Codes for Updating Linear Functions over Small Fields

Suman Ghosh and Lakshmi Natarajan

Abstract

We consider a point-to-point communication scenario where the receiver intends to maintain a specific linear function of a message vector over a finite field. When the value of the message vector changes, which is modelled as a sparse update, the transmitter broadcasts a coded version of the modified message while the receiver uses this codeword and the current value of the linear function to update its contents. It is assumed that the transmitter has access to only the modified message and is unaware of the exact difference vector between the original and modified messages. Under the assumption that the difference vector is sparse and that its Hamming weight is at the most a known constant, the objective is to design a linear code with as small a codelength as possible that allows successful update of the linear function at the receiver. This problem is motivated by applications to distributed data storage systems. Recently, Prakash and Médard derived a lower bound on the codelength, which is independent of the size of the underlying finite field, and provided constructions that achieve this bound if the size of the finite field is sufficiently large. However, this requirement on the field size can be prohibitive for even moderate values of the system parameters. In this paper, we provide a field-size aware analysis of the function update problem, including a tighter lower bound on the codelength, and design codes that trade-off the codelength for a smaller field size requirement. We also show that the problem of designing codes for updating linear functions is related to functional index coding or generalized index coding. We first characterize the family of function update problems where linear coding can provide reduction in codelength compared to a naive transmission scheme. We then provide field-size dependent bounds on the optimal codelength, and construct coding schemes based on error correcting codes and subspace codes when the receiver maintains linear functions of striped message vector. These codes provide a trade-off between the codelength and the size of the operating finite field, and whenever the achieved codelengths equal those reported by Prakash and Médard the requirements on the size of the finite field are matched as well. Finally, for any given function update problem, we construct an equivalent functional index coding or generalized index coding problem such that any linear coding scheme is valid for the function update problem if and only if it is valid for the constructed functional index coding problem.

I. Introduction

We consider a point-to-point communication scenario as shown in Fig. 1 where the receiver maintains a linear function $\mathbf{Ax}$ of a message vector $\mathbf{x}$. The message $\mathbf{x}$ is an n-length column vector over a finite field $\mathbb{F}_q$, where q is any prime power, and $\mathbf{A}$ is an $m \times n$ matrix over $\mathbb{F}_q$ with $m \leq n$ and $\text{rank}(\mathbf{A}) = m$. Suppose the value of the message vector is updated to $\mathbf{x} + \mathbf{e}$, where $\mathbf{e}$ represents a sparse update to the message, i.e., we assume that $\text{wt}(\mathbf{e}) \leq \epsilon$ where wt denotes the Hamming weight of a vector and ϵ is a known constant. In other words at the most ϵ entries of the original message $\mathbf{x}$ are updated to new values. We assume that the transmitter has access to the updated message $\mathbf{x} + \mathbf{e}$, but is unaware of the original message $\mathbf{x}$ or the sparse update $\mathbf{e}$. Note that the message update is modelled here as substitutions only and not as insertions or deletions. The objective is to design a linear encoder that uses an $l \times n$ matrix $\mathbf{H}$ to generate the codeword $\mathbf{c} = \mathbf{H}(\mathbf{x} + \mathbf{e})$, with as small a codelength l as possible, such that the receiver can decode $\mathbf{A}(\mathbf{x} + \mathbf{e})$ using the transmitted codeword $\mathbf{c}$ and the older version of its content $\mathbf{Ax}$.

The problem is motivated by distributed storage systems (DSS) where information is stored in linearly coded form across a number of nodes to provide resilience against storage node failures [1]. In the scenario where multiple users can simultaneously edit a single file stored in a DSS, it is possible that a user who wishes to apply his update $\mathbf{x} + \mathbf{e}$ is unaware of the current version of the message $\mathbf{x}$ stored in the DSS,

The authors are with the Department of Electrical Engineering, Indian Institute of Technology Hyderabad, Sangareddy 502 285, India (email: {ee16resch11006, lakshminatarajan}@iith.ac.in).

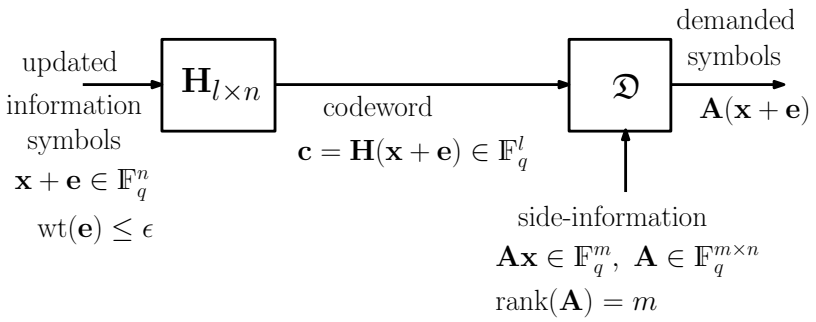

Figure 1. System model for the point-point function update problem.

for instance when another user has recently edited this file. Letting the user first learn the version $\mathbf{x}$ stored in the DSS, and then apply his update will incur additional communication cost. As an alternative, if it is known that the update vector $\mathbf{e}$ is sparse, it is possible to design schemes that do not require the knowledge of the value of $\mathbf{e}$ at the transmitter [1]–[3].

The function update problem was considered in [2], [3] for DSS's for updating one of the storage nodes with the help of the other nodes in the system. Note that each node in a DSS stores a linear function of the message. A node can become *stale* in such systems, for instance if the node goes offline while the message and the corresponding linear functions stored in the other nodes undergo an update. Once it is back online, the stale node connects to the other nodes in the distributed storage system to update its own linear function, and the stale data already stored in this node acts as side information. The authors of [2], [3] design both the code for distributed storage and the code for function update to minimize the amount of data downloaded by the stale node to update its contents. This is unlike the problem statement considered in [1] as well as this paper, where it is assumed that an arbitrary matrix $\mathbf{A}$ is given and a code for updating the function $\mathbf{A}\mathbf{x}$ is to be designed.

The authors in [1] also consider a broadcast scenario where a codeword is broadcast to multiple nodes in order to update the (different) linear functions stored in each of the nodes. Problems related to updating linear functions have been considered in [4]–[6]. In [4], codes for updating linear functions are used in cache-aided networks to reduce the cost of multicasting a sequence of correlated data frames. The problem of efficiently storing multiple versions of a file in a DSS while ensuring a property called *consistency* is considered in [5], [6].

In the study of the point-to-point function update problem given in [1]–[3] the authors derive the following field-size independent lower bound on the codelength

$$l \geq \min(m, 2\epsilon).$$

Note that, if $m \leq 2\epsilon$, the lower bound on the codelength $l \geq m$ can be trivially achieved by transmitting $\mathbf{A}(\mathbf{x}+\mathbf{e})$. Hence, we will always assume that $m > 2\epsilon$. The results in [1] show that codelength $l = 2\epsilon$ is achievable using maximally recoverable subcodes of $\mathscr{C}_A$, the subspace spanned by the rows of $\mathbf{A}$, which are guaranteed to exist if the field size $q \geq 2\epsilon n^{2\epsilon}$. Note that this requirement imposed on the field size can be large even for moderate values of ϵ and n. The authors of [1] also consider the special case where the matrix $\mathbf{A}$ is *striped*, i.e.,

$$\mathbf{A} = \mathbf{I}_a \otimes \mathbf{C} = \begin{bmatrix} \mathbf{C} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{C} & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{C} \end{bmatrix}$$

where $\mathbf{I}_a$ is the $a \times a$ identity matrix, $\mathbf{C} \in \mathbb{F}_q^{t\times K}$ and $\otimes$ denotes the Kronecker product. Note that $m = at$ and $n = aK$. This structure frequently arises in distributed storage systems where the n-length data $\mathbf{x}$ is partitioned into a subvectors $\mathbf{x}_1, \dots, \mathbf{x}_a$, each of length K, each subvector is encoded independently by

multiplying with $\mathbf{C}$, and all the encoded vectors are stored in a single storage node, see Examples 1–3 of [1]. In [1, Section IV], a code is constructed for the case $t = 1$ that achieves the codelength $l = 2\epsilon$ using an $[m, m - 2\epsilon]$ MDS code, which is guaranteed to exist if the field size $q \geq m$. In Remark 4 of [1] the authors consider a modified system model for the function update problem which we show in Section V-A3 of this paper to be equivalent to the case where $\mathbf{A}$ is striped with the number of stripes $a = t$. Construction 1 and Remark 4 of [1] provide a code construction for this modified system model, and hence for the case $a = t$, that achieves codelength of $2t\epsilon$ over any field.

In this paper we provide a field-size aware characterization of the point-to-point function update problem. In particular, we provide bounds on the achievable codelength that take into account the effect of the field size and we provide constructions that trade-off the codelength for a smaller field size requirement. This is unlike the point-to-point results in [1] which provide constructions only for the case $l = 2\epsilon$ but assume that the field size q is sufficiently large. To the best of our knowledge, no prior analysis of this problem as a function of the field size q is available in the literature except [1] which assumes that the field size q is large enough for a maximally recoverable code to exist.

We characterize the family of point-to-point function update problems where linear coding scheme is useful to save at least one transmission, i.e., $l \leq m - 1$ is achievable (Theorem 3, Section III). This characterization is analyzed in terms of the covering radius of $\mathscr{C}_A^{\perp}$, the dual of the code $\mathscr{C}_A$, in Section III-B. We provide a lower bound (Theorem 4, Section IV) and an upper bound (Theorem 5, Section V) on optimal codelength based on linear error correcting codes. Similar to [1] we also provide code constructions when $\mathbf{A}$ is striped (Section V-A1,V-A2) but our focus is on the general case where $t \geq 1$ and $a \geq 1$. For the case when $t = 1$ we provide a construction (Section V-A1) which achieves the optimal codelength for the respective operating field size q, for any prime power $q \geq 2$. For the special case $q \geq m$ this code construction achieves codelength 2ϵ and this matches the achieved codelength in Construction 2 of [1] for $t = 1$ which also requires $q \geq m$. Section V-A2 provides code constructions for $t \geq 1$ using subspace codes and error correcting codes over field extensions. All these code constructions yield a trade-off between the chosen field size and achieved codelength where operating over a smaller field size results in a larger codelength than operating over a larger field size (for instance, see Example 3). When restricted to the special case $a = t$ our construction provides a valid coding scheme for the modified function update problem mentioned in [1, Remark 4] that matches codelength $2t\epsilon$ over any field $\mathbb{F}_q$ reported in [1] (Section V-A3). The performance comparison of the constructed codes are discussed in Section V-A4. Finally, we show that the point-to-point function update problem is equivalent a *functional index coding* or a *generalized index coding* problem [7]–[9]. Given a point-to-point function update problem we construct a functional index coding problem (Algorithm 1, Section VI-B) such that a coding scheme is valid for the function update problem if and only if it is valid for the constructed functional index coding problem (Theorem 9, Section VI-B). This paper starts with describing the system model and providing relevant preliminary results in Section II.

Notation: Matrices and column vectors are denoted by bold uppercase and lowercase letters, respectively. For any positive integer n, the symbol $[n]$ denotes the set $\{1, \ldots, n\}$. The Hamming weight of a vector $\mathbf{x}$ is denoted as $\mathrm{wt}(\mathbf{x})$. The symbol $\mathbb{F}_q$ denotes the finite field of size q and $\mathbb{F}_q^n$ denotes a column vector of n elements over $\mathbb{F}_q$ where q is a prime power. The $n \times n$ identity matrix is denoted as $\mathbf{I}_n$.

II. System Model and Preliminaries

We consider a noiseless communication scenario with single transmitter and single receiver. The transmitter knows a column vector $\mathbf{x}$ of n information symbols where each information symbol is an element over finite field $\mathbb{F}_q$. The receiver stores the coded message $\mathbf{Ax} \in \mathbb{F}_q^m$ where $\mathbf{A} \in \mathbb{F}_q^{m \times n}$ $(m \leq n)$ and rank($\mathbf{A}$) = m. Now suppose the information symbol vector $\mathbf{x}$ is updated to $\mathbf{x}+\mathbf{e}$ where $\mathbf{e}$ is the update vector which is also a column vector of length n over $\mathbb{F}_q$ with $\mathrm{wt}(\mathbf{e}) \leq \epsilon$, where wt denotes the Hamming weight of a vector. The objective is to generate a codeword $\mathbf{c} = (c_1, c_2, \ldots, c_l)^T$ with codelength l as small as possible such that the receiver can update its content to $\mathbf{A}(\mathbf{x}+\mathbf{e})$ using the transmitted codeword $\mathbf{c}$ and

the older version of its content $\mathbf{Ax}$. We assume the transmitter doesn't know about original information symbol vector $\mathbf{x}$ or update vector $\mathbf{e}$ but only knows the updated information symbol vector $(\mathbf{x}+\mathbf{e})$. The problem of designing coding scheme to update the coded data $\mathbf{Ax}$ available at the receiver to $\mathbf{A}(\mathbf{x}+\mathbf{e})$ with $\mathrm{wt}(\mathbf{e}) \leq \epsilon$ will be called as $(\mathbf{A}, \epsilon)$ *function update problem*.

Definition 1. A valid encoding function of codelength l for the $(\mathbf{A}, \epsilon)$ function update problem over the field $\mathbb{F}_q$ is a function

$$\mathfrak{E} : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^l$$

such that there exists a decoding function $\mathfrak{D} : \mathbb{F}_q^l \times \mathbb{F}_q^m \longrightarrow \mathbb{F}_q^m$ satisfying the following property: $\mathfrak{D}(\mathfrak{E}(\mathbf{x}+\mathbf{e}), \mathbf{Ax}) = \mathbf{A}(\mathbf{x}+\mathbf{e})$ for every $\mathbf{x} \in \mathbb{F}_q^n$ and $\mathbf{e} \in \mathbb{F}_q^n$ with $\mathrm{wt}(\mathbf{e}) \leq \epsilon$.

The objective of the code construction is to design a pair $(\mathfrak{E}, \mathfrak{D})$ of encoding and decoding functions that minimizes the codelength l and to calculate the optimal codelength over $\mathbb{F}_q$ which is the minimum codelength among all valid coding schemes.

A coding scheme $(\mathfrak{E}, \mathfrak{D})$ is said to be linear if the encoding function is an $\mathbb{F}_q$-linear transformation. For a linear coding scheme, the codeword $\mathbf{c} = \mathbf{H}(\mathbf{x}+\mathbf{e})$, where $\mathbf{H} \in \mathbb{F}_q^{l \times n}$. The matrix $\mathbf{H}$ is the encoder matrix of the linear coding scheme. The minimum codelength among all valid linear coding schemes for the $(\mathbf{A}, \epsilon)$ function update problem over the field $\mathbb{F}_q$ will be denoted as $l_{q,\mathrm{opt}}$.

The trivial coding scheme that transmits the updated coded information symbols $\mathbf{A}(\mathbf{x}+\mathbf{e})$ i.e., $\mathbf{c} = \mathbf{A}(\mathbf{x}+\mathbf{e})$ is a valid coding scheme with codelength m since the receiver can directly update its content using $\mathbf{c}$. We refer to this trivial coding scheme as *naive scheme* where $\mathbf{H} = \mathbf{A}$. Thus, we have the following trivial upper bound on the optimum linear codelength

$$l_{q,\mathrm{opt}} \leq m. \tag{1}$$

In [1] the authors provided a necessary and sufficient condition for a matrix $\mathbf{H}$ to be a valid encoder matrix for $(\mathbf{A}, \epsilon)$ function update problem. In Theorem 2 of [1] the proof is given only for necessary condition for a matrix $\mathbf{H}$ to be a valid encoder matrix for $(\mathbf{A}, \epsilon)$ function update problem. For the sake of completeness here we first prove that the criterion 1 in [1, Theorem 2] is a necessary and sufficient condition for a matrix $\mathbf{H}$ to be a valid encoder matrix for $(\mathbf{A}, \epsilon)$ function update problem and then state the relevant results which will be helpful to derive other results of this paper. Let $\mathscr{C}_A$ and $\mathscr{C}_H$ denote the linear codes generated by the rows of $\mathbf{A}$ and $\mathbf{H}$ respectively. Also let $\mathscr{C} = \mathscr{C}_A \cap \mathscr{C}_H$ and let $\mathbf{P}$ be a generator matrix of $\mathscr{C}$.

Theorem 1 (Theorem 2, [1])**.** *A matrix $\mathbf{H} \in \mathbb{F}_q^{l \times n}$ is a valid encoder matrix for the $(\boldsymbol{A}, \epsilon)$ function update problem if and only if $\mathbf{Py} \neq \mathbf{0}$ for any $\mathbf{y} \in \mathbb{F}_q^n$ with $\mathrm{wt}(\mathbf{y}) \leq 2\epsilon$ and $\boldsymbol{A}\mathbf{y} \neq \mathbf{0}$.*

Proof: A matrix $\mathbf{H} \in \mathbb{F}_q^{l \times n}$ is a valid encoder matrix for the $(\mathbf{A}, \epsilon)$ function update problem if and only if the receiver can uniquely determine $\mathbf{A}(\mathbf{x}+\mathbf{e})$ from the received codeword $\mathbf{H}(\mathbf{x}+\mathbf{e})$ and the side information $\mathbf{Ax}$. Hence for two pairs of information symbol vectors and update vectors $(\mathbf{x}, \mathbf{e})$ and $(\mathbf{x}', \mathbf{e}')$ such that the coded information symbol vectors available at the receiver are identical i.e., $\mathbf{Ax} = \mathbf{Ax}'$ but updated coded information symbol vectors are distinct i.e., $\mathbf{A}(\mathbf{x}+\mathbf{e}) \neq \mathbf{A}(\mathbf{x}'+\mathbf{e}')$ then the transmitted codeword $\mathbf{H}(\mathbf{x}+\mathbf{e})$ must be distinct from $\mathbf{H}(\mathbf{x}'+\mathbf{e}')$ to distinguish the two different updated coded information symbol vectors. Equivalently, the condition $\mathbf{H}(\mathbf{x}+\mathbf{e}) \neq \mathbf{H}(\mathbf{x}'+\mathbf{e}')$ should hold for every choice of $\mathbf{x}, \mathbf{x}', \mathbf{e}, \mathbf{e}' \in \mathbb{F}_q^n$ with $\mathrm{wt}(\mathbf{e}), \mathrm{wt}(\mathbf{e}') \leq \epsilon$ satisfying $\mathbf{Ax} = \mathbf{Ax}'$ and $\mathbf{A}(\mathbf{x}+\mathbf{e}) \neq \mathbf{A}(\mathbf{x}'+\mathbf{e}')$. Therefore $\mathbf{H}$ is a valid encoder matrix if and only if

$$\mathbf{H}(\mathbf{x}-\mathbf{x}') \neq \mathbf{H}(\mathbf{e}'-\mathbf{e})$$

for all $\mathbf{x}, \mathbf{x}' \in \mathbb{F}_q^n$ such that $\mathbf{Ax} = \mathbf{Ax}'$ and $\mathbf{A}(\mathbf{x}-\mathbf{x}') \neq \mathbf{A}(\mathbf{e}'-\mathbf{e})$. Now denoting $\mathbf{z} = \mathbf{x}-\mathbf{x}'$ and $\mathbf{y} = \mathbf{e}'-\mathbf{e}$ we have

$$\mathbf{Hz} \neq \mathbf{Hy} \tag{2}$$

for all $\mathbf{z}, \mathbf{y} \in \mathbb{F}_q^n$ and $\mathrm{wt}(\mathbf{y}) = \mathrm{wt}(\mathbf{e}' - \mathbf{e}) \leq 2\epsilon$ such that $\mathbf{Az} = \mathbf{0}$ and $\mathbf{Az} \neq \mathbf{Ay}$. Now reformulating the condition given in (2) we obtain $\mathbf{H}(\mathbf{z} - \mathbf{y}) \neq \mathbf{0}$ for all $\mathbf{z}, \mathbf{y} \in \mathbb{F}_q^n$ that satisfy $\mathrm{wt}(\mathbf{y}) \leq 2\epsilon$, $\mathbf{Az} = \mathbf{0}$ and $\mathbf{Ay} \neq \mathbf{0}$. Therefore $\mathbf{H}$ is a valid encoder matrix if and only if for all $\mathbf{z}, \mathbf{y} \in \mathbb{F}_q^n$ and $\mathrm{wt}(\mathbf{y}) \leq 2\epsilon$ if $\mathbf{z} \in \mathscr{C}_A^\perp$ and $\mathbf{y} \notin \mathscr{C}_A^\perp$ then $(\mathbf{y} - \mathbf{z}) \notin \mathscr{C}_H^\perp$. Hence $\mathbf{H}$ is a valid encoder matrix if and only if for all $\mathbf{y} \in \mathbb{F}_q^n$ with $\mathrm{wt}(\mathbf{y}) \leq 2\epsilon$ if $\mathbf{y} \notin \mathscr{C}_A^\perp$ then $\mathbf{y} \notin \mathscr{C}_A^\perp + \mathscr{C}_H^\perp$. Now using the fact that $\mathscr{C}_A^\perp + \mathscr{C}_H^\perp = (\mathscr{C}_A \cap \mathscr{C}_H)^\perp = \mathscr{C}^\perp$ we deduce that $\mathbf{H}$ is a valid encoder matrix if and only if for all $\mathbf{y} \in \mathbb{F}_q^n$ with $\mathrm{wt}(\mathbf{y}) \leq 2\epsilon$ such that $\mathbf{y} \notin \mathscr{C}_A^\perp$ also satisfies $\mathbf{y} \notin \mathscr{C}^\perp$. Hence the statement of the theorem follows. ■

Lemma 1 (Remark 2, [1])**.** *Let $\mathbf{H} \in \mathbb{F}_q^{l \times n}$ be a valid encoder matrix for the $(\boldsymbol{A}, \epsilon)$ function update problem. Let $\mathbf{P}$ be a generator matrix of the code $\mathscr{C} = \mathscr{C}_A \cap \mathscr{C}_H$. Then $\mathbf{P}$ is also a valid encoder matrix for the $(\boldsymbol{A}, \epsilon)$ function update problem.*

If we consider a valid encoder matrix $\mathbf{H}' \in \mathbb{F}_q^{l' \times n}$ such that $\mathscr{C}_{H'} \nsubseteq \mathscr{C}_A$, then we can find another valid encoder matrix $\mathbf{H} \in \mathbb{F}_q^{l \times n}$ as the generator matrix of the code $\mathscr{C}_A \cap \mathscr{C}_{H'}$. Since $\mathscr{C}_H$ is a subcode of $\mathscr{C}_A \cap \mathscr{C}_{H'}$, we have $l > l'$. Therefore the encoder matrix $\mathbf{H}'$ has sub-optimal codelength. So from now we only consider encoder matrices $\mathbf{H}$ such that $\mathscr{C}_H \subseteq \mathscr{C}_A$. Since we assume $\mathscr{C}_H \subseteq \mathscr{C}_A$ we can write $\mathbf{H} = \mathbf{SA}$ for some matrix $\mathbf{S} \in \mathbb{F}_q^{l \times m}$.

Now using $\mathbf{P} = \mathbf{H}$ we restate Theorem 1 as follows. A matrix $\mathbf{H} \in \mathbb{F}_q^{l \times n}$ such that $\mathscr{C}_H \subseteq \mathscr{C}_A$ is a valid encoder matrix for the $(\mathbf{A}, \epsilon)$ function update problem if and only if for any $\mathbf{y} \in \mathbb{F}_q^n$ with $\mathrm{wt}(\mathbf{y}) \leq 2\epsilon$ and $\mathbf{Ay} \neq \mathbf{0}$ satisfies $\mathbf{Hy} \neq \mathbf{0}$. We define the collection $\mathcal{I}(\mathbf{A}, \epsilon)$ as the set of all vectors $\mathbf{y} \in \mathbb{F}_q^n$ with $\mathrm{wt}(\mathbf{y}) \leq 2\epsilon$ such that $\mathbf{Ay} \neq \mathbf{0}$ i.e.,

$$\mathcal{I}(\mathbf{A}, \epsilon) = \{\mathbf{y} \in \mathbb{F}_q^n \mid \mathbf{Ay} \neq \mathbf{0},\ 0 < \mathrm{wt}(\mathbf{y}) \leq 2\epsilon\}. \tag{3}$$

Theorem 2. *A matrix $\mathbf{H} = \boldsymbol{SA}$ for some matrix $\boldsymbol{S} \in \mathbb{F}_q^{l \times m}$ is a valid encoder matrix for the $(\boldsymbol{A}, \epsilon)$ function update problem if and only if*

$$\mathbf{Hy} \neq \mathbf{0}, \quad \forall \mathbf{y} \in \mathcal{I}(\boldsymbol{A}, \epsilon).$$

Now we define the collection $\mathcal{I}_{\text{FU}}(\mathbf{A}, \epsilon)$ as the set of all non-zero linear combinations of 2ϵ or fewer columns of $\mathbf{A}$ over $\mathbb{F}_q$ i.e.,

$$\mathcal{I}_{\text{FU}}(\mathbf{A}, \epsilon) = \{\mathbf{Ay} \mid 0 < \mathrm{wt}(\mathbf{y}) \leq 2\epsilon\} \backslash \{\mathbf{0}\} = \{\mathbf{Ay} \mid \mathbf{y} \in \mathcal{I}(\mathbf{A}, \epsilon)\}.$$

Note that $|\mathcal{I}_{\text{FU}}| \leq q^m - 1$ since $\mathbf{0} \notin \mathcal{I}_{\text{FU}}$.

Corollary 1. *$\mathbf{H} = \boldsymbol{SA}$ is a valid encoder matrix for the $(\boldsymbol{A}, \epsilon)$ function update problem if and only if*

$$\boldsymbol{S}\mathbf{z} \neq \mathbf{0}, \quad \forall \mathbf{z} \in \mathcal{I}_{FU}(\boldsymbol{A}, \epsilon).$$

III. Necessary and Sufficient Condition for $l_{q,\text{opt}} < m$

In this section we will characterize the family of point-to-point function update problems where linear coding is useful to save at least one transmission compared to the naive scheme i.e., $l_{q,\text{opt}} < m$. First we will derive some preliminary results which will be helpful to derive the main result of this section.

Lemma 2. *The collection $\mathcal{I}_{FU}(\boldsymbol{A}, \epsilon)$ is closed under non-zero scalar multiplication.*

Proof: Suppose $\mathbf{z} \in \mathcal{I}_{\text{FU}}$. There exists a $\mathbf{y} \in \mathbb{F}_q^n$ with $0 < \mathrm{wt}(\mathbf{y}) \leq 2\epsilon$ such that $\mathbf{z} = \mathbf{Ay}$. For any $\alpha \in \mathbb{F}_q^*$, $\alpha\mathbf{z} = \alpha\mathbf{Ay} = \mathbf{A}(\alpha\mathbf{y}) = \mathbf{Ay}'$, where $\mathbf{y}' = \alpha\mathbf{y}$. Now as $0 < \mathrm{wt}(\mathbf{y}) \leq 2\epsilon$, it follows that $0 < \mathrm{wt}(\mathbf{y}') \leq 2\epsilon$. Again $\mathbf{Ay}' = \mathbf{A}(\alpha\mathbf{y}) = \alpha\mathbf{Ay} \neq \mathbf{0}$ as $\mathbf{Ay} \in \mathcal{I}_{\text{FU}}$ and $\alpha \neq 0$. Therefore for any $\alpha \in \mathbb{F}_q^*$, $\alpha\mathbf{z} \in \mathcal{I}_{\text{FU}}$. Hence the lemma holds. ■

A. A coding scheme for a family of $(\boldsymbol{A}, \epsilon)$ function update problems

Consider any $(\mathbf{A}, \epsilon)$ function update problem where there exists a non-zero $\mathbf{u} \in \mathbb{F}_q^m$ such that $\mathbf{u} \notin \mathcal{I}_{\text{FU}}$. Let $\mathscr{C}_u$ be the subspace of $\mathbb{F}_q^m$ generated by $\mathbf{u}$. Therefore $\dim(\mathscr{C}_u) = 1$. Note that $\dim(\mathscr{C}_u^{\perp}) = m - 1$. Let $\mathbf{S} \in \mathbb{F}_q^{(m-1)\times m}$ be a generator matrix of the code $\mathscr{C}_u^{\perp}$. The matrix $\mathbf{S}$ is a parity check matrix of the code $\mathscr{C}_u$.

Lemma 3. *The matrix $\boldsymbol{S}$ satisfies $\boldsymbol{S}\mathbf{z} \neq \mathbf{0}$ for all $\mathbf{z} \in \mathcal{I}_{FU}(\boldsymbol{A}, \epsilon)$.*

Proof: Proof by contradiction. Let there exist a $\mathbf{z} \in \mathcal{I}_{\text{FU}}$ such that $\mathbf{Sz} = \mathbf{0}$. This implies that $\mathbf{z} \in \mathscr{C}_u$. Therefore there exists an $\alpha \in \mathbb{F}_q^*$ such that $\mathbf{z} = \alpha\mathbf{u}$. Now as $\alpha \in \mathbb{F}_q^*$, α^{-1} exists and hence $\mathbf{u} = \alpha^{-1}\mathbf{z}$. Now as $\mathbf{z} \in \mathcal{I}_{\text{FU}}$ and $\mathcal{I}_{\text{FU}}$ is closed under non-zero scalar multiplication (using Lemma 3), $\mathbf{u} \in \mathcal{I}_{\text{FU}}$ which is a contradiction. Hence the lemma holds. ∎

Now using Corollary 1, we obtain a valid encoder matrix for the $(\mathbf{A}, \epsilon)$ function update problem over $\mathbb{F}_q$ as $\mathbf{H} = \mathbf{SA}$ with codelength $l = m - 1$, whenever there exists a non-zero vector in $\mathbb{F}_q^m \backslash \mathcal{I}_{\text{FU}}$. We do not claim that this coding scheme yields the optimal codelength $l_{q,\text{opt}}$.

Example 1. Consider the $(\mathbf{A}, 1)$ function update problem over binary field $\mathbb{F}_2$ where $m = 5$, $n = 8$, $\epsilon = 1$ and the matrix $\mathbf{A} \in \mathbb{F}_2^{5\times 8}$ is given by

$$\mathbf{A} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Note that $\text{rank}(\mathbf{A}) = 5$ over $\mathbb{F}_2$. The non-zero vector $\mathbf{u} = [0\ 1\ 1\ 0\ 0] \in \mathbb{F}_2^5$ satisfies $\mathbf{u} \notin \mathcal{I}_{\text{FU}}(\mathbf{A}, 1)$. The parity check matrix of the code $\mathscr{C}_u$, generated by $\mathbf{u}$ is given by

$$\mathbf{S} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Therefore we obtain a valid encoder matrix $\mathbf{H} \in \mathbb{F}_2^{4\times 8}$ with codelength $l = 4$ for the function update problem as

$$\mathbf{H} = \mathbf{SA} = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

∎

Now we derive a necessary and sufficient condition for any $(\mathbf{A}, \epsilon)$ function update problem to save at least one transmission using linear coding scheme compared to the naive scheme.

Theorem 3. *For an $(\boldsymbol{A}, \epsilon)$ function update problem, $l_{q,\text{opt}} = m$ if and only if $|\mathcal{I}_{FU}(\boldsymbol{A}, \epsilon)| = q^m - 1$.*

Proof: To prove the theorem we first show that for any $(\mathbf{A}, \epsilon)$ function update problem if $|\mathcal{I}_{\text{FU}}(\mathbf{A}, \epsilon)| = (q^m - 1)$ then $l_{q,\text{opt}} = m$. Next we show that if $|\mathcal{I}_{\text{FU}}(\mathbf{A}, \epsilon)| < (q^m - 1)$ then $l_{q,\text{opt}} \leq (m - 1)$.

Proof of first part i.e., if $|\mathcal{I}_{FU}(\boldsymbol{A}, \epsilon)| = (q^m - 1)$ then $l_{q,\text{opt}} = m$:

Let $\mathbf{H}$ be an optimal encoder matrix with $l = l_{q,\text{opt}}$. Then there exists a matrix $\mathbf{S} \in \mathbb{F}_q^{l_{q,\text{opt}}\times m}$ such that $\mathbf{H} = \mathbf{SA}$. From Corollary 1 we obtain $\mathbf{Sz} \neq \mathbf{0}$ for all $\mathbf{z} \in \mathcal{I}_{\text{FU}}$. Since $\mathcal{I}_{\text{FU}}$ contains all non-zero vectors from $\mathbb{F}_q^m$, the columns of $\mathbf{S}$ are linearly independent. Hence $l_{q,\text{opt}} \geq m$. Again from (1), we have $l_{q,\text{opt}} \leq m$. Hence $l_{q,\text{opt}} = m$.

Proof of second part i.e., if $|\mathcal{I}_{FU}(\boldsymbol{A},\epsilon)| < (q^m-1)$ then $l_{q,\text{opt}} \leq (m-1)$:

If $|\mathcal{I}_{\text{FU}}(\mathbf{A},\epsilon)| < (q^m-1)$ then there exists a non-zero vector $\mathbf{u} \in \mathbb{F}_q^m$ such that $\mathbf{u} \notin \mathcal{I}_{\text{FU}}(\mathbf{A},\epsilon)$. Therefore using the technique described in Section III-A we can construct a valid encoder matrix such that we save one transmission compared to the naive scheme, i.e., $l_{q,\text{opt}} \leq (m-1)$. Hence the lemma holds. ■

Now we provide a sufficient condition on the field size q to save at least one transmission compared to the naive scheme for any $(\mathbf{A},\epsilon)$ function update problem.

Corollary 2. *For any $\boldsymbol{A} \in \mathbb{F}_q^{m\times n}$ with rank$(\boldsymbol{A}) = m$ where $m > 2\epsilon$,*

$$l_{q,\text{opt}} \leq (m-1) \text{ if } q \geq \tbinom{n}{2\epsilon}^{1/(m-2\epsilon)}$$

.

Proof: If $q \geq \binom{n}{2\epsilon}^{1/(m-2\epsilon)}$ then

$$q^{m-2\epsilon} \geq \binom{n}{2\epsilon}$$
$$\text{or, } \frac{q^m}{q^{2\epsilon}} \geq \binom{n}{2\epsilon}.$$

Using the fact that if $a > b$ then $\frac{a-1}{b-1} > \frac{a}{b}$, we have

$$\frac{q^m-1}{q^{2\epsilon}-1} > \frac{q^m}{q^{2\epsilon}} \quad (\text{since } q^m > q^{2\epsilon})$$
$$\text{or, } \frac{q^m-1}{q^{2\epsilon}-1} > \binom{n}{2\epsilon}$$
$$\text{or, } q^m - 1 > \binom{n}{2\epsilon}(q^{2\epsilon}-1).$$

Now for any $\mathbf{A} \in \mathbb{F}_q^{m\times n}$ with rank$(\mathbf{A}) = m$, the number of distinct non-zero linear combinations of 2ϵ or fewer columns of $\mathbf{A}$ is at the most $\binom{n}{2\epsilon}(q^{2\epsilon}-1)$. Therefore $|\mathcal{I}_{\text{FU}}| \leq \binom{n}{2\epsilon}(q^{2\epsilon}-1)$. Hence $(q^m-1) > \binom{n}{2\epsilon}(q^{2\epsilon}-1) \geq |\mathcal{I}_{\text{FU}}|$. Now using Theorem 3 we have $l_{q,\text{opt}} \leq (m-1)$. ■

B. Relation with covering radius

The covering radius of an $[n,k]$ linear code $\mathscr{C}$ over $\mathbb{F}_q$, denoted by $r_{\text{cov}}(\mathscr{C})$, is defined as the smallest integer r such that the spheres of radius r centered at each codeword of $\mathscr{C}$ cover the whole space $\mathbb{F}_q^n$. We can determine covering radius of a linear code in terms of the cosets of the code. For any vector $\mathbf{a} \in \mathbb{F}_q^n$, the set $\mathbf{a}+\mathscr{C} = \{\mathbf{a}+\mathbf{c} \mid \mathbf{c} \in \mathscr{C}\}$ is called a coset of the code $\mathscr{C}$ and in any coset, a vector with minimum Hamming weight is called a coset leader. The covering radius $r_{\text{cov}}(\mathscr{C})$ of the code $\mathscr{C}$ is the largest among the Hamming weight of all the coset leaders. Upon denoting $\mathbf{H}'$ as a parity check matrix of $\mathscr{C}$, $\mathbf{H}'\mathbf{u}$ is the syndrome of the vector $\mathbf{u} \in \mathbb{F}_q^n$. Two vectors $\mathbf{u},\mathbf{v} \in \mathbb{F}_q^n$ have the same syndrome if and only if they belong to the same coset of $\mathscr{C}$. Hence there is an one-to-one correspondence between syndromes and cosets [10].

For the $(\mathbf{A},\epsilon)$ function update problem let $\mathscr{C}_A$ be the linear code generated by $\mathbf{A}$. Hence $\mathbf{A}$ is a parity check matrix of the code $\mathscr{C}_A^\perp$ which is the dual code of $\mathscr{C}_A$. Now considering a vector $\mathbf{z} \in \mathcal{I}_{\text{FU}}$, $\mathbf{z}$ can be expressed as $\mathbf{A}\mathbf{y}$ where $\mathbf{y} \in \mathbb{F}_q^n$ with $0 < \text{wt}(\mathbf{y}) \leq 2\epsilon$. Therefore the vector $\mathbf{z}$ denotes the syndrome of a vector $\mathbf{y} \in \mathbb{F}_q^n$ with $0 < \text{wt}(\mathbf{y}) \leq 2\epsilon$ that belongs to some coset of $\mathscr{C}_A^\perp$. Note that any vector that belongs to $\mathcal{I}_{\text{FU}}$ is non-zero, hence can not be the syndrome of the codewords of $\mathscr{C}_A^\perp$. Note that $\mathbf{z}$ is the syndrome of the coset leader of the coset $\mathbf{y}+\mathscr{C}_A^\perp$. Since $\mathbf{y}$ is a vector that belongs to the coset and $0 < \text{wt}(\mathbf{y}) \leq 2\epsilon$, the Hamming weight of the coset leader of the coset is at the most 2ϵ.

Corollary 3. *For an $(\boldsymbol{A},\epsilon)$ function update problem, $l_{q,\text{opt}} = m$ if and only if $r_{\text{cov}}(\mathscr{C}_A^\perp) \leq 2\epsilon$.*

Proof: From Theorem 3 we have $l_{q,\text{opt}} = m$ if and only if $|\mathcal{I}_{\text{FU}}| = q^m - 1$. Hence to prove the corollary we prove that for any $(\mathbf{A}, \epsilon)$ function update problem $|\mathcal{I}_{\text{FU}}| = q^m - 1$ if and only if $r_{\text{cov}}(\mathscr{C}_A^{\perp}) \leq 2\epsilon$.

Proof of $r_{\text{cov}}(\mathscr{C}_A^{\perp}) \leq 2\epsilon$ if $|\mathcal{I}_{FU}| = q^m - 1$: Since the collection $\mathcal{I}_{\text{FU}}$ contains all non-zero vectors over $\mathbb{F}_q^m$, each non-zero vector $\mathbf{z} \in \mathbb{F}_q^m$ is the syndrome of some vector $\mathbf{y} \in \mathbb{F}_q^n$ with $0 < \text{wt}(\mathbf{y}) \leq 2\epsilon$ that belongs to some coset of $\mathscr{C}_A^{\perp}$. Since there exists a one-to-one correspondence between the syndromes and cosets, for each vector $\mathbf{z} \in \mathcal{I}_{\text{FU}}$ there exists a coset of $\mathscr{C}_A^{\perp}$ that contains a vector $\mathbf{y}$ with $0 < \text{wt}(\mathbf{y}) \leq 2\epsilon$. Hence the coset leader of each coset has Hamming weight at the most 2ϵ. Therefore the largest Hamming weight of the coset leaders among all cosets of $\mathscr{C}_A^{\perp}$ is at the most 2ϵ. Hence $r_{\text{cov}}(\mathscr{C}_A^{\perp}) \leq 2\epsilon$.

Proof of $|\mathcal{I}_{FU}| = q^m - 1$ if $r_{\text{cov}}(\mathscr{C}_A^{\perp}) \leq 2\epsilon$: Since $r_{\text{cov}}(\mathscr{C}_A^{\perp}) \leq 2\epsilon$, the largest Hamming weight of the coset leaders among all cosets of $\mathscr{C}_A^{\perp}$ is at the most 2ϵ. Since there exists a one-to-one correspondence between the syndromes and cosets, each syndrome $\mathbf{z} \in \mathbb{F}_q^m$ can be expressed as $\mathbf{Ay}$ for some coset leader $\mathbf{y} \in \mathbb{F}_q^n$ satisfies $0 < \text{wt}(\mathbf{y}) \leq 2\epsilon$. We know that the syndromes of a particular linear code covers the whole space. Hence any vector $\mathbf{z} \in \mathbb{F}_q^m \backslash \{\mathbf{0}\}$ can be expressed as $\mathbf{Ay}$ for some $\mathbf{y} \in \mathbb{F}_q^n$ with $0 < \text{wt}(\mathbf{y}) \leq 2\epsilon$. Since $\mathcal{I}_{\text{FU}}$ consists only non-zero vectors that satisfies the above property, $|\mathcal{I}_{\text{FU}}| = q^m - 1$.

Hence $l_{q,\text{opt}} = m$ if and only if $r_{\text{cov}}(\mathscr{C}_A^{\perp}) \leq 2\epsilon$. ■

Example 2. In this example we calculate the minimum number of rows of $\mathbf{A}_{m\times n}$ such that $l_{q,\text{opt}} \leq (m-1)$ is guaranteed for $q = 2$, $\epsilon = 1$ and $n = 8$. Now $l_{q,\text{opt}} \leq (m-1)$ if and only if $r_{\text{cov}}(\mathscr{C}_A^{\perp}) \geq 2\epsilon + 1 = 3$. From Table I of [11] we observe that for any binary code of length 8 and dimension up to 3, covering radius is at least 3. Thus $\dim(\mathscr{C}_A^{\perp}) \geq 3$ implies $l_{q,\text{opt}} \leq (m-1)$. Hence $(n-m) \leq 3$ and $m \geq (n-3) = 5$. Therefore for any matrix $\mathbf{A} \in \mathbb{F}_2^{5\times 8}$ with $\text{rank}(\mathbf{A}) = 5$ we can save one transmission compared to the naive scheme. One such example of $\mathbf{A}$ is given in Example 1. ■

IV. Lower Bound on Optimal Codelength

In this section we derive a lower bound on the optimal codelength $l_{q,\text{opt}}$ over $\mathbb{F}_q$. First we derive two preliminary lemmas which will help to derive the lower bound.

Lemma 4. *For any $(\boldsymbol{A}, \epsilon)$ function update problem and for any invertible matrix $\boldsymbol{K} \in \mathbb{F}_q^{m\times m}$, $\mathcal{I}(\boldsymbol{A}, \epsilon) = \mathcal{I}(\boldsymbol{KA}, \epsilon)$.*

Proof: To prove the lemma we first show that $\mathcal{I}(\mathbf{A}, \epsilon) \subseteq \mathcal{I}(\mathbf{KA}, \epsilon)$ and then $\mathcal{I}(\mathbf{KA}, \epsilon) \subseteq \mathcal{I}(\mathbf{A}, \epsilon)$.

Proof for $\mathcal{I}(\boldsymbol{A}, \epsilon) \subseteq \mathcal{I}(\boldsymbol{KA}, \epsilon)$: Suppose $\mathbf{y} \in \mathcal{I}(\mathbf{A}, \epsilon)$. Then from (3) we have $\mathbf{Ay} \neq \mathbf{0}$. Now left multiplying both side by $\mathbf{K}$ we obtain $\mathbf{KAy} \neq \mathbf{0}$ since $\mathbf{K}$ is invertible. Hence $\mathbf{y} \in \mathcal{I}(\mathbf{KA}, \epsilon)$.

Proof for $\mathcal{I}(\boldsymbol{KA}, \epsilon) \subseteq \mathcal{I}(\boldsymbol{A}, \epsilon)$: Suppose $\mathbf{y} \in \mathcal{I}(\mathbf{KA}, \epsilon)$. Then from (3) we have $\mathbf{KAy} \neq \mathbf{0}$. Since $\mathbf{K}$ is invertible, $\mathbf{K}^{-1}$ exists. Now left multiplying both side by $\mathbf{K}^{-1}$ we obtain $\mathbf{Ay} \neq \mathbf{0}$. Hence $\mathbf{y} \in \mathcal{I}(\mathbf{A}, \epsilon)$.

Hence the lemma holds. ■

For any $(\mathbf{A}, \epsilon)$ function update problem $\mathbf{A} \in \mathbb{F}_q^{m\times n}$ with rank($\mathbf{A}$)=m. Hence $\mathbf{A}$ contains m linearly independent columns. Now consider a matrix $\mathbf{K'}$ which contains m linearly independent columns of $\mathbf{A}$. Note that $\mathbf{K'}$ is an $m \times m$ full rank matrix and hence invertible. Denote $\mathbf{K} = \mathbf{K'}^{-1}$ and $\mathbf{A'} = \mathbf{KA}$. From Lemma 4 we observe that $(\mathbf{A}, \epsilon)$ and $(\mathbf{A'}, \epsilon)$ are equivalent function update problems and any matrix $\mathbf{H}$ is a valid encoder matrix of $(\mathbf{A}, \epsilon)$ function update problem if and only if $\mathbf{H}$ is a valid encoder matrix of $(\mathbf{A'}, \epsilon)$ function update problem. Hence we conclude that the linear code generated by the rows of $\mathbf{H}$ is a subcode of the linear code generated by the rows of $\mathbf{A'}$ i.e., $\mathscr{C}_H \subseteq \mathscr{C}_{A'}$. Hence there exists a matrix $\mathbf{S'} \in \mathbb{F}_q^{l\times m}$ such that $\mathbf{H} = \mathbf{S'A'}$. Now using the equivalence between $(\mathbf{A}, \epsilon)$ and $(\mathbf{A'}, \epsilon)$ function update problems and using Corollary 1 we say that $\mathbf{H} = \mathbf{S'A'}$ is a valid encoder matrix of the $(\mathbf{A}, \epsilon)$ function update problem if and only if $\mathbf{S'z} \neq \mathbf{0}$ for all $\mathbf{z} \in \mathcal{I}_{\text{FU}}(\mathbf{A'}, \epsilon)$.

Let $\mathcal{B}^*(m, 2\epsilon) = \{\mathbf{z} \in \mathbb{F}_q^m \mid 0 < \text{wt}(\mathbf{z}) \leq 2\epsilon\}$ be the set of all non-zero vectors in $\mathbb{F}_q^m$ of Hamming weight at the most 2ϵ.

Lemma 5. *For any $(\boldsymbol{A}, \epsilon)$ function update problem*

$$\mathcal{B}^*(m, 2\epsilon) \subseteq \mathcal{I}_{FU}(\boldsymbol{A}, \epsilon).$$

Proof: For an $(\mathbf{A}, \epsilon)$ function update problem, $\mathbf{A}' = \mathbf{K}\mathbf{A}$ where $\mathbf{K} = \mathbf{K}'^{-1}$ and $\mathbf{K}'$ consists of m linearly independent columns of $\mathbf{A}$. Note that the sub-matrix of $\mathbf{A}'$ that contains the corresponding columns forms an $m \times m$ identity matrix. Now if we consider any non-zero linear combination of 2ϵ of fewer columns of this sub-matrix we obtain all non-zero vectors over $\mathbb{F}_q^m$ with Hamming weight at the most 2ϵ. Hence $\mathcal{B}^*(m, 2\epsilon) \subseteq \mathcal{I}_{\text{FU}}(\mathbf{A}', \epsilon) = \mathcal{I}_{\text{FU}}(\mathbf{A}, \epsilon)$. The last equality holds due to Lemma 4. ■

Let $k_q(m, 2\epsilon + 1)$ be the maximum dimension among all linear codes over $\mathbb{F}_q$ with blocklength m and minimum distance $d_{\min} \geq 2\epsilon + 1$.

Theorem 4. *The optimal codelength of the $(\boldsymbol{A}, \epsilon)$ function update problem over $\mathbb{F}_q$ satisfies*

$$l_{q,\text{opt}} \geq m - k_q(m, 2\epsilon + 1).$$

Proof: Let $\mathbf{H}$ be an optimal encoder matrix of $(\mathbf{A}, \epsilon)$ function update problem with codelength $l = l_{q,\text{opt}}$. Then there exists a matrix $\mathbf{S} \in \mathbb{F}_q^{l_{q,\text{opt}} \times m}$ such that $\mathbf{H} = \mathbf{S}\mathbf{A}$. Now using Corollary 1 we have $\mathbf{S}\mathbf{z} \neq \mathbf{0}$ for all $\mathbf{z} \in \mathcal{I}_{\text{FU}}(\mathbf{A}, \epsilon)$. Since $\mathcal{B}^*(m, 2\epsilon) \subseteq \mathcal{I}_{\text{FU}}(\mathbf{A}, \epsilon)$, it follows that $\mathbf{S}\mathbf{z} \neq \mathbf{0}$ for all $\mathbf{z} \in \mathcal{B}^*(m, 2\epsilon)$. Therefore any set of 2ϵ columns of $\mathbf{S}$ are linearly independent. Hence $\mathbf{S}$ is a parity check matrix of a linear code of block length m and minimum distance at least $2\epsilon + 1$. Thus the dimension of this code satisfies $m - l_{q,\text{opt}} \leq k_q(m, 2\epsilon + 1)$. Then $l_{q,\text{opt}} \geq m - k_q(m, 2\epsilon + 1)$. ■

Theorem 4 provides a lower bound that is aware of the field size q. This is tighter than the bound $l \geq 2\epsilon$ given in [1]–[3] since from Singleton bound we know that $k_q(m, 2\epsilon + 1) \leq m - 2\epsilon$, and this combined with Theorem 4 yields $l \geq 2\epsilon$. Hence, irrespective of the matrix $\mathbf{A}$, a necessary condition for $l_{q,\text{opt}} = 2\epsilon$ is that an $[m, m - 2\epsilon]$ MDS code over $\mathbb{F}_q$ must exist.

V. Code constructions

In this section we first derive an upper bound on the optimal codelength $l_{q,\text{opt}}$ over $\mathbb{F}_q$ and then provide code constructions for $(\mathbf{A}, \epsilon)$ function update problem when $\mathbf{A}$ is in form given by (4). Define $\eta = \max_{\mathbf{z} \in \mathcal{I}_{\text{FU}}} \text{wt}(\mathbf{z})$.

Theorem 5. *The optimal codelength of the $(\boldsymbol{A}, \epsilon)$ function update problem over $\mathbb{F}_q$ satisfies*

$$l_{q,\text{opt}} \leq m - k_q(m, \eta + 1).$$

Proof: From Corollary 1 we have that a matrix $\mathbf{H} = \mathbf{S}\mathbf{A} \in \mathbb{F}_q^{l \times n}$ for some matrix $\mathbf{S} \in \mathbb{F}_q^{l \times m}$, is a valid encoder matrix if and only if $\mathbf{S}\mathbf{z} \neq \mathbf{0},\ \forall \mathbf{z} \in \mathcal{I}_{\text{FU}}$. To satisfy this condition it is sufficient that any set of η columns of $\mathbf{S}$ are linearly independent. Now consider $\mathbf{S}$ as a parity check matrix of the largest linear code with blocklength m and minimum distance $d_{\min} \geq \eta + 1$. The resulting codelength $l = m - k_q(m, \eta + 1)$. Hence the upper bound on the optimal codelength holds. ■

A. Code constructions for striped data

In this section we provide linear code construction of an $(\mathbf{A}^S, \epsilon)$ function update problem where $\mathbf{A}^S \in \mathbb{F}_q^{m \times n}$ follows the structure given by

$$\mathbf{A}^S = \begin{bmatrix} \mathbf{C} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{C} & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{C} \end{bmatrix} \tag{4}$$

where $\mathbf{C} \in \mathbb{F}_q^{t \times K}$ and $\mathbf{0}$ is a $t \times K$ matrix over $\mathbb{F}_q$ whose all elements are 0. Let a be the number of repetitions of $\mathbf{C}$ in the matrix $\mathbf{A}^S$. Hence we write $m = at$ and $n = aK$. First we consider the family of $(\mathbf{A}^S, \epsilon)$ function update problems where $t = 1$ and show that for this case the lower bound on optimal

codelength given in Theorem 4 and the upper bound on optimal codelength given in Theorem 5 exactly matches with each other. Hence we characterize the optimal codelength for this family of function update problems. Our code construction is based on an appropriately chosen linear error correcting code. Note that in Section IV of [1] the authors provided a linear code construction based on maximally recoverable subcodes (MRSC) which requires field size $q \geq m$ and uses an $[m, m-2\epsilon]$ MDS code. In comparison our code construction is suitable for any field size.

1) Code Constructions for the family of $(\boldsymbol{A}^S, \epsilon)$ function update problems with $t = 1$: In this sub-section we first calculate the optimal codelength for such family of function update problems and then provide a code construction based on an appropriately chosen linear error correcting code.

Theorem 6. *For the family of $(\boldsymbol{A}^S, \epsilon)$ function update problems with $t = 1$ the optimal codelength over $\mathbb{F}_q$ is given by*

$$l_{q,\text{opt}} = m - k_q(m, 2\epsilon + 1).$$

Proof: Consider any $\mathbf{z} \in \mathcal{I}_{\text{FU}}(\mathbf{A}^S, \epsilon)$. Then $\mathbf{z}$ can be written as $\mathbf{z} = \mathbf{A}^S\mathbf{y}$ for some $\mathbf{y} \in \mathbb{F}_q^n$ with $0 < \text{wt}(\mathbf{y}) \leq 2\epsilon$. Hence we write $\mathbf{z} = [\mathbf{A}^{S,1}\ \mathbf{A}^{S,2}\ \dots\ \mathbf{A}^{S,n}]\mathbf{y}$ where $\mathbf{A}^{S,i}$ denotes the i^{th} column of $\mathbf{A}^S$ and $\text{wt}(\mathbf{A}^{S,i}) = 1$ for all $i \in [n]$. Now $\text{wt}(\mathbf{z}) = \text{wt}(\mathbf{A}^{S,1}y_1 + \mathbf{A}^{S,2}y_2 + \cdots + \mathbf{A}^{S,n}y_n) \leq \text{wt}(\mathbf{A}^{S,1}y_1) + \text{wt}(\mathbf{A}^{S,2}y_2) + \cdots + \text{wt}(\mathbf{A}^{S,n}y_n)$. Since $0 < \text{wt}(\mathbf{y}) \leq 2\epsilon$, at the most 2ϵ terms among $\mathbf{A}^{S,1}y_1, \mathbf{A}^{S,2}y_2, \dots, \mathbf{A}^{S,n}y_n$ are non-zero and each $\mathbf{A}^{S,i}y_i,\ i \in [n]$ has Hamming weight at the most 1. Hence for any $\mathbf{z} \in \mathcal{I}_{\text{FU}}(\mathbf{A}^S, \epsilon)$, we have $\text{wt}(\mathbf{z}) \leq 2\epsilon$. It is easy to observe that $\eta = \max_{\mathbf{z} \in \mathcal{I}_{\text{FU}}(\mathbf{A}^S, \epsilon)} \text{wt}(\mathbf{z}) = 2\epsilon$. So using Theorem 5 we have $l_{q,\text{opt}} \leq m - k_q(m, 2\epsilon + 1)$. Again from Theorem 4 we have $l_{q,\text{opt}} \geq m - k_q(m, 2\epsilon + 1)$. Since the lower bound and the upper bound matches with each other we have $l_{q,\text{opt}} = m - k_q(m, 2\epsilon + 1)$. ■

Now we provide a code construction for the family of $(\mathbf{A}^S, \epsilon)$ function update problems with $t = 1$. Since for any $(\mathbf{A}^S, \epsilon)$ function update problem with $t = 1$ the value of η is 2ϵ, it is sufficient that $\mathbf{Sz} \neq \mathbf{0}$ for any $\mathbf{z}$ with $0 < \text{wt}(\mathbf{z}) \leq 2\epsilon$. Hence it is sufficient that any 2ϵ columns of $\mathbf{S}$ are linearly independent. Now consider $\mathbf{S}$ as a parity check matrix of a linear code of maximum dimension with blocklength m and minimum distance $d_{\text{min}} \geq 2\epsilon + 1$ and set the encoder matrix $\mathbf{H} = \mathbf{SA}^S$. This code achieves the optimal codelength $l_{q,\text{opt}} = m - k_q(m, 2\epsilon + 1)$. Now if $q \geq m$ then there exists an MDS code over $\mathbb{F}_q$ with blocklength m and minimum distance $d_{\text{min}} = 2\epsilon + 1$ which has maximum dimension $k_q(m, 2\epsilon + 1) = m - 2\epsilon$ among all linear codes over $\mathbb{F}_q$. Hence choosing $\mathbf{S}$ as a parity check matrix of an $[m, m - 2\epsilon]$ MDS code $\mathbb{F}_q,\ q \geq m$ and encoder matrix $\mathbf{H} = \mathbf{SA}^S$ we achieve codelength $l_{q,\text{opt}} = 2\epsilon$ which matches the codelength achieved by the construction given in Section IV of [1] which also requires $q \geq m$.

Example 3. Consider an $(\mathbf{A}^S, \epsilon)$ function update problem over $\mathbb{F}_2$ where $\epsilon = 1$ and $\mathbf{A}^S$ is given by

$$\mathbf{A}^S = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Now from [12] we have $k_2(4, 3) = 1$. Hence choosing $\mathbf{S}$ as parity check matrix of a $[4, 1]$ repetition code over $\mathbb{F}_2$ we achieve codelength $l_{2,\text{opt}} = 3$.

If we view the above matrix $\mathbf{A}^S$ as over $\mathbb{F}_4$ and the $(\mathbf{A}^S, \epsilon)$ function update problem over $\mathbb{F}_4$ where $\epsilon = 1$, from [12] we have $k_4(4, 3) = 2$. Hence choosing $\mathbf{S}$ as parity check matrix of a $[4, 2, 3]$ MDS code over $\mathbb{F}_4$ we achieve codelength $l_{4,\text{opt}} = 2$. ■

2) Code constructions for the family of $(\boldsymbol{A}^S, \epsilon)$ function update problems where $t \geq 1$: In this sub-section we provide a linear code construction for the family of $(\mathbf{A}^S, \epsilon)$ function update problems where $\mathbf{A}^S$ is given in (4) with $t \geq 1$. A matrix $\mathbf{H} \in \mathbb{F}_q^{l \times n}$ is a valid encoder matrix if and only if there exists a matrix $\mathbf{S} \in \mathbb{F}_q^{l \times m}$ such that $\mathbf{H} = \mathbf{SA}^S$ satisfies $\mathbf{Sz} \neq \mathbf{0}$ for all $\mathbf{z} \in \mathcal{I}_{\text{FU}}(\mathbf{A}^S, \epsilon)$. For any vector $\mathbf{z} \in \mathcal{I}_{\text{FU}}(\mathbf{A}^S, \epsilon)$ we

write $\mathbf{z} = \mathbf{A}\mathbf{y}$ for some $\mathbf{y} \in \mathbb{F}_q^n$ with $0 < \mathrm{wt}(\mathbf{y}) \leq 2\epsilon$. Hence

$$\mathbf{z} = \mathbf{A}\mathbf{y} = \begin{bmatrix} \mathbf{C} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{C} & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{C} \end{bmatrix} \begin{bmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \\ \vdots \\ \mathbf{y}_a \end{bmatrix} = \begin{bmatrix} \mathbf{C}\mathbf{y}_1 \\ \mathbf{C}\mathbf{y}_2 \\ \vdots \\ \mathbf{C}\mathbf{y}_a \end{bmatrix}$$

where $\mathbf{y} = [\mathbf{y}_1^T \ \mathbf{y}_2^T \ \dots \ \mathbf{y}_a^T]^T$ with $a = \frac{n}{K} = \frac{m}{t}$ and each $\mathbf{y}_i \in \mathbb{F}_q^K, \ \forall i \in [a]$. Since $0 < \mathrm{wt}(\mathbf{y}) \leq 2\epsilon$, at the most 2ϵ vectors among $\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_a$ are non-zero. Hence at the most 2ϵ vectors among $\mathbf{C}\mathbf{y}_1, \mathbf{C}\mathbf{y}_2, \dots, \mathbf{C}\mathbf{y}_a$ are non-zero. Denote $\mathbf{z} = [\mathbf{z}_1^T \ \mathbf{z}_2^T \ \dots \ \mathbf{z}_a^T]^T$ where each $\mathbf{z}_i = \mathbf{C}\mathbf{y}_i \in \mathbb{F}_q^t, \ \forall i \in [a]$. Therefore we have that at the most 2ϵ vectors among $\mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_a$ are non-zero. Now for any $\mathbf{z} \in \mathcal{I}_{\mathrm{FU}}(\mathbf{A}^S, \epsilon)$ we write

$$\mathbf{S}\mathbf{z} \neq \mathbf{0} \tag{5}$$

$$\Rightarrow \begin{bmatrix} \mathbf{S}_1 & \mathbf{S}_2 \cdots \mathbf{S}_a \end{bmatrix} [\mathbf{z}_1^T \ \mathbf{z}_2^T \ \cdots \ \mathbf{z}_a^T]^T \neq \mathbf{0} \tag{6}$$

$$\Rightarrow \mathbf{S}_1\mathbf{z}_1 + \mathbf{S}_2\mathbf{z}_2 + \cdots + \mathbf{S}_a\mathbf{z}_a \neq \mathbf{0}. \tag{7}$$

where $\mathbf{S}_i \in \mathbb{F}_q^{l \times t}, \ i \in [a]$ is the sub-matrix of $\mathbf{S}$ containing $(i-1)t + 1^{\mathrm{th}}$ to it^{th} columns of $\mathbf{S}$.

I. Case-1, $t \geq 1$**,** $\epsilon = 1$**:** To satisfy the condition given in (7) for $\epsilon = 1$ it is sufficient that the columns of any two or fewer sub-matrices among $\mathbf{S}_1, \mathbf{S}_2, \dots, \mathbf{S}_a$ form linearly independent set. Hence the columns of each sub-matrix $\mathbf{S}_i, \ i \in [a]$ are linearly independent. Let $\mathcal{S}_i$ be the t-dimensional subspace of $\mathbb{F}_q^l$ generated by the columns of $\mathbf{S}_i$ over $\mathbb{F}_q$. Now to satisfy the linear independence property of the columns of two or fewer sub-matrices among $\mathbf{S}_1, \mathbf{S}_2, \dots, \mathbf{S}_a$, it is sufficient to have $\mathcal{S}_i \cap \mathcal{S}_j = \{\mathbf{0}\}$ for any $i, j \in [a]$ and $i \neq j$. Our code construction for an $(\mathbf{A}^S, 1)$ function update problem where $t \geq 1$ is based on subspace codes.

Code Construction 1. Our aim is to construct a matrix $\mathbf{S} = [\mathbf{S}_1 \ \mathbf{S}_2 \ \dots \ \mathbf{S}_a] \in \mathbb{F}_q^{l \times m}$ where $\mathbf{S}_i \in \mathbb{F}_q^{l \times t}, \ i \in [a]$ is the sub-matrix of $\mathbf{S}$ containing $(i-1)t + 1^{\mathrm{th}}$ to it^{th} columns of $\mathbf{S}$ such that the subspaces generated by the columns any two sub-matrices $\mathbf{S}_i$ and $\mathbf{S}_j$ for $i \neq j, \ i, j \in [a]$ are trivially intersecting. Note that for any $i \neq j, \ i, j \in [a]$ the subspaces $\mathcal{S}_i$ and $\mathcal{S}_j$ generated by the columns of $\mathbf{S}_i$ and $\mathbf{S}_j$ respectively are t dimensional subspace of $\mathbb{F}_q^l$ and satisfies $\mathcal{S}_i \cap \mathcal{S}_j = \{\mathbf{0}\}$. Hence to construct such $\mathbf{S}$ matrix we utilize pairwise trivially intersecting t-dimensional subspaces $\mathcal{S}_1, \mathcal{S}_2, \dots, \mathcal{S}_a$ of $\mathbb{F}_q^l$. From the literature on subspace codes [13]–[15], we know that if $l \geq 2t$ then there exist at least q^{l-t} pairwise trivially intersecting t-dimensional subspaces in $\mathbb{F}_q^l$. Hence if $q \geq a^{\frac{1}{l-t}}$ and provided $l \geq 2t$ it is possible to find pairwise trivially intersecting t-dimensional subspaces $\mathcal{S}_1, \mathcal{S}_2, \dots, \mathcal{S}_a$ of $\mathbb{F}_q^l$. Now to construct $\mathbf{S} = [\mathbf{S}_1 \ \mathbf{S}_2 \ \dots \ \mathbf{S}_a]$ we choose a basis of i^{th} subspace $\mathcal{S}_i, \ i \in [a]$ which contains t vectors over $\mathbb{F}_q^l$ and these t linearly independent vectors form the columns of the sub-matrix $\mathbf{S}_i$. After constructing such $\mathbf{S}$ matrix, we set $\mathbf{H} = \mathbf{S}\mathbf{A}^S$ which is a valid encoder matrix for the $(\mathbf{A}^S, 1)$ function update problem with $t \geq 1$. Using this code construction we achieve codelength $l \geq 2t$ for $(\mathbf{A}^S, 1)$ function update problem if $q \geq a^{\frac{1}{l-t}}$.

Example 4. Consider an $(\mathbf{A}^S, \epsilon)$ function update problem over $\mathbb{F}_2$ with $\epsilon = 1$ where $\mathbf{A}^S \in \mathbb{F}_2^{9 \times 12}$ is given by

$$\mathbf{A}^S = \begin{bmatrix} \mathbf{C} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{C} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{C} \end{bmatrix}$$

where $\mathbf{C} \in \mathbb{F}_2^{3 \times 4}$ is given by

$$\mathbf{C} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Now our aim is to construct a matrix $\mathbf{S} = [\mathbf{S}_1\ \mathbf{S}_2\ \mathbf{S}_3] \in \mathbb{F}_q^{l\times 9}$ such that the subspaces $\mathcal{S}_1,\ \mathcal{S}_2,\ \mathcal{S}_3$ generated by the columns of $\mathbf{S}_1,\ \mathbf{S}_2$ and $\mathbf{S}_3$ respectively are pairwise trivially intersecting. From our construction we have that it is possible to find 3 pairwise trivially intersecting 3-dimensional subspaces of $\mathbb{F}_q^l$ if $q \geq 3^{\frac{1}{l-3}}$ and provided $l \geq 6$. If we let $l = 6$ then $q \geq 3^{\frac{1}{3}}$ i.e., $q \geq 2$. Hence over $\mathbb{F}_2$ it is possible to construct a 6×9 matrix $\mathbf{S}$ such that $\mathbf{H} = \mathbf{S}\mathbf{A}^S$ is a valid encoder matrix for the $(\mathbf{A}^S, 1)$ function update problem. One possible choice of 3 pairwise trivially intersecting 3-dimensional subspaces of $\mathbb{F}_q^6$ is $\mathcal{S}_1 = \text{span}\{(1,0,0,0,0,0),(0,1,0,0,0,0),(0,0,1,0,0,0)\}$, $\mathcal{S}_2 = \text{span}\{(0,0,0,1,0,0),(0,0,0,0,1,0),(0,0,0,0,0,1)\}$ and $\mathcal{S}_3 = \text{span}\{(1,0,0,1,0,0),(0,1,0,0,1,0),(0,0,1,0,0,1)\}$. Hence the matrix $\mathbf{S} \in \mathbb{F}_2^{6\times 9}$ is given by

$$\mathbf{S} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

■

II. **Case-2,** $t \geq 1$**,** $\epsilon \geq 1$**:** Here we provide a linear code construction for the family of $(\mathbf{A}^S, \epsilon)$ function update problem where $\epsilon \geq 1$ and $\mathbf{A}^S$ is given in (4) with $t \geq 1$. To satisfy the condition given in (7) for $\epsilon \geq 1$ it is sufficient that the columns of any 2ϵ or fewer sub-matrices among $\mathbf{S}_1, \mathbf{S}_2, \ldots, \mathbf{S}_a$ form a linearly independent set.

Code Construction 2. Our code construction uses a linear code over $\mathbb{F}_{q^t}$ of maximum possible dimension with block length a and minimum distance $d_{\min} \geq 2\epsilon + 1$. Let $\hat{\mathbf{S}} \in \mathbb{F}_{q^t}^{\hat{l}\times a}$ be a parity check matrix of such linear code with $\hat{l} = a - k_{q^t}(a, 2\epsilon+1)$ where $k_{q^t}(a, 2\epsilon+1)$ denotes the maximum dimension of a linear code over $\mathbb{F}_{q^t}$ with block length a and minimum distance $d_{\min} \geq 2\epsilon + 1$. Note that any 2ϵ columns of $\hat{\mathbf{S}}$ are linearly independent over $\mathbb{F}_{q^t}$. Let α be a primitive element of $\mathbb{F}_{q^t}$ and $p(x) = p_0 + p_1 x + p_2 x^2 + \cdots + p_{t-1}x^{t-1} + x^t$ be the primitive polynomial corresponding to α where each $p_j \in \mathbb{F}_q$ for all $j \in \{0, 1, \ldots, t-1\}$. The corresponding companion matrix is given by

$$\mathbf{M} = \begin{bmatrix} 0 & 0 & \ldots & 0 & -p_0 \\ 1 & 0 & \ldots & 0 & -p_1 \\ 0 & 1 & \ldots & 0 & -p_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -p_{t-1} \end{bmatrix}.$$

Now we define a matrix $\mathbf{S} = [\mathbf{S}_1\ \mathbf{S}_2\ \ldots\ \mathbf{S}_a] \in \mathbb{F}_q^{\hat{l}t\times at}$ where for each $j \in [a]$, $\mathbf{S}_j \in \mathbb{F}_q^{\hat{l}t\times t}$ is given by $\mathbf{S}_j = [\mathbf{S}_{1,j}^T\ \mathbf{S}_{2,j}^T\ \ldots\ \mathbf{S}_{\hat{l},j}^T\ ]^T$. Now for each $i \in [\hat{l}]$ and $j \in [a]$, $\mathbf{S}_{i,j} \in \mathbb{F}_q^{t\times t}$ is given by

$$\mathbf{S}_{i,j} = \begin{cases} \mathbf{0}_{t\times t} & \text{if} \quad \hat{s}_{i,j} = 0 \\ \mathbf{I}_{t\times t} & \text{if} \quad \hat{s}_{i,j} = 1 \\ \mathbf{M}^k & \text{if} \quad \hat{s}_{i,j} = \alpha^k,\ k \in \{1, 2 \ldots, q^t - 2\} \end{cases} \tag{8}$$

where $\hat{s}_{i,j}$ is the $(i,j)^{\text{th}}$ entry of $\hat{\mathbf{S}}$. Since any 2ϵ or fewer columns of $\hat{\mathbf{S}}$ are linearly independent then using Theorem 3 in [13] we have that the columns of any 2ϵ or fewer block matrices among $\mathbf{S}_1, \mathbf{S}_2, \ldots, \mathbf{S}_a$ are linearly independent. Hence the matrix $\mathbf{H} = \mathbf{S}\mathbf{A}^S$ is a valid encoder matrix over $\mathbb{F}_q$ with codelength $l = \hat{l}t = t(a - k_{q^t}(a, 2\epsilon+1))$. Since any 2ϵ or fewer columns of $\hat{\mathbf{S}}$ are linearly independent we have $\hat{l} \geq 2\epsilon$ and hence $l \geq 2\epsilon t$ with equality if and only if $\hat{\mathbf{S}}$ is a parity check matrix of an $[a, a-2\epsilon, 2\epsilon+1]$ MDS code over $\mathbb{F}_{q^t}$. Such an MDS code is guaranteed to exist if $q^t \geq a$. Hence using this code construction we achieve codelength $l = 2\epsilon t$ if $q \geq a^{\frac{1}{t}}$.

Example 5. Consider an $(\mathbf{A}^S, \epsilon)$ function update problem over $\mathbb{F}_2$ with $\epsilon = 2$ where $\mathbf{A}^S \in \mathbb{F}_2^{15\times 20}$ is given by

$$\mathbf{A}^S = \begin{bmatrix} \mathbf{C} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{C} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{C} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{C} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{C} \end{bmatrix}$$

where $\mathbf{C} \in \mathbb{F}_2^{3\times 4}$ is given by

$$\mathbf{C} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Note that $x^3 + x + 1$ is a primitive polynomial corresponding to $\mathbb{F}_8$ and companion matrix corresponding to the primitive polynomial $x^3 + x + 1 = 0$ is given by

$$\mathbf{M} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Now we set $\hat{\mathbf{S}}$ as a parity check matrix of a $[5, 1, 5]$ MDS code over $\mathbb{F}_8$ which is repetition code over $\mathbb{F}_8$. Hence $\hat{\mathbf{S}} \in \mathbb{F}_8^{4\times 5}$ is given by

$$\hat{\mathbf{S}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Now we obtain the matrix $\mathbf{S} \in \mathbb{F}_2^{12\times 15}$ from $\hat{\mathbf{S}}$ using (8) as

$$\mathbf{S} = \begin{bmatrix} \mathbf{I}_{3\times 3} & 0 & 0 & 0 & \mathbf{I}_{3\times 3} \\ 0 & \mathbf{I}_{3\times 3} & 0 & 0 & \mathbf{I}_{3\times 3} \\ 0 & 0 & \mathbf{I}_{3\times 3} & 0 & \mathbf{I}_{3\times 3} \\ 0 & 0 & 0 & \mathbf{I}_{3\times 3} & \mathbf{I}_{3\times 3} \end{bmatrix}.$$

Now we obtain a valid encoder matrix $\mathbf{H} = \mathbf{S}\mathbf{A}^S$ with codelength 12 over $\mathbb{F}_2$. ■

3) Comparison with the code in Remark 4 of [1]: Let us first briefly describe about the system model given in Remark 4 in [1] using our notations. In Remark 4 of [1] the authors considered transmission of t updated information symbol vectors $\mathbf{x}_1 + \mathbf{e}_1, \mathbf{x}_2 + \mathbf{e}_2, \ldots, \mathbf{x}_t + \mathbf{e}_t$, $\mathbf{x}_i + \mathbf{e}_i \in \mathbb{F}_q^K,\ \forall i \in [t]$. The receiver knows coded version of each information symbol vector denoted by $\mathbf{C}\mathbf{x}_1, \mathbf{C}\mathbf{x}_2, \ldots, \mathbf{C}\mathbf{x}_t$ where $\mathbf{C} \in \mathbb{F}_q^{t\times K}$ and $\mathbf{C}\mathbf{x}_i \in \mathbb{F}_q^t,\ \forall i \in [t]$ and demands updated version of the coded demands i.e., $\mathbf{C}(\mathbf{x}_1 + \mathbf{e}_1), \mathbf{C}(\mathbf{x}_2 + \mathbf{e}_2), \ldots, \mathbf{C}(\mathbf{x}_t + \mathbf{e}_t)$. We can view this problem as an $(\mathbf{A}^S, \epsilon)$ function update problem where $\mathbf{A}^S \in \mathbb{F}_q^{t^2\times tK}$ takes the form given in (4) with the number of repetitions of the matrix $\mathbf{C}$ along the block diagonal entries of $\mathbf{A}^S$ being equal to t. We denote the information symbol vector as $\mathbf{x} = [\mathbf{x}_1^T\ \mathbf{x}_2^T\ \ldots\ \mathbf{x}_t^T]^T \in \mathbb{F}_q^{tK}$ and the update vector as $\mathbf{e} = [\mathbf{e}_1^T\ \mathbf{e}_2^T\ \ldots\ \mathbf{e}_t^T]^T \in \mathbb{F}_q^{tK}$ with $\mathrm{wt}(\mathbf{e}) \leq \epsilon$. The authors of [1] provide a valid code construction with codelength $2t\epsilon$ based on an MRSC using the Construction 1 in [1]. This construction from [1] is valid over any field $\mathbb{F}_q$.

To construct a valid code for the above function update problem we choose $\hat{\mathbf{S}}$ as a parity check matrix of a $[t, t - 2\epsilon, 2\epsilon + 1]$ MDS code over $\mathbb{F}_{q^t}$ and such a code exists if $q^t \geq t$. Then we construct the matrix $\mathbf{S} \in \mathbb{F}_q^{2t\epsilon\times t^2}$ from $\hat{\mathbf{S}}$ using (8). Hence if $q \geq t^{1/t}$ we construct a valid code with codelength $2t\epsilon$ for the $(\mathbf{A}^S, \epsilon)$ function update problem. Note that for any positive integer t, $t^{1/t} < 2$. Hence over any finite field $\mathbb{F}_q$ our construction yields a valid encoder matrix with codelength $2t\epsilon$ for the $(\mathbf{A}^S, \epsilon)$ function update problem described above.

4) Comparison of Code Construction 1 and Code Construction 2 for $(\mathbf{A}^S, 1)$ function update problem with $t \geq 1$: In this sub-section we consider the Code Construction 2 for the special case of $\epsilon = 1$ and then compare the performance with the performance of the Code Construction 1. Consider an $(\mathbf{A}^S, 1)$ function update problem where $\mathbf{A}^S$ is of the form given in (4). To obtain a valid code for the $(\mathbf{A}^S, 1)$ function update problem using the Code Construction 2, we use a linear code over $\mathbb{F}_{q^t}$ of maximum possible dimension with blocklength a and minimum distance $d_{\min} \geq 3$. Let $\hat{\mathbf{S}} \in \mathbb{F}_{q^t}^{\hat{l} \times a}$ be a parity of such linear code with $\hat{l} = a - k_{q^t}(a, 3)$ where $k_{q^t}(a, 3)$ denotes the maximum possible dimension of a linear code over $\mathbb{F}_{q^t}$ with blocklength a and minimum distance is at least 3. We construct a matrix $\mathbf{S} \in \mathbb{F}_q^{\hat{l}t \times at}$ from $\hat{\mathbf{S}}$ using (8) and obtain a valid encoder matrix $\mathbf{H}$ with code length $\hat{l}t$ by multiplying $\mathbf{S}$ with $\mathbf{A}^S$. Note that any two or fewer columns of $\hat{\mathbf{S}}$ are linearly independent. Hence the subspace generated by each column of $\hat{\mathbf{S}}$ are pairwise trivially intersecting. Therefore to construct such a matrix $\hat{\mathbf{S}}$ it is necessary and sufficient that the number of trivially intersecting 1-dimensional subspaces of space $\mathbb{F}_{q^t}^{\hat{l}}$ is at least a. From [16] we know that the space $\mathbb{F}_{q^t}^{\hat{l}}$ contains exactly $(q^{\hat{l}t} - 1)/(q^t - 1)$ trivially intersecting 1-dimensional subspaces. Hence to construct a matrix $\mathbf{S}$ it is necessary and sufficient that

$$\frac{q^{\hat{l}t} - 1}{q^t - 1} \geq a.$$

Now using the fact $(q^{\hat{l}t} - 1)/(q^t - 1) \geq q^{\hat{l}t}/q^t$ (since $\hat{l}t \geq t$) we observe that $q^{\hat{l}t}/q^t \geq a$ i.e., $q \geq a^{\frac{1}{t(\hat{l}-1)}}$ is a sufficient condition for such an encoder matrix to exist. Hence applying the Code Construction 2 for an $(\mathbf{A}^S, 1)$ function update problem over $\mathbb{F}_q$ we achieve codelength $l = t(a - k_{q^t}(a, 3))$ if the field size $q \geq a^{\frac{1}{t(\hat{l}-1)}}$. Hence if $q \geq a^{1/t}$ we achieve codelength $l = 2t$ using the Code Construction 2 by choosing a parity check matrix of an $[a, a-2, 3]$ MDS code over $\mathbb{F}_{q^t}$ and such a MDS code exists over $\mathbb{F}_{q^t}$ since $q^t \geq a$. Note that we also achieve codelength $l = 2t$ for $(\mathbf{A}^S, 1)$ function update problem using the Code Construction 1 if $q \geq a^{1/t}$. Note that in Code Construction 2, the achieved codelength $l = \hat{l}t$ is always an integer multiple of t. But applying the Code Construction 1 for $(\mathbf{A}^S, 1)$ function update problem we can achieve any codelength $l \geq 2t$ provided the field size $q \geq a^{1/l-t}$. Hence for $(\mathbf{A}^S, 1)$ function update problem the Code Construction 2 becomes a special case of the Code Construction 1. This also inspires us to study the Code Construction 1 separately for $(\mathbf{A}^S, 1)$ function update problem.

VI. Equivalence with a Functional Index Coding problem

In this section we discuss a variation of the classical index coding problem where each user demands a coded version of the information symbols present at the transmitter and already knows a subset of the (uncoded) information symbols as side information. This is a special case of the Generalized Index Coding problem [7], [8] and the Functional Index Coding problem [9]. The authors of [7], [8] generalized the classical index coding problem where each receiver knows some linearly coded information symbols as side-information and demands some linearly coded information symbols. Additionally the authors of [7] assume that the information symbols present in the transmitter are also linearly coded information symbols. In [9], authors generalized the index coding problem, where the side-information as well as demanded messages can be arbitrary functions of information symbols, called *functional index coding* problem. Here we consider a special case of generalized index coding problem and functional index coding problem and then we introduce the relation between function update problem and this family of functional index coding problems.

A. Functional Index Coding with Coded Demand and Uncoded Side Information

Consider a broadcast network scenario with single transmitter and $\hat{K}$ receivers $u_1, u_2, \ldots, u_{\hat{K}}$. The transmitter has a vector of n information symbols $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$. Each receiver knows a subset of the information symbols as side-information. Let $\mathbf{x}_{\mathcal{X}_i}$ be the side-information vector of i^{th} receiver u_i

where $\mathcal{X}_i \subseteq [n],\ i \in [\hat{K}]$. Each receiver demands a coded version of the information symbols vector $\mathbf{x}$. Let $\mathbf{A}_i\mathbf{x}$ be the coded demand of i^{th} receiver u_i where $\mathbf{A}_i \in \mathbb{F}_q^{m\times n}$ with $\text{rank}(\mathbf{A}_i) = m$. Upon denoting $\mathcal{A} = (\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_{\hat{K}})$ and $\mathcal{X} = (\mathcal{X}_1, \mathcal{X}_1, \ldots, \mathcal{X}_{\hat{K}})$ we describe the problem instance as $(\hat{K}, n, \mathcal{X}, \mathcal{A})$ *functional index coding problem*. A valid *encoding function* $\mathfrak{E}_{\text{FIC}}$ over $\mathbb{F}_q$ for an $(\hat{K}, n, \mathcal{X}, \mathcal{A})$ functional index coding problem is

$$\mathfrak{E}_{\text{FIC}} : \mathbb{F}_q^n \to \mathbb{F}_q^l$$

such that for each receiver u_i, $i \in [\hat{K}]$ there exists a *decoding function* $\mathfrak{D}_{i,\text{FIC}} : \mathbb{F}_q^l \times \mathbb{F}_q^{|\mathcal{X}_i|} \to \mathbb{F}_q^m$ satisfying the following property: $\mathfrak{D}_{i,\text{FIC}}(\mathfrak{E}_{\text{FIC}}(\mathbf{x}), \mathbf{x}_{\mathcal{X}_i}) = \mathbf{A}_i\mathbf{x}$ for every $\mathbf{x} \in \mathbb{F}_q^n$.

The design objective is to design a tuple $(\mathfrak{E}_{\text{FIC}}, \mathfrak{D}_{1,\text{FIC}}, \mathfrak{D}_{2,\text{FIC}}, \ldots, \mathfrak{D}_{\hat{K},\text{FIC}})$ of encoding and decoding functions that minimizes the codelength l and determine the *optimal codelength* for the given functional index coding problem which is the minimum codelength among all coding schemes.

A linear code for an $(\hat{K}, n, \mathcal{X}, \mathcal{A})$ functional index coding problem is defined as a coding scheme where the encoding function $\mathfrak{E}_{\text{FIC}} : \mathbb{F}_q^n \to \mathbb{F}_q^l$ is a linear transformation over $\mathbb{F}_q$ described as $\mathfrak{E}_{\text{FIC}}(\mathbf{x}) = \mathbf{H}\mathbf{x}$, where $\mathbf{H} \in \mathbb{F}_q^{l\times n}$ is the *encoder matrix* for linear functional index code. The minimum codelength among all valid linear coding schemes for the $(\hat{K}, n, \mathcal{X}, \mathcal{A})$ functional index coding problem over the field $\mathbb{F}_q$ will be denoted as $l_{q,\text{opt,FIC}}$.

Now we derive a design criterion for a matrix $\mathbf{H}$ to be a valid encoder matrix for $(\hat{K}, n, \mathcal{X}, \mathcal{A})$ functional index coding problem. We define the set $\mathcal{I}_{\text{FIC}}(\hat{K}, n, \mathcal{X}, \mathcal{A})$, or equivalently $\mathcal{I}_{\text{FIC}}$, of vectors $\mathbf{y}$ of length n such that $\mathbf{y}_{\mathcal{X}_i} = \mathbf{0} \in \mathbb{F}_q^{|\mathcal{X}_i|}$ and $\mathbf{A}_i\mathbf{y} \neq \mathbf{0}$ for some choice of $i \in [\hat{K}]$ i.e.,

$$\mathcal{I}_{\text{FIC}}(\hat{K}, n, \mathcal{X}, \mathcal{A}) = \bigcup_{i=1}^{\hat{K}} \{\mathbf{y} \in \mathbb{F}_q^n \mid \mathbf{y}_{\mathcal{X}_i} = \mathbf{0} \text{ and } \mathbf{A}_i\mathbf{y} \neq \mathbf{0}\}. \tag{9}$$

Theorem 7. *The matrix $\mathbf{H} \in \mathbb{F}_q^{l\times n}$ is a valid encoder matrix for the $(\hat{K}, n, \mathcal{X}, \mathcal{A})$ functional index coding problem if and only if*

$$\mathbf{H}\mathbf{y} \neq \mathbf{0}, \quad \forall \mathbf{y} \in \mathcal{I}_{\text{FIC}}.$$

Proof: A matrix $\mathbf{H} \in \mathbb{F}_q^{l\times n}$ is a valid encoder matrix for the $(\hat{K}, n, \mathcal{X}, \mathcal{A})$ functional index coding problem if and only if at each receiver $u_i,\ i \in [\hat{K}]$, $\mathbf{A}_i\mathbf{x}$ can be uniquely determined from the received codeword $\mathbf{H}\mathbf{x}$ and the side information $\mathbf{x}_{\mathcal{X}_i}$. Hence for two distinct pair of the information symbol vectors $(\mathbf{x}, \mathbf{x}')$ such that the side-information symbol vectors available at the i^{th} receiver are identical i.e., $\mathbf{x}_{\mathcal{X}_i} = \mathbf{x}'_{\mathcal{X}_i}$ but demanded coded information symbol vectors are distinct i.e., $\mathbf{A}_i\mathbf{x} \neq \mathbf{A}_i\mathbf{x}'$ then the transmitted codeword $\mathbf{H}\mathbf{x}$ must be distinct from $\mathbf{H}\mathbf{x}'$ to distinguish two different demanded coded information symbol vectors. Equivalently, the condition $\mathbf{H}\mathbf{x} \neq \mathbf{H}\mathbf{x}'$ should hold for every pair $\mathbf{x}, \mathbf{x}' \in \mathbb{F}_q^n$ such that $\mathbf{A}_i\mathbf{x} \neq \mathbf{A}_i\mathbf{x}'$ and $\mathbf{x}_{\mathcal{X}_i} = \mathbf{x}'_{\mathcal{X}_i}$ for some $i \in [K]$. Therefore $\mathbf{H}$ is a valid encoder matrix if and only if

$$\mathbf{H}(\mathbf{x} - \mathbf{x}') \neq \mathbf{0}$$

for all $\mathbf{x}, \mathbf{x}' \in \mathbb{F}_q^n$ such that $\mathbf{A}_i\mathbf{x} \neq \mathbf{A}_i\mathbf{x}'$ and $\mathbf{x}_{\mathcal{X}_i} = \mathbf{x}'_{\mathcal{X}_i}$ for some $i \in [\hat{K}]$. Now denoting $\mathbf{y} = \mathbf{x} - \mathbf{x}'$ we have

$$\mathbf{H}\mathbf{y} \neq \mathbf{0}$$

for all $\mathbf{y} \in \mathbb{F}_q^n$ such that $\mathbf{A}_i\mathbf{y} \neq \mathbf{0}$ and $\mathbf{y}_{\mathcal{X}_i} = \mathbf{0}$ for some $i \in [\hat{K}]$. Hence the statement of the theorem follows. ■

Algorithm 1: Construction of an functional index coding problem from a given function update problem

Input: $\mathbf{A} \in \mathbb{F}_q^{m\times n}, \epsilon$ corresponding to an $(\mathbf{A}, \epsilon)$ function update problem
Output: $\hat{K}, \mathcal{X}, \mathcal{A}$ corresponding to a functional index coding problem
% % Iteration:
$j = 0$
for *each* $Q \subseteq [n] = \{1, 2, \ldots, n\}$ *with* $|Q| = \min(2\epsilon, n)$ **do**
  $j \leftarrow j + 1$
  $\mathcal{X}_j \leftarrow [n] \setminus Q$
  $\mathbf{A}_j \leftarrow \mathbf{A}$
end
if $n > 2\epsilon$ **then**
  $\hat{K} = \binom{n}{2\epsilon}$
else
  $K = n$
end
$\mathcal{X} = (\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_{\hat{K}})$
$\mathcal{A} = (\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_{\hat{K}})$

B. Construction of a Equivalent Functional Index Coding Problem from a given Function Update problem

Now we construct an $(\hat{K}, n, \mathcal{X}, \mathcal{A})$ functional index coding problem starting from an $(\mathbf{A}, \epsilon)$ function update problem. The number of receivers $\hat{K}$, the tuple of the side information indices $\mathcal{X}$ and the tuple of coded demands $\mathcal{A}$ are obtained from Algorithm 1.

Algorithm 1 considers every possible choice of $Q \subseteq [n]$ such that $|Q| = \min(2\epsilon, n)$ and defines a new user u_j in the functional index coding problem with demand matrix $\mathbf{A}_j = \mathbf{A}$ and side information $\mathcal{X}_j = [n] \setminus Q$.

Now we relate the set $\mathcal{I}(\mathbf{A}, \epsilon)$ defined for the $(\mathbf{A}, \epsilon)$ Function Update problem and the set $\mathcal{I}_{\text{FIC}}$ defined in (9) for the constructed $(\hat{K}, n, \mathcal{X}, \mathcal{A})$ functional index coding problem.

Theorem 8. *For any given* $(\boldsymbol{A}, \epsilon)$ *function update problem and its corresponding* $(\hat{K}, n, \mathcal{X}, \mathcal{A})$ *functional index coding problem,* $\mathcal{I}(\boldsymbol{A}, \epsilon) = \mathcal{I}_{\text{FIC}}(\hat{K}, n, \mathcal{X}, \mathcal{A})$.

Proof: To show that $\mathcal{I}(\mathbf{A}, \epsilon) = \mathcal{I}_{\text{FIC}}(\hat{K}, n, \mathcal{X}, \mathcal{A})$, we will show that $\mathcal{I}(\mathbf{A}, \epsilon) \subseteq \mathcal{I}_{\text{FIC}}$ and $\mathcal{I}_{\text{FIC}} \subseteq \mathcal{I}(\mathbf{A}, \epsilon)$.

Proof for $\mathcal{I}(\mathbf{A}, \epsilon) \subseteq \mathcal{I}_{\text{FIC}}$: Suppose a vector $\mathbf{y} \in \mathcal{I}(\mathbf{A}, \epsilon)$. Then from (3), we have $\mathbf{A}\mathbf{y} \neq \mathbf{0}$ and $0 < \text{wt}(\mathbf{y}) \leq 2\epsilon$. Hence there exists a $Q \subseteq [n]$ such that $|Q| = \min(2\epsilon, n)$ and $\mathbf{y}_{[n]\setminus Q} = \mathbf{0}$. Now using the construction procedure described in Algorithm 1 we see that there exists a user u_j in the constructed functional index coding problem such that $\mathcal{X}_j = [n] \setminus Q$ and $\mathbf{A}_j = \mathbf{A}$. The vector $\mathbf{y}$ satisfies $\mathbf{y}_{\mathcal{X}_j} = \mathbf{0}$ and $\mathbf{A}_j\mathbf{y} \neq \mathbf{0}$. Hence $\mathbf{y} \in \mathcal{I}_{\text{FIC}}$.

Proof for $\mathcal{I}_{\text{FIC}} \subseteq \mathcal{I}(\mathbf{A}, \epsilon)$: Suppose a vector $\mathbf{y} \in \mathcal{I}_{\text{FIC}}$. Then there exists at least one user $j \in [\hat{K}]$ such that $\mathbf{A}_j\mathbf{y} \neq \mathbf{0}$ and $\mathbf{y}_{\mathcal{X}_j} = \mathbf{0}$. Since $\mathbf{A}_j\mathbf{y} \neq \mathbf{0}$ we have $\mathbf{y} \neq \mathbf{0}$. From Algorithm 1 we see that for any $j \in [\hat{K}]$, $|\mathcal{X}_j| = n - \min(2\epsilon, n)$. Note that $\text{wt}(\mathbf{y}) = \text{wt}(\mathbf{y}_{\mathcal{X}_j}) + \text{wt}(\mathbf{y}_{[n]\setminus\mathcal{X}_j}) \leq 2\epsilon$. Again from the construction we have $\mathbf{A}_i = \mathbf{A},\ \forall j \in [K]$. Therefore $\mathbf{A}\mathbf{y} \neq \mathbf{0}$. Hence $\mathbf{y} \in \mathcal{I}(\mathbf{A}, \epsilon)$.

Hence the theorem holds. ■

Now we relate the problem of constructing linear codes for function update problem to the problem of designing linear coding scheme for the corresponding functional index coding problem.

Theorem 9. *A matrix* $\mathbf{H} \in \mathbb{F}_q^{l\times n}$ *such that* $\mathbf{H} = \boldsymbol{SA}$ *for some matrix* $\boldsymbol{S} \in \mathbb{F}_q^{l\times m}$ *is a valid encoder matrix*

for the $(\boldsymbol{A}, \epsilon)$ *function update problem if and only if* $\mathbf{H}$ *is a valid encoder matrix for the* $(\hat{K}, n, \mathcal{X}, \mathcal{A})$ *functional index coding problem.*

Proof: From Theorem 2 we know that $\mathbf{H}$ is a valid encoder matrix for the $(\mathbf{A}, \epsilon)$ function update problem if and only if it satisfies

$$\mathbf{H}\mathbf{y} \neq \mathbf{0}, \quad \forall \mathbf{y} \in \mathcal{I}(\mathbf{A}, \epsilon).$$

Now from Theorem 8 we have $\mathcal{I}(\mathbf{A}, \epsilon) = \mathcal{I}_{\mathrm{FIC}}(\hat{K}, n, \mathcal{X}, \mathcal{A})$. Therefore using Theorem 7 we conclude that $\mathbf{H}$ is a valid encoder matrix for the $(\hat{K}, n, \mathcal{X}, \mathcal{A})$ functional index coding problem if and only if $\mathbf{H}$ is a valid encoder matrix for the $(\mathbf{A}, \epsilon)$ function update problem. ■

ACKNOWLEDGMENT

The authors thank Dr V. Lalitha for discussions regarding the topic of this paper.

REFERENCES

[1] N. Prakash and M. Médard, "Communication Cost for Updating Linear Functions When Message Updates are Sparse: Connections to Maximally Recoverable Codes," *IEEE Transactions on Information Theory*, vol. 64, no. 12, pp. 7557–7576, Dec 2018.

[2] P. Nakkiran, N. B. Shah, and K. V. Rashmi, "Fundamental limits on communication for oblivious updates in storage networks," in *2014 IEEE Global Communications Conference*, Dec 2014, pp. 2363–2368.

[3] P. Nakkiran, N. B. Shah, K. V. Rashmi, A. Sahai, and K. Ramchandran, "Optimal Oblivious Updates in Distributed Storage Networks." [Online]. Available: www.cs.cmu.edu/%7Ervinayak/papers/ObUp.pdf

[4] M. Mahdian, N. Prakash, M. Médard, and E. Yeh, "Updating Content in Cache-Aided Coded Multicast," *CoRR*, vol. abs/1805.00396, 2018. [Online]. Available: https://arxiv.org/abs/1805.00396

[5] R. E. Ali and V. R. Cadambe, "Multi-version Coding for Consistent Distributed Storage of Correlated Data Updates," *CoRR*, vol. abs/1708.06042, 2017. [Online]. Available: https://arxiv.org/abs/1708.06042

[6] Z. Wang and V. R. Cadambe, "Multi-Version Coding–An Information-Theoretic Perspective of Consistent Distributed Storage," *IEEE Transactions on Information Theory*, vol. 64, no. 6, pp. 4540–4561, June 2018.

[7] M. Dai, K. W. Shum, and C. W. Sung, "Data Dissemination With Side Information and Feedback," *IEEE Transactions on Wireless Communications*, vol. 13, no. 9, pp. 4708–4720, Sep. 2014.

[8] N. Lee, A. G. Dimakis, and R. W. Heath, "Index Coding With Coded Side-Information," *IEEE Communications Letters*, vol. 19, no. 3, pp. 319–322, March 2015.

[9] A. Gupta and B. S. Rajan, "Error-correcting functional index codes, generalized exclusive laws and graph coloring," in *2016 IEEE International Conference on Communications (ICC)*, May 2016, pp. 1–7.

[10] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*. North-Holland publishing company, 1997.

[11] R. Graham and N. Sloane, "On the Covering Radius of Codes," *IEEE Transactions on Information Theory*, vol. 31, no. 3, pp. 385–401, May 1985.

[12] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," Online available at http://www.codetables.de, 2007, accessed on 2018-12-29.

[13] T. Etzion and A. Wachter-Zeh, "Vector Network Coding Based on Subspace Codes Outperforms Scalar Linear Network Coding," *IEEE Transactions on Information Theory*, vol. 64, no. 4, pp. 2460–2473, April 2018.

[14] T. Etzion and N. Silberstein, "Codes and Designs Related to Lifted MRD Codes," *IEEE Transactions on Information Theory*, vol. 59, no. 2, pp. 1004–1017, Feb 2013.

[15] R. Koetter and F. R. Kschischang, "Coding for Errors and Erasures in Random Network Coding," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3579–3591, Aug 2008.

[16] F. E. Oggier, N. J. A. Sloane, S. N. Diggavi, and A. R. Calderbank, "Nonintersecting subspaces based on finite alphabets," *IEEE Transactions on Information Theory*, vol. 51, no. 12, pp. 4320–4325, Dec 2005.