Product Construction of Affine Codes

Han Mao Kiah
joint work with Yeow Meng Chee, Punarbasu Purkayasatha, Patrick Solé

Coordinated Science Lab,
University of Illinois at Urbana-Champaign

Jul 1, 2014

Motivation

Design Objective

We construct codes over matrices.
Fix 'good' codes $\mathcal{C}$ and $\mathcal{D}$ that satisfy certain constraints.
We construct a code such that for each matrix codeword,

(i) each row belongs to $\mathcal{C}$, **and**

(ii) each column belongs to $\mathcal{D}$.

$$\begin{matrix} \in\mathcal{D} & \in\mathcal{D} & \in\mathcal{D} & \in\mathcal{D} & \\ \end{matrix}$$
$$\begin{pmatrix} \triangle & \triangle & \triangle & \triangle \\ \triangle & \triangle & \triangle & \triangle \\ \triangle & \triangle & \triangle & \triangle \\ \triangle & \triangle & \triangle & \triangle \end{pmatrix} \begin{matrix} \in\mathcal{C} \\ \in\mathcal{C} \\ \in\mathcal{C} \\ \in\mathcal{C} \end{matrix}$$

Motivation

Design Objective

We construct codes over matrices.
Fix 'good' codes $\mathcal{C}$ and $\mathcal{D}$ that satisfy certain constraints.
We construct a code such that for each matrix codeword,

(i) each row belongs to $\mathcal{C}$, **and**

(ii) each column belongs to $\mathcal{D}$.

$$\begin{matrix} \in\mathcal{D} & \in\mathcal{D} & \in\mathcal{D} & \in\mathcal{D} & \\ \left(\begin{matrix} \triangle & \triangle & \triangle & \triangle \\ \triangle & \triangle & \triangle & \triangle \\ \triangle & \triangle & \triangle & \triangle \\ \triangle & \triangle & \triangle & \triangle \end{matrix}\right) & & & & \begin{matrix} \in\mathcal{C} \\ \in\mathcal{C} \\ \in\mathcal{C} \\ \in\mathcal{C} \end{matrix} \end{matrix}$$

Classical Solution: If $\mathcal{C}$ and $\mathcal{D}$ are linear codes, use **Product Construction**!

Motivation

Design Objective

We construct codes over matrices.
Fix 'good' codes $\mathcal{C}$ and $\mathcal{D}$ that satisfy certain constraints.
We construct a code such that for each matrix codeword,

(i) each row belongs to $\mathcal{C}$, **and**

(ii) each column belongs to $\mathcal{D}$.

$$\begin{array}{cccccc} \in\mathcal{D} & \in\mathcal{D} & \in\mathcal{D} & \in\mathcal{D} & & \\ \left(\begin{array}{cccc} \triangle & \triangle & \triangle & \triangle \\ \triangle & \triangle & \triangle & \triangle \\ \triangle & \triangle & \triangle & \triangle \\ \triangle & \triangle & \triangle & \triangle \end{array}\right) & & & & \begin{array}{c} \in\mathcal{C} \\ \in\mathcal{C} \\ \in\mathcal{C} \\ \in\mathcal{C} \end{array} \end{array}$$

Classical Solution: If $\mathcal{C}$ and $\mathcal{D}$ are linear codes, use **Product Construction**!

Question: What if $\mathcal{C}$ and $\mathcal{D}$ are **not linear**?
This talk gives a partial solution...

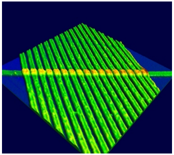
Motivation

Practical Applications for nonlinear constraints

Codes over matrices with weight constraints on **both** rows and columns and with “good” error-correcting capabilities:

(i) coded modulation schemes for power line channels [Chee *et al.* 2013] (considered only columns with weight constraints),

(ii) crossbar arrays of resistive devices [Ordentlich Roth 2000, 2011] (considered only efficient encoding without error correction).



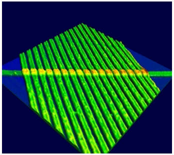
Motivation

Practical Applications for nonlinear constraints

Codes over matrices with weight constraints on **both** rows and columns and with "good" error-correcting capabilities:

(i) coded modulation schemes for power line channels [Chee *et al.* 2013] (considered only columns with weight constraints),

(ii) crossbar arrays of resistive devices [Ordentlich Roth 2000, 2011] (considered only efficient encoding without error correction).



Potential for other applications with "**nonlinear**" constraints...

Motivation

Why Product Codes?

(i) Product codes retain the good rates and good decoding complexity from the smaller component codes

Motivation

Why Product Codes?

(i) Product codes retain the good rates and good decoding complexity from the smaller component codes

(ii) Component codes – affine codes = translates of linear codes

Motivation

Why Product Codes?

(i) Product codes retain the good rates and good decoding complexity from the smaller component codes

(ii) Component codes – affine codes = translates of linear codes

Previous Work

- Amrani '07: guarantees that all the columns belong to the column code; however **only the first few rows** are guaranteed to belong to the row code.

$$\begin{array}{cccc} \in \mathcal{D} & \in \mathcal{D} & \in \mathcal{D} & \in \mathcal{D} \end{array}$$

$$\begin{pmatrix} \triangle & \triangle & \triangle & \triangle \\ \triangle & \triangle & \triangle & \triangle \\ \triangle & \triangle & \triangle & \triangle \\ \triangle & \triangle & \triangle & \triangle \end{pmatrix} \begin{array}{l} \in \mathcal{C} \\ \in \mathcal{C} \\ ??? \\ ??? \end{array}$$

A Toy Problem

Consider the two codes,

$$\begin{aligned}\mathcal{C}^* &= \{\cancel{0000}, 0011, 0101, 0110, 1001, 1010, 1100, \cancel{1111}\} \\ &= \text{span}\{0011, 0101, 1001\} \setminus \{0000, 1111\}, \\ \mathcal{D}^* &= \{\cancel{0000}, 0011, 0101, 0110, 1001, 1010, 1100, \cancel{1111}\} \\ &= \text{span}\{0011, 0101, 1001\} \setminus \{0000, 1111\}.\end{aligned}$$

A Toy Problem

Consider the two codes,

$$
\begin{aligned}
\mathcal{C}^* &= \{\cancel{0000}, 0011, 0101, 0110, 1001, 1010, 1100, \cancel{1111}\} \\
&= \mathrm{span}\{0011, 0101, 1001\} \setminus \{0000, 1111\}, \\
\mathcal{D}^* &= \{\cancel{0000}, 0011, 0101, 0110, 1001, 1010, 1100, \cancel{1111}\} \\
&= \mathrm{span}\{0011, 0101, 1001\} \setminus \{0000, 1111\}.
\end{aligned}
$$

Let us construct a code such that for any matrix codeword

(i) each row belongs to $\mathcal{C}^*$, and

(ii) each column belongs to $\mathcal{D}^*$.

$$
\begin{array}{cccc}
\in \mathcal{D}^* & \in \mathcal{D}^* & \in \mathcal{D}^* & \in \mathcal{D}^*
\end{array}
$$

$$
\begin{pmatrix}
\triangle & \triangle & \triangle & \triangle \\
\triangle & \triangle & \triangle & \triangle \\
\triangle & \triangle & \triangle & \triangle \\
\triangle & \triangle & \triangle & \triangle
\end{pmatrix}
\begin{array}{l}
\in \mathcal{C}^* \\
\in \mathcal{C}^* \\
\in \mathcal{C}^* \\
\in \mathcal{C}^*
\end{array}
$$

In other words, each row and column has weight exactly two.

Attempt: Constrain the Information Array?

Recall that $\mathcal{C}^*$, $\mathcal{D}^*$ come from linear codes of dimension three, say $\mathcal{C}'$, $\mathcal{D}'$. Then a typical codeword from the product code of $\mathcal{C}'$ and $\mathcal{D}'$ is of the form:

$$\begin{pmatrix} x & x & x & \triangle \\ x & x & x & \triangle \\ x & x & x & \triangle \\ \triangle & \triangle & \triangle & \triangle \end{pmatrix}.$$

Attempt: Constrain the Information Array?

Recall that $\mathcal{C}^*$, $\mathcal{D}^*$ come from linear codes of dimension three, say $\mathcal{C}'$, $\mathcal{D}'$. Then a typical codeword from the product code of $\mathcal{C}'$ and $\mathcal{D}'$ is of the form:

$$\begin{pmatrix} x & x & x & \triangle \\ x & x & x & \triangle \\ x & x & x & \triangle \\ \triangle & \triangle & \triangle & \triangle \end{pmatrix}.$$

(i) Observation: the *'bad'* codewords 0000 and 1111 have systematic parts 000 and 111.

(ii) Set the information array such that it consists of no all-zero or all-one row or column.

Attempt: Constrain the Information Array?

Recall that $\mathcal{C}^*$, $\mathcal{D}^*$ come from linear codes of dimension three, say $\mathcal{C}'$, $\mathcal{D}'$. Then a typical codeword from the product code of $\mathcal{C}'$ and $\mathcal{D}'$ is of the form:

$$\begin{pmatrix} x & x & x & \triangle \\ x & x & x & \triangle \\ x & x & x & \triangle \\ \triangle & \triangle & \triangle & \triangle \end{pmatrix}.$$

(i) Observation: the *'bad'* codewords 0000 and 1111 have systematic parts 000 and 111.

(ii) Set the information array such that it consists of no all-zero or all-one row or column.

Bad Idea

Consider the following example:

$$\begin{pmatrix} 1 & 0 & 0 & \triangle \\ 0 & 1 & 0 & \triangle \\ 0 & 0 & 1 & \triangle \\ \triangle & \triangle & \triangle & \triangle \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Classical Product Construction of Linear Codes

Consider linear codes:

$\mathcal{C}$ - length n, dimension k, with generator matrix $(\mathbf{I}_k, \mathbf{A})$,

$\mathcal{D}$ - length m, dimension ℓ, with generator matrix $(\mathbf{I}_\ell, \mathbf{B})$.

Classical Product Construction of Linear Codes

Consider linear codes:

$\mathcal{C}$ - length n, dimension k, with generator matrix $(\mathbf{I}_k, \mathbf{A})$,

$\mathcal{D}$ - length m, dimension ℓ, with generator matrix $(\mathbf{I}_\ell, \mathbf{B})$.

Then codewords (of the product code $\mathcal{C} \otimes \mathcal{D}$) are of the form:

$$\left(\begin{array}{c|c} \mathbf{M} & \mathbf{MA} \\ \hline \mathbf{B}^T\mathbf{M} & \mathbf{B}^T\mathbf{MA} \end{array}\right),$$

where $\mathbf{M}$ is an $\ell \times k$ matrix.

Systematic Representation of Affine Codes

Affine code

- Of the form $\mathcal{C} + \mathbf{u}$, where $\mathcal{C}$ is linear and $\mathbf{u}$ any vector of length n.
- WLOG, assume $\mathbf{u} = (\mathbf{0}_k, \mathbf{a})$.
- Let $\mathcal{C}$ have generator matrix $(\mathbf{I}_k, \mathbf{A})$.
- Any codeword in $\mathcal{C} + \mathbf{u}$ may be written as

$$(\mathbf{x}, \mathbf{x}\mathbf{A} + \mathbf{a}).$$

Systematic Representation of Affine Codes

Affine code

- Of the form $\mathcal{C} + \mathbf{u}$, where $\mathcal{C}$ is linear and $\mathbf{u}$ any vector of length n.
- WLOG, assume $\mathbf{u} = (\mathbf{0}_k, \mathbf{a})$.
- Let $\mathcal{C}$ have generator matrix $(\mathbf{I}_k, \mathbf{A})$.
- Any codeword in $\mathcal{C} + \mathbf{u}$ may be written as

$$(\mathbf{x}, \mathbf{x}\mathbf{A} + \mathbf{a}).$$

Consider affine codes:

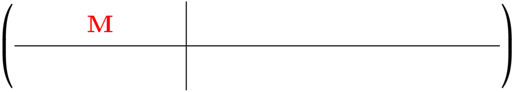
$\mathcal{C} + \mathbf{u}$ - length n, size 2^k, with codewords $(\mathbf{x}, \mathbf{x}\mathbf{A} + \mathbf{a})$,

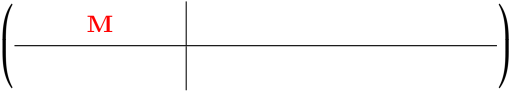
$\mathcal{D} + \mathbf{v}$ - length m, size 2^ℓ, with codewords $(\mathbf{x}, \mathbf{x}\mathbf{B} + \mathbf{b})$.

Product Construction of Affine Codes

$\mathcal{C} + \mathbf{u}$ - length n, size 2^k, with codewords $(\mathbf{x}, \mathbf{x}\mathbf{A} + \mathbf{a})$,

$\mathcal{D} + \mathbf{v}$ - length m, size 2^ℓ, with codewords $(\mathbf{x}, \mathbf{x}\mathbf{B} + \mathbf{b})$.

Def 1: 

Def 2: 

Product Construction of Affine Codes

$\mathcal{C} + \mathbf{u}$ - length n, size 2^k, with codewords $(\mathbf{x}, \mathbf{x}\mathbf{A} + \mathbf{a})$,

$\mathcal{D} + \mathbf{v}$ - length m, size 2^ℓ, with codewords $(\mathbf{x}, \mathbf{x}\mathbf{B} + \mathbf{b})$.

Def 1: $$\left(\begin{array}{c|c} \mathbf{M} & \\ \hline \mathbf{B}^T\mathbf{M} + \mathbf{b}^T\mathbf{1}_k & \end{array}\right)$$

Def 2: $$\left(\begin{array}{c|c} \mathbf{M} & \\ \hline & \end{array}\right)$$

Product Construction of Affine Codes

$\mathcal{C} + \mathbf{u}$ - length n, size 2^k, with codewords $(\mathbf{x}, \mathbf{xA} + \mathbf{a})$,
$\mathcal{D} + \mathbf{v}$ - length m, size 2^ℓ, with codewords $(\mathbf{x}, \mathbf{xB} + \mathbf{b})$.

Def 1: $$\left(\begin{array}{c|c} \mathbf{M} & \mathbf{MA} + \mathbf{1}_\ell^T \mathbf{a} \\ \hline \mathbf{B}^T\mathbf{M} + \mathbf{b}^T\mathbf{1}_k & \left(\mathbf{B}^T\mathbf{M} + \mathbf{b}^T\mathbf{1}_k\right)\mathbf{A} + \mathbf{1}_{m-\ell}^T\mathbf{a} \end{array}\right)$$

Def 2: $$\left(\begin{array}{c|c} \mathbf{M} & \\ \hline & \end{array}\right)$$

Definition 1 guarantees all rows belong to $\mathcal{C} + \mathbf{u}$.

Product Construction of Affine Codes

$\mathcal{C} + \mathbf{u}$ - length n, size 2^k, with codewords $(\mathbf{x}, \mathbf{x}\mathbf{A} + \mathbf{a})$,

$\mathcal{D} + \mathbf{v}$ - length m, size 2^ℓ, with codewords $(\mathbf{x}, \mathbf{x}\mathbf{B} + \mathbf{b})$.

Def 1: $$\left(\begin{array}{c|c} \mathbf{M} & \mathbf{M}\mathbf{A} + \mathbf{1}_\ell^T \mathbf{a} \\ \hline \mathbf{B}^T\mathbf{M} + \mathbf{b}^T\mathbf{1}_k & \left(\mathbf{B}^T\mathbf{M} + \mathbf{b}^T\mathbf{1}_k\right)\mathbf{A} + \mathbf{1}_{m-\ell}^T \mathbf{a} \end{array}\right)$$

Def 2: $$\left(\begin{array}{c|c} \mathbf{M} & \mathbf{M}\mathbf{A} + \mathbf{1}_\ell^T \mathbf{a} \\ \hline & \end{array}\right)$$

Definition 1 guarantees all rows belong to $\mathcal{C} + \mathbf{u}$.

Product Construction of Affine Codes

$\mathcal{C} + \mathbf{u}$ - length n, size 2^k, with codewords $(\mathbf{x}, \mathbf{x}\mathbf{A} + \mathbf{a})$,
$\mathcal{D} + \mathbf{v}$ - length m, size 2^ℓ, with codewords $(\mathbf{x}, \mathbf{x}\mathbf{B} + \mathbf{b})$.

Def 1:
$$\left(\begin{array}{c|c} \mathbf{M} & \mathbf{M}\mathbf{A} + \mathbf{1}_\ell^T\mathbf{a} \\ \hline \mathbf{B}^T\mathbf{M} + \mathbf{b}^T\mathbf{1}_k & \left(\mathbf{B}^T\mathbf{M} + \mathbf{b}^T\mathbf{1}_k\right)\mathbf{A} + \mathbf{1}_{m-\ell}^T\mathbf{a} \end{array}\right)$$

Def 2:
$$\left(\begin{array}{c|c} \mathbf{M} & \mathbf{M}\mathbf{A} + \mathbf{1}_\ell^T\mathbf{a} \\ \hline \mathbf{B}^T\mathbf{M} + \mathbf{b}^T\mathbf{1}_k & \mathbf{B}^T\left(\mathbf{M}\mathbf{A} + \mathbf{1}_\ell^T\mathbf{a}\right) + \mathbf{b}^T\mathbf{1}_{n-k} \end{array}\right)$$

Definition 1 guarantees all rows belong to $\mathcal{C} + \mathbf{u}$.
Definition 2 guarantees all columns belong to $\mathcal{D} + \mathbf{v}$.

Product Construction of Affine Codes

$\mathcal{C} + \mathbf{u}$ - length n, size 2^k, with codewords $(\mathbf{x}, \mathbf{x}\mathbf{A} + \mathbf{a})$,

$\mathcal{D} + \mathbf{v}$ - length m, size 2^ℓ, with codewords $(\mathbf{x}, \mathbf{x}\mathbf{B} + \mathbf{b})$.

Def 1:
$$\left(\begin{array}{c|c} \mathbf{M} & \mathbf{M}\mathbf{A} + \mathbf{1}_\ell^T \mathbf{a} \\ \hline \mathbf{B}^T\mathbf{M} + \mathbf{b}^T \mathbf{1}_k & \left(\mathbf{B}^T\mathbf{M} + \mathbf{b}^T\mathbf{1}_k\right)\mathbf{A} + \mathbf{1}_{m-\ell}^T \mathbf{a} \end{array}\right)$$

Def 2:
$$\left(\begin{array}{c|c} \mathbf{M} & \mathbf{M}\mathbf{A} + \mathbf{1}_\ell^T \mathbf{a} \\ \hline \mathbf{B}^T\mathbf{M} + \mathbf{b}^T \mathbf{1}_k & \mathbf{B}^T\left(\mathbf{M}\mathbf{A} + \mathbf{1}_\ell^T\mathbf{a}\right) + \mathbf{b}^T \mathbf{1}_{n-k} \end{array}\right)$$

Definition 1 guarantees all rows belong to $\mathcal{C} + \mathbf{u}$.
Definition 2 guarantees all columns belong to $\mathcal{D} + \mathbf{v}$.

Proposition (Sufficient Condition)

If $\mathbf{1}_n \in \mathcal{C}$ and $\mathbf{1}_m \in \mathcal{D}$, then both definitions coincide!

Product Construction of Affine Codes

$\mathcal{C}$ - length n, dimension k, with generator matrix $(\mathbf{I}_k, \mathbf{A})$,

$\mathcal{D}$ - length m, dimension ℓ, with generator matrix $(\mathbf{I}_\ell, \mathbf{B})$.

Pick $\mathbf{u} = (\mathbf{0}_k, \mathbf{a})$ and $\mathbf{v} = (\mathbf{0}_\ell, \mathbf{b})$.

Theorem (Construction I)

If $\mathbf{1}_n \in \mathcal{C}$ and $\mathbf{1}_m \in \mathcal{D}$, then the code

$$\left\{ \left(\begin{array}{c|c} \mathbf{M} & \mathbf{M}\mathbf{A} + \mathbf{1}_\ell^T \mathbf{a} \\ \hline \mathbf{B}^T\mathbf{M} + \mathbf{b}^T\mathbf{1}_k & \left(\mathbf{B}^T\mathbf{M} + \mathbf{b}^T\mathbf{1}_k\right)\mathbf{A} + \mathbf{1}_{m-\ell}^T \mathbf{a} \end{array} \right) : \mathbf{M} \text{ is a } \ell \times k \text{ matrix} \right\}$$

is a systematic code of size 2^{kl} and is a coset of $\mathcal{C} \otimes \mathcal{D}$ with coset leader

$$\mathbf{U} \triangleq \left(\begin{array}{c|c} \mathbf{0}_{\ell\times k} & \mathbf{1}_\ell^T \mathbf{a} \\ \hline \mathbf{b}^T\mathbf{1}_k & \mathbf{b}^T\mathbf{1}_{n-k} + \mathbf{1}_{m-\ell}^T \mathbf{a} \end{array} \right).$$

For any codeword $\mathbf{N}$,

(i) *each row of $\mathbf{N}$ belongs to $\mathcal{C} + \mathbf{u}$, and*

(ii) *each column of $\mathbf{N}$ belongs to $\mathcal{D} + \mathbf{v}$.*

Product Construction of Affine Codes

$\mathcal{C}$ - length n, dimension k, with generator matrix $(\mathbf{I}_k, \mathbf{A})$,

$\mathcal{D}$ - length m, dimension ℓ, with generator matrix $(\mathbf{I}_\ell, \mathbf{B})$.

Pick $\mathbf{u} = (\mathbf{0}_k, \mathbf{a})$ and $\mathbf{v} = (\mathbf{0}_\ell, \mathbf{b})$.

Theorem (Construction I)

If $\mathbf{1}_n \in \mathcal{C}$ and $\mathbf{1}_m \in \mathcal{D}$, then the code

$$\left\{ \left(\begin{array}{c|c} \mathbf{M} & \mathbf{MA} + \mathbf{1}_\ell^T \mathbf{a} \\ \hline \mathbf{B}^T\mathbf{M} + \mathbf{b}^T\mathbf{1}_k & \left(\mathbf{B}^T\mathbf{M} + \mathbf{b}^T\mathbf{1}_k\right)\mathbf{A} + \mathbf{1}_{m-\ell}^T \mathbf{a} \end{array} \right) : \mathbf{M} \text{ is a } \ell \times k \text{ matrix} \right\}$$

is a systematic code of size $2^{k\ell}$ and is a coset of $\mathcal{C} \otimes \mathcal{D}$ with coset leader

$$\mathbf{U} \triangleq \left(\begin{array}{c|c} \mathbf{0}_{\ell \times k} & \mathbf{1}_\ell^T \mathbf{a} \\ \hline \mathbf{b}^T \mathbf{1}_k & \mathbf{b}^T \mathbf{1}_{n-k} + \mathbf{1}_{m-\ell}^T \mathbf{a} \end{array} \right).$$

For any codeword $\mathbf{N}$,

(i) *each row of $\mathbf{N}$ belongs to $\mathcal{C} + \mathbf{u}$, and*

(ii) *each column of $\mathbf{N}$ belongs to $\mathcal{D} + \mathbf{v}$.*

Product Construction of Affine Codes

Remarks

- Encoding and decoding complexities are very similar to usual product codes.

Theorem (Construction I)

If $\mathbf{1}_n \in \mathcal{C}$ and $\mathbf{1}_m \in \mathcal{D}$, then the code

$$\left\{ \left(\begin{array}{c|c} \mathbf{M} & \mathbf{M}\mathbf{A} + \mathbf{1}_\ell^T \mathbf{a} \\ \hline \mathbf{B}^T\mathbf{M} + \mathbf{b}^T\mathbf{1}_k & \left(\mathbf{B}^T\mathbf{M} + \mathbf{b}^T\mathbf{1}_k\right)\mathbf{A} + \mathbf{1}_{m-\ell}^T \mathbf{a} \end{array} \right) : \mathbf{M} \text{ is a } \ell \times k \text{ matrix} \right\}$$

is a systematic code of size $2^{k\ell}$ and is a coset of $\mathcal{C} \otimes \mathcal{D}$ with coset leader

$$\mathbf{U} \triangleq \left(\begin{array}{c|c} \mathbf{0}_{\ell \times k} & \mathbf{1}_l^T \mathbf{a} \\ \hline \mathbf{b}^T \mathbf{1}_k & \mathbf{b}^T \mathbf{1}_{n-k} + \mathbf{1}_{m-\ell}^T \mathbf{a} \end{array} \right).$$

For any codeword $\mathbf{N}$,

(i) *each row of $\mathbf{N}$ belongs to $\mathcal{C} + \mathbf{u}$, and*

(ii) *each column of $\mathbf{N}$ belongs to $\mathcal{D} + \mathbf{v}$.*

Product Construction of Affine Codes

Remarks

- Many well-known codes contain $\mathbf{1}$. Examples: primitive narrow-sense BCH, Reed-Muller, extended Golay.

Theorem (Construction I)

If $\mathbf{1}_n \in \mathcal{C}$ and $\mathbf{1}_m \in \mathcal{D}$, then the code

$$\left\{ \left(\begin{array}{c|c} \mathbf{M} & \mathbf{MA} + \mathbf{1}_\ell^T \mathbf{a} \\ \hline \mathbf{B}^T\mathbf{M} + \mathbf{b}^T \mathbf{1}_k & \left(\mathbf{B}^T\mathbf{M} + \mathbf{b}^T\mathbf{1}_k\right)\mathbf{A} + \mathbf{1}_{m-\ell}^T \mathbf{a} \end{array} \right) : \mathbf{M} \text{ is a } \ell \times k \text{ matrix} \right\}$$

is a systematic code of size $2^{k\ell}$ and is a coset of $\mathcal{C} \otimes \mathcal{D}$ with coset leader

$$\mathbf{U} \triangleq \left(\begin{array}{c|c} \mathbf{0}_{\ell \times k} & \mathbf{1}_\ell^T \mathbf{a} \\ \hline \mathbf{b}^T \mathbf{1}_k & \mathbf{b}^T \mathbf{1}_{n-k} + \mathbf{1}_{m-\ell}^T \mathbf{a} \end{array} \right).$$

For any codeword $\mathbf{N}$,

(i) *each row of $\mathbf{N}$ belongs to $\mathcal{C} + \mathbf{u}$, and*

(ii) *each column of $\mathbf{N}$ belongs to $\mathcal{D} + \mathbf{v}$.*

Toy Problem - Continued

Recall the two codes,

$$\mathcal{C}^* = \{\cancel{0000}, 0011, 0101, 0110, 1001, 1010, 1100, \cancel{1111}\},$$
$$\mathcal{D}^* = \{\cancel{0000}, 0011, 0101, 0110, 1001, 1010, 1100, \cancel{1111}\}.$$

Toy Problem - Continued

Recall the two codes,

$$\mathcal{C}^* = \{\cancel{0000}, 0011, 0101, 0110, 1001, 1010, 1100, \cancel{1111}\},$$
$$\mathcal{D}^* = \{\cancel{0000}, 0011, 0101, 0110, 1001, 1010, 1100, \cancel{1111}\}.$$

Let $\mathcal{C} = \mathcal{D} = \mathrm{span}\{0101, 1010\}$ and $\mathbf{u} = \mathbf{v} = 0011$.
Then

$$\mathcal{C} + \mathbf{u} \subseteq \mathcal{C}^*, \quad \mathcal{D} + \mathbf{v} \subseteq \mathcal{D}^*.$$

Toy Problem - Continued

Recall the two codes,

$$\mathcal{C}^* = \{\cancel{0000}, 0011, 0101, 0110, 1001, 1010, 1100, \cancel{1111}\},$$
$$\mathcal{D}^* = \{\cancel{0000}, 0011, 0101, 0110, 1001, 1010, 1100, \cancel{1111}\}.$$

Let $\mathcal{C} = \mathcal{D} = \mathrm{span}\{0101, 1010\}$ and $\mathbf{u} = \mathbf{v} = 0011$.
Then

$$\mathcal{C} + \mathbf{u} \subseteq \mathcal{C}^*, \quad \mathcal{D} + \mathbf{v} \subseteq \mathcal{D}^*.$$

Applying Construction I, we have

$$\begin{pmatrix} 0&0&1&1\\0&0&1&1\\1&1&0&0\\1&1&0&0 \end{pmatrix} \begin{pmatrix} 0&0&1&1\\0&1&1&0\\1&1&0&0\\1&0&0&1 \end{pmatrix} \begin{pmatrix} 0&0&1&1\\1&0&0&1\\1&1&0&0\\0&1&1&0 \end{pmatrix} \begin{pmatrix} 0&0&1&1\\1&1&0&0\\1&1&0&0\\0&0&1&1 \end{pmatrix} \begin{pmatrix} 0&1&1&0\\0&0&1&1\\1&0&0&1\\1&1&0&0 \end{pmatrix} \begin{pmatrix} 0&1&1&0\\0&1&1&0\\1&0&0&1\\1&0&0&1 \end{pmatrix} \begin{pmatrix} 0&1&1&0\\1&0&0&1\\1&0&0&1\\0&1&1&0 \end{pmatrix} \begin{pmatrix} 0&1&1&0\\1&1&0&0\\1&0&0&1\\0&0&1&1 \end{pmatrix}$$

$$\begin{pmatrix} 1&0&0&1\\0&0&1&1\\0&1&1&0\\1&1&0&0 \end{pmatrix} \begin{pmatrix} 1&0&0&1\\0&1&1&0\\0&1&1&0\\1&0&0&1 \end{pmatrix} \begin{pmatrix} 1&0&0&1\\1&0&0&1\\0&1&1&0\\0&1&1&0 \end{pmatrix} \begin{pmatrix} 1&0&0&1\\1&1&0&0\\0&1&1&0\\0&0&1&1 \end{pmatrix} \begin{pmatrix} 1&1&0&0\\0&0&1&1\\0&0&1&1\\1&1&0&0 \end{pmatrix} \begin{pmatrix} 1&1&0&0\\0&1&1&0\\0&0&1&1\\1&0&0&1 \end{pmatrix} \begin{pmatrix} 1&1&0&0\\1&0&0&1\\0&0&1&1\\0&1&1&0 \end{pmatrix} \begin{pmatrix} 1&1&0&0\\1&1&0&0\\0&0&1&1\\0&0&1&1 \end{pmatrix}.$$

Matrices with Bounded Row and Column Weights

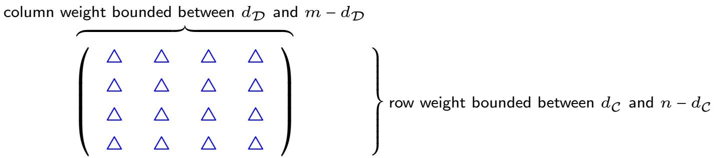
We generalize the previous construction.

Proposition

Let $\mathcal{C}$, $\mathcal{D}$ be binary linear $[n, k, d_\mathcal{C}]$, and $[m, \ell, d_\mathcal{D}]$ codes respectively. Suppose $\mathbf{1}_n \in \mathcal{C}$, and $\mathbf{1}_m \in \mathcal{D}$. Then we have a systematic code over binary $m \times n$ matrices of size $2^{(k-1)(\ell-1)}$ whose codeword matrices have

(i) *row weight bounded between $d_\mathcal{C}$ and $n - d_\mathcal{C}$,*

(ii) *column weight bounded between $d_\mathcal{D}$ and $m - d_\mathcal{D}$.*



Variants of Construction I

Construction I can be modified so that

(a) the component codes are unions of affine codes; i.e.

$$\mathcal{C}^* = \bigcup \mathcal{C} + \mathbf{u}, \text{ and } \mathcal{D}^* = \bigcup \mathcal{D} + \mathbf{v},$$

where $\mathcal{C}$ and $\mathcal{D}$ are linear codes.

(b) the component code is an expurgated code; i.e.

$$\mathcal{C}^* = \mathcal{C}_1 \setminus \mathcal{C}_2, \text{ and } \mathcal{D}^* = \mathcal{D}_1 \setminus \mathcal{D}_2,$$

where $\mathcal{C}_1, \mathcal{C}_2, \mathcal{D}_1, \mathcal{D}_2$ are linear codes such that $\mathcal{C}_2 \subseteq \mathcal{C}_1$ and $\mathcal{D}_2 \subseteq \mathcal{D}_1$.

$$\begin{matrix} \in \mathcal{D}^* & \in \mathcal{D}^* & \in \mathcal{D}^* & \in \mathcal{D}^* & \\ \end{matrix}$$

$$\begin{pmatrix} \triangle & \triangle & \triangle & \triangle \\ \triangle & \triangle & \triangle & \triangle \\ \triangle & \triangle & \triangle & \triangle \\ \triangle & \triangle & \triangle & \triangle \end{pmatrix} \begin{matrix} \in \mathcal{C}^* \\ \in \mathcal{C}^* \\ \in \mathcal{C}^* \\ \in \mathcal{C}^* \end{matrix}$$

Variants of Construction I

Construction I can be modified so that

(c) each row (column) belongs to a different component affine code (*a la* Alipour *et al.* '12: Irregular product codes).

$$\begin{array}{cccc} \in \mathcal{D}_1^* & \in \mathcal{D}_2^* & \in \mathcal{D}_3^* & \in \mathcal{D}_4^* \end{array}$$

$$\begin{pmatrix} \triangle & \triangle & \triangle & \triangle \\ \triangle & \triangle & \triangle & \triangle \\ \triangle & \triangle & \triangle & \triangle \\ \triangle & \triangle & \triangle & \triangle \end{pmatrix} \begin{array}{l} \in \mathcal{C}_1^* \\ \in \mathcal{C}_2^* \\ \in \mathcal{C}_3^* \\ \in \mathcal{C}_4^* \end{array}$$

Conclusion

(i) Construction of systematic affine matrix codes that are obtained by taking product of affine codes.
- Property: every row and every column belongs to the row code and column code, respectively.
- Construct matrix codes with restricted column and row weights and with error-correcting capabities.

(ii) Potential applications in array codes with “affine-like” constraints.

Questions?