Compressed sensing with Hadamard matrices and combinatorial designs

Darryn Bryant, Charles Colbourn, Daniel Horsley, Padraig Ó Catháin

Monash University

3 December 2014
Outline

1. Compressed sensing
2. Design theory
3. Asymptotic Existence
What is compressed sensing?

- Redundancy in real world data - allows compression of images, audio, etc.
- Collecting large volumes of data requires high quality sensors.
- But most of that data is discarded in a compression step.
- Can we collect only the data that isn’t immediately thrown away?
- Cheaper sensors, faster data acquisition, less computation time for compression...
Compressed sensing as linear algebra

Data $\iff$ points in $\mathbb{R}^N$
Measurement $\iff$ linear functional
Compressible data $\iff$ Sparse vectors

$\Phi x = b$

- Under the assumption that $x$ is sparse, can we recover it in less than $N$ linear measurements?
- Short answer: yes. If we assume that the columns of $\Phi$ are ‘approximately orthogonal’.
Approximate orthogonality

Assumption throughout this talk: columns have $\ell_2$-norm 1.

**Definition (Easy)**
A matrix $\Phi$ is $\epsilon$-weakly-approximately-orthogonal if for all distinct pairs of columns

$$\langle c_i, c_j \rangle \leq \epsilon.$$ 

**Definition (Hard)**
A matrix $\Phi$ is $\epsilon$-strongly-approximately-orthogonal if, for any column-submatrix $S$ containing at most $t$ columns, all eigenvalues of $S^* S$ satisfy

$$1 - \epsilon \leq \lambda \leq 1 + \epsilon.$$
Theorem (Welch)

In an $n \times N$ matrix, some pair of columns has inner product at least

$$\sqrt{\frac{N - n}{n(N - 1)}} \sim \frac{1}{\sqrt{n}}$$

- Welch bound is fairly sharp for $N \leq n^2$: limit on $\epsilon$-weak-approximate-orthogonality.
- How close can we get to the Welch bound in this region?

Theorem

Let $\alpha \in \mathbb{R}$. There exists a constant $C_\alpha$ such that for every $n > C_\alpha$, there exists an $n \times \lfloor \alpha n \rfloor$ matrix in which all inner products are at most twice the Welch bound.
Definition

A Hadamard matrix of order $n$ has all entries on the complex unit circle and satisfies $HH^\top = nI_n$.

$$\begin{bmatrix}
1 & 1 & 1 & 1 \\
1 & -1 & a & -a \\
1 & 1 & -1 & -1 \\
1 & -1 & -a & a \\
\end{bmatrix} \quad (a = e^{i\theta})$$

There exists a Hadamard matrix of order $n$ for all $n$. 
Definition
Let $K$ be a set of integers. An incidence structure $\Delta$ on $v$ points is a *pairwise balanced design* if every block of $\Delta$ has size contained in $K$, and every pair of points occurs in a single block. We denote such a design by $\text{PBD}(v, K)$.

Example
A PBD($11$, {$3, 5$}):

\[
\{ abcde, 01a, 02b, 03c, 04d, 05e, \\
25a, 31b, 42c, 53d, 14e, 34a, 45b, 15c, 12d, 23e \}.
\]
We construct a matrix $\Phi$ as follows:

- Let $A$ be the incidence matrix of a PBD($\nu$, $K$), $\Delta$, with rows labelled by blocks and columns by points.
- So the inner product of a pair of columns is 1 (since any pair of points is contained in a unique block).
- For each column $c$, of $A$, we construct $|c|$ columns of $\Phi$ as follow:
  - Let $H_c$ be a complex Hadamard matrix of order $|c|$.
  - If row $i$ of $c$ is 0, so is row $i$ of each of the $|c|$ columns of $\Phi$.
  - If row $i$ of $c$ is 1, row $i$ of the $|c|$ columns of $\Phi$ is a row of $\frac{1}{|c|}H_c$.
  - No row of $H_c$ is repeated.
Theorem (Bryant, Ó C., 2014)

Suppose there exists a PBD\((v, K)\) with

- \(n\) blocks
- \(\sum_{b \in B} |b| = N\)
- \(\max(K) \leq \sqrt{2} \min(K)\)

Then there exists an \(n \times N\) matrix \(\Phi\) for which

\[
\langle c_i, c_j \rangle \leq 2\sqrt{\frac{N - n}{n(N - 1)}}.
\]

This is a generalisation of a construction Fickus, Mixon and Tremain for Steiner triple systems.

Our results can be improved in many directions: e.g. reducing the constant 2 is possible, as is adding additional columns to the construction using MUBS, etc.
When do PBDs exist?

**Theorem (Wilson)**

*Let* $K$ *be a set of integers with*

$$\gcd\{k - 1 \mid k \in K\} = \gcd\{k(k - 1) \mid k \in K\} = 1.$$

*Then there exists a constant* $C$ *such that, for every* $v > C$, *there exists a PBD* $(v, K, 1)$.

This says nothing about the total number of blocks or the average block size.
What do we want?

For fixed $r \in \mathbb{R}$ and every sufficiently large $n$, we want a PBD with

- $n$ blocks
- sum of block sizes $N = \lfloor rn \rfloor$

Set $k = \lfloor r \rfloor$. Restrict attention to PBDs with blocks of sizes \{ $k - 1$, $k$, $k + 1$ \}. Some necessary conditions:

\[
\begin{align*}
\alpha_{k-1} &+ \alpha_k + \alpha_{k+1} = n \\
\alpha_{k-1}(k - 1) &+ \alpha_k k + \alpha_{k+1}(k + 1) = N \\
\alpha_{k-1} \binom{k-1}{2} &+ \alpha_k \binom{k}{2} + \alpha_{k+1} \binom{k+1}{2} = \binom{v}{2}
\end{align*}
\]
A tool: graph decompositions

Say that a set of graphs $\mathcal{F}$ is *good* if, for every $G \in \mathcal{F}$, the gcd of the vertex degrees of $G$ is 1.

**Theorem (Caro-Yuster)**

Let $\mathcal{F}$ be a good family of graphs. Denote by $\alpha_G$ the number of edges in $G$. Then exists a constant $C$ such that for all $v > C$, every solution of the equation

\[
\sum_{G \in \mathcal{F}} \alpha_G |G| = \binom{v}{2}
\]

is realisable.

Decompositions into complete graphs $\iff$ PBDs
But: a family of complete graphs is never *good*...
A work-around

The following are ‘good’ graphs.

\begin{align*}
F_1 &= K_{k-1} + K_k \\
F_2 &= K_{k-1} + K_k + K_{k+1} \\
F_3 &= K_k + K_{k+1}
\end{align*}

Caro-Yuster applies: for all sufficiently large \( v \), we can decompose \( K_v \) into \( \beta_i \) copies of \( F_i \) as long as

\[ \beta_1 |F_1| + \beta_2 |F_2| + \beta_3 |F_3| = \binom{v}{2}. \]
Putting it all together

Suppose that there exists a decomposition of $K_v$ in $\beta_i$ copies of $F_i$. How many blocks of each size?

\[
\begin{pmatrix}
1 & 0 & 1 \\
1 & 1 & 1 \\
0 & 1 & 1 \\
\end{pmatrix}
\begin{pmatrix}
\beta_1 \\
\beta_2 \\
\beta_3 \\
\end{pmatrix}
= 
\begin{pmatrix}
\alpha_{k-1} \\
\alpha_k \\
\alpha_{k+1} \\
\end{pmatrix}^T.
\]
Matrix inversion

\[
\begin{pmatrix}
0 & 1 & -1 \\
-1 & 1 & 0 \\
1 & -1 & 1 \\
\end{pmatrix}
\begin{pmatrix}
\alpha_{k-1} \\
\alpha_k \\
\alpha_{k+1} \\
\end{pmatrix}
= 
\begin{pmatrix}
\beta_1 \\
\beta_2 \\
\beta_3 \\
\end{pmatrix}^\top.
\]

- The matrix is **unimodular** and **integral**: it sends integer vectors to integer vectors.
- By Caro-Yuster, **any** decomposition satisfying the necessary conditions and in which the \( \beta_i \) are non-negative corresponds to a design.
- These conditions together with our original necessary conditions give...
Asymptotic Existence

Theorem

For all sufficiently large \( v \), and every choice of \( \alpha_i \) satisfying the following conditions, there exists a PBD\((v, \{k - 1, k, k + 1\}, 1)\) with \( \alpha_i \) blocks of size \( i \).

\[
\begin{align*}
\alpha_k &\geq \alpha_{k-1} \\
\alpha_k &\geq \alpha_{k+1} \\
\alpha_{k+1} + \alpha_{k-1} &\geq \alpha_k \\
\alpha_{k-1} \binom{k - 1}{2} + \alpha_k \binom{k}{2} + \alpha_{k+1} \binom{k + 1}{2} &\equiv \binom{v}{2}
\end{align*}
\]

Corollary

For any \( r \in \mathbb{R} \), all sufficiently large \( n \), these exists a design with \( n \) blocks and sum of block sizes \( \lfloor rn \rfloor \).
Questions

Definition (Easy)
A matrix $\Phi$ is $\epsilon$-weakly-approximately-orthogonal if for all distinct pairs of columns, $\langle c_i, c_j \rangle \leq \epsilon$.

Definition (Hard)
A matrix $\Phi$ is $\epsilon$-strongly-approximately-orthogonal if, for any column-submatrix $S$ containing at most $t$ columns, all eigenvalues of $S^* S$ satisfy

$$1 - \epsilon \leq \lambda \leq 1 + \epsilon.$$