Low-Rank Matrix Recovery: The Matrix-Analogue of Compressed Sensing

Sven Müelich

Institute of Communications Engineering, Ulm University, Germany

Workshop “Compressive Sensing basierte Kryptographie”
Ulm, July 7, 2016
Outline

1. Low-Rank Matrix Recovery
2. Known Approaches
3. Theoretical Results
4. Gabidulin Codes in Characteristic Zero
5. New Approach to Low-Rank Matrix Recovery
### Low-Rank Matrix Recovery (LRMR)

#### Compressed Sensing
*(Donoho, Candès, Tao 2006)*

\[ b = Ax, \]

- \( b \in \mathbb{C}^m \) (known)
- \( A \in \mathbb{C}^{m \times n} \) (known)
- \( x \in \mathbb{C}^n \) sparse (unknown)
- \((n \ll m)\)

#### LRMR
*(Candès, Tao, Recht 2009)*

\[ b = A(X), \]

- \( b \in \mathbb{C}^p \) (known)
- \( A : \mathbb{C}^{m \times n} \to \mathbb{C}^p \) linear (known)
- \( X \in \mathbb{C}^{m \times n} \) low rank (unknown)
- \((p \ll n \cdot m)\)

#### Hamming Metric Coding Problem

\[ s = H(c + e) = He \]

- \( s \in K^{n-k} \) syndrome (known)
- \( H \in K^{n-k \times n} \) pc matrix (known)
- \( c \in K^n \) codeword (unknown)
- \( e \in K^n \), \(\text{wt}_H(e)\) small (unknown)

#### Rank Metric Coding Problem

\[ s = H(c + e) = He \]

- \( s \in L^{n-k} \) syndrome (known)
- \( H \in L^{n-k \times n} \) pc matrix (known)
- \( c \in L^n \) codeword (unknown)
- \( e \in L^n \), \(\text{wt}_R(e)\) small (unknown)
- \(L^n \simeq K^{m \times n}\)
Why do we need matrix recovery?

- Size of data grows
- Observing matrices often impossible
- Applications want to process complete matrices
- Goal: Recover matrices from indirect or incomplete information

(Recovery of) Low-rank matrices occurs in:

- Collaborative Filtering (e.g. recommendation systems)
- Adjacency matrices (e.g. social networks)
- Machine Learning (e.g. multi-task learning, natural language processing)
- Distance matrices (e.g. nuclear magnetic resonance spectroscopy)
- Ensembles of signals (e.g. sensor networks)
- System identification
- Quantum state tomography
- ...
### Compressed Sensing

<table>
<thead>
<tr>
<th>Problem</th>
<th>Compressed Sensing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naive</td>
<td>$\min |x|_0 \text{ s.t. } Ax = b$</td>
</tr>
<tr>
<td>Better</td>
<td>$\min |x|_1 \text{ s.t. } Ax = b$</td>
</tr>
<tr>
<td>How to solve?</td>
<td>Linear Programming</td>
</tr>
<tr>
<td>Algorithms</td>
<td>Basis Pursuit</td>
</tr>
<tr>
<td></td>
<td>Greedy Algorithms</td>
</tr>
<tr>
<td></td>
<td>Thresholding-based Algs.</td>
</tr>
</tbody>
</table>
Low-Rank Matrix Recovery (LRMR)

\[ b = A(X), \]

- \( b \in \mathbb{C}^p \) (known)
- \( A : \mathbb{C}^{m \times n} \rightarrow \mathbb{C}^p \) linear (known)
- \( X \in \mathbb{C}^{m \times n} \) low rank (unknown)
  \((p \ll n \cdot m)\)

**Task:**

Reconstruct \( X \) from \( b \)

**Algorithm:**

\[
\min \text{ rank}(X) \text{ subject to } A(X) = b
\]
Nuclear Norm Approximation

SVD of $X \in \mathbb{C}^{m \times n}$:

$$X = U \Sigma V^* = \sum_{l=1}^{n} \sigma_l u_l v_l^T$$

- $n = \min\{n, m\}$
- $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_n \geq 0$ (singular values of $X$)
- $u_l \in \mathbb{C}^m$ (left singular vectors)
- $v_l \in \mathbb{C}^n$ (right singular vectors)

Nuclear Norm:

$$\|X\|_* = \|\sigma(X)\|_1 = \sum_{l=1}^{n} \sigma_l(X)$$

- $\sigma = \sigma(X) = (\sigma_1, \ldots, \sigma_n)$

Remarks:

- Rank of $X \equiv l_0$-norm of $\sigma$
- Nuclear norm $\equiv l_1$-norm of $\sigma$
Naive approach:

\[
\min \text{ rank}(X) \text{ subject to } A(X) = b
\]

Nuclear Norm Minimization:

\[
\min \|X\|_* \text{ subject to } A(X) = b
\]
## Compressed Sensing and Low-Rank Matrix Recovery

<table>
<thead>
<tr>
<th>Problem</th>
<th>Compressed Sensing</th>
<th>Low-Rank Matrix Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$b = Ax$</td>
<td>$b = \mathcal{A}(X)$</td>
</tr>
<tr>
<td>Naive</td>
<td>$\min |x|_0$ s.t. $Ax = b$</td>
<td>$\min \rank(X)$ s.t. $\mathcal{A}(X) = b$</td>
</tr>
<tr>
<td>Better</td>
<td>$\min |x|_1$ s.t. $Ax = b$</td>
<td>$\min |X|_*$ s.t. $\mathcal{A}(X) = b$</td>
</tr>
<tr>
<td>How to solve?</td>
<td>Linear Programming</td>
<td>Semidefinite Programming</td>
</tr>
<tr>
<td>Algorithms</td>
<td>Basis Pursuit</td>
<td>Proximal Algorithm</td>
</tr>
<tr>
<td></td>
<td>Greedy Algorithms</td>
<td>(Greedy Algorithms?)</td>
</tr>
<tr>
<td></td>
<td>Thresholding-based Algs.</td>
<td>Thresholding-based Algs.</td>
</tr>
</tbody>
</table>
Restricted Isometry Property RIP (Recht, Fazel, Parrilo)

\[ b = \mathcal{A}(X) \]

\( r \)-restricted isometry constant: smallest number \( \delta_r(\mathcal{A}) \) such that

\[ (1 - \delta_r) \|X\|_F \leq \|\mathcal{A}(X)\| \leq (1 + \delta_r) \|X\|_F \]

holds for all \( X \in \mathbb{C}^{m \times n} \) of rank \( \leq r \).

(defined \( \forall 1 \leq r \leq m \))

Theorem (Recht, Fazel, Parrilo)

If

\[ \delta_{2r} < 1 \quad \text{for some integer } r \geq 1 \]

then \( X \) is the only matrix of rank \( \leq r \) satisfying \( \mathcal{A}(X) = b \)
$L/K$ Galois extension (i.e. normal and separable), $[L : K] =: m$

Galois group

$\text{Gal} (L/K) = \{ \theta : L \to L \text{ automorphism s.t. } \theta(x) = x \ \forall x \in K \} $

Assumption: $\text{Gal} (L/K)$ is cyclic, $\theta$ generator
\( L/K \) Galois extension, \( \theta \in \text{Gal} (L/K) \).

\[
L[x; \theta] = \left\{ a = \sum_{i=0}^{d} a_i x^i : a_i \in L, d \in \mathbb{N} \right\}
\]

Addition (+) \( a + b = \sum_i (a_i + b_i)x^i \)

Multiplication (\( \cdot \)) \( a \cdot b = \sum_i \left( \sum_{j=0}^{i} a_j \theta^j (b_{i-j}) \right)x^i \) (non-commutative)

**Generalization of Linearized Polynomials**

- Isomorphic to linearized polynomials in case \( \mathbb{F}_{q^m} / \mathbb{F}_q, \theta = \cdot^q \)
Gabidulin Codes

$L/K$ Galois extension, $\theta \in \text{Gal}(L/K)$ generator.

**Definition**

$g_1, \ldots, g_n \in L$, linearly independent over $K$, $k \leq n \leq m = [L : K]$

$$C_G[n, k] = \{ c = [f(g_1), \ldots, f(g_n)] : f \in L[x; \theta] \land \deg f < k \} \subseteq L^n$$

**Rank Metric:**

$$\text{wt}_R(c) = \text{rank}(C), \quad d_R(c_1, c_2) = \text{rank}(C_1 - C_2)$$

**Theorem (Augot, Loidreau, Robert)**

Minimum rank distance

$$d = \min_{c_1 \neq c_2} d_R(c_1, c_2) = n - k + 1 \quad \text{(MRD)}$$

**Decoding:**

Augot, Loidreau, Robert (2013): $O(n^3)$
Müelich, Puchinger, Mödinger, Bossert (2016): $O(n^2)$
LRMR: New Approach \((K\text{-linear map } \mathcal{A} : \mathbb{C}^{m \times n} \rightarrow \mathbb{C}^p)\)

\[
E \in K^{m \times n}
\]

(Linear) \(\downarrow\) Inverse extension in basis of \(L\)

\[
e \in L^n
\]

(Linear) \(\downarrow\) Syndrome computation

\[
s = eH^T \in L^{n-k}
\]

(Linear) \(\downarrow\) Extension in basis of \(L\)

\[
\cdots \quad b \in K^{(n-k)m}
\]

\[
E \in K^{m \times n}
\]

(Linear) \(\uparrow\) Decoding & ext. in basis of \(L\)

\[
r = c + e \in L^n
\]

(Linear) \(\uparrow\) Find a solution of \(rH^T = s\)

\[
s = eH^T \in L^{n-k}
\]

(Linear) \(\uparrow\) Inverse extension in basis of \(L\)

\[
\cdots \quad b \in K^{(n-k)m}
\]

**Theorem** Müelich, Puchinger, Bossert

If \(\text{rank}(E) \leq \frac{d-1}{2} = \frac{n-k}{2}\), \(E\) can be reconstructed from \(b = \mathcal{A}(E)\).
LRMR: New Approach (Choice of $K$ and $L$)

\[ \mathbf{X} \in \mathbb{C}^{m \times n} \]

↓ Rank-preserving mapping

\[ \mathbf{E} \in K^{m \times n} \]

↓ Inverse extension in basis of $L$

\[ \mathbf{e} \in L^n \]

↓ Syndrome computation

\[ \mathbf{s} = \mathbf{eH}^T \in L^{n-k} \]

↓ Extension in basis of $L$

\[ \cdots \mathbf{b} \in K^{(n-k)m} \]

**Needed:** $K \in \{\mathbb{R}, \mathbb{C}\}$. Possible $L$:
- $K = \mathbb{R}$: $L \in \{\mathbb{R}, \mathbb{C}\}$ ($m \leq 2$)
- $K = \mathbb{C}$: $L = \mathbb{C}$ ($m = 1$)

**Idea:** Choose $K$ to be a dense subfield of $\mathbb{R}$ or $\mathbb{C}$, e.g.,

<table>
<thead>
<tr>
<th>$K$</th>
<th>$\mathbb{R}$</th>
<th>$\mathbb{C}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K$</td>
<td>$\mathbb{Q}$</td>
<td>$\mathbb{Q}(\zeta_r)$</td>
</tr>
<tr>
<td>$L$</td>
<td>$\mathbb{Q}(\zeta_r)$</td>
<td>Kummer extension</td>
</tr>
<tr>
<td>$m$</td>
<td>$\varphi(r)$</td>
<td>$r$</td>
</tr>
</tbody>
</table>
**Fundamental Work:**

<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Venue</th>
</tr>
</thead>
</table>

**Overview Articles:**

<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Venue</th>
</tr>
</thead>
</table>

**CS and LRMR**

<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Venue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fazel, Candès, Recht, Parillo</td>
<td>Compressed Sensing and Robust Recovery of Low-Rank Matrices (2008)</td>
<td>42nd Asilomar Conference on Signals, Systems and Computers</td>
</tr>
</tbody>
</table>

**Our Work:**

<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Venue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Müllich, Puchinger, Bossert</td>
<td>Low-Rank Matrix Recovery using Gabidulin Codes in Characteristic Zero (2016)</td>
<td>Int. Workshop on Algebraic and Combinatorial Coding Theory nt.uni-ulm.de/mueelich → Publications</td>
</tr>
</tbody>
</table>