Appl. Comput. Harmon. Anal. ••• (••••) •••–•••

Contents lists available at ScienceDirect

Applied and Computational Harmonic Analysis

www.elsevier.com/locate/acha

# Erasure recovery matrices for encoder protection

Deguang Han [a,1], David Larson [b], Sam Scholze [c,*], Wenchang Sun [d,2]

[a] Department of Mathematics, University of Central Florida, Orlando, FL 32816, USA
[b] Department of Mathematics, Texas A&M University, College Station, TX, USA
[c] Department of Mathematics, University of Wisconsin-Eau Claire, Eau Claire, WI, USA
[d] School of Mathematical Sciences and LPMC, Nankai University, Tianjin 300071, China

ARTICLE INFO

*Article history:*
Received 10 August 2017
Received in revised form 28 August 2018
Accepted 17 September 2018
Available online xxxx
Communicated by Rachel Ward

*MSC:*
primary 46G10, 46L07, 46L10, 46L51, 47A20
secondary 42C15, 46B15, 46B25, 47B48

*Keywords:*
Frames
Erasures
Fourier series
Erasure recovery matrices
Encoding and decoding frames

ABSTRACT

In this article, we investigate the privacy issues that arise from a new frame-based kernel analysis approach to reconstruct from frame coefficient erasures. We show that while an erasure recovery matrix is needed in addition to a decoding frame for a receiver to recover the erasures, the erasure recovery matrix can be designed in such a way that it protects the encoding frame. The set of such erasure recovery matrices is shown to be an open and dense subset of a certain matrix space. We present algorithms to construct concrete examples of encoding frame and erasure recovery matrix pairs for which the erasure reconstruction process is robust to additive channel noise. Using the Restricted Isometry Property, we also provide quantitative bounds on the amplification of sparse additive channel noise. Numerical experiments are presented on the amplification of additive normally distributed random channel noise. In both cases, the amplification factors are demonstrated to be quite small.


## 1. Introduction

In recent years frames have proven to be very useful in many applications, and in particular in signal or information processing. Typically a signal (message) is analyzed or encoded as a sequence of frame coefficients by using an encoding frame. These frame coefficients (or codes) are then transmitted to a receiver and the receiver reconstructs (decodes) the signal (message) by using a decoding frame. In this process the transmitted data set may get corrupted due to erasures, distortions and noises. However, if the

* Corresponding author.
*E-mail addresses:* deguang.han@ucf.edu (D. Han), larson@math.tamu.edu (D. Larson), scholzsl@uwec.edu (S. Scholze), sunwch@nankai.edu.cn (W. Sun).
[1] Deguang Han was partially supported by NSF grants DMS-1403400 and DMS-1712602.
[2] Wenchang Sun was partially supported by the National Natural Science Foundation of China (11525104 and 11531013).

https://doi.org/10.1016/j.acha.2018.09.004
1063-5203/

encoding frames have an appropriate amount of redundancy then the reconstruction procedure is robust to these corruptions, and in many cases perfect reconstruction from erasure corrupted data sets is possible. For several good references on frame erasures, see [4,5,8,12,14,17–29,31,34–36].

A standard method of perfectly reconstructing a signal from erasure corrupted frame coefficients at known locations is to invert the frame operator of the frame whose indices correspond to the non-erased frame coefficients. However, this method is relatively slow since it requires an $n \times n$ matrix inversion, where $n$ denotes the dimension of the underlying Hilbert space.

This work was motivated by two recent approaches to the problem of perfect reconstruction from frame erasures. The first was due to the first and fourth authors in [17], and the second was due to the second and third authors in [24]. The method of [17] uses *erasure recovery matrices* whose kernels are the range spaces of the analysis operators for the encoding frame or part of the encoding frame. The method of [24], called *bridging*, is to recover the lost frame coefficient data using a small subset of the good frame coefficients. Both approaches recover lost data by inverting an $L \times L$ matrix, where $L$ denotes the cardinality of the erased set of indices. Thus, these methods significantly reduce the computational complexity of perfect reconstruction from frame erasures.

In cryptography, a *man-in-the-middle attack* occurs when an eavesdropper impersonates a signal sender in order to send either a false or modified message to a signal recipient. A man-in-the-middle attack can occur if an eavesdropper is able to steal the encoding frame (or encoding device) of a signal sender. Unfortunately, in order to reconstruct a signal from frame coefficient erasures, a signal recipient must have some knowledge of the encoding (or analysis) frame. The method of reconstruction that is used in this paper allows for erasure reconstruction in such a way that an eavesdropper, or the signal recipient does not receive enough information to completely determine the encoding device. Thus, by protecting the encoding device, this erasure reconstruction method can be used to safeguard against a man-in-the-middle attack.

Clearly the standard dual frame of the encoding frame can not be provided to the receiver since the standard dual of the standard dual is the original encoding frame. We will show (Proposition 3.4) that, in fact, to protect the encoding frame, the range space of the analysis operator for the encoding frame must be a *proper* subspace of the kernel of the erasure recovery matrix. The goal of this paper is to address the problem of erasure recovery, while still protecting the encoding device (i.e., the encoding frame).

In Section 4, it is shown that $m$-encoding frame protected erasure recovery matrices for a given frame, $\{g_j\}_{j=1}^N$ exist provided that $\{g_j\}_{j\in\{1,\cdots,N\}\setminus\Gamma}$ still forms a frame whenever $|\Gamma| \leq m$, and $n < N-m$. Moreover, it is shown that these matrices exist in great abundance, as they form an open dense subset of a certain convex matrix space. In Section 5, three constructions of erasure recovery matrix, encoding frame pairs are provided.

The remainder of the paper is devoted to the effects of additive channel noise on our reconstruction. Any erasure reconstruction technique has the potential to heavily amplify channel noise. However, in Section 5, by utilizing tools from compressive sensing, we give two constructions of frames and erasure recovery matrices for which this amplification factor is small ($\frac{2}{1-\delta}$ where $\delta$ is the restricted isometry constant for the erasure recovery matrix) for sparse additive channel noise. In Section 7, we provide numerical experiments which suggest that the amplification factor for normally distributed additive random channel noise is also quite small.

## 2. Frames and erasures

We begin with some background on frames (cf. [9,10,15,16]). A sequence $\{g_j\}_{j=1}^N$ is said to be a *frame* for a finite dimensional Hilbert space $\mathcal{H}$ if there exist positive constants $A$ and $B$ such that

$$A\|f\|^2 \leq \sum_{j=1}^{N} |\langle f, g_j\rangle|^2 \leq B\|f\|^2, \quad \forall f \in \mathcal{H}. \tag{1}$$

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004

The constants $A$ and $B$ are called *lower* and *upper frame bounds*, respectively. The optimal lower frame bound is the supremum over all lower bounds, and the optimal upper frame bound is the infimum over all upper frame bounds. A frame $\{g_j\}_{j=1}^N$ with optimal frame bounds $A$ and $B$ is said to be tight if $A = B$, and Parseval if $A = B = 1$. For the remainder of this article, we will use $\mathcal{H}_n$ to denote $\mathbb{R}^n$ or $\mathbb{C}^n$.

Let $\{g_j\}_{j=1}^N$ be a frame for $\mathcal{H}_n$. Its *analysis operator* $\Theta : \mathcal{H}_n \to \mathcal{H}_N$ is defined by

$$\Theta(f) = \{\langle f, g_j\rangle\}_{j=1}^N, \quad \forall f \in \mathcal{H}_n. \tag{2}$$

It is easily seen that a matrix representation for the analysis operator is the matrix $G^*$ whose $j$th row is $g_j^*$ (the conjugate transpose of the $j$th frame vector). The *synthesis operator* is the adjoint of $\Theta$, and we have

$$\Theta^* c = \sum_{j=1}^N c_j g_j \quad \forall c = (c_j)_{j=1}^N \in \mathcal{H}_N. \tag{3}$$

The matrix representation for this operator is the matrix $G$, whose $j$th column is the $j$th frame vector, $g_j$.

**Remark 2.1.** We will sometimes abuse notation and denote a frame $\{g_j\}_{j=1}^N$ by its synthesis matrix, $G$. If the reader sees the sequence $\{g_j\}_{j=1}^N$, he/she should automatically associate this with the matrix $G$ whose $j$th column is the vector $g_j$, and vice versa.

It can be easily verified that the operator $S := \Theta^*\Theta = GG^*$ is invertible on $\mathcal{H}_n$ and $\{\tilde{g}_j = S^{-1}g_j\}_{j=1}^N$ is also a frame for $\mathcal{H}_n$, which is called the *canonical or standard dual frame* for $\{g_j\}_{j=1}^N$. The standard dual provides us the following reconstruction formula:

$$f = \sum_{j=1}^N \langle f, \tilde{g}_j\rangle\, g_j, \quad \forall f \in \mathcal{H}_n. \tag{4}$$

Note that whenever $\{g_j\}_{j=1}^N$ is a frame but not a basis, then there are many (actually, infinitely many) other choices of $f_j$ for which

$$f = \sum_{j=1}^N \langle f, f_j\rangle\, g_j, \quad \forall f \in \mathcal{H}_n.$$

Any such frame $\{f_j\}_{j=1}^N$ is called a *dual frame* to $\{g_j\}_{j=1}^N$. Two sequences $\{g_j\}_{j=1}^N$ and $\{h_j\}_{j=1}^N$ are called *strongly disjoint (or orthogonal)* if the range spaces of their analysis operators are orthogonal subspaces of $\mathcal{H}_N$, and they are *strongly complementary* if their range spaces form orthogonal complementary subspaces. It is well known (cf. [15,16]) that a sequence $\{f_j\}_{j=1}^N$ is a dual frame for $\{g_j\}_{j=1}^N$ if and only if $f_j = S^{-1}g_j + h_j$, where $S$ is the frame operator for $\{g_j\}_{j=1}^N$ and $\{h_j\}_{j=1}^N$ is strongly disjoint to $\{g_j\}_{i=1}^N$.

In applications, a frame $\{g_j\}_{j=1}^N$ is often used to analyze a signal $f \in \mathcal{H}_n$ (or to encode a message $f$) by computing its frame coefficients $c_j = \langle f, g_j\rangle$. We will refer to such a frame as an encoding frame. The frame coefficients are transmitted to receivers to reconstruct (or decode) $f$ by using various methods. The simplest method is to use a dual frame $\{f_j\}_{i=1}^N$, known as the decoding frame to recover $f$:

$$f = Fc = \sum_{j=1}^N c_j f_j. \tag{5}$$

Since $\{f_j\}_{j=1}^N$ is not a basis, there are infinitely many different choices for the encoding frame, which consequently provides a high level of security for the encoding device. If the receiver does not have the

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004

information about the range space of the analysis operator for the encoding frame, then it is difficult for the receiver to recover the encoding frame. However, in the case that a receiver is provided with some additional tools to deal with problems coming from, for example, erasures, then the additional tools may jeopardize the privacy of the encoding frame. In this paper we present requirements, existence and constructions of erasure recovery matrices (introduced in [17,18]) that can preserve the privacy for the encoding frame when they are provided to the decoder as additional tools for signal/image recovery.

We say that a subset $\Lambda$ of $\{1, \cdots, N\}$ satisfies the *minimal redundancy condition* for a frame $\{g_j\}_{j=1}^N$ if $\{g_j\}_{j\in\Lambda^c}$ remains to be a frame for $\mathcal{H}_n$ (cf. [24,25]). It is easily seen that if $\Lambda$ does not satisfy the minimal redundancy condition, then we cannot recover every signal from frame coefficient erasures indexed by $\Lambda$. However, if $\Lambda$ satisfies the minimal redundancy condition, any signal can be reconstructed from frame coefficient erasures indexed by $\Lambda$. If every subset $\Lambda$ of cardinality $m$ satisfies the minimal redundancy condition for $F$, then we say that $F$ has the *minimal redundancy condition* for $m$-erasures.

In following the conventions set in [1], the *spark* of a matrix is the size of the smallest linearly dependent subset of the columns. Moreover, we will define the *spark* of a collection of vectors $\{g_j\}_{j=1}^N$ in an $n$-dimensional Hilbert space $\mathcal{H}_n$ as the size of the smallest linearly dependent subset of $\{g_j\}_{j=1}^N$ (i.e. as the spark of its synthesis matrix, $G$). Furthermore, if $N \geq n$, the collection $\{g_j\}_{j=1}^N$ is said to have *full spark* if it has spark $n+1$. Frames which satisfy the full spark property were also known as frames with *maximal robustness to erasures* in [23]. It was shown in [30] that if $N \geq n$, then the set of full spark frames is open and dense in the set of all frames. In [1], this was extended to a proof of density in the Zariski topology. Thus, most frames satisfy the full spark property.

The *restricted isometry constant* of order $s$ for an $m \times N$ matrix $M$ is the smallest number $\delta_s > 0$ so that for all s-sparse vectors $x \in \mathbb{C}^N$,

$$(1-\delta_s)\|x\|^2 \leq \|Mx\|^2 \leq (1+\delta_s)\|x\|^2. \tag{6}$$

It is well known (cf. [13]) that there is a universal constant $C$, so that whenever

$$m \geq \frac{C}{\delta^2}\left(s\ln\left(\frac{eN}{s}\right)+\ln\left(\frac{2}{\epsilon}\right)\right), \tag{7}$$

for $\delta, \epsilon \in (0,1)$, the probability that the restricted isometry constant $\delta_s$ for an $m \times N$ Gaussian random matrix $M$ satisfies $\delta_s \leq \delta$ is greater than $1-\epsilon$ (cf. [2,7,11,32,37]). Later on, we will be using restricted isometry constants to provide bounds on the amplification of sparse additive channel noise for our reconstruction.

## 3. Erasure recovery matrices

The following concept of an erasure recovery matrix was introduced in [17]:

**Definition 3.1.** Let $\{g_j\}_{j=1}^N$ be a frame for an $n$-dimensional Hilbert space, $\mathcal{H}_n$ and $k$ be a positive integer. An *$m$-erasure recovery matrix* is a $k \times N$ matrix $M$ with spark $m+1$ satisfying $Mc = 0$ for any vector $c \in \Theta(\mathcal{H})$, where $\Theta$ denotes the analysis operator for the frame $G$. That is, $M\Theta = 0$, or

$$M\left(\langle f, g_j\rangle\right)_{j=1}^N = 0 \quad \forall f \in \mathcal{H}.$$

Notice that in Definition 3.1 we must have $k \geq m$, however, for any practical application, we will only consider $k = m$. Definition 3.1 has many useful equivalents which are given in the next proposition. In particular, parts (4) and (5) below will give us formulas on how to reconstruct a signal from erasures at known locations (see Remark 3.3).

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004

**Proposition 3.2.** *Let $\{g_j\}_{j=1}^N$ be a frame for $\mathcal{H}_n$ and $\Theta$ be its analysis operator. Suppose that $m \geq 1$ is an integer. Then the following are equivalent for a $k \times N$ matrix, $M$:*

(1) *$M$ is an $m$-erasure recovery matrix.*
(2) *$M$ has spark $m+1$ and $\ker(M) \supseteq \Theta(\mathcal{H}_n)$.*
(3) *The columns of $M$ have spark $m+1$ and are strongly disjoint (i.e. orthogonal) to $\{g_j\}_{j=1}^N$.*
(4) *$\ker(M) \supseteq \Theta(\mathcal{H}_n)$ and for every set $\Lambda \subset \{1, 2, \cdots, N\}$ satisfying $|\Lambda| \leq m$, $(M_\Lambda^* M_\Lambda)^{-1}$ exists, where $M_\Lambda$ denotes the minor of $M$ formed by the columns indexed by $\Lambda$.*
(5) *$\ker(M) \supseteq \Theta(\mathcal{H}_n)$ and for any $\Lambda$ with $|\Lambda| \leq m$, there exists a subset $I$ of $\{1, ..., k\}$ such that $M_{I,\Lambda}$ is invertible, where $M_{I,\Lambda}$ denotes the minor of $M$ with rows indexed by $I$ and columns indexed by $\Lambda$.*

**Proof.** Clearly we have (1) $\Rightarrow$ (2) $\Rightarrow$ (3). For (3) $\Rightarrow$ (4), write $M = [h_1, \cdots, h_N]$. Since $|\Lambda| \leq m$, $M_\Lambda^* M_\Lambda$ is the Gramian of the linearly independent sequence $\{h_j\}_{j\in\Lambda}$, $M_\Lambda^* M_\Lambda$ is invertible. To prove (4) $\Rightarrow$ (5), notice that $M_\Lambda^* M_\Lambda$ is invertible $\{h_j\}_{j\in\Lambda}$ is linearly independent. Thus $M_\Lambda$ has rank $|\Lambda|$. Thus, we can find a set $I \subset \{1, 2, \cdots, k\}$ such that $|I| = |\Lambda|$, and $M_{I,\Lambda}^{-1}$ exists. To prove (5) $\Rightarrow$ (1), clearly $M\Theta(\mathcal{H}_n) = 0$. Assume $\Lambda \subset \{1, \cdots, N\}$ satisfying $|\Lambda| = m$. Then, we can find $I \subset \{1, \cdots, k\}$ such that $M_{I,\Lambda}^{-1}$ exists. Thus, the columns of $M_{I,\Lambda}$ are linearly independent, and it follows that the columns of $M_\Lambda$ must be linearly independent. Since $\Lambda$ was chosen arbitrarily, this shows that every subset of $m$ columns of $M$ are linearly independent. That is, $M$ has spark $m+1$. □

**Remark 3.3.** Assume that $M$ is an $m$-erasure matrix for a frame $\{g_j\}_{j=1}^N$ for $\mathcal{H}_n$. Assume that $f \in \mathcal{H}_n$, and $c = (c_j)_{j=1}^N$, where $c_j = \langle f, g_j \rangle$. Then, by definition, we have

$$Mc = 0.$$

Hence, if we let $M_\Lambda$ denote the matrix with columns indexed by $\Lambda$, and $c_\Lambda$ denote the vector $(c_j)_{j\in\Lambda}$ for any $\Lambda \subset \{1, \cdots, N\}$, we have

$$M_\Lambda c_\Lambda + M_{\Lambda^c} c_{\Lambda^c} = 0.$$

Rearranging the equation gives

$$M_\Lambda c_\Lambda = -M_{\Lambda^c} c_{\Lambda^c}. \tag{8}$$

If the goal is to reconstruct the vector $c$ from erasures indexed by erasures at $\Lambda$, our goal is to solve equation (8) for $c_\Lambda$. Using Proposition 3.2, we have two ways to proceed.

Using part (5) of Proposition 3.2, we can find $I \subset \{1, \cdots, k\}$ so that $M_{I,\Lambda}^{-1}$ exists. Therefore, if we chop off rows indexed by $I^c$ from equation (8), we get

$$M_{I,\Lambda} c_\Lambda = -M_{I,\Lambda^c} c_{\Lambda^c}.$$

Thus, we can reconstruct $c_\Lambda$ as

$$c_\Lambda = -M_{I,\Lambda}^{-1} M_{I,\Lambda^c} c_{\Lambda^c}. \tag{9}$$

If we instead use part (4) of Proposition 3.2 we will be able to use a pseudoinverse method to solve for $c_\Lambda$. Multiplying both sides of equation (8) by $M_\Lambda^*$ gives

$$M_\Lambda^* M_\Lambda c_\Lambda = -M_\Lambda^* M_{\Lambda^c} c_{\Lambda^c}.$$

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004

Now, simply inverting we can reconstruct $c_\Lambda$ as

$$c_\Lambda = -(M_\Lambda^* M_\Lambda)^{-1} M_\Lambda^* M_{\Lambda^c} c_{\Lambda^c}. \tag{10}$$

In our experiments, we will use the pseudo-inversive method given by equation (10) not only because it is more stable, but we also will not need to implement a search for the set $I$ used in equation (9).

The following is an important observation that tells us that if the receiver is given a dual frame and an erasure recovery matrix $M$ such that $\ker(M) = \Theta(\mathcal{H}_n)$, then the receiver can easily recover the encoding frame $\{g_j\}_{j=1}^N$ and consequently the encoding devices are not protected from the decoder.

**Proposition 3.4.** *Any finite frame can be explicitly computed from the range space of its analysis operator and any one of its dual frames.*

**Proof.** Assume that $K$ is the range space of the analysis operator $\Theta$ of an encoding frame $\{g_j\}_{j=1}^N$ for $\mathcal{H}_n$, and that $\{f_j\}_{j=1}^N$ is a dual frame to $\{g_j\}_{j=1}^N$. Then,

$$I_n = \sum_{j=1}^N f_j \otimes g_j, \tag{11}$$

where $I_n$ denotes the $n \times n$ identity matrix and $f \otimes g$ denotes the rank-one operator defined by $(f \otimes g)(x) = \langle x, g\rangle\, f\ \forall x \in \mathcal{H}_n$. Let $\{e_j\}_{j=1}^N$ be the standard orthonormal basis for $\mathcal{H}_N$ and $P$ be the orthogonal projection from $\mathcal{H}_N$ onto $K$. Let $h_j = Pe_j$. Then the range space of the analysis operator for $\{h_j\}_{j=1}^N$ is also $K$. Hence, by Proposition 2.6 in [16], we have that $\{g_j\}_{j=1}^N$ and $\{h_j\}_{j=1}^N$ are similar. I.e., there exists an invertible operator $A : K \to \mathcal{H}_n$ such that $g_j = Ah_j$ $(j = 1, \cdots, N)$. All we need to prove is that $A$ can be computed in terms of $\{h_j\}_{j=1}^N$ and $\{f_j\}$. Indeed, since

$$I_n = \sum_{j=1}^N f_j \otimes g_j = \sum_{j=1}^N f_j \otimes Ah_j = \left(\sum_{j=1}^N f_j \otimes h_j\right) A^*,$$

we get that $\sum_{j=1}^N f_j \otimes h_j$ is invertible, and so

$$A = \left(\sum_{j=1}^N h_j \otimes f_j\right)^{-1}.$$

Therefore we get $g_j = \left(\sum_{j=1}^N Pe_j \otimes f_j\right)^{-1} Pe_j$. □

From the above result we know that in order to protect the encoding frame, the range space of its analysis operator and a dual frame can not be simultaneously made available to the decoder. Since a dual frame must be given so that the receiver can reconstruct the signal after erasure recovery, we need to provide the decoder an erasure recovery matrix $M$ such that $\ker(M) \neq \Theta(\mathcal{H}_n)$ and a dual frame which is not the standard dual.

**Definition 3.5.** An $m$-erasure recovery matrix, $M$, for an encoding frame $\{g_j\}_{j=1}^N$ is called an *encoding frame protected $m$-erasure recovery matrix* if the range of the analysis operator, $\Theta$, for $\{g_j\}_{j=1}^N$ is a proper subspace of the kernel of $M$.

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004

**Remark 3.6.** Notice that by sending a signal, we are providing an eavesdropper, or the signal recipient with information on the range of the analysis operator, $\Theta_G$, for $\{g_j\}_{j=1}^N$. Thus, if the signal sender transmits too many ($\geq n$) signals, the encoding frame will be compromised. However, provided that fewer than $\min\{n, N-m-n\}$ signals are sent, if a receiver is provided with an erasure recovery matrix and a decoding frame, the encoding frame will remain protected. That is, if the signal recipient possesses a decoding frame $F = \{f_j\}_{j=1}^N$, an $m \times N$ erasure recovery matrix $M$, and receives $P < \min\{N-m-n, n\}$ messages $x_j = \Theta_F^* c_j$ for $1 \leq j \leq P$, then there are still infinitely many possibilities for the encoding frame, $G = \{g_j\}_{j=1}^N$. To see this, notice that the encoding frame must satisfy the following conditions:

(1) $M\Theta_G = 0$,
(2) $\Theta_F^* \Theta_G = I$, and
(3) $\Theta_G x_j = c_j$ for $1 \leq j \leq P$.

If we treat every entry of the analysis matrix for $G$, $\Theta_G$, as an unknown, then conditions (1), (2), and (3) make up a system of $nm + n^2 + nP = n(m+n+P)$ equations in $nN$ unknowns. Since we know that an encoding frame exists, we know that the system has a solution. Furthermore, since $P < N-m-n$, there are more unknowns than equations. Thus, under this condition there actually exist infinitely many possible choices for the encoding frame.

Definition 3.5 leads to the investigation of the existence and constructions of encoding frame protected $m$-erasure recovery matrices. Our main results in Sections 4 and 5 show that such matrices can be explicitly constructed and they form an open and dense subset in the set of all matrices which annihilate the range of $\Theta$.

## 4. Existence of erasure recovery matrices

In this section, we will give a necessary and sufficient condition for the existence of erasure recovery matrices, and prove that when this condition is satisfied, erasure recovery matrices exist in great abundance. We first point out a simple necessary condition for the existence of erasure recovery matrices.

**Lemma 4.1.** *Let $\{g_j\}_{j=1}^N$ be a frame for $\mathcal{H}_n$. If there exists an $m$-erasure recovery matrix, then $\{g_j\}_{j=1}^N$ satisfies the minimal redundancy condition for $m$ erasures. Moreover, if an $m$-erasure recovery matrix exists, then $m \leq N-n$.*

**Proof.** Since there exists an $m$-erasure recovery matrix $M$, it follows that every $f \in \mathcal{H}_n$ can be exactly reconstructed from $\{\langle f, g_j\rangle\}_{j\in\Lambda^c}$ whenever $|\Lambda| \leq m$. If there exists a subset $\Lambda$ such that $|\Lambda| = m$ and $\{g_j\}_{j\in\Lambda^c}$ is not a frame for $\mathcal{H}_n$, then there exists a non-zero vector $f \in \mathcal{H}_n$ such that $f \perp g_j$ for all $j \in \Lambda^c$. Let $c = (c_j)_{j=1}^N = \Theta(f)$. Then $c_j = 0$ for $j \in \Lambda^c$. Since every $m$-column vectors are linearly independent, we have that $c_j = 0$ for $j \in \Lambda$. Thus $\Theta(f) = 0$ and hence $f = 0$. This contradiction shows that every $N-m$ vectors in $\{g_j\}_{j=1}^N$ form a frame for $\mathcal{H}_n$.

For the moreover part, notice that since $\{g_j\}_{j=1}^{N-m}$ forms a frame, $\dim(\text{span}\{g_j\}_{j=1}^{N-m}) = n$. That is, $N-m \geq n$. Rearranging gives $m \leq N-n$. □

Lemma 4.1 tells us that the minimal redundancy condition for $m$ erasures is necessary for the existence of erasure recovery matrices. In what follows we show that this necessary condition is also sufficient. Moreover, there are many choices for $m$-erasure recovery matrices. Let $\{g_j\}_{j=1}^N$ be a frame for $\mathcal{H}_n$ and $m \leq N-n$. We define $\mathcal{M}_G$ to be the set of all sequences $\{h_j\}_{j=1}^N$ in $\mathcal{H}_m$ that are strongly disjoint to $\{g_j\}_{j=1}^N$. Then, $\mathcal{M}_G$ is a norm closed, convex subset of $\mathcal{H}_m^N = \bigoplus_{j=1}^N \mathcal{H}_m$ ($N$-copies of $\mathcal{H}_m$). We denote by $\tilde{\mathcal{M}}_G$ the set of all $\{h_j\}_{j=1}^N \in \mathcal{M}_G$ with spark $m+1$. Then every sequence in $\tilde{\mathcal{M}}_G$ is a frame for $\mathcal{H}_m$.

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004

**Theorem 4.2.** *Let $\{g_j\}_{j=1}^N$ be a frame for $\mathcal{H}_n$ that satisfies the minimal redundancy condition for $m$-erasures. Then the set $\tilde{\mathcal{M}}_G$ is open and dense in $\mathcal{M}_G$.*

The method of proof of this result is similar to Theorem 5.7 in [24] in that at no point will we actually construct an $m$-erasure matrix for a given analysis frame. Thus, this problem is different from Theorems 13 and 15 in [1] because they were able to provide an example of a full spark matrix (namely, the first $k$ rows of the $N \times N$ DFT matrix). However, once we obtain an existence result, it is easy to get Zariski density using their techniques.

For the proof of Theorem 4.2, we require a lemma.

**Lemma 4.3.** *Assume $\{g_j\}_{j=1}^N$ is a frame for $\mathcal{H}_n$, and $\Lambda$ satisfies the minimal redundancy condition with respect to $\{g_j\}_{j=1}^N$. If $\{h_j\}_{j\in\Lambda}$ spans $\mathcal{H}_m$, then $\{h_j\}_{j\in\Lambda}$ can be extended to a frame $\{h_j\}_{j=1}^N$ for $\mathcal{H}_m$ that is strongly disjoint with respect to $\{g_j\}_{j=1}^N$.*

**Proof.** Since $\Lambda$ satisfies the minimal redundancy property with respect to $\{g_j\}_{j=1}^N$, for each $j \in \Lambda$, we can find scalars $c_\ell^{(j)} \in \mathbb{C}$ so that

$$g_j = \sum_{\ell\in\Lambda^c} c_\ell^{(j)} g_\ell.$$

For $\ell \in \Lambda^c$, let

$$h_\ell = -\sum_{j\in\Lambda} \overline{c_\ell^{(j)}} h_j.$$

Then,

$$\begin{aligned}
\sum_{j=1}^N g_j \otimes h_j &= \sum_{j\in\Lambda} g_j \otimes h_j + \sum_{\ell\in\Lambda^c} g_\ell \otimes h_\ell \\
&= \sum_{j\in\Lambda} \left( \sum_{\ell\in\Lambda^c} c_\ell^{(j)} g_\ell \right) \otimes h_j \\
&\quad + \sum_{\ell\in\Lambda^c} g_\ell \otimes \left( -\sum_{j\in\Lambda} \overline{c_\ell^{(j)}} h_j \right) \\
&= \sum_{j\in\Lambda} \sum_{\ell\in\Lambda^c} c_\ell^{(j)} g_\ell \otimes h_j - \sum_{\ell\in\Lambda^c} \sum_{j\in\Lambda} c_\ell^{(j)} g_\ell \otimes h_j \\
&= 0.
\end{aligned}$$

Therefore $\{h_j\}_{j=1}^N$ is strongly disjoint with respect to $F$. □

**Corollary 4.4.** *Let $\{g_j\}_{j=1}^N$ be a frame for $\mathcal{H}_n$ satisfying the minimal redundancy condition for $m$-erasures. For each $\Lambda \subset \{1, 2, \cdots, N\}$ satisfying $|\Lambda| = m$, let $\tilde{\mathcal{M}}_G^\Lambda$ denote the set of frames $\{h_j\}_{j=1}^N$ in $\mathcal{M}_G$ for which $\{h_j\}_{j\in\Lambda}$ is a linearly independent set. Then $\tilde{\mathcal{M}}_G^\Lambda$ is non-empty.*

**Proof.** Since $|\Lambda| = m \leq N - n$, $\Lambda$ satisfies the minimal redundancy condition with respect to $\{g_j\}_{j=1}^N$. Let $\{h_j\}_{j\in\Lambda}$ be a basis for $\mathcal{H}_m$. Then by the previous lemma, $\{h_j\}_{j\in\Lambda}$ can be extended to a frame $\{h_j\}_{j=1}^N$ that is strongly disjoint with respect to $\{g_j\}_{j=1}^N$. Since $\{h_j\}_{j\in\Lambda}$ is a linearly independent set, $\{h_j\}_{j=1}^N \in \tilde{\mathcal{M}}_G^\Lambda$. □

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004

**Proof of Theorem 4.2.** Let $\Gamma = \{\Lambda \subset \{1, 2, \cdots, N\} : |\Lambda| = m\}$. Then,

$$\tilde{\mathcal{M}}_G = \cap_{\Lambda\in\Gamma}\tilde{\mathcal{M}}_G^{\Lambda}. \tag{12}$$

We proceed by showing that each $\tilde{\mathcal{M}}_G^{\Lambda}$ is an open and dense set.

To show that $\tilde{\mathcal{M}}_G^{\Lambda}$ is open, first define the continuous mapping $\gamma_\Lambda : \tilde{\mathcal{M}}_G \to \mathbb{C}^{m\times m}$ defined by

$$\gamma_\Lambda(\{h_j\}_{j=1}^N) = \begin{pmatrix} | & | & & | \\ h_{j_1} & h_{j_2} & \cdots & h_{j_m} \\ | & | & & | \end{pmatrix}$$

where $\Lambda = \{j_\ell\}_{\ell=1}^m$. Since $\tilde{\mathcal{M}}_G^{\Lambda} = \gamma_\Lambda^{-1}(\det^{-1}(\mathbb{C}\setminus\{0\}))$, $\tilde{\mathcal{M}}_G^{\Lambda}$ is open.

To show that $\tilde{\mathcal{M}}_G^{\Lambda}$ is dense, assume $\{h_j^{(0)}\}_{j=1}^N \in \mathcal{M}_G \setminus \tilde{\mathcal{M}}_G^{\Lambda}$. Let $\epsilon > 0$. Since $\tilde{\mathcal{M}}_G^{\Lambda}$ is non-empty, we can find a $\{h_j^{(1)}\}_{j=1}^N \in \tilde{\mathcal{M}}_G^{\Lambda}$. Let $h_j^{(t)} = (1-t)h_j^{(0)} + h_j^{(1)}$. By convexity, $\{h_j^{(t)}\}_{j=1}^N \in \mathcal{M}_G$. Note that $p(t) = \det(\gamma_\Lambda(\{h_j^{(t)}\}_{j=1}^N))$ is a polynomial. Since $\{h_j^{(1)}\}_{j=1}^N \in \tilde{\mathcal{M}}_G^{\Lambda}$, $p(1) \neq 0$. Since $p$ has only finitely many zeros, we can find $t_0$ so small that $\|\{h_j^{(t_0)}\}_{j=1}^N - \{h_j^{(0)}\}_{j=1}^N\| < \epsilon$, and $p(t_0) \neq 0$. Since $p(t_0) \neq 0$, $\{h_j^{(t_0)}\}_{j=1}^N \in \tilde{\mathcal{M}}_G^{\Lambda}$. Therefore, $\tilde{\mathcal{M}}_G^{\Lambda}$ is dense in $\mathcal{M}_G$.

Therefore, $\tilde{\mathcal{M}}_G$ is dense in $\mathcal{M}_G$ since the intersection of a finite collection of open dense subsets in a metric space is open and dense. □

From Lemma 4.1 we know that the condition $N - m \geq n$ is needed in order for an $m$-erasure recovery matrix $M$ to exist. Note that an $m$-erasure recovery matrix $M$ of size $m \times N$ has full rank. We get that $\dim(\ker(M)) = N-m$. Thus the condition $n < N-m$ is necessary for the existence of $m$-erasure matrices $M$ for a frame $\{g_j\}_{j=1}^N$ such that $\ker(M) \supsetneq \Theta(\mathcal{H}_n)$. Theorem 4.2 tells us that this is also sufficient if $\{g_j\}_{j=1}^N$ satisfies the minimal redundancy condition for $m$-erasures. Therefore we get the following:

**Theorem 4.5.** *Let $\{g_j\}_{j=1}^N$ be a frame for $\mathcal{H}_n$. Then there exists an encoding frame protected $m$-erasure recovery matrix if and only if $\{g_j\}_{j=1}^N$ satisfies the minimal redundancy condition for $m$-erasures and $n < N - m$.*

## 5. Constructions of erasure recovery matrices

While erasure recovery matrices for a fixed frame are abundant from Theorem 4.2, the theorem and its proof do not provide any constructions of such frames. In this section we will present several algorithms for the construction of strongly disjoint frame pairs $\{g_j, h_j\}_{j=1}^N$ with $M = [h_1, \cdots, h_N]$ serving as the erasure recovery matrix for $\{g_j\}_{j=1}^N$.

For the first construction, we need the following result due to Bodmann, Casazza, Paulsen, and Speegle (cf. [3]).

**Lemma 5.1.** *Let $\{g_j\}_{j=1}^N$ be a frame for $\mathcal{H}_n$ and $\Theta$ be its analysis operator. Set $h_j = P^\perp e_j$, where $P$ is the orthogonal projection from $\mathcal{H}_N$ onto $\Theta(\mathcal{H}_n)$ and $\{e_j\}_{i=1}^N$ is the standard orthonormal basis for $\mathcal{H}_N$. Then $G$ satisfies the minimal redundancy condition for $m$-erasures if and only if $\{h_j\}_{i=1}^N$ has spark $m+1$.*

Now we are ready to present the first construction procedure for strongly disjoint frame pairs $\{g_j, h_j\}_{j=1}^N$ based on Lemma 5.1.

**Construction Algorithm 1.**

**Step 1.** *Generate an $m \times N$ matrix $M_0$ whose entries are drawn independently from the standard normal distribution, and let $M = \frac{1}{\sqrt{m}}M_0 = [h_1, \cdots, h_N]$.*

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004

**Step 2.** *Compute the orthogonal projection $P$ for the range space of the analysis operator for $\{h_j\}_{j=1}^N$, and let $\tilde{g}_j = P^\perp e_j = (I_N - P)e_j$ for $j = 1, \cdots, N$.*

**Step 3.** *Generate an $n \times N$ matrix $T$ whose entries are drawn independently from the standard normal distribution.*

**Step 4.** *Let $g_j = T\tilde{g}_j$.*

**Proposition 5.2.** *Assume that $m \leq N - n$, and $G$, $M$, $P$, and $T$ are constructed as in Construction Algorithm 1. If $M$ has full spark, and $T$ maps Range$(P^\perp)$ onto $\mathcal{H}_n$, then $M$ is an erasure recovery matrix for $\{g_j\}_{j=1}^N$. Moreover, $\{g_j\}_{j=1}^N$ satisfies the minimal redundancy condition for $m$ erasures, and if $m < N - n$, $M$ is an encoding frame protected $m$-erasure recovery matrix.*

**Proof.** Since $T$ is surjective, $\{g_j\}_{j=1}^N$ is a frame. We have

$$\sum_{j=1}^N g_j \otimes h_j = \sum_{j=1}^N TP^\perp e_j \otimes h_j = TP^\perp \sum_{j=1}^N e_j \otimes h_j$$
$$= TP^\perp \Theta_H = 0$$

where $\Theta_H$ denotes the analysis operator for $\{h_j\}_{j=1}^N$. Furthermore, since $M$ has full spark, $M$ is an $m$-erasure recovery matrix for $\{g_j\}_{j=1}^N$.

From Lemma 4.1, we know that $\{g_j\}_{j=1}^N$ satisfies the minimal redundancy condition for $m$ erasures.

If $m < N-n$, then $\dim(\ker M) = N - m > n$. Hence, $\Theta_G(\mathcal{H}_n)$ is properly contained in $\ker M$. Therefore, $M$ is an encoding frame protected $m$-erasure recovery matrix. □

**Remark 5.3.** In practice, the conditions on $M$ and $T$ are always satisfied. In [1], Alexeev, Cahill, and Mixon proved that the set of $m \times N$ full spark matrices is open and dense in the set of all $n \times N$ matrices. Furthermore, any matrix $T$ will map the range of $P^\perp$ onto $\mathcal{H}_n$ with probability 1 since $N - m \geq n$.

The next construction is useful because it provides robustness to signal noise, which is the main subject of the next section.

**Construction Algorithm 2.**

**Step 1.** *Generate an $m \times N$ matrix $M_0$ whose entries are drawn independently from the standard normal distribution, and let $M = \frac{1}{\sqrt{m}} M_0 = [h_1, \cdots, h_N]$.*

**Step 2.** *Let $A$ be an $N \times (m + n)$ matrix whose first $m$ columns are the rows of $M$, and the rest of the entries are selected independently according to the standard normal distribution.*

**Step 3.** *Let $Q$ be the matrix obtained by performing the Gram-Schmidt orthonormalization procedure to the columns of $A$.*

**Step 4.** *Let $G = F$ be the $n \times N$ matrix whose rows are made up of columns $m + 1$ through $m + n$ of $Q$.*

**Proposition 5.4.** *Assume $m \leq N - n$, and $A$, $G$, and $M$ are as constructed in Construction Algorithm 2. If $M$ has full spark and $A$ has full rank, then $M$ is an $m$-erasure recovery matrix for the Parseval frame $\{g_j\}_{j=1}^N$.*

**Proof.** Since $A$ has orthonormal columns, $GG^* = I_n$. Thus, $\{g_j\}_{j=1}^N$ is a Parseval frame. By the Gram-Schmidt orthonormalization procedure, the rows of $M$ are orthogonal to the rows of $G$. Thus, $MG^* = M\Theta_G = 0$. Thus, $M$ is an $m$-erasure recovery matrix for $\{g_j\}_{j=1}^N$. □

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004

While Construction Algorithm 2 does not provide protection for the encoding frame because the encoding frame is a Parseval frame, an encoding frame protected $m$-erasure recovery matrix can be obtained by extending Construction Algorithm 2 to give a non-standard dual frame pair. This is provided by Construction Algorithm 3 below.

**Construction Algorithm 3.**

**Step 1.** *Generate an $m \times N$ matrix $M_0$ whose entries are drawn independently from the standard normal distribution, and let $M = \frac{1}{\sqrt{m}} M_0 = [h_1, \cdots, h_N]$.*
**Step 2.** *Let $A$ be an $N \times (m + 2n)$ matrix whose first $m$ columns are the rows of $M$, and the rest of the entries are selected independently according to the standard normal distribution.*
**Step 3.** *Let $Q$ be the matrix obtained by performing the Gram-Schmidt orthonormalization procedure to the columns of $A$.*
**Step 4.** *Let $F$ be the $n \times N$ matrix whose rows are made up of columns $m + 1$ through $m + n$ of $Q$.*
**Step 5.** *Let $K$ be the $n \times N$ matrix whose rows are made up of columns $m + n + 1$ through $m + 2n$ of $Q$.*
**Step 6.** *Let $G = F + K$.*

**Proposition 5.5.** *Assume $m \leq N - 2n$, and $M$, $F$, and $G$ are as in Construction Algorithm 2. If $M$ has full spark and $A$ has full rank, then $M$ is an encoding frame protected $m$-erasure recovery matrix for $\{g_j\}_{j=1}^N$.*

**Proof.** As in the proof of Proposition 5.4, $M$ is an $m$-erasure recovery matrix for the Parseval frames $F$ and $K$. Thus

$$M\Theta_G = M\left(\Theta_F + \Theta_K\right) = MF^* + MK^* = 0 + 0 = 0.$$

Therefore, $M$ is an $m$-erasure recovery matrix for $\{g_j\}_{j=1}^N$. Furthermore, since $A$ has full rank, $m < N - n$, and as in the proof of Proposition 5.2, $M$ is also an encoding frame protected $m$-erasure recovery matrix. □

**Remark 5.6.**

(1) As with Proposition 5.2, the hypotheses of Propositions 5.4 and 5.5 are almost always satisfied for random matrices.
(2) Using Matlab, we recommend the qr-decomposition of the matrix $A$ instead of implementing the classical Gram-Schmidt orthonormalization procedure, for the sake of stability. To save time, we also recommend that the "economy-sized" qr-decomposition be used ($qr(A, 0)$ in Matlab).
(3) To ensure greater privacy, Construction Algorithm 3 could be modified so that the encoder is given by $G = F + \alpha K$ for $\alpha > 1$. This way, the encoding device is further from the decoder. However this comes at the expense of a less stable reconstruction (see Remark 6.6).

## 6. Noise mitigation

Let $M$ be an encoding frame protected $m$-erasure recovery matrix for an encoding frame $\{g_j\}_{j=1}^N$ for $\mathcal{H}_n$, and let $\{f_j\}_{j=1}^N$ be a dual frame to $\{g_j\}_{j=1}^N$. Assume $\Lambda$ is an erasure set. For a given set $\Gamma \subset \{1, 2, \cdots, N\}$, let $M_\Gamma$ denote the minor of $M$ consisting of the columns indexed by $\Gamma$. For a fixed signal $f \in \mathcal{H}_n$, let $c_j = \langle f, g_j \rangle$, $c = (c_j)_{j=1}^N$, and $c_\Gamma = (c_j)_{j \in \Gamma}$. Then from equation (10), we have:

$$c_\Lambda = -(M_\Lambda^* M_\Lambda)^{-1} M_\Lambda^* M_{\Lambda^c} c_{\Lambda^c}. \tag{13}$$

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004

In this section, we would like to know what happens to our reconstruction when the frame coefficients indexed by $\Lambda^c$ are subject to additive channel noise. Since our reconstruction operator $\Delta : \mathcal{H}_{(N-|\Lambda|)} \to \mathcal{H}_{|\Lambda|}$ defined by

$$\Delta c = -(M_\Lambda^* M_\Lambda)^{-1} M_\Lambda^* M_{\Lambda^c} c \tag{14}$$

is linear, if we introduce a noise term $\epsilon = (\epsilon_j)_{j\in\Lambda^c}$ to the good coefficients, the corresponding error in the reconstructed coefficients is given by

$$\Delta\epsilon = -(M_\Lambda^* M_\Lambda)^{-1} M_\Lambda^* M_{\Lambda^c} \epsilon. \tag{15}$$

Thus, if $\|\epsilon\|$ or $\|\Delta\|$ is large, the reconstructed signal will be highly inaccurate. However, we will see that this is not the case for this situation when we use Construction Algorithms 2 and 3. The next lemma shows that if $M$ satisfies the Restricted Isometry Property and $\epsilon$ is sparse, then the error in the coefficients is only slightly amplified.

**Remark 6.1.**

(1) This sparse noise model was motivated by [6]. In that paper, a similar model for erasure reconstruction was given. Assume that a signal recipient receives the frame coefficients, $c = (\langle f, g_j\rangle)_{j=1}^N$ plus a sparse additive noise term, $\alpha$ (here $\alpha$ may represent either noise, or erasures). Their method uses a linear program to reconstruct the noise term, $\alpha$. Since $c \in \ker(M)$, $M(c+\alpha) = M\alpha$. Since $c+\alpha$ and $M$ are known, to determine the additive noise term, $\alpha$ they consider the minimization problem:

$$\text{argmin}\|\alpha\|_0 \quad \text{subject to} \quad M\alpha = M(c+\alpha),$$

where $\|\alpha\|_0$ denotes the number of non-zero entries of $\alpha$. However, this combinatorial problem is quite slow, so they solve the equivalent convex optimization problem instead:

$$\text{argmin}\|\alpha\|_1 \quad \text{subject to} \quad M\alpha = M(c+\alpha),$$

which is much faster.

(2) In [12] classes of frames for which the amplification of additive channel noise was small were discussed. However, their analysis was for a different reconstruction which requires an $n \times n$ matrix inversion. Frames which had small error amplification factors were called *NERFs*, or *Numerically Erasure-Robust Frames*.

**Lemma 6.2.** *Assume that $\{g_j\}_{j=1}^N$ is a frame for $\mathcal{H}_n$ and $M$ is a $k \times N$ encoding frame protected $m$-erasure recovery matrix for $\{g_j\}_{j=1}^N$ which satisfies the Restricted Isometry Property of order $s$ with constant $\delta_s$. If $\epsilon$ is $s$-sparse, $|\Lambda| \le s$, and $\Delta$ is the reconstruction operator as defined in equation (14), then,*

$$\|\Delta\epsilon\| \le \frac{1+\delta_s}{1-\delta_s}\|\epsilon\|. \tag{16}$$

**Proof.** From equation (15), we have

$$\|\Delta\epsilon\| \le \|(M_\Lambda^* M_\Lambda)^{-1}\|\|M_\Lambda\|\|M_\Lambda^c \epsilon\|. \tag{17}$$

Since $|\Lambda| \le s$, using the restricted isometry property, whenever $\|x\| = 1$, we get

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004

$$\langle M_\Lambda^* M_\Lambda x, x\rangle = \|M_\Lambda x\|^2 \geq 1 - \delta_s.$$

Thus,

$$\min \sigma(M_\Lambda^* M_\Lambda) \geq 1 - \delta_s,$$

where $\sigma(M_\Lambda^* M_\Lambda)$ denotes the spectrum of $M_\Lambda^* M_\Lambda$. Therefore

$$\|(M_\Lambda^* M_\Lambda)^{-1}\| = \frac{1}{\min \sigma(M_\Lambda^* M_\Lambda)} \leq \frac{1}{1-\delta_s}. \tag{18}$$

Again, since $|\Lambda| \leq s$ the restricted isometry property gives

$$\|M_\Lambda\| \leq \sqrt{1+\delta_s}. \tag{19}$$

Since $\epsilon$ is $s$-sparse, the restricted isometry property yields

$$\|M_{\Lambda^c}\epsilon\| \leq \sqrt{1+\delta_s}\|\epsilon\|. \tag{20}$$

Combining equations (17), (18), (19), and (20) gives the result. □

The previous lemma gave a bound on the error of the frame coefficients. Next we will build on this error estimate for the reconstruction of a signal $f \in \mathcal{H}_n$. Recall that if $\{f_j\}_{j=1}^N$ is a dual frame to $\{g_j\}_{j=1}^N$, then

$$f = \sum_{j=1}^N \langle f, g_j\rangle\, f_j = \sum_{j=1}^N c_j f_j \quad \forall f \in \mathcal{H}, \tag{21}$$

where $c_j = \langle f, g_j\rangle$ for all $j \in \{1, \cdots, N\}$. If the coefficients indexed by an erasure set $\Lambda$ are erased, and the coefficients indexed by $\Lambda^c$ are subject to an additive noise term, given by $\epsilon$, then the corresponding error in the reconstruction of the erased coefficients is $\Delta\epsilon$. Thus the reconstructed signal, after synthesizing with $\{f_j\}_{j=1}^N$ is

$$\tilde{f} = \sum_{j\in\Lambda}(c_j + (\Delta\epsilon)_j)f_j + \sum_{j\in\Lambda^c}(c_j+\epsilon_j)f_j = f + \sum_{j\in\Lambda}(\Delta\epsilon)_j f_j + \sum_{j\in\Lambda^c}\epsilon_j f_j. \tag{22}$$

The following lemma gives a bound on the reconstruction error, $\|f - \tilde{f}\|$.

**Lemma 6.3.** *Assume that $\{f_j\}_{j=1}^N$ is a Parseval dual frame to $\{g_j\}_{j=1}^N$, and that $M$ is a $k \times N$ encoding frame protected $m$-erasure recovery matrix for $\{g_j\}_{j=1}^N$ which satisfies the RIP of order $s$ with constant $\delta_s$. Suppose $|\Lambda| \leq s$, $\epsilon$ is $s$-sparse, and let $f$ and $\tilde{f}$ be defined as in equation (22). Then,*

$$\|f - \tilde{f}\| \leq \frac{2}{1-\delta_s}\|\epsilon\|. \tag{23}$$

**Proof.** From equation (22),

$$\|f - \tilde{f}\| = \left\|\sum_{j\in\Lambda}(\Delta\epsilon)_j f_j + \sum_{j\in\Lambda^c}\epsilon_j f_j\right\| = \|F_\Lambda \Delta\epsilon + F_{\Lambda^c}\epsilon\| \leq \|F_\Lambda\Delta\epsilon\| + \|F_{\Lambda^c}\epsilon\|$$
$$\leq \|\Delta\epsilon\| + \|\epsilon\| \leq \left(\frac{1+\delta_s}{1-\delta_s} + 1\right)\|\epsilon\| = \frac{2}{1-\delta_s}\|\epsilon\|. \quad \square$$

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004

**Remark 6.4.** If we replace the condition that $\{f_j\}_{j=1}^N$ is a Parseval frame with the condition that $\{f_j\}_{j=1}^N$ has an upper frame bound of $B$, then it is easy to see that the error bound in equation (23) becomes

$$\|f - \tilde{f}\| \leq \frac{2\sqrt{B}}{1-\delta_s}\|\epsilon\|.$$

With Lemma 6.3 in mind, it should be fairly clear why Construction Algorithms 2 and 3 work well. In those algorithms, since $F$ is Parseval, and $M$ is a standard normally distributed random matrix, $M$ will satisfy the Restricted Isometry Property with good constants.

By combining the results from this section with Construction Algorithm 2 or 3 and the RIP for Gaussian random matrices into one we get the following theorem. The theorem tells us that with high probability, our reconstruction scheme will not amplify noise, provided $m$ is $\mathcal{O}\left(s \ln\left(\frac{N}{s}\right)\right)$.

**Theorem 6.5.** *Assume that $F$ and $M$ are constructed using Construction Algorithm 2 or 3, where*

$$m \geq \frac{C}{\delta^2}\left(s \ln\left(\frac{eN}{s}\right) + \ln\left(\frac{2}{\gamma}\right)\right) \tag{24}$$

*for $\delta, \gamma \in (0,1)$, and $C$ is the universal constant in the proof of the restricted isometry property for Gaussian random matrices. Then with probability at least $1-\gamma$, for any $s$-sparse vector $x \in \mathcal{H}_N$,*

$$(1-\delta)\|x\|^2 \leq \|Mx\|^2 \leq (1+\delta)\|x\|^2.$$

*Moreover, for $f$, $\tilde{f}$, and $\epsilon$ defined as in Lemma 6.3,*

$$\|f - \tilde{f}\| \leq \frac{2}{1-\delta}\|\epsilon\|, \tag{25}$$

*with probability greater than $1-\gamma$.*

**Remark 6.6.** Both Construction Algorithm 2 and 3 start by specifying an erasure recovery matrix, after which the RIP constant for the erasure recovery matrix is fixed. Thus, they should have roughly the same error bound. However, the frame expansion

$$f = \sum_{j=1}^{N} \langle f, g_j \rangle f_j$$

is more stable for Construction Algorithm 2 since we are encoding with the standard dual, which is known to minimize the $\ell^2$ norm of the coefficient sequence $(\langle f, g_j \rangle)_{j=1}^N$. Thus, there is a tradeoff between Construction Algorithm 2 which is more stable, and Construction Algorithm 3 which protects the encoding frame.

In the next section, we will experimentally illustrate that Theorem 6.5 is satisfied. Moreover, we will give evidence that our reconstruction method may not amplify normally distributed random noise, even if the noise term is not necessarily sparse.

## 7. Numerical results

Our first three experiments were designed to examine the effects of noise on our erasure reconstruction. In particular, we wanted to assure in these experiments that additive noise introduced in the frame coefficients indexed by $\Lambda^c$ was not heavily amplified by our reconstruction process, backing up our results in Section 6. Each experiment corresponds to one of the Construction Algorithms in Section 5. For each experiment, we

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004


**Fig. 1.** Noise amplification for Construction Algorithm 1.

used frames of length 1000 for $\mathbb{R}^{250}$ with erasure recovery matrices of size $250 \times 1000$. We ran 50 trials for each erasure set size, for erasure set sizes of $|\Lambda| = 10, 20, 30, \cdots, 250$. The trials for each experiment were run simultaneously so that the same erasure recovery matrix was used for each construction algorithm. Similarly, the experiments corresponding to Construction Algorithms 2 and 3 share a synthesis (or decoding) frame. For each trial, new frames and erasure recovery matrices were generated by using the construction algorithms in Section 5. In each trial, we generated a standard normally distributed random vector $f \in \mathbb{R}^{250}$ (the same vector was used for each construction algorithm) and added a 5% additive normally distributed random noise term to the frame coefficients indexed by $\Lambda^c$. By 5% noise, we mean that the norm of the noise term, $\epsilon$, was 5% of the norm of the frame coefficients indexed by $\Lambda^c$. The noise terms for each trial were the same for each construction algorithm, up to a scalar multiple (to obtain the correct noise percentage). The plot shows all 50 trials for each erasure set size with the exception of $|\Lambda| = 250$. These data points were omitted to avoid distortion in the plot. The $\times$'s denote $\|f - \tilde{f}_R\|$, and the $+$'s denote $\|f - \tilde{f}\|$, where $\tilde{f}_R = \sum_{j \in \Lambda^c} (\langle f, g_j \rangle + \epsilon_j) f_j$ and $\tilde{f}$ is as in Section 6. That is, $\tilde{f}_R$ is a noisy partial reconstruction, and $\tilde{f}$ is the signal obtained after performing our reconstruction algorithm on the noisy and erased data set. For more details on these experiments, see the attached reproducible file.

**Remark 7.1.** It is important to note that 5% channel noise does not necessarily lead to 5% reconstruction error. In fact after synthesis with a Parseval frame, this error frequently shrinks. This is why the reconstruction errors in the following graphs tend to drop below .05 for unit norm signals. Use of a filter may further reduce this noise.

Even though there was no noise analysis in Section 6 for Construction Algorithm 1, Fig. 1 still suggests that this construction is stable. It is also important to note that in Fig. 1, we used the standard dual to the analysis (or encoding) frame. If a different dual were used, we would expect to see a less stable reconstruction.

In Fig. 2 we see a slight improvement over Fig. 1 in terms of stability to noise. In Fig. 3 we see a decline in stability, however, this is because we are not using the standard dual as the encoder (cf. Remark 6.6). In fact we are using the sum of the standard dual and a Parseval frame which is strongly disjoint with respect to the decoder.

In each of the figures, $\tilde{f}$ is a better approximation of $f$ than $\tilde{f}_R$ is, except for the extreme case $|\Lambda| = 250$. This data backs up our results in Section 6. We note that the mathematical theory is not as strong as the

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004


**Fig. 2.** Noise amplification for Construction Algorithm 2.


**Fig. 3.** Noise amplification for Construction Algorithm 3.

experiments seem to suggest for two reasons. The first reason is because we are using normally distributed random noise as opposed to sparse noise in the experiments. The second reason is that $|\Lambda| \ln(\frac{N}{|\Lambda|})$ is larger than $m = 250$ for $|\Lambda| > 117$. However, even for larger values of $|\Lambda|$, we still get relatively little noise amplification.

In Table 1, we list the averages of $\|f - \tilde{f}_R\|$ and $\|f - \tilde{f}\|$ for each set of 50 trials. It is also useful to note that the maximal reconstruction errors for $|\Lambda| = 250$ were 7.0725 for Construction Algorithm 1, 5.3486 for Construction Algorithm 2, and 7.5135 for Construction Algorithm 3.

Fig. 4 is a comparison of our algorithms with the $\ell^1$ minimization algorithm from the article [6] as described in Remark 6.1, as well as a variation of $\ell^1$ minimization suggested by one of our referees. To reconstruct the noise term (in this case erasures and noise), $\alpha$, we solve the quadratically constrained basis pursuit problem (cf. [13]):

$$\tilde{\alpha} = \text{argmin}\|z\|_{\ell^1} \quad \text{subject to} \quad \|Mz - b\|_{\ell^2} < \delta, \tag{26}$$

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004

**Table 1**
Table of average reconstruction errors.

| | Algorithm 1 | | Algorithm 2 | | Algorithm 3 | |
|---|---|---|---|---|---|---|
| $\lvert\Lambda\rvert$ | $\lVert f-\tilde{f}\rVert$ | $\lVert f-\tilde{f}_R\rVert$ | $\lVert f-\tilde{f}\rVert$ | $\lVert f-\tilde{f}_R\rVert$ | $\lVert f-\tilde{f}\rVert$ | $\lVert f-\tilde{f}_R\rVert$ |
| 10 | 0.0317 | 0.0655 | 0.0256 | 0.0557 | 0.0362 | 0.0780 |
| 20 | 0.0329 | 0.0928 | 0.0266 | 0.0776 | 0.0377 | 0.1063 |
| 30 | 0.0329 | 0.1104 | 0.0269 | 0.0929 | 0.0381 | 0.1290 |
| 40 | 0.0340 | 0.1298 | 0.0277 | 0.1107 | 0.0392 | 0.1464 |
| 50 | 0.0355 | 0.1461 | 0.0286 | 0.1232 | 0.0405 | 0.1672 |
| 60 | 0.0357 | 0.1588 | 0.0293 | 0.1345 | 0.0415 | 0.1796 |
| 70 | 0.0371 | 0.1751 | 0.0302 | 0.1489 | 0.0427 | 0.1977 |
| 80 | 0.0380 | 0.1889 | 0.0315 | 0.1572 | 0.0445 | 0.2106 |
| 90 | 0.0392 | 0.2003 | 0.0321 | 0.1684 | 0.0454 | 0.2204 |
| 100 | 0.0403 | 0.2136 | 0.0332 | 0.1792 | 0.0469 | 0.2346 |
| 110 | 0.0424 | 0.2195 | 0.0343 | 0.1931 | 0.0485 | 0.2514 |
| 120 | 0.0446 | 0.2389 | 0.0359 | 0.2061 | 0.0507 | 0.2636 |
| 130 | 0.0460 | 0.2430 | 0.0380 | 0.2131 | 0.0537 | 0.2733 |
| 140 | 0.0486 | 0.2554 | 0.0394 | 0.2284 | 0.0559 | 0.2845 |
| 150 | 0.0507 | 0.2673 | 0.0412 | 0.2340 | 0.0583 | 0.2935 |
| 160 | 0.0521 | 0.2777 | 0.0427 | 0.2451 | 0.0604 | 0.3078 |
| 170 | 0.0561 | 0.2854 | 0.0464 | 0.2544 | 0.0657 | 0.3189 |
| 180 | 0.0592 | 0.2993 | 0.0483 | 0.2650 | 0.0682 | 0.3292 |
| 190 | 0.0634 | 0.3071 | 0.0525 | 0.2733 | 0.0741 | 0.3368 |
| 200 | 0.0715 | 0.3160 | 0.0588 | 0.2811 | 0.0832 | 0.3461 |
| 210 | 0.0801 | 0.3275 | 0.0651 | 0.2938 | 0.0920 | 0.3586 |
| 220 | 0.0934 | 0.3327 | 0.0764 | 0.3025 | 0.1082 | 0.3661 |
| 230 | 0.1148 | 0.3410 | 0.0941 | 0.3093 | 0.1328 | 0.3751 |
| 240 | 0.1527 | 0.3527 | 0.1262 | 0.3256 | 0.1778 | 0.3938 |
| 250 | 1.1241 | 0.3666 | 0.9261 | 0.3283 | 1.3049 | 0.3948 |

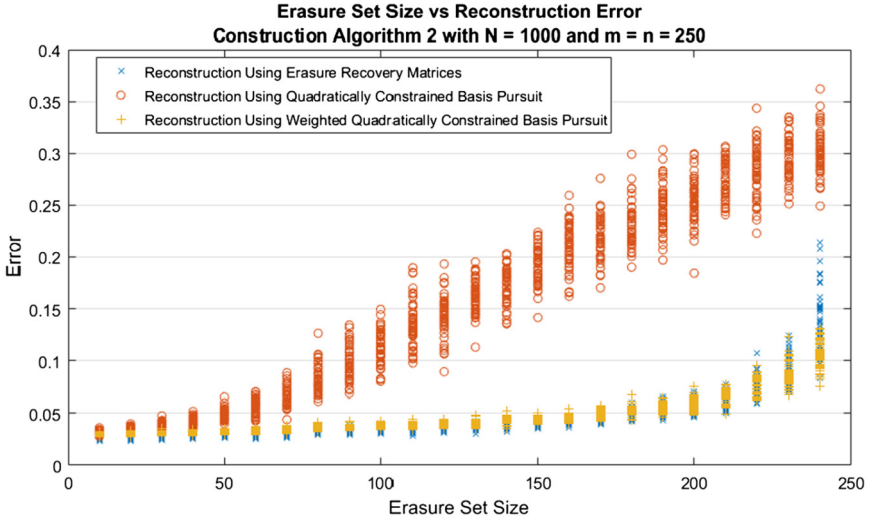


**Fig. 4.** Noise amplification comparison for Construction Algorithm 2 using erasure recovery matrices, $\ell^1$ minimization, and weighted $\ell^1$ minimization.

where $M$ denotes the erasure recovery matrix, $b$ denotes the frame coefficients subject to both noise and erasures, and $\delta$ denotes the noise level. We denote the result of the minimization procedure as $\tilde{\alpha}$ because it is only an approximation of the true erased coefficients, subject to noise, $\alpha$.

The variation of $\ell^1$ minimization suggested by our referee uses the knowledge of the erasure set, $\Lambda$, to give a more accurate approximation of the noise term, $\alpha$, by penalizing noise terms with the wrong support. To approximate $\alpha$, we solve the following minimization problem:

$$\tilde{\alpha} = \operatorname{argmin} \sum_{j=1}^{N} w_j |z_j| \quad \text{subject to} \quad \|Mz - b\|_{\ell^2} < \delta, \tag{27}$$

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004

where $w_j = 1$ for $j \in \Lambda$, and $w_j = \kappa$ for $j \in \Lambda^c$, where $\kappa > 1$ is some penalty factor. Both $\delta$ and $b$ are the same as the regular, unweighted $\ell^1$ minimization problem above. For the following experiment, we used $\kappa = 1000$. This constant was selected because larger penalty factors did not seem to provide significantly smaller error terms.

For both $\ell^1$ minimization algorithms, we used the software provided within the yall1 (Your Algorithms for $L^1$) toolbox for Matlab, with a tolerance level set to $10^{-3}$ (cf. [38]). The plot shows the reconstruction errors for various erasure set sizes using erasure recovery matrices (as denoted by $\times$'s), $\ell^1$ minimization (as denoted by $o$'s), and weighted $\ell^1$ minimization (as denoted by $+$'s). To create the figure, we used Construction Algorithm 2 to create frames of length $N = 1000$ for $\mathbb{R}^{250}$ with an erasure recovery matrix of height $m = 250$. We performed 50 trials for erasure set sizes of $10, 20, 30, \cdots, 240$. For each trial new frames and erasure recovery matrices were used. As with the first three experiments, for each trial, we generated a standard normally distributed random vector $f \in \mathbb{R}^{250}$ and added a 5% additive normally distributed random noise to the frame coefficients indexed by $\Lambda^c$.

Fig. 4 shows that our reconstruction procedure as well as weighted $\ell^1$ minimization both outperform $\ell^1$ minimization. For smaller erasure set sizes, erasure recovery matrices outperform weighted $\ell^1$ minimization. However, for larger erasure set sizes, weighted $\ell^1$ minimization outperforms erasure recovery matrices. In general, erasure recovery matrices also seem to perform the reconstruction procedure faster than $\ell^1$ minimization. However, the erasure recovery matrix algorithm and weighted $\ell^1$ minimization are not a suitable replacement for the unweighted $\ell^1$ minimization algorithm if the erasure set is unknown. We thank one of our referees for suggesting the inclusion of these comparisons.

The figures for the next set of experiments are given in Appendix A. These results were provided to give a visualization of the previous set of experiments. For each experiment, we compressed a $256 \times 256$ pixel image (Mandrill). To perform the compression, we simply erased 80% of the least significant fast Fourier coefficients. Thus, the compressed images lies in $\mathbb{C}^n$ for $n = 13107$. Each experiment corresponds to one of the construction algorithms in Section 5. For each algorithm, we used the same erasure recovery matrix, $M$. For the experiments, our erasure recovery matrix contained $m = 3000$ rows, and we used frames of length $N = 2n + m = 29214$. We used a 10% normally distributed noise term, and used erasure percentages of 1%, 3%, 5%, 7%, and 9%. New noise terms were used for each erasure percentage. In each figure, the top row shows the image corrupted only by the 10% noise term with no erasures. The second row shows the noisy partial reconstruction of the image, $\tilde{f}_R$, and the third row shows the noisy reconstructed image, $\tilde{f}$, for various erasure set sizes.

In Figs. 5–7 in Appendix A, we see that the reconstructed image, $\tilde{f}$, gives a better approximation to the compressed image than the erased image with noise, $\tilde{f}_R$, with the exception of 9% erasures. However, 9% erasures corresponds to $|\Lambda| = 2629$ which is close to $m = 3000$. Thus, since $|\Lambda| \approx m$, it is reasonable to expect a high degree of noise amplification.

## 8. Concluding remarks

We proposed a frame based kernel analysis approach to information recovery that also ensures encoding frame protections when additional tools, the erasure recovering matrices, are provided to the decoders. We also presented several necessary and sufficient conditions under which the erasure recovery matrix protects the encoding frame. We proved that such erasure recovery matrices actually form an open and dense subset in a particular matrix space, and concrete examples can be easily constructed by using the three proposed algorithms. Moreover, the construction algorithms also imply that any randomly generated matrix can serve (with probability one) as such an erasure recovery matrix with a proper choice of a encoding frame. For two of the three construction algorithms, we were able to provide proofs that these methods have small channel noise amplification factors. Detailed numerical experiments are presented pertaining to channel noise amplification for our the three construction algorithms.

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004

Besides the application to frame erasures, this method can possibly be applied to signal authentication yielding a method for protection from identity theft. Suppose that a communications group shares a common decoding (or synthesis) frame, $\{f_j\}_{j=1}^N$ held by a designated receiver. In general, there are many duals $\{g_j^{(k)}\}_{j=1}^N$ to $\{f_j\}_{j=1}^N$. Assume that the $k$th member of the communications group has his/her own encoding frame $\{g_j^{(k)}\}_{j=1}^N$ and erasure recovery matrix $M_k$. If the recipient wishes to verify which user sent a signal, the recipient can deliberately introduce erasures in the received signal and then reconstruct using each erasure recovery matrix $M_k$. As indicated by preliminary experiments, if there is a sufficient amount of randomness in the construction of the erasure recovery matrix, then the $k$ value for which this reconstruction is sharp is the signal sender with a high probability. For example, suppose the designated receiver is the IRS and each taxpayer has his/her own encoding frame. Then, a file encoded by a taxpayer named Alice can be decoded by an agent named Bob holding the IRS decoder. Furthermore, Bob can authenticate Alice's identity by using the erasure recovery matrix Bob has on file for Alice in a library of erasure recovery matrices, one for each taxpayer. Electronic signatures, for instance, could thus be authenticated in order to protect against man-in-the-middle attacks. Since the file of a recovery matrix can be vastly smaller than the file of an encoder, maintaining a library of recovery matrices would not be difficult. In this way, the erasure recovery matrix can be thought of as a fingerprint of the encoding frame. This method would not be a new public key method of encryption. However, since it is a natural outgrowth of the methods in our paper, we feel it adds to the exposition of our methods and might have some merit for potential considerations. (For another proposed application of frame theory to digital fingerprinting, see [33].)

## Acknowledgments

The authors would like to thank the referees for their many useful comments and suggestions, many of which have helped us to strengthen the results of this paper.

## Appendix A. Visualizing numerical results using the mandrill image

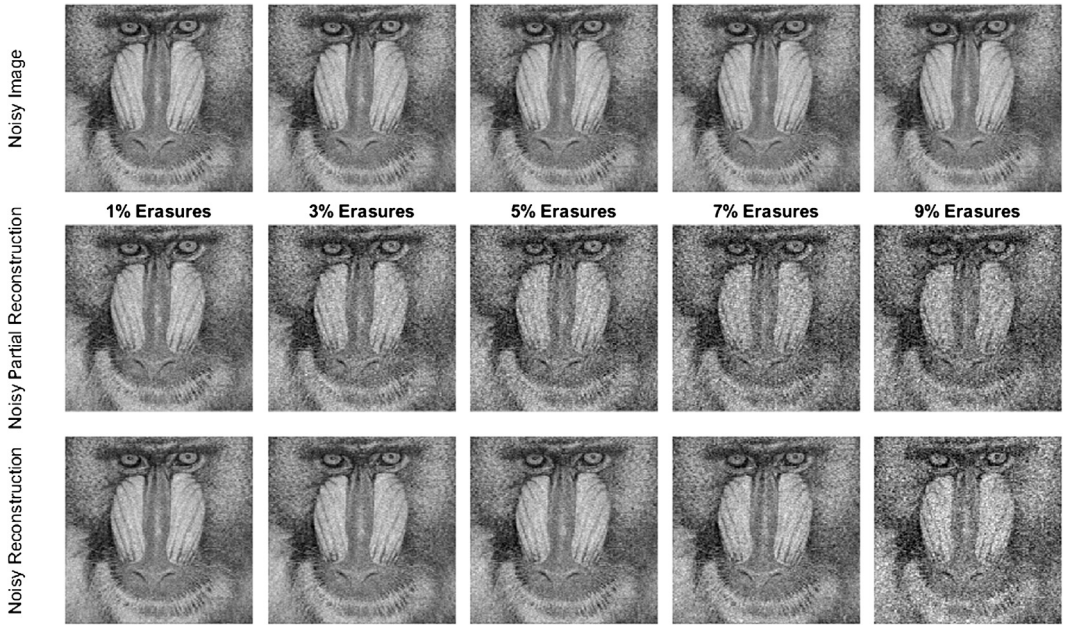


**Fig. 5.** Noise amplification for Construction Algorithm 1 using the mandrill image.

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004

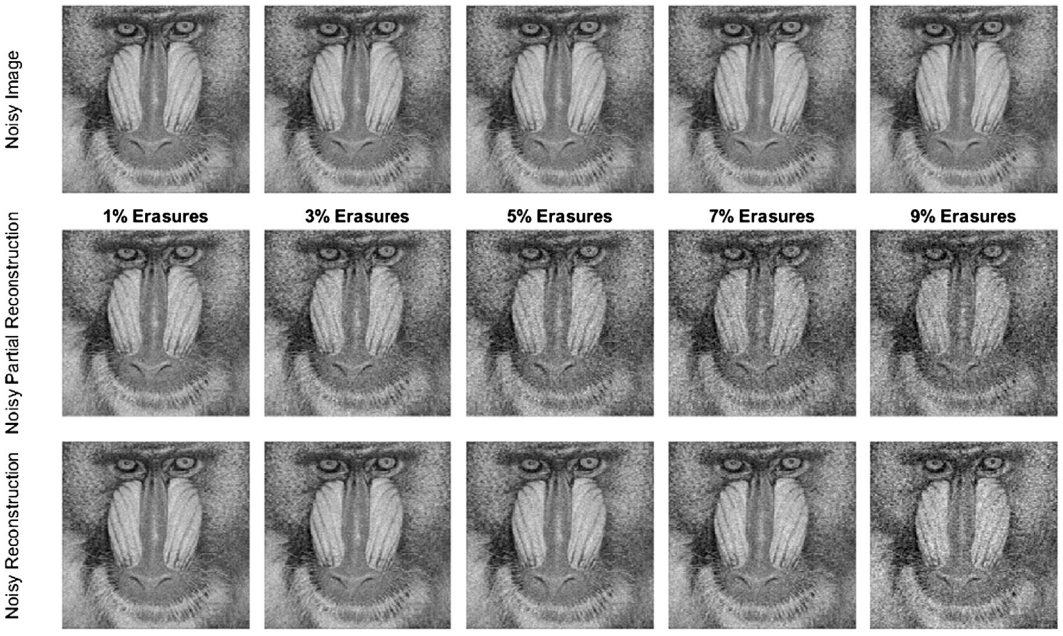


**Fig. 6.** Noise amplification for Construction Algorithm 2 using the mandrill image.

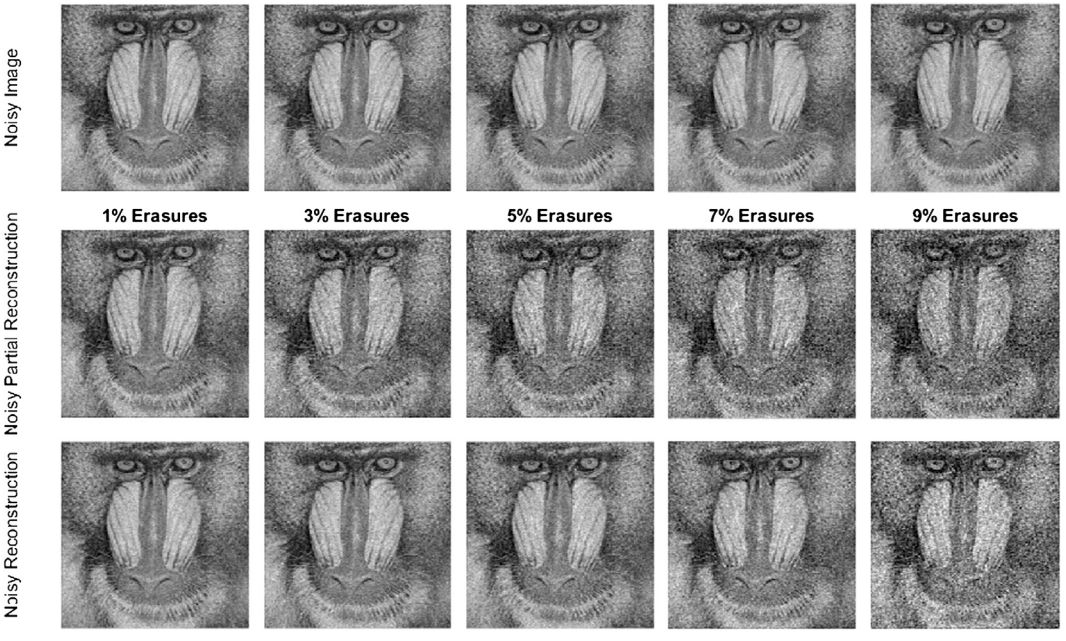


**Fig. 7.** Noise amplification for Construction Algorithm 3 using the mandrill image.

## References

[1] B. Alexeev, J. Cahill, D. Mixon, Full spark frames, J. Fourier Anal. Appl. 18 (6) (2012) 1167–1194.
[2] R.G. Baraniuk, M. Davenport, R.A. DeVore, M. Wakin, A simple proof of the restricted isometry property for random matrices, Constr. Approx. 28 (3) (2008) 253–263.
[3] B. Bodmann, P. Casazza, V. Paulsen, D. Speegle, Spanning and independence properties of frame partitions, Proc. Amer. Math. Soc. 140 (2012) 2193–2207.
[4] B. Bodmann, V.I. Paulsen, Frames, graphs and erasures, Linear Algebra Appl. 404 (2005) 118–146.
[5] B. Bodmann, P. Singh, Burst erasures and the mean-square error for cyclic Parseval frames, IEEE Trans. Inform. Theory 57 (7) (2011) 4622–4635.
[6] E. Càndes, T. Tao, Decoding by linear programming, IEEE Trans. Inform. Theory 51 (12) (2005) 4203–4215.

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004

[7] E. Càndes, T. Tao, Near optimal signal recovery from random projections: universal encoding strategies?, IEEE Trans. Inform. Theory 52 (12) (2006) 5406–5425.
[8] P. Casazza, J. Kovacević, Equal-norm tight frames with erasures, Adv. Comput. Math. 18 (2003) 387–430.
[9] P. Casazza, G. Kutyniok, Finite Frames: Theory and Applications, Appl. Numer. Harmon. Anal., Birkhäuser Springer, New York, 2013.
[10] O. Christensen, An Introduction to Frames and Riesz Bases, Birkhäuser Springer, New York, 2003.
[11] K. Davidson, S. Szarek, Local operator theory, random matrices and Banach spaces, Book Chapter, in: W.B. Johnson, J. Lindenstrauss (Eds.), Handbook of the Geometry of Banach Spaces, vol. 1, Elsevier, Amsterdam, 2001, pp. 317–366.
[12] M. Fickus, D.G. Mixon, Numerically erasure-robust frames, Linear Algebra Appl. 437 (6) (2012) 1394–1407.
[13] S. Foucart, H. Rauhut, A Mathematical Introduction to Compressive Sensing, Appl. Numer. Harmon. Anal., Birkhäuser Springer, New York, 2013.
[14] V.K. Goyal, J. Kovacević, J.A. Kelner, Quantized frame expansions with erasures, Appl. Comput. Harmon. Anal. 10 (3) (2001) 203–233.
[15] D. Han, K. Kornelson, D. Larson, E. Weber, Frames for Undergraduates, Stud. Math. Libr., vol. 40, American Mathematical Society, Providence, RI, 2007.
[16] D. Han, D.R. Larson, Frames, Bases and Group Representations, Mem. Amer. Math. Soc., vol. 147(697), 2000.
[17] D. Han, W. Sun, Reconstruction of signals from frame coefficients with erasures at unknown locations, IEEE Trans. Inform. Theory 60 (7) (2014) 4013–4025.
[18] D. Han, F. Lv, W. Sun, Stable recovery of signals from frame coefficients with erasures at unknown locations, Sci. China Math. 61 (2018) 151–172.
[19] D. Han, F. Lv, W. Sun, Recovery of signals from unordered partial frame coefficients, Appl. Comput. Harmon. Anal. 44 (2018) 38–58.
[20] T. Hoffman, J. Solazzo, Complex equiangular tight frames and erasures, Linear Algebra Appl. 437 (2) (2012) 549–568.
[21] R. Holmes, V. Paulsen, Optimal frames for erasures, Linear Algebra Appl. 377 (2004) 31–51.
[22] D. Kalra, Complex equiangular cyclic frames and erasures, Linear Algebra Appl. 419 (2006) 373–399.
[23] J. Kovačević, M. Püschel, Real, tight frames with maximal robustness to erasures, Book Chapter, in: J.A. Storer, M. Cohn (Eds.), Proceedings of DCC 2005: Data Compression Conference, The Institute of Electrical and Electronics Engineers, Inc., Los Alamitos, CA, 2005, pp. 63–72.
[24] D. Larson, S. Scholze, Signal reconstruction from frame and sampling erasures, J. Fourier Anal. Appl. 21 (5) (2015) 1146–1167.
[25] D. Larson, S. Scholze, Bridging erasures and the infrastructure of frames, Book Chapter, in: R. Balan, M. Begué, J.J. Benedetto, W. Czaja, K.A. Okoudjou (Eds.), Excursions in Harmonic Analysis, Volume 4: The February Fourier Talks at the Norbert Wiener Center, in: Appl. Numer. Harmon. Anal., Birkhäuser Springer, New York, 2015, pp. 27–64.
[26] J. Leng, D. Han, Optimal dual frames for erasures II, Linear Algebra Appl. 435 (6) (2011) 1464–1472.
[27] J. Leng, D. Han, T. Huang, Optimal dual frames for communication coding with probabilistic erasures, IEEE Trans. Signal Process. 59 (11) (2011) 5380–5389.
[28] J. Leng, D. Han, T. Huang, Probability modelled optimal frames for erasures, Linear Algebra Appl. 438 (11) (2013) 4222–4236.
[29] J. Lopez, D. Han, Optimal dual frames for erasures, Linear Algebra Appl. 432 (1) (2010) 471–482.
[30] Y.M. Lu, M.N. Do, A theory for sampling signals from a union of subspaces, IEEE Trans. Signal Process. 56 (6) (2008) 2334–2345.
[31] F. Lv, W. Sun, Construction of robust frames in erasure recovery, Linear Algebra Appl. 479 (2015) 155–170.
[32] S. Mendelson, A. Pajor, N. Tomczak-Jaegermann, Uniform uncertainty principle for Bernoulli and subgaussian ensembles, Constr. Approx. 28 (3) (2008) 277–289.
[33] D.G. Mixon, C. Quinn, N. Kiyavash, Matthew Fickus, Fingerprinting with equiangular tight frames, IEEE Trans. Inform. Theory 59 (3) (2013) 1855–1865.
[34] A.V. Oppenheim, V.K. Goyal, P. Boufounos, Causal compensation for erasures in frame representations, IEEE Trans. Signal Process. 56 (3) (2008) 1071–1082.
[35] S. Pehilvan, D. Han, R. Mohapatra, Linearly connected sequences and spectrally optimal dual frames for erasures, J. Funct. Anal. 265 (11) (2013) 2855–2876.
[36] S. Pehilvan, D. Han, R. Mohapatra, Spectrally two-uniform frames for erasures, Oper. Matrices 9 (2) (2015) 383–399.
[37] M. Rudelson, R. Vershynin, On sparse reconstruction from Fourier and Gaussian measurements, Comm. Pure Appl. Math. 61 (8) (2008) 1025–1045.
[38] Y. Zhang, User's Guide for Yall1: Your Algorithms for L1 Optimization, Technical Report, Rice University, 2009.

Please cite this article in press as: D. Han et al., Erasure recovery matrices for encoder protection, Appl. Comput. Harmon. Anal. (2018), https://doi.org/10.1016/j.acha.2018.09.004