),
   (0, 0, 0, 1, 1, 1, \ldots, 0, 0, 0),
   \ldots
   (0, 0, 0, 0, 0, 0, \ldots, 1, 1, 1)\}.
   $$

2. For the eigenvalue $\gamma_1$, a basis of the eigenspace is
   $$
   \{(1, \gamma_1, \gamma_2, 0, 0, 0, \ldots, 0, 0, 0),
   (0, 0, 0, 1, \gamma_1, \gamma_2, \ldots, 0, 0, 0),
   \ldots
   (0, 0, 0, 0, 0, 0, \ldots, 1, \gamma_1, \gamma_2)\}.
   $$

3. For the eigenvalue $\gamma_2$, a basis of the eigenspace is
   $$
   \{(1, \gamma_2, \gamma_1, 0, 0, 0, \ldots, 0, 0, 0),
   (0, 0, 0, 1, \gamma_2, \gamma_1, \ldots, 0, 0, 0),
   \ldots
   (0, 0, 0, 0, 0, 0, \ldots, 1, \gamma_2, \gamma_1)\}.
   $$

In addition, the subspace $S \triangleq \langle e_0, e_3, e_6, \ldots \rangle$ is an independent subspace of $A$.

The matrices in our $(A, S)$-sets are similar to a constant multiple of the matrix $A$, and thus they are also diagonalizable. The structure of their eigenspaces, which follows from Lemma \ref{lemma2} is as follows.

**Lemma 13.** If $P \in \mathbb{F}_{q^3}^{\ell \times \ell}$ is an invertible matrix whose rows are $p_0, \ldots, p_{\ell-1}$, and $M \triangleq \lambda P^{-1}AP$ for some $\lambda \in \mathbb{F}_q^*$, then $M$ has the following eigenspaces,

1. For the eigenvalue $\lambda$, a basis of the eigenspace is $\{p_{3i} + p_{3i+1} + p_{3i+2} \mid i \in \{0, \ldots, \ell/3 - 1\}\}$.

2. For the eigenvalue $\gamma_1 \lambda$, a basis of the eigenspace is $\{p_{3i} + \gamma_1 p_{3i+1} + \gamma_2 p_{3i+2} \mid i \in \{0, \ldots, \ell/3 - 1\}\}$.

3. For the eigenvalue $\gamma_2 \lambda$, a basis of the eigenspace is $\{p_{3i} + \gamma_2 p_{3i+1} + \gamma_1 p_{3i+2} \mid i \in \{0, \ldots, \ell/3 - 1\}\}$.

In addition, the subspace $S \triangleq \langle p_0, p_3, p_6, \ldots \rangle$ is an independent subspace of $M$.

We are now in a position to describe the $(A, S)$-set, of size three, that is given by a single matching. $(A, S)$-sets that are given by a union of single-matching $(A, S)$-sets will be discussed in the sequel. As mentioned earlier, all three matrices of this $(A, S)$-set are similar to $A$. The $\ell \times \ell$ change matrices are defined using $3 \times \ell$ constituent blocks (see \eqref{blocks}) as follows. For $\alpha, \beta \in \mathbb{F}_q^*$ and $u, v, w \in \mathbb{F}_{q^3}$, let

$$
N(\alpha, \beta, u, v, w) = \begin{pmatrix}
1 & 0 & 0 \\
0 & -\frac{\alpha \gamma_1}{\gamma_1 - 1} & \frac{\beta}{\gamma_1 - 1} \\
0 & \frac{\beta}{\gamma_1 - 1} & -\frac{\alpha \gamma_1}{\gamma_1 - 1}
\end{pmatrix} \cdot \begin{pmatrix}
u \\
v \\
w
\end{pmatrix}.
$$

\text{(23)}

The determinant of the $3 \times 3$ matrix in \eqref{blocks} equals $\alpha \beta \gamma_1^{\ell - 1}$, which is nonzero, and thus $N(\alpha, \beta, u, v, w)$ is row-equivalent to a matrix whose rows are $u, v, w$, for any choice of $\alpha, \beta \in \mathbb{F}_q^*$. This fact gives rise to the following necessary lemma, which can be easily proved.
Lemma 14. If \( \mathcal{M} = (M, M', M'') \) is a matching, then for any choice of \( \alpha, \alpha', \alpha'' \) and \( \beta, \beta', \beta'' \), in \( \mathbb{F}_q^* \), the following matrices are invertible.

\[
P_M \triangleq \begin{pmatrix}
N(\alpha, \beta, m_1, m_1', m_1'') \\
N(\alpha, \beta, m_2, m_2', m_2'') \\
\vdots \\
N(\alpha, \beta, m_{\ell/3}, m_{\ell/3}', m_{\ell/3}'')
\end{pmatrix},
P_{M'} \triangleq \begin{pmatrix}
N(\alpha', \beta', m_1', m_1'', m_1) \\
N(\alpha', \beta', m_2', m_2'', m_2) \\
\vdots \\
N(\alpha', \beta', m_{\ell/3}', m_{\ell/3}'', m_{\ell/3})
\end{pmatrix},
P_{M''} \triangleq \begin{pmatrix}
N(\alpha'', \beta'', m_1'', m_1, m_1') \\
N(\alpha'', \beta'', m_2'', m_2, m_2') \\
\vdots \\
N(\alpha'', \beta'', m_{\ell/3}'', m_{\ell/3}, m_{\ell/3}')
\end{pmatrix}
\]

Lemma 15. If \( \mathcal{M} = (M, M', M'') \) is a matching, then for any \( \lambda \in \mathbb{F}_q^* \), the following \((A, S)\)-set satisfies the subspace condition.

\[
A_M(\lambda) \triangleq \lambda \cdot P_M^{-1} A P_M, \quad S_M \triangleq \langle M \rangle \quad (24)
\]
\[
A_{M'}(\lambda) \triangleq \lambda \cdot P_{M'}^{-1} A P_{M'}, \quad S_{M'} \triangleq \langle M' \rangle \quad (25)
\]
\[
A_{M''}(\lambda) \triangleq \lambda \cdot P_{M''}^{-1} A P_{M''}, \quad S_{M''} \triangleq \langle M'' \rangle, \quad (26)
\]

where \( \alpha, \alpha', \alpha'', \beta, \beta', \beta'' \) are nonzero field elements that will be chosen according to the field characteristic.

4.2 Three Parities from Two Matchings

We are now in a position to describe a construction of an \((A, S)\)-set for three parities from more than one matching. The following lemma shows that it is possible to unite \((A, S)\)-sets \( C_X, C_Y \) which were constructed using different matchings satisfying the pairing condition (Definition), as long as a simple condition regarding the chosen constants \( \lambda_x, \lambda_y \) is met.

Lemma 16. If \( X = (X, X', X'') \), \( Y = (Y, Y', Y'') \) are two matchings that satisfy the pairing condition,

\[
C_X \triangleq \{(A_X(\lambda_x), S_X), (A_X(\lambda_x), S_X'), (A_X(\lambda_x), S_X'')\},
\]
\[
C_Y \triangleq \{(A_Y(\lambda_y), S_Y), (A_Y(\lambda_y), S_Y'), (A_Y(\lambda_y), S_Y'')\}
\]

are the corresponding \((A, S)\)-sets, and \( \lambda^6 \neq \lambda^6 \), then \( C_X \cup C_Y \) satisfies the subspace condition.

4.3 Construction of Matchings for Three Parities

In this subsection we present a set of matchings \( \{X_i\}_{i \in \mathbb{Z}} \) such that any two satisfy the pairing condition, and construct the resulting \((A, S)\)-set. Recall that each vertex in the complete 3-uniform hypergraph \( K_3^3 \) is represented by a unique unit vector of length \( \ell \). For convenience, we describe this set of matchings by considering vertex \( e_i \) as the integer \( i \) in its ternary representation. The construction of a proper set of matchings relies on the following definition, which is the three parity equivalent of Definition.
Definition 7. Given an integer \( i \in [m] \) and a value \( b \in \{0,1,2\} \), the ternary cube \( C(i,b) \) is the set of all length \( m \) vectors over \( \{0,1,2\} \) that have \( b \) in entry \( i \). That is,

\[
C(i,b) \triangleq \{ x \in \{0,1,2\}^m \mid x_i = b \}
\]

For convenience, we consider the elements in a ternary cube as ordered according to the lexicographic order (see Example 3 below).

Example 3. If \( m = 3 \) then the ternary cube \( C(2,2) \) is the set \( \{v_1, \ldots, v_9\} \) such that

\[
(v_1, \ldots, v_9) = (020, 021, 022, 120, 121, 122, 220, 221, 222).
\]

Definition 8. For any \( m \in \mathbb{N} \), define \( m \) matchings \( \{X_i = (X_i, X'_i, X''_i)\}_{i \in [m]} \) as follows

\[
X'_i : \begin{cases} 
X_i = C(i,0) \\
X'_i = C(i,1) \\
X''_i = C(i,2).
\end{cases}
\]

Lemma 17. The matchings from Definition 8 satisfy the pairing condition.

We conclude with the following theorem.

Theorem 3. If \( m \) is a positive integer, and \( q \) is a prime power such that

1. if \( q \) is odd, then \( 3|q - 1 \) and \( q \geq 6m + 1 \),

2. if \( q \) is even, then \( 3|q - 1 \) and \( q \geq 3m + 1 \),

then there exists an explicitly defined \((A,S)\)-set \( C \) of size \( 3m \) and \( 3^m \times 3^m \) matrices over \( \mathbb{F}_q \), which satisfies the subspace condition.

5 An Improved Construction over a Larger Field

In this section, a construction with \( r = 3 \) and \( k = (r + 1)m = 4m \) is presented, which requires a field larger than the one in Section 4 yet still linear in \( m \). This construction is comparable to [13] in terms of the parameter \( k \), but outperforms it in terms of explicitness and field size. As in [15], the construction considered in this section is not access-optimal, and is not known to achieve the sub-packetization bound. The ideas behind the construction follow the outline described in Subsection 2.3.

5.1 A Code from One Matching

A matching \( \mathcal{M} = (M, M', M'') \) will provide an \((A,S)\)-set of size \( r + 1 = 4 \), denoted by

\[
(A_M, S_M), (A_{M'}, S_{M'}), (A_{M''}, S_{M''}), (A_{M^*}, S_{M^*}).
\]

As in Section 4 we assume that \( 3|q - 1 \) in order to have three roots of unity of order 3, denoted by 1, \( \gamma_1, \gamma_2 \). The matrices in this construction are of the form \( P^{-1}AP \), where \( A \) was defined in [22].
Such a matrix $P$, of size $\ell \times \ell$, consists of constituent $3 \times \ell$ matrices which are defined using the following operator $N$. For $u,v,w \in \mathbb{F}_q^\ell$, let

$$N(u,v,w) \triangleq \begin{pmatrix} 1 & 1 & 1 \\ 1 & \gamma_2 & \gamma_1 \\ 1 & \gamma_1 & \gamma_2 \end{pmatrix} \begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} u + v + w \\ u + \gamma_2 v + \gamma_1 w \\ u + \gamma_1 v + \gamma_2 w \end{pmatrix}. \quad (27)$$

Notice that the $3 \times \ell$ matrix $N(u,v,w)$ is row equivalent to a matrix whose rows are $u,v,w$, since $N(u,v,w)$ is defined as the multiplication of a matrix whose rows are $u,v,w$ by a Vandermonde matrix (since $\gamma_1^2 = \gamma_2$ and $\gamma_1^2 = \gamma_2$).

**Lemma 18.** If $\{u_i\}_{i=0}^{\ell/3-1} \cup \{v_i\}_{i=0}^{\ell/3-1} \cup \{w_i\}_{i=0}^{\ell/3-1}$ is a basis of $\mathbb{F}_q^\ell$, then the matrix $P^{-1}AP$, where

$$P \triangleq \begin{pmatrix} N(u_0, & v_0, & w_0) \\ \vdots & \vdots & \vdots \\ N(u_{\ell/3-1}, & v_{\ell/3-1}, & w_{\ell/3-1}) \end{pmatrix},$$

has $\langle \{u_i\}_{i=0}^{\ell/3-1} \rangle$ as an eigenspace for the eigenvalue $1$, $\langle \{v_i\}_{i=0}^{\ell/3-1} \rangle$ as an eigenspace for the eigenvalue $\gamma_1$, and $\langle \{w_i\}_{i=0}^{\ell/3-1} \rangle$ as an eigenspace for the eigenvalue $\gamma_2$. In addition, the subspace $\langle \{u_i + v_i + w_i\}_{i=0}^{\ell/3-1} \rangle$ is an independent subspace.

**Proof.** According to Lemma 2 the matrix $P^{-1}AP$, where the rows of $P$ are $p_0, \ldots, p_{\ell-1}$, has the following eigenspaces.

1. For the eigenvalue $1$, a basis of the eigenspace is

$$\{p_{3i} + p_{3i+1} + p_{3i+2} \mid i \in \{0, \ldots, \ell/3 - 1\}\} = \{(u_i + v_i + w_i) + (u_i + \gamma_2 v_i + \gamma_1 w_i) + (u_i + \gamma_1 v_i + \gamma_2 w_i) \mid i \in \{0, \ldots, \ell/3 - 1\}\} = \{3u_i + (1 + \gamma_1 + \gamma_2)v_i + (1 + \gamma_1 + \gamma_2)w_i \mid i \in \{0, \ldots, \ell/3 - 1\}\} = \{3u_i\}_{i=0}^{\ell/3-1}$$

2. For the eigenvalue $\gamma_1$, a basis of the eigenspace is

$$\{p_{3i} + \gamma_1 p_{3i+1} + \gamma_2 p_{3i+2} \mid i \in \{0, \ldots, \ell/3 - 1\}\} = \{(u_i + v_i + w_i) + \gamma_1(u_i + \gamma_2 v_i + \gamma_1 w_i) + \gamma_2(u_i + \gamma_1 v_i + \gamma_2 w_i) \mid i \in \{0, \ldots, \ell/3 - 1\}\} = \{3v_i + (1 + \gamma_1 + \gamma_2)u_i + (1 + \gamma_1 + \gamma_2)w_i \mid i \in \{0, \ldots, \ell/3 - 1\}\} = \{3v_i\}_{i=0}^{\ell/3-1}$$

3. For the eigenvalue $\gamma_2$, a basis of the eigenspace is

$$\{p_{3i} + \gamma_2 p_{3i+1} + \gamma_1 p_{3i+2} \mid i \in \{0, \ldots, \ell/3 - 1\}\} = \{(u_i + v_i + w_i) + \gamma_2(u_i + \gamma_2 v_i + \gamma_1 w_i) + \gamma_1(u_i + \gamma_1 v_i + \gamma_2 w_i) \mid i \in \{0, \ldots, \ell/3 - 1\}\} = \{3w_i + (1 + \gamma_1 + \gamma_2)u_i + (1 + \gamma_1 + \gamma_2)v_i \mid i \in \{0, \ldots, \ell/3 - 1\}\} = \{3w_i\}_{i=0}^{\ell/3-1}$$

In addition, by Lemma 2 we have that $\langle \{u_i + v_i + w_i\}_{i=0}^{\ell/3-1} \rangle$ is an independent subspace. \qed

Similarly, we have the following claim about matrices of the form $P^{-1}A^2P$. 

---

23
Lemma 19. If \( \{u_i\}_{i=0}^{\ell/3-1} \cup \{v_i\}_{i=0}^{\ell/3-1} \cup \{w_i\}_{i=0}^{\ell/3-1} \) is a basis of \( \mathbb{F}_q^3 \), then the matrix \( P^{-1}A^2P \) (where \( P \) was defined in Lemma 18) has \( \{u_i\}_{i=0}^{\ell/3-1} \) as an eigenspace for the eigenvalue 1, \( \{v_i\}_{i=0}^{\ell/3-1} \) as an eigenspace for the eigenvalue \( \gamma_1 \), and \( \{w_i\}_{i=0}^{\ell/3-1} \) as an eigenspace for the eigenvalue \( \gamma_2 \). In addition, the subspace \( \{u_i + v_i + w_i\}_{i=0}^{\ell/3-1} \) is an independent subspace.

Proof. According to Lemma 12 we have that

\[
\begin{align*}
u_i \cdot P^{-1}A^2P &= u_i \cdot (P^{-1}AP) \cdot (P^{-1}AP) \\
&= u_i \cdot (P^{-1}AP) = u_i \\
w_i \cdot P^{-1}A^2P &= w_i \cdot (P^{-1}AP) \cdot (P^{-1}AP) \\
&= \gamma_2 w_i \cdot (P^{-1}AP) = \gamma_2^2 w_i = \gamma_1 w_i \\
v_i \cdot P^{-1}A^2P &= v_i \cdot (P^{-1}AP) \cdot (P^{-1}AP) \\
&= \gamma_1 v_i \cdot (P^{-1}AP) = \gamma_2^2 v_i = \gamma_2 v_i
\end{align*}
\]

So see that \( S \triangleq \{u_i + v_i + w_i\}_{i=0}^{\ell/3-1} \) is an independent subspace of \( A^2 \), recall that by Lemma 12 we have that \( S \) is an independent subspace of \( A \), namely, \( S + SA + SA^2 = \mathbb{F}_q^3 \). Since the minimal polynomial of \( A \) is \( x^3 - 1 \), we have that \( A^4 = A \), and hence \( S + SA^2 + SA^4 = S + SA + SA^2 = \mathbb{F}_q^3 \), and therefore \( S \) is an independent subspace of \( A^2 \) as well.

Recall that the matching \( \mathcal{M} \) consists of the edges \( \{\{m_i, m'_i, m''_i\}\}_{i=0}^{\ell/3-1} \). The following invertible matrices are used in the construction.

\[
\begin{align*}
P_M & \triangleq \begin{pmatrix}
N(m_0 + m'_0 + m''_0, & -m'_0, & -m''_0 \\
\vdots & \vdots & \vdots \\
N(m_{\ell/3-1} + m'_{\ell/3-1} + m''_{\ell/3-1}, & -m'_{\ell/3-1}, & -m''_{\ell/3-1})
\end{pmatrix}

P_{M'} & \triangleq \begin{pmatrix}
N(-m''_0, & -m_0, & m_0 + m'_0 + m''_0) \\
\vdots & \vdots & \vdots \\
N(-m''_{\ell/3-1}, & -m_{\ell/3-1} + m'_{\ell/3-1} + m''_{\ell/3-1})
\end{pmatrix}

P_{M''} & \triangleq \begin{pmatrix}
N(-m'_0, & m_0 + m'_0 + m''_0, & -m_0) \\
\vdots & \vdots & \vdots \\
N(-m'_{\ell/3-1}, & m_{\ell/3-1} + m'_{\ell/3-1} + m''_{\ell/3-1}, & -m_{\ell/3-1})
\end{pmatrix}

P_{M^*} & \triangleq \begin{pmatrix}
N(m_0, & m'_0, & m''_0) \\
\vdots & \vdots & \vdots \\
N(m_{\ell/3-1} + m'_{\ell/3-1} + m''_{\ell/3-1})
\end{pmatrix}
\end{align*}
\]

Construction 1. For a matching \( \mathcal{M} = (M, M', M'') \) and any distinct nonzero field elements \( \lambda_M, \lambda_{M'}, \lambda_{M''}, \) and \( \lambda_{M^*} \), let

\[
\begin{align*}
A_M & \triangleq \lambda_M \cdot P_M^{-1}AP_M, & S_M & \triangleq \langle M \rangle = \{m_i\}_{i=0}^{\ell/3-1} \\
A_{M'} & \triangleq \lambda_{M'} \cdot P_{M'}^{-1}AP_{M'}, & S_{M'} & \triangleq \langle M' \rangle = \{m'_i\}_{i=0}^{\ell/3-1} \\
A_{M''} & \triangleq \lambda_{M''} \cdot P_{M''}^{-1}AP_{M''}, & S_{M''} & \triangleq \langle M'' \rangle = \{m''_i\}_{i=0}^{\ell/3-1} \\
A_{M^*} & \triangleq \lambda_{M^*} \cdot P_{M^*}^{-1}AP_{M^*}, & S_{M^*} & \triangleq \langle m_i + m'_i + m''_i \rangle_{i=0}^{\ell/3-1}.
\end{align*}
\]
In the following we show that in a large enough field, there exists a choice of field elements \( \lambda_M, \lambda_{M'}, \lambda_{M''}, \lambda_M \) such that Construction \( \Pi \) satisfies the subspace property, and this choice may be done efficiently. For convenience, we assume that \( \lambda_{M'} = \lambda_M \cdot h, \lambda_{M''} = \lambda_M \cdot h^2, \) and \( \lambda_M = \lambda_M \cdot h^3 \) for some \( h \in \mathbb{F}_q^* \). A suitable value of \( h \) and \( \lambda_M \) will be chosen at the end of the proof of the following theorem.

**Theorem 4.** If \( q \) is large enough (yet linear in \( m \)), then there exists a choice of values \( \lambda_M, \lambda_{M'}, \lambda_{M''}, \lambda_M \) such that Construction \( \Pi \) satisfies the subspace condition.

**Proof.** By Lemma \( \Delta \) we have the following table.

| \( A_M, \lambda = \lambda_M \) | Eigenspace for \( \lambda \) | Eigenspace for \( \lambda \gamma_1 \) | Eigenspace for \( \lambda \gamma_2 \) | Independent subspace |
|---|---|---|---|---|
| \( A_M, \lambda = \lambda_M \) | \( S_M \) | \( S_M \) | \( S_M \) | \( S_M \) |
| \( A_{M'}, \lambda = \lambda_{M'} \) | \( S_{M'} \) | \( S_M \) | \( S_{M'} \) | \( S_M \) |
| \( A_{M''}, \lambda = \lambda_{M''} \) | \( S_{M''} \) | \( S_M \) | \( S_M \) | \( S_{M''} \) |
| \( A_{M''}, \lambda = \lambda_{M''} \) | \( S_M \) | \( S_{M''} \) | \( S_{M'} \) | \( S_{M''} \) |

Table 1: Eigenspaces of \( A_M, A_{M'}, A_{M''}, \) and \( A_{M''} \). and hence, the independence and the invariance properties hold.

To show the nonsingular property, assume for now that \( h \) is chosen such that every distinct \( \lambda_1, \lambda_2 \) in \( \{ \lambda_M, \lambda_{M'}, \lambda_{M''}, \lambda_M \} \) satisfy \( \lambda_1^6 \neq \lambda_2^6 \). A specific choice of \( h \) which satisfies this condition, as well as additional conditions that will emerge in the sequel, will be shown at the end of this proof.

We first show that the difference between any two matrices is of full rank. To show that \( A_M - A_{M'} \) is of full rank, notice that

\[
\begin{align*}
m_i''(A_M - A_{M'}) &= (\lambda_M \gamma_2 - \lambda_{M'}) m_i'' \\
(m_i + m_i' + m_i'')(A_M - A_{M'}) &= (\lambda_M - \lambda_{M'} \gamma_2) (m_i + m_i' + m_i'') \\
m_i(A_M - A_{M'}) &= \lambda_M (m_i + (1 - \gamma_1)m_i' + (1 - \gamma_2)m_i'') - \lambda_M \gamma_1 m_i \\
&= (\lambda_M - \lambda_{M'} \gamma_1) m_i + \lambda_M (1 - \gamma_1)m_i' + \lambda_M (1 - \gamma_2)m_i'' \\
&= \lambda_M (m_i + m_i' + m_i'') - \lambda_M \gamma_1 m_i' - \lambda_{M'} \gamma_2 m_i'' - \lambda_M \gamma_1 m_i'. \quad (28)
\end{align*}
\]

Since \( \lambda_M^6 \neq \lambda_{M'}^6 \) implies that \( \lambda_M \gamma_2 \neq \lambda_{M'} \gamma_2 \) and \( \lambda_M \neq \lambda_{M'} \gamma_2 \), it follows that \( m_i'', m_i + m_i' + m_i'' \in \text{Im}(A_M - A_{M'}) \). Therefore, since the image of a linear transformation is a subspace, it follows from (28) that \( \lambda_M \gamma_1 m_i' + \lambda_{M'} \gamma_1 m_i \in \text{Im}(A_M - A_{M'}) \). To show that \( m_i, m_i', m_i'' \in \text{Im}(A_M - A_{M'}) \) it suffices to show that \( \lambda_M \gamma_1 \neq \lambda_{M'} \gamma_1 \), which also follows from \( \lambda_M^6 \neq \lambda_{M'}^6 \). The rest of the cases are similar, and are given in Appendix \( A \).

To show that the difference between any two squares of matrices is of full rank, notice that by Lemma \( \Delta \) we have the following table.

To show that \( A_M^2 - A_{M'}^2 \) is of full rank, notice that

\[
\begin{align*}
m_i''(A_M^2 - A_{M'}^2) &= (\lambda_M^2 \gamma_1 - \lambda_{M'}^2) m_i'' \\
(m_i + m_i' + m_i'')(A_M^2 - A_{M'}^2) &= (\lambda_M^2 - \lambda_{M'}^2 \gamma_1) (m_i + m_i' + m_i'') \\
m_i(A_M^2 - A_{M'}^2) &= \lambda_M^2 (m_i + (1 - \gamma_2)m_i' + (1 - \gamma_1)m_i'') - \lambda_{M'}^2 \gamma_2 m_i \\
&= \lambda_M^2 (m_i + m_i' + m_i'') - \lambda_M^2 \gamma_1 m_i' - \lambda_{M'}^2 \gamma_2 m_i'' - \lambda_M^2 \gamma_1 m_i. \quad (29)
\end{align*}
\]
Since $\lambda_6^M \neq \lambda_6^{M'}$ implies that $\lambda_2^M \gamma_1 \neq \lambda_2^{M'} \gamma_1$, and $\lambda_2^M \neq \lambda_2^{M'} \gamma_2$, it follows that $m''_i, m_i + m'_i + m''_i \in \text{Im}(A^2_M - A^2_{M'})$. Therefore, \[29\] implies that $\lambda_2^M \gamma_2 m'_i + \lambda_2^{M'} \gamma_2 m_i \in \text{Im}(A^2_M - A^2_{M'})$. Hence, to have that $m_i, m'_i, m''_i \in \text{Im}(A^2_M - A^2_{M'})$, it suffices to show that $\lambda_2^M \gamma_2 \neq \lambda_2^{M'} \gamma_2$, which is implies by $\lambda_6^M \neq \lambda_6^{M'}$.

The rest of the cases are similar, and are given in Appendix B.

To show that Condition 3 of the nonsingular property (i.e., that any $3 \times 3$ block submatrix of the non systematic part of the generator matrix is invertible, as mentioned at the beginning of Section 4), we must show that the following matrices are invertible

\[
V(M, M', M'') \triangleq \begin{pmatrix}
I & I & I \\
A_M & A_{M'} & A_{M''} \\
A^2_M & A^2_{M'} & A^2_{M''}
\end{pmatrix}, \quad V(M, M', M^*) \triangleq \begin{pmatrix}
I & I & I \\
A_M & A_{M'} & A_{M^*} \\
A^2_M & A^2_{M'} & A^2_{M^*}
\end{pmatrix},
\]

\[
V(M, M'', M^*) \triangleq \begin{pmatrix}
I & I & I \\
A_M & A_{M''} & A_{M^*} \\
A^2_M & A^2_{M''} & A^2_{M^*}
\end{pmatrix}, \quad V(M', M'', M^*) \triangleq \begin{pmatrix}
I & I & I \\
A_{M'} & A_{M''} & A_{M^*} \\
A^2_{M'} & A^2_{M''} & A^2_{M^*}
\end{pmatrix}.
\]

Using elementary block row operations, we have that $V(M, M', M'')$ is invertible if and only if

\[
\begin{pmatrix}
I & I & I \\
0 & I & (A_{M'} - A_M)^{-1}(A_{M''} - A_M) \\
0 & 0 & (A^2_M - A^2_{M'}) - (A^2_M - A^2_{M''})(A_M - A_{M'})^{-1}(A_M - A_{M''})
\end{pmatrix}
\]

is invertible. Clearly, this matrix is invertible if and only if

\[
L_1 \triangleq (A^2_M - A^2_{M''})(A_M - A_{M''})^{-1} - (A^2_M - A^2_{M'})(A_M - A_{M'})^{-1}
\]

is invertible. Similarly, $V(M, M', M^*)$, $V(M, M'', M^*)$, and $V(M', M'', M^*)$ are invertible if and only if

\[
L_2 \triangleq (A^2_M - A^2_{M'})(A_M - A_{M'})^{-1} - (A^2_M - A^2_{M''})(A_M - A_{M'})^{-1}
\]

\[
L_3 \triangleq (A^2_M - A^2_{M'})(A_M - A_{M'})^{-1} - (A^2_M - A^2_{M''})(A_M - A_{M''})^{-1}
\]

\[
L_4 \triangleq (A^2_{M'} - A^2_{M''})(A_{M'} - A_{M''})^{-1} - (A^2_{M'} - A^2_{M''})(A_{M'} - A_{M''})^{-1}
\]

are invertible. To show that $L_1, L_2, L_3,$ and $L_4$ are invertible, we show that the image of each of them
contains \( m_i, m'_i, m''_i \) for all \( i \in \{0, \ldots, \ell/3 - 1\} \). Notice that
\[
(m_i + m'_i + m''_i)L_1 = (m_i + m'_i + m''_i)(A_M^2 - A_{M'})^1 \cdot (A_M - A_{M''})^{-1} - \]
\[
(m_i + m'_i + m''_i)(A_M^2 - A_{M'})^1 \cdot (A_M - A_{M''})^{-1} = \]
\[
(A_M^2 - A_{M'}^2)(A_M - A_{M''})^{-1} - \]
\[
(\lambda_M^2 - \lambda_{M''}^2)(m_i + m'_i + m''_i)(A_M - A_{M''})^{-1} - \]
\[
(\lambda_M^2 - \lambda_{M'}^2)(m_i + m'_i + m''_i)(A_M - A_{M'})^{-1} \]
\[
m_i L_1 = m_i(A_M - A_{M'})^{-1} - m_i(A_M - A_{M''})^{-1} - \]
\[
(\lambda_M^2(m_i + m'_i + m''_i) - \lambda_M^2 \gamma_2 m'_i - \lambda_M^2 \gamma_1 m''_i) (A_M - A_{M''})^{-1} - \]
\[
(\lambda_M^2(m_i + m'_i + m''_i) - \lambda_M^2 \gamma_2 m'_i - \lambda_M^2 \gamma_1 m''_i) (A_M - A_{M'})^{-1} \]
\[
m'_i L_1 = m'_i(A_M - A_{M''})^{-1} - m'_i(A_M - A_{M'})^{-1} - \]
\[
(\lambda_M^2 \gamma_2 - \lambda_M^2)(m'_i - m''_i)(A_M - A_{M''})^{-1} - \]
\[
(\lambda_M^2 \gamma_2 - \lambda_M^2)(m'_i - m''_i)(A_M - A_{M'})^{-1} \]
\[
(m_i + m'_i + m''_i)L_1 = D_1 \cdot \begin{pmatrix} m_i \\ m'_i \\ m''_i \end{pmatrix}, \]
\[
(31) \]
for some \( 3 \times 3 \) matrix \( D_1 \) whose entries are functions of \( \lambda_M \) and \( h \). To show that \( m_i, m'_i, m''_i \in \text{Im}(L_1) \) we must show that \( \det D_1 \neq 0 \). This requirement will result in conditions on \( h \) and \( \lambda_M \). It will be shown in the sequel that if \( q \) is large enough (yet linear in \( m \), then these conditions may be satisfied, and proper values of \( \lambda_M \) and \( h \) may easily be found.

We now show that each entry in \( D_1 \) is a linear polynomial in \( \lambda_M \) with coefficients in \( \mathbb{F}_q(h) \) (the set of rational functions in the variable \( h \)). Notice that by Construction 1
\[
(A_M^2 - A_{M'}^2)(A_M - A_{M''})^{-1} = \lambda_M \left( P_M^{-1}A_M^2P_M - h^2P_M^{-1}A_{M'}A_{M''} \right) \left( P_M^{-1}A_M - hP_M^{-1}A_{M'}P_{M''} \right)^{-1} \]
\[
(A_M^2 - A_{M''}^2)(A_M - A_{M'})^{-1} = \lambda_M \left( P_M^{-1}A_M^2P_M - h^4P_M^{-1}A_{M''}A_{M'} \right) \left( P_M^{-1}A_M - h^2P_M^{-1}A_{M'}P_{M''} \right)^{-1}. \]

Hence, (30) may be rewritten as
\[
\begin{pmatrix} m_i + m'_i + m''_i \\ m_i \\ m'_i \\ m''_i \end{pmatrix} L_1 = \lambda_M D'_1 \cdot \begin{pmatrix} m_i \\ m'_i \\ m''_i \end{pmatrix}, \]
where \( D'_1 \) is a matrix depending only on \( \gamma_1, \gamma_2, \) and \( h \), which may easily be computed from [28], [33] and Table 2. Since \( \lambda_M D'_1 = D_1 \), it follows that \( \det D_1 \) is a homogeneous polynomial in \( \lambda_M \) of degree at most three, with coefficients in \( \mathbb{F}_q(h) \). Therefore, there exists polynomials \( P_{1,1}, P_{1,2}, P_{1,3}, P_{1,4} \) over \( \mathbb{F}_q \) such that
\[
\Delta_1(\lambda_M) \triangleq \det D_1 = \frac{P_{1,3}(h)\lambda_M^3 + P_{1,2}(h)\lambda_M^2 + P_{1,1}(h)\lambda_M}{P_{1,4}(h)}. \]
By symmetry, similar arguments show that $L_2$, $L_3$, and $L_4$ are invertible if and only if there exist matrices $D_2, D_3,$ and $D_4,$ defined as in (31). It can similarly be shown that

\[
\Delta_2(\lambda_M) \triangleq \det D_2 = \frac{P_{2,2}(h)\lambda_M^3 + P_{2,2}(h)\lambda_M^2 + P_{2,1}(h)\lambda_M}{P_{2,4}(h)}
\]

\[
\Delta_3(\lambda_M) \triangleq \det D_3 = \frac{P_{3,3}(h)\lambda_M^3 + P_{3,2}(h)\lambda_M^2 + P_{3,1}(h)\lambda_M}{P_{3,4}(h)}
\]

\[
\Delta_4(\lambda_M) \triangleq \det D_4 = \frac{P_{4,3}(h)\lambda_M^3 + P_{4,2}(h)\lambda_M^2 + P_{4,1}(h)\lambda_M}{P_{4,4}(h)}
\]

for certain polynomials $P_{2,1}, \ldots, P_{4,4}$. Thus, to show that $L_1, \ldots, L_4$ are invertible, it suffices to show that there exists $h$ and $\lambda_M$ such that all determinants are well-defined and nonzero. To this end, consider the polynomial

\[
Q(h) \triangleq (h^6 - 1)(h^{12} - 1)(h^{18} - 1) \cdot P_{4,4}(h) \cdot \prod_{i=1}^{4} (P_{i,1}(h) + P_{i,2}(h) + P_{i,3}(h)).
\]

According to the fundamental theorem of algebra, if $q > \deg Q + 1$, then $Q$ is not the zero polynomial. Hence, by assuming that $q > \deg Q + 1$ and choosing an arbitrary $h \in \mathbb{F}_q$ such that $Q(h) \neq 0$, we have that $\Delta_1, \Delta_2, \Delta_3,$ and $\Delta_4$ are well-defined, nonzero polynomials of degree at most three in the variable $\lambda_M$.

After choosing a proper $h$, consider the polynomial $W(\lambda_M) \triangleq \prod_{i=1}^{4} \Delta_i(\lambda_M)$. Once again, according to the fundamental theorem of algebra, and since $q > \deg Q + 1 \geq \deg W$, we have that $W$ is not the zero polynomial. Hence, there exists $\lambda_M \in \mathbb{F}_q$ such that $D_1, \ldots, D_4$ are invertible, and such $\lambda_M$ may easily be found by factoring $W$ over $\mathbb{F}_q$. Note that by choosing this $h$, for all $\lambda_i, \lambda_j \in \{\lambda_M, \lambda_{M'}, \lambda_{M''}, \lambda_{M'''}\}$ we have that $\lambda_i^6 \neq \lambda_j^6$, since $\lambda_{M'} = \lambda_M \cdot h, \lambda_{M''} = \lambda_M \cdot h^2, \lambda_{M'''} = \lambda_M \cdot h^3$, and since $Q(h) \neq 0$ ensures that $h^6 \neq 1, h^{12} \neq 1,$ and $h^{18} \neq 1$. Notice also that the required size of $q$ is independent of $m$, since the exact polynomial $Q$ results from any edge in the matching, and $\deg Q$ is independent of $m$.

This theorem showed that a single matching provides an $(A, S)$-set of size four, satisfying the subspace property, over a field of constant size. In the next subsection it will be shown that by taking $q$ to be at least linear in $m$, $(A, S)$-sets from different matchings, that satisfy the pairing condition in pairs, may be united without compromising the subspace property.

### 5.2 A Code from Two Matchings

In this subsection we show that $(A, S)$-sets that were constructed from different matchings may be united, as long as the pairing condition holds. The following lemmas, whose proofs will appear at the full version of this paper, are required.

**Lemma 20.** If $A$ and $B$ are $\ell \times \ell$ simultaneously diagonalizable matrices with no mutual eigenvalues, then $A - B$ is invertible.

In the remaining part of this subsection, let $X = (X, X', X''), Y = (Y, Y', Y'')$ be two matchings which satisfy the pairing condition, and let the resulting $(A, S)$-sets be as in Construction [1]

\[
C_X \triangleq \{(A_X, S_X), (A_{X'}, S_{X'}), (A_{X''}, S_{X''}), (A_{X'}, S_{X'})\}
\]

\[
C_Y \triangleq \{(A_Y, S_Y), (A_{Y'}, S_{Y'}), (A_{Y''}, S_{Y''}), (A_{Y'}, S_{Y'})\}.
\]

The required values of $\lambda_X, \lambda_Y$ which are involved in the definition of these $(A, S)$-sets will be discussed in the sequel.
Lemma 21. If \( C \in \{ A_X, A_{X'}, A_{X''}, A_{X'''} \} \) and \( D \in \{ A_Y, A_{Y'}, A_{Y''}, A_{Y'''} \} \), then \( C \) and \( D \) are simultaneously diagonalizable. Furthermore, \( C^2 \) and \( D^2 \) are simultaneously diagonalizable.

Recall that the definition of an \((A, S)\)-set from a single matching involved the choice of two field constants \( \lambda_M \) and \( h \). In what follows we use the same \( h \) for all matchings, and choose proper distinct values for the constants which correspond to \( \lambda_M \). The next lemma is required for the construction.

Lemma 22. If \( \lambda_X \) and \( \lambda_Y \) are two nonzero field elements such that \( \lambda_Y^6 \notin \{ \lambda_X^6, \lambda_X^6 h^{\pm 6}, \lambda_X^6 h^{\pm 12}, \lambda_X^6 h^{\pm 18} \} \) and

\[
\begin{align*}
\lambda_1 &\in \{ \lambda_X, \lambda_{X'}, \lambda_{X''}, \lambda_{X'''}, \lambda_{X'} \} = \{ \lambda_X, \lambda_X h, \lambda_X h^2, \lambda_X h^3 \}, \\
\lambda_2 &\in \{ \lambda_Y, \lambda_{Y'}, \lambda_{Y''}, \lambda_{Y'''}, \lambda_{Y'} \} = \{ \lambda_Y, \lambda_Y h, \lambda_Y h^2, \lambda_Y h^3 \},
\end{align*}
\]

then

\[
\begin{align*}
\{ \lambda_1, \lambda_1 \gamma_1, \lambda_1 \gamma_2 \} \cap \{ \lambda_2, \lambda_2 \gamma_1, \lambda_2 \gamma_2 \} &= \emptyset, \\
\{ \lambda_2^2, \lambda_2^2 \gamma_2, \lambda_1^2 \gamma_1 \} \cap \{ \lambda_2^2, \lambda_2^2 \gamma_2, \lambda_2^2 \gamma_1 \} &= \emptyset.
\end{align*}
\]

Lemma 20 and Lemma 22 enable an easy choice of field elements, which induces distinct eigenvalues for the simultaneously diagonalizable matrices which correspond to distinct matchings. These distinct eigenvalues, together with the simultaneous diagonalizability, will greatly assist the proof of the following lemma, from which the construction will follow.

Lemma 23. If the field constants \( \lambda_X, \lambda_Y \) are chosen such that

\( \lambda_Y^6 \notin \{ \lambda_X^6, \lambda_X^6 h^{\pm 6}, \lambda_X^6 h^{\pm 12}, \lambda_X^6 h^{\pm 18} \} \),

then \( C_X \cup C_Y \) satisfies the subspace condition.

Proof. Since each of \( C_X \) and \( C_Y \) satisfies the subspace condition separately, we are left to show the parts of the nonsingular property and the invariance property which involve matrices and subspaces from different matchings.

To prove the invariance property, for any \( C \in \{ A_X, A_{X'}, A_{X''}, A_{X'''} \} \) and any \( T \in \{ S_Y, S_{Y'}, S_{Y''}, S_{Y'''} \} \) we must show that \( TC = T \). Let \( S_1, S_2, S_3 \in \{ S_X, S_{X'}, S_{X''}, S_{X'''} \} \) be the eigenspaces of \( C \). It follows from Lemma 4 that \( \text{dim}(S_i \cap T) = \ell/9 \) for all \( i \in [3] \). Therefore, since \( S_1 + S_2 + S_3 = \mathbb{F}_6^\ell \) by Lemma 12 it follows that there exists a basis \( t_1, \ldots, t_{\ell/3} \) of \( T \) in which all vectors are eigenvectors of \( C \). Hence, for all \( i \in [\ell/3] \) we have that \( t_i C \in T \), and thus \( TC = T \). The inverse case, where \( C \in \{ A_Y, A_{Y'}, A_{Y''}, A_{Y'''} \} \) and \( T \in \{ S_X, S_{X'}, S_{X''}, S_{X'''} \} \), is symmetric.

To prove the nonsingular property, let \( C \in \{ A_X, A_{X'}, A_{X''}, A_{X'''} \} \) and \( D \in \{ A_Y, A_{Y'}, A_{Y''}, A_{Y'''} \} \). According to Construction 1 the eigenvalues of \( C \) are \( \lambda_C, \lambda_C \gamma_1, \) and \( \lambda_C \gamma_2 \) for some

\( \lambda_C \in \{ \lambda_X, \lambda_X h, \lambda_X h^2, \lambda_X h^3 \} \),

and similarly, the eigenvalues of \( D \) are \( \lambda_D, \lambda_D \gamma_1, \) and \( \lambda_D \gamma_2 \) for some

\( \lambda_D \in \{ \lambda_Y, \lambda_Y h, \lambda_Y h^2, \lambda_Y h^3 \} \).

By Lemma 22 and since \( \lambda_Y^6 \notin \{ \lambda_X^6, \lambda_X^6 h^{\pm 6}, \lambda_X^6 h^{\pm 12}, \lambda_X^6 h^{\pm 18} \} \), it follows that

\[
\begin{align*}
\{ \lambda_C, \lambda_C \gamma_1, \lambda_C \gamma_2 \} \cap \{ \lambda_D, \lambda_D \gamma_1, \lambda_D \gamma_2 \} &= \emptyset, \\
\{ \lambda_C^2, \lambda_C^2 \gamma_2, \lambda_C^2 \gamma_1 \} \cap \{ \lambda_D^2, \lambda_D^2 \gamma_2, \lambda_D^2 \gamma_1 \} &= \emptyset.
\end{align*}
\]
that is, \( C \) and \( D \) have no eigenvalue in common, and \( C^2 \) and \( D^2 \) have no eigenvalue in common. Since Lemma 21 implies that \( C \) and \( D \) are simultaneously diagonalizable, and so are \( C^2 \) and \( D^2 \), by Lemma 20 we have that \( C - D \) and \( C^2 - D^2 \) are invertible.

We are left to prove that any \( 3 \times 3 \) block submatrix is invertible. Let \( A_i, A_j, A_k \) be three matrices from \( C_X \cup C_Y \) such that \( A_i \) and \( A_j \) are not from the same matching, and so are \( A_i \) and \( A_k \). Recall that, as in the proof of Theorem 4, the matrix

\[
\begin{pmatrix}
I & I & I \\
A_i & A_j & A_k \\
A_i^2 & A_j^2 & A_k^2
\end{pmatrix}
\]

is invertible if and only if

\[
L \triangleq (A_i^2 - A_k^2)(A_i - A_k)^{-1} - (A_i^2 - A_j^2)(A_i - A_j)^{-1}
\]

is invertible. Notice that by Lemma 21, \( A_i \) and \( A_j \) are simultaneously diagonalizable, and hence they commute. In addition, so are \( A_i \) and \( A_k \). Therefore,

\[
L = (A_i^2 - A_k^2)(A_i - A_k)^{-1} - (A_i^2 - A_j^2)(A_i - A_j)^{-1}
= A_i + A_k - A_i + A_j = A_k - A_j,
\]

and hence \( L \) is invertible.

We conclude in the following theorem, in which \( Q \) and \( W \) are the polynomials mentioned in the proof of Theorem 4.

**Theorem 5.** If \( q > \max\{42m + 13, \deg Q\} \), and \( \{X_i = (X_i, X_i', X_i'')\}_{i=1}^m \) is the set of matchings from Definition 8, then the \((A, S)\)-set \( \cup_{i=1}^m C_{X_i} \) satisfies the subspace condition.

### 6 Concluding Remarks

We have shown constructions of \((A, S)\)-sets which satisfy the subspace condition (Section 2.2). These \((A, S)\)-sets may be used to construct minimum storage MDS array codes for distributed storage systems, which allow a minimum repair bandwidth of a single failure of a systematic node.

The \((A, S)\)-sets in Section 3 and Section 4 allow optimal access repair, while the larger construction of Section 5 is not access-optimal. All constructions are defined over smaller fields comparing to existing constructions.

Proofs omitted from Section 4 will be given in the full version of this paper.

### Acknowledgments

The authors would like to thank Prof. Joachim Rosenthal for many helpful discussions, which contributed to this paper.

### References

[1] G. K. Agarwal, B. Sasidharan, and P. V. Kumar, “An alternative construction of an access-optimal regenerating codes with optimal sub-packetization level,” arXiv:1501.04760v1, 2015.
[2] M. Blaum and R. M. Roth, “On lowest density MDS codes,” *IEEE Transactions on Information Theory*, vol. 45, pp. 46–59, 1999.

[3] Y. Cassuto and J. Bruck, “Cyclic low-density MDS array codes,” *In Proc. IEEE International Symposium on Information Theory (ISIT)*, pp. 2794–2798, 2006.

[4] A. G. Dimakis, P. Godfrey, M. Wainwright, and K. Ramachandran, “Network coding for distributed storage system,” *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4539–4551, Sep. 2010.

[5] S. Goparaju, I. Tamo, and R. Calderbank, “An improved sub-packetization bound form minimum storage regenerating codes,” *IEEE Transactions on Information Theory*, vol. 60, no. 5, pp. 2770–2779, 2014.

[6] S. Goparaju, R. Calderbank, “A new sub-packetization bound for minimum storage regenerating codes,” *In Proc. International Symposium on Information Theory (ISIT)*, pp. 1616–1620, 2013.

[7] J. Li, X. Tang, U. Parampalli, “A framework of constructions of minimal storage regenerating codes with the optimal access/update property,” *IEEE Transactions on Information Theory*, vol. 61, no. 4, pp.1920–1932, 2015.

[8] R. Lidl, and H. Niederreiter, “Finite Fields,” *Encyclopedia of Mathematics and Its Applications*, Cambridge University Press, vol. 20, 1997.

[9] S. MacLane and G. Birkhoff, *Algebra*, Chelsea Publishing Company, New York, 1988.

[10] D.S. Papailiopoulos, A.G. Dimakis, and V.R. Cadambe, “Repair Optimal Erasure Codes Through Hadamard Designs,” *IEEE Transactions on Information Theory*, vol. 59, no. 5, pp. 3021–3037, 2013.

[11] K. V. Rashmi, N. B. Shah, and P. V. Kumar, “Optimal exact-regenerating codes for distributed storage at the MSR and MBR point via a product-matrix construction,” *IEEE Transactions on Information Theory*, vol. 57, no. 8 pp. 5227–5239, 2011.

[12] K. V. Rashmi, N. B. Shah, P. V. Kumar, and K. Ramchandran, “Distributed storage codes with repair-by-transfer and nonachievabilityof interior points on the storage-bandwidth tradeoff,” *IEEE Transactions on Information Theory*, vol. 58, pp. 1837–1852, 2012.

[13] K. V. Rashmi, N. B. Shah, P. V. Kumar, and K. Ramchandran, “Explicit construction of optimal exact regenerating codes for distributed storage,” *in Proc. 47th Annual Allerton Conf. on Communication, Control, and Computing (Allerton)*, pp. 1243–1249, 2009.

[14] C. Suh and K. Ramchandran, “Exact-repair MDS codes for distributed storage using interference alignment,” *In Proc. IEEE International Symposium on Information Theory (ISIT)*, pp. 161–165, 2010.

[15] I. Tamo, Z. Wang, and J. Bruck, “Long MDS codes for optimal repair bandwidth,” *In Proc. IEEE International Symposium on Information Theory (ISIT)*, pp. 1182–1186, 2012.

[16] I. Tamo, Z. Wang, and J. Bruck, “Zigzag codes: MDS array codes with optimal rebuilding,” *IEEE Transactions on Information Theory*, vol. 59, no. 3, pp. 1597–1616, 2013.

[17] I. Tamo, Z. Wang, and J. Bruck, “Access versus bandwidth in codes for storage”, *IEEE Transactions on Information Theory*, vol. 60, no. 4, pp. 2028–2037, 2014.
Appendix A

To show that $A_M - A_{M^*}$ is of full rank, notice that

\begin{align*}
m'_i(A_M - A_{M^*}) &= (\lambda Mr_1 - \lambda r_2)m'_i \\
m''_i(A_M - A_{M^*}) &= (\lambda Mr_2 - \lambda r_1)m''_i \\
m_i(A_M - A_{M^*}) &= \lambda M (m_i + (1 - r_1)m'_i + (1 - r_2)m''_i) - \lambda M m_i \\
&= (\lambda M - \lambda M^*)m_i + \lambda M (1 - r_1)m'_i + \lambda M (1 - r_2)m''_i \\
\end{align*}

(32)

Since $\lambda Mr_1 \neq \lambda r_2$ and $\lambda Mr_2 \neq \lambda r_1$, we have that $m'_i, m''_i \in \text{Im}(A_M - A_{M^*})$. Therefore, it follows from (32) that $m_i \in \text{Im}(A_M - A_{M^*})$, since $\lambda M \neq \lambda M^*$.

To show that $A_M - A_{M''}$ is of full rank, notice that

\begin{align*}
m'_i(A_M - A_{M''}) &= (\lambda M r_1 - \lambda M r_2)m'_i \\
(m_i + m'_i + m''_i)(A_M - A_{M''}) &= (\lambda M - \lambda M r_1)(m_i + m'_i + m''_i) \\
m_i(A_M - A_{M''}) &= \lambda M (m_i + (1 - r_1)m'_i + (1 - r_2)m''_i) - \lambda M r_2 m_i \\
&= \lambda M (m_i + m'_i + m''_i) - \lambda M r_1 m_i - \lambda M r_2 m''_1 - \lambda M r_2 m_i \\
\end{align*}

(33)

Since $\lambda M r_1 \neq \lambda M$ and $\lambda M \neq \lambda M r_1$, we have that $m'_i, m_i + m'_i + m''_i \in \text{Im}(A_M - A_{M''})$. Therefore, it follows from (33) that $m_i, m'_i, m''_i \in \text{Im}(A_M - A_{M''})$. To show that $m_i, m'_i, m''_i \in \text{Im}(A_M - A_{M''})$ it suffices to show that $\lambda M r_2 \neq \lambda M r_2$, which also follows from $\lambda M^6 \neq \lambda M^6$.

To show that $A_{M'} - A_{M''}$ is of full rank notice that

\begin{align*}
m_i(A_{M'} - A_{M''}) &= (\lambda M' r_1 - \lambda M' r_2)m_i \\
(m_i + m'_i + m''_i)(A_{M'} - A_{M''}) &= (\lambda M' r_2 - \lambda M' r_1)(m_i + m'_i + m''_i) \\
m'_i(A_{M'} - A_{M''}) &= \lambda M' ((r_2 - r_1)m_i + r_2 m_i + (r_2 - 1)m''_i) - \lambda M' m_i' \\
&= \lambda M' (r_2 - r_1)m_i + (\lambda M' r_2 - \lambda M' r_2)m_i + \lambda M' (r_2 - 1)m''_1 \\
\end{align*}

(34)

Since $\lambda M' r_1 \neq \lambda M' r_2$ and $\lambda M' r_2 \neq \lambda M' r_1$, we have that $m_i, m'_i + m''_i \in \text{Im}(A_{M'} - A_{M''})$. Therefore, it follows from (34) that $m_i, m'_i, m''_i \in \text{Im}(A_{M'} - A_{M''})$. To show that $m_i, m'_i, m''_i \in \text{Im}(A_{M'} - A_{M''})$ it suffices to show that $\lambda M' \neq \lambda M r_1$, which also follows from $\lambda M^6 \neq \lambda M^6$.

To show that $A_{M'} - A_{M^*}$ is of full rank notice that

\begin{align*}
m_i(A_{M'} - A_{M^*}) &= (\lambda M' r_1 - \lambda M^*)m_i \\
m''_i(A_{M'} - A_{M^*}) &= (\lambda M' - \lambda M^*)m''_i \\
m'_i(A_{M'} - A_{M^*}) &= \lambda M' ((r_2 - r_1)m_i + r_2 m_i + (r_2 - 1)m''_i) - \lambda M' r_2 m'_i \\
&= \lambda M' (r_2 - r_1)m_i + (\lambda M' r_2 - \lambda M' r_2)m_i + \lambda M' (r_2 - 1)m''_1 \\
\end{align*}

(35)

Since $\lambda M' r_1 \neq \lambda M^*$ and $\lambda M' \neq \lambda M^* r_1$, we have that $m_i, m''_i \in \text{Im}(A_{M'} - A_{M^*})$. Therefore, it follows from (35) that $m'_i \in \text{Im}(A_{M'} - A_{M^*})$, since $\lambda M' r_2 \neq \lambda M^* r_2$.

To show that $A_{M''} - A_{M^*}$ is of full rank notice that

\begin{align*}
m_i(A_{M''} - A_{M^*}) &= (\lambda M'' r_1 - \lambda M^*)m_i \\
m''_i(A_{M''} - A_{M^*}) &= (\lambda M'' - \lambda M^*)m''_i \\
m'_i(A_{M''} - A_{M^*}) &= \lambda M'' ((r_2 - r_1)m_i + (r_1 - 1)m'_i + r_1 m''_i) - \lambda M'' r_1 m'_i \\
&= \lambda M'' (r_2 - r_1)m_i + (\lambda M'' r_1 - \lambda M^*)m''_1 + (\lambda M'' r_1 - \lambda M^*)m''_1 \\
\end{align*}

(36)

Since $\lambda M'' r_2 \neq \lambda M^*$ and $\lambda M'' \neq \lambda M^* r_2$, we have that $m_i, m'_i \in \text{Im}(A_{M''} - A_{M^*})$. Therefore, it follows from (36) that $m'_i \in \text{Im}(A_{M''} - A_{M^*})$, since $\lambda M' r_1 \neq \lambda M^* r_1$. 

32
Appendix B

To show that $A^2_M - A^2_{M^*}$ is of full rank, notice that

$$
m'_i(A^2_M - A^2_{M^*}) = (\lambda^2_M r_2 - \lambda^2_{M^*} r_1)m'_i
$$

$$
m''_i(A^2_M - A^2_{M^*}) = (\lambda^2_M r_1 - \lambda^2_{M^*} r_2)m''_i
$$

$$
m_i(A^2_M - A^2_{M^*}) = \lambda^2_M (m_i + (1 - r_2)m'_i + (1 - r_1)m''_i) - \lambda^2_{M^*} m_i
$$

$$
= (\lambda^2_M - \lambda^2_{M^*})m_i + \lambda^2_M (1 - r_2)m'_i + \lambda^2_M (1 - r_1)m''_i
$$

(37)

Since $\lambda^2_M r_2 \neq \lambda^2_{M^*} r_1$ and $\lambda^2_M r_1 \neq \lambda^2_{M^*} r_2$, it follows that $m'_i, m''_i \in \text{Im}(A^2_M - A^2_{M^*})$. Therefore, (37) implies that $m_i \in \text{Im}(A^2_M - A^2_{M^*})$, since $\lambda^2_M \neq \lambda^2_{M^*}$.

To show that $A^2_M - A^2_{M^*}$ is of full rank notice that

$$
m'_i(A^2_M - A^2_{M''}) = (\lambda^2_M r_2 - \lambda^2_{M''} r_1)m'_i
$$

$$
(m_i + m'_i + m''_i)(A^2_M - A^2_{M''}) = (\lambda^2_M r_1 - \lambda^2_{M''} r_2)(m_i + m'_i + m''_i)
$$

$$
m_i(A^2_M - A^2_{M''}) = \lambda^2_M (m_i + (1 - r_2)m'_i + (1 - r_1)m''_i) - \lambda^2_{M''} r_1 m_i
$$

$$
= \lambda^2_M (m_i + m'_i + m''_i) - \lambda^2_{M''} r_2 m'_i - \lambda^2_{M''} r_1 m''_i - \lambda^2_{M''} r_1 m_i
$$

(38)

Since $\lambda^2_M r_2 \neq \lambda^2_{M''}$ and $\lambda^2_M \neq \lambda^2_{M''} r_2$, it follows that $m'_i, m_i + m'_i + m''_i \in \text{Im}(A^2_M - A^2_{M''})$. Therefore, (38) implies that $\lambda^2_M r_1 m''_i + \lambda^2_{M''} r_2 m_i \in \text{Im}(A^2_M - A^2_{M''})$. Hence, to have that $m_i, m'_i, m''_i \in \text{Im}(A^2_M - A^2_{M''})$, it suffices to show that $\lambda^2_M r_1 \neq \lambda^2_{M''} r_2$, which is implied by $\lambda^2_M \neq \lambda^2_{M''}$.

To show that $A^2_M - A^2_{M''}$ is of full rank notice that

$$
m_i(A^2_M - A^2_{M''}) = (\lambda^2_M r_2 - \lambda^2_{M''} r_1)m_i
$$

$$
(m_i + m'_i + m''_i)(A^2_M - A^2_{M''}) = (\lambda^2_M r_1 - \lambda^2_{M''} r_2)(m_i + m'_i + m''_i)
$$

$$
m_i(A^2_M - A^2_{M''}) = \lambda^2_M ((r_1 - r_2)m_i + r_1 m'_i + (r_1 - 1)m''_i) - \lambda^2_{M''} m_i
$$

$$
= \lambda^2_M r_1 (m_i + m'_i + m''_i) - \lambda^2_{M''} r_2 m'_i - \lambda^2_{M''} r_1 m''_i - \lambda^2_{M''} r_1 m_i
$$

(39)

Since $\lambda^2_M r_2 \neq \lambda^2_{M''}$ and $\lambda^2_M \neq \lambda^2_{M''} r_2$, it follows that $m'_i, m_i + m'_i + m''_i \in \text{Im}(A^2_M - A^2_{M''})$. Therefore, (39) implies that $\lambda^2_M m''_i + \lambda^2_{M''} r_2 m_i \in \text{Im}(A^2_M - A^2_{M''})$. Hence, to have that $m_i, m'_i, m''_i \in \text{Im}(A^2_M - A^2_{M''})$, it suffices to show that $\lambda^2_M \neq \lambda^2_{M''}$, which is implied by $\lambda^2_M \neq \lambda^2_{M''}$.

To show that $A^2_M - A^2_{M''}$ is of full rank notice that

$$
m_i(A^2_M - A^2_{M''}) = (\lambda^2_M r_2 - \lambda^2_{M''} r_1)m_i
$$

$$
m'_i(A^2_M - A^2_{M''}) = (\lambda^2_M - \lambda^2_{M''} r_2)m'_i
$$

$$
m''_i(A^2_M - A^2_{M''}) = \lambda^2_M ((r_1 - r_2)m_i + r_1 m'_i + (r_1 - 1)m''_i) - \lambda^2_{M''} m_i
$$

$$
= \lambda^2_M (r_1 - r_2)m_i + (\lambda^2_M r_1 - \lambda^2_{M''} r_1)m'_i + \lambda^2_M (r_1 - 1)m''_i
$$

(40)

Since $\lambda^2_M r_2 \neq \lambda^2_{M''} r_1$ and $\lambda^2_M \neq \lambda^2_{M''} r_2$, it follows that $m_i, m''_i \in \text{Im}(A^2_M - A^2_{M''})$. Therefore, (40) implies that $m'_i \in \text{Im}(A^2_M - A^2_{M''})$, since $\lambda^2_M r_1 \neq \lambda^2_{M''} r_1$.

To show that $A^2_{M''} - A^2_{M^*}$ is of full rank notice that

$$
m_i(A^2_{M''} - A^2_{M^*}) = (\lambda^2_{M''} r_1 - \lambda^2_{M^*} r_1)m_i
$$

$$
m'_i(A^2_{M''} - A^2_{M^*}) = (\lambda^2_{M''} - \lambda^2_{M^*} r_1)m'_i
$$

$$
m''_i(A^2_{M''} - A^2_{M^*}) = \lambda^2_{M''} ((r_2 - r_1)m_i + (r_1 - 1)m'_i + (r_2 - 1)m''_i) - \lambda^2_{M^*} r_2 m'_i
$$

$$
= \lambda^2_{M''} (r_2 - r_1)m_i + (\lambda^2_{M''} r_2 - \lambda^2_{M^*} r_2)m'_i + \lambda^2_{M''} (r_2 - 1)m''_i
$$

(41)

Since $\lambda^2_{M^*} r_1 \neq \lambda^2_{M''}$ and $\lambda^2_{M''} \neq \lambda^2_{M^*} r_1$, it follows that $m_i, m'_i \in \text{Im}(A^2_{M''} - A^2_{M^*})$. Therefore, (41) implies that $m''_i \in \text{Im}(A^2_{M''} - A^2_{M^*})$, since $\lambda^2_{M''} r_2 \neq \lambda^2_{M^*} r_2$.