Reed-Solomon Frames From Vandermonde Matrices

Vahid Tarokh

Harvard University

July 29, 2004

Outline

- Introduction
- Connection Between Frames and Codes
- Reed-Solomon Frames From Vandermonde Matrices
- Decoding Algorithm
- Stability
- Conclusions

Introduction

- Sparse representations have recently received wide attention because of their numerous potential applications.
- These applications are all based on approximation of input signals with a linear combination of a large dependent collection of signals (known as a dictionary).
- Because many approximations of input signals in terms of elements of a pre-defined dictionary exist, the sparsity of representation is imposed by penalizing nonzero coefficients. In particular, one may look for the representation of a signal with smallest number of non-zero elements.

Notation

- To this end, let a frame $\mathcal{F} = \{\phi_1, \phi_2, \cdots, \phi_N\}$ of N non-zero vectors in an $N - K$ dimensional subspace $\mathcal{W} \leq \mathbb{C}^N$ be given such that $\mathcal{F}$ spans $\mathcal{W}$.
- Any vector $\mathbf{r}$ in $\mathcal{W}$ can be written in a non-unique way as the sum of elements of $\mathcal{F}$. Let $\mathbf{r} = \sum_{i=1}^{N} c_i \phi_i$ be such a representation.
- We define $\|r\|_{0,\mathcal{F}}$ to be the smallest number of non-zero coefficients of any such expansion. Also, for an arbitrary vector $\mathbf{c} = (c_1, c_2, \cdots, c_N) \in \mathbb{C}^N$, we define $\|\mathbf{c}\|_0$ to be the number of non-zero elements of $\mathbf{c}$.
- Thus $\|\mathbf{r}\|_{0,\mathcal{F}}$ is simply the $\min(\|\mathbf{c}\|_0)$ over all possible expansions $\mathbf{c}$ of $\mathbf{r}$ as above.

The Main Problem

- A main problem of interest is
  - **The Most Compact Representation (MCR) Problem**: Given $\mathcal{F}$ a frame spanning $\mathcal{W}$, and $\mathbf{r} \in \mathcal{W}$ find an expansion $\mathbf{r} = \sum_{i=1}^{N} c_i \phi_i$ for which $\mathbf{c} = (c_1, c_2, \cdots, c_N)$ has minimum $\|\mathbf{c}\|_0$, i.e. $\|\mathbf{r}\|_{0,\mathcal{F}} = \|\mathbf{c}\|_0$.
- This optimization problem is in general difficult to solve. In this light, much attention has been paid to solutions minimizing $\|\mathbf{c}\|_1 = \sum_{i=1}^{N} |c_i|$ instead, and then establishing criteria under which the minimizing $\mathbf{c}$ also solves the MCR Problem.

Our Approach

- In this talk, we take a different approach. We construct frames $\mathcal{F}$ for which the :
  - **Decoding Problem**: Whenever $\mathbf{r}$ has a representation $\mathbf{c}$ with $\|\mathbf{c}\|_0 \leq (N-K)/2$, then find $\mathbf{c}$

  can be solved with a *unique* answer for which the solution coincides with that of the MCR Problem. The solution to the Decoding problem will be found using *algebraic methods* with running time $O(N(N-K))$.

Frames and Associated Codes

- Consdier a frame $\mathcal{F} = \{\phi_1, \phi_2, \cdots, \phi_N\}$ of N non-zero vectors that span an $N - K$ dimensional subspace $\mathcal{W} \leq \mathbb{C}^N$ as above. Consider

$$\mathcal{V} = \{\mathbf{d} = (d_1, d_2, \cdots, d_N) \in \mathbb{C}^N \text{ forwhich } \sum_{\mathrm{i}=1}^{\mathrm{N}} \mathrm{d_i}\phi_\mathrm{i} = 0\}$$

  We refer to $\mathcal{V}$ as the underlying code of frame $\mathcal{F}$.

- The vector space $\mathcal{V}$ is clearly a K dimensional subspace of $\mathbb{C}^N$. If $\mathbf{r} \in \mathcal{W}$ can be represented by $\mathbf{c}$ with respect to the above frame $\mathcal{F}$, then all possible representations of $\mathbf{r}$ are given by $\mathbf{c} - \mathcal{V} = \{\mathbf{c} - \mathbf{d} \mid \mathbf{d} \in \mathcal{V}\}$.

- Thus the problem of finding the shortest representation of $\mathbf{r}$ is equivalent to finding $\mathbf{d} \in \mathcal{V}$ which minimizes $\|\mathbf{c} - \mathbf{d}\|_0$.

Main Idea

- If one thinks of $\mathbf{V}$ as a linear code defined over the field of complex numbers, and of $\mathbf{r}$ as the received word, the MCR Problem is equivalent to finding the error vector $\mathbf{e} = \mathbf{c} - \mathbf{d}$ of minimum (Hamming weight) $\|\mathbf{e}\|_0$ over all the codewords $\mathbf{d} \in \mathcal{V}$. Problems of this nature have been widely studied in the language of the coding theory, however these codes are typically defined over finite fields.
- we construct frames that generalize Reed-Solomon codes using Vandermonde matrices. Under the assumption that $\|r\|_{0,\mathcal{F}} \leq (N-K)/2$, a Reed-Solomon decoding algorithm (which corrects up to half of the minimum distance bound) can find the solution to the decoding problem and the MCR problem. Such decoding algorithms and their improvements are well-known in the coding theory literature.

Reed-Solomon Frames

- Consider the matrix given below:

$$\mathbf{A} = \begin{pmatrix} 1 & z_1 & z_1^2 & \cdots & \cdots & z_1^{N-K-1} \\ 1 & z_2 & z_2^2 & \cdots & \cdots & z_2^{N-K-1} \\ 1 & z_3 & z_3^2 & \cdots & \cdots & z_3^{N-K-1} \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 1 & z_N & z_N^2 & \cdots & \cdots & z_N^{N-K-1} \end{pmatrix} \tag{1}$$

  where z_i, $i = 1, 2, \cdots, N$ are *distinct, non-zero* complex numbers. The following

  - **Condition I**: Any arbitrary set of $N - K$ distinct rows of $\mathbf{A}$ are linearly independent

  holds. This is clear since any such $N - K$ rows form a Vandermonde matrix with non-zero determinant.

Reed-Solomon Frames

- We define frame $\mathcal{F}$ to consist of the rows of $\mathbf{A}$, i.e.

$$\mathcal{F} = \{\phi_j = (1, z_j^1, z_j^2, \cdots, z_j^{N-K-1}) \text{ for } j = 1, \cdots, N\}, \qquad (2)$$

  and refer to it as a *Reed-Solomon* frame.

- Let $\mathcal{W}$ be the subspace spanned by the elements of $\mathcal{F}$. As in the above, one can think of $\mathcal{W}$ as an $N - K$ dimensional subspace of $\mathbb{C}^N$ consisting of N vectors.

Reed-Solomon Codes

- The associated code $\mathcal{V}$ is given by the vectors $\mathbf{d} = (d_1, d_2, \cdots, d_N)$ for which

$$d^1 = d^2 = \cdots = d^{N-K} = 0, \tag{3}$$

where

$$d^i = \sum_{j=1}^{N} d_j z_j^{i-1}. \tag{4}$$

Clearly the subspace (code) $\mathcal{V}$ is K dimensional.

Reed-Solomon Codes

- The code $\mathcal{V}$ has the following interesting property.

  Lemma 1 *For any non-zero vector* $\mathbf{v} \in \mathbf{V}$, *we have* $\|\mathbf{v}\|_0 > N - K$. *Moreover, there exist vectors* $\mathbf{v} \in \mathbf{V}$ *with* $\|\mathbf{v}\|_0 = N - K + 1$.

- In the terminology of coding theory the code $\mathcal{V}$ is an $[N, K, N - K + 1]$ linear code.

- We will decode this code up to half minimum distance bound. Equivalently, we solve the Decoding problem for frame $\mathcal{F}$.

- **Lemma 2** *Given that* $\|\mathbf{r}\|_{0,\mathcal{F}} \leq (N - K)/2$, *the solution to the Decoding problem is unique.*

The Decoder

- We next provide a polynomial time algorithm that outputs the sparsest representation of $\mathbf{r}$ under the assumption that $\|\mathbf{r}\|_{0,\mathcal{F}} \leq (N-K)/2$.
- Let $\mathbf{r} = \sum_{j=1}^{N} r_j \phi_j$ be an arbitrary representation of $\mathbf{r}$ in this frame. A candidate $\mathbf{r}$ can be easily computed using $O((N-K)^2)$ operations. For example if we let $r_{N-K+1} = \cdots = r_N = 0$, then $r_1, r_2, \cdots, r_{N-K}$ can be computed by multiplying the inverse of a Vandermonde matrix (that can be once computed off-line) by $\mathbf{r}$, requiring at most $2(N-K)^2$ operations.
- We fix the representation $(r_1, r_2, \cdots, r_N)$ of $\mathbf{r}$ and seek to compute the most compact description $\mathbf{e} = (e_1, e_2, \cdots, e_N)$ of $\mathbf{r} = \sum_{j=1}^{N} e_j \phi_j$ in this frame with $\|\mathbf{e}\|_0 \leq (N-K)/2$.

The Decoder

- Clearly

$$(r_1, r_2, \cdots, r_N) = \mathbf{e} + \mathbf{d}, \tag{5}$$

  where $\mathbf{d} = (d_1, d_2, \cdots, d_N) \in \mathcal{V}$.

- Let

$$d^i = \sum_{j=1}^{N} d_j z_j^{i-1},$$

  and

$$e^i = \sum_{j=1}^{N} e_j z_j^{i-1}, \tag{6}$$

$$r^i = \sum_{j=1}^{N} r_j z_j^{i-1}, \tag{7}$$

then by Equation (3), we have

$$r^i = e^i \tag{8}$$

for $i = 1, 2, \cdots, N - K$.

The Key Equation

- Let the nonzero elements of $\mathbf{e} = (e_1, e_2, \cdots, e_N)$ be in $i_1, i_2, \cdots, i_w$ where $w \leq (N-K)/2$. For $j = 1, 2, \cdots, w$, let $X_j = z_{i_j}$ and $Y_j = e_{i_j}$.

  Lemma 3 *Define*

$$\sigma[z] = \prod_{i=1}^{w}(1 - X_i z), \tag{9}$$

$$\omega[z] = \sum_{i=1}^{w} Y_i \prod_{j=1, j\neq i}^{w} (1 - X_j z), \tag{10}$$

$$S[z] = \sum_{i=1}^{\infty} e^i z^{i-1}, \tag{11}$$

then

$$\omega[z] = S[z]\sigma[z], \tag{12}$$

anywhere in the disk $|z| < \min_{1\leq j\leq N}(|z_j|^{-1})$.

Proof

- Clearly

$$\frac{\omega[z]}{\sigma[z]} = \sum_{i=1}^{w} \frac{Y_i}{1 - X_i z}. \tag{13}$$

Under the assumption of $|z| < \min_{1 \le j \le N}(|z_j|^{-1})$, we have

$$\frac{1}{1 - X_i z} = \sum_{j=0}^{\infty} (z X_i)^j.$$

Replacing this in Equation (13), we have

$$\frac{\omega[z]}{\sigma[z]} = \sum_{i=1}^{w} \sum_{j=1}^{\infty} Y_i X_i^{j-1} z^{j-1}. \tag{14}$$

Clearly $e^j = \sum_{i=1}^{w} Y_i X_i^{j-1}$. Thus the result follows.

The Decoder

- Since $\deg(\omega[x]) \leq \frac{(N-K)}{2} - 1$ and $\deg(\sigma[x]) \leq \frac{(N-K)}{2}$ only $e^1, e^2, \cdots, e^{N-K}$ are needed to compute $\omega[x]$ and $\sigma[x]$ from the above (for instance by solving a linear system of equations for the coefficients of $\omega[x]$ and $\sigma[x]$).
- It is well-known that this task can be achieved more efficiently using the Euclid division algorithm.
- In fact, letting $S_1[z] = \sum_{j=1}^{N-K} e^j z^{j-1}$ one can write:

$$\omega[z] = S_1[z]\sigma[z] \,\mathrm{mod}(\mathrm{z}^{\mathrm{N-K}})$$

for all $z \in \mathbb{C}$. The computation of $\omega[z]$ and $\sigma[z]$ can be performed using the Euclid division algorithm as described for instance in MacWilliams and Sloane (Section 9, Chapter 12). The number of operations required is clearly $O(N(N-K))$.

The Original Euclid Algorithm

- Given polynomials $r_{-1}[z]$ and $r_0[z]$ with $deg(r0[z]) \leq deg(r{-}1[z])$, we can make repeated divisions to obtain the series of equations:

$$\begin{aligned} r_{-1}[z] &= q_1[z]r_0[z] + r_1[z] \; deg(r_1[z]) \leq deg(r_0[z]), \\ r_0[z] &= q_1[z]r_1[z] + r_2[z] \; deg(r_2[z]) \leq deg(r_1[z]), \\ &\vdots \; \vdots \; \vdots \\ r_{k-2}[z] &= q_k[z]r_{k-1}[z] + r_k[z] \; deg(r_k[z]) \leq deg(r_{k-1}[z]), \\ r_{k-1}[z] &= q_{k+1}[z]r_k[z], \end{aligned}$$

  then $r_k[z]$ is the gcd of $r_{-1}[z]$ and $r_0[z]$.

The Original Euclid Algorithm

- Let $U_{-1}[z] = 0$, $U_0[z] = 1$, $V_{-1}[z] = 1$ and $V_0[z] = 0$.
- Define

$$U_i[z] = q_i[z]U_{i-1}[z] + U_{i-2}[z], \tag{15}$$

$$V_i[z] = q_i[z]V_{i-1}[z] + V_{i-2}[z], \tag{16}$$

then $r_k[z]$ is the gcd of $r_{-1}[z]$ and $r_0[z]$.

Modified Euclid Algorithm

- Let $r_{-1}[z] = z^{N-K}$ and $r_0[z] = S_1[z]$ and proceed with the Euclid original algorithm until reaching an $r_l[z]$ such that

$$deg(r_l[z]) \leq \frac{(N-K)}{2} - 1 \tag{17}$$

$$deg(r_{l-1}[z] \geq \frac{(N-K)}{2}, \tag{18}$$

  Then $\sigma[z] = \delta U_l[z]$ and $\omega[z] = (-1)^l \delta r_l[z]$ where δ is a constant chosen such that $\sigma[0] = 1$.

Decoding Algorithm

- Once $\sigma[z]$ and $\omega[z]$ are found, we first compute $\sigma[z]$ for $z_1^{-1}, z_2^{-1}, \cdots, z_N^{-1}$. This step only requires $O(N(N-K))$ computations (since the required powers of z_j, $j = 1, 2, \cdots, N$ must only be once computed off-line).
- In this way, the roots $z_{i_1}^{-1}, \cdots, z_{i_w}^{-1}$ of $\sigma[z]$ (and hence the locations of non-zero elements of $\mathbf{e}$) can be found. The values $e_{i_1}, \cdots, e_{i_w}$ can then be found using the formula (attributed to Forney)

$$Y_j = \omega(X_j^{-1}) / \prod_{i=1, i\neq j}^{w} (1 - X_i X_j^{-1}) = X_j \omega(X_j^{-1}) / \sigma'[X_j^{-1}], \quad (19)$$

  where $\sigma'[z]$ is the derivative of $\sigma[z]$.

Stability Issues

- What if $\mathbf{r}$ is a noisy version of a sparse signal with respect to $\mathbf{F}$, or it is approximately sparse?
- This can be handled using ideas from "adaptive equalization theory".
- Three facts will be used:
  - There is a recurrence with constant coefficients $A_0, A_1, \cdots, A_{N-1}$ such that

$$e^{N+j} = A_0 e^{N+j-1} + A_1 e^{N+j-2} + \cdots + A_{N-1} e^{j}$$

for $j = 1, 2, 3, 4 \cdots$

- If $\sigma[z] = \sum_{i=0}^{w} \sigma_i z_i$ and $\sigma_0 = 1, \sigma_1, \cdots, \sigma_w$ are taps of an FIR filter corresponding to an "equalizer" for a frequency selective channel, then the infinite length received sequence $e^0, e^1, e^2, \cdots$ will generate equalizer output sequence $\omega_0, \omega_1, \cdots, \omega_{w-1}, 0, 0, 0, 0, \cdots$, where $\omega[z] = \sum_{i=0}^{w-1} \omega_i z_i$.
- Noisy versions of $e^0, \cdots, e^{N-K-1}$ are known.

- Casting the problem in this framework. we can apply techniques from vast theory of adaptive equalization to find very good estimates of $\sigma[z]$ and $\omega[z]$.
- These techniques are known to give optimal performance in low noise regime.

Extensions

- Our constructions can be easily extended to provide frames based on analogs of algebraic geometry codes and many other codes, for which the decoding can be achieved using algebraic techniques.
- Another extension to our results can be achieved using well-known list decoding algorithms for Reed-Solomon codes (e.g. Sudan's work). By applying these algorithms, a list of all sparse representations of a given vector $\mathbf{r}$ in the Reed-Solomon frame can be constructed.