# Matrix Product Codes over Finite Commutative Rings

Hongwei Liu
School of Mathematics and Statistics
Central China Normal University, Wuhan, China

(Joint work with Yun Fan and San Ling)

Korea Institute for Advanced Study, Seoul, Korea

November 15, 2012

# CONTENTS

# Construction of Codes: Introduction

$\mathbb{F}_q^n$: vector space over a finite field $\mathbb{F}_q$. *Code*: $C \subseteq \mathbb{F}_q^n$.

$\langle -, - \rangle$: usual Euclidean inner product in $\mathbb{F}_q^n$. That is

$$\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1 + \cdots + x_n y_n \in \mathbb{F}_q, \ \forall\, \mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n.$$

*Dual code*: $C^\perp := \left\{ \mathbf{x} \in \mathbb{F}_q^n \mid \langle \mathbf{c}, \mathbf{x} \rangle = 0, \ \forall\ \mathbf{c} \in C \right\}$.

*Self-orthogonal*: $C \subseteq C^\perp$. *Self-dual*: $C = C^\perp$.

*Minimum Hamming distance*: $d_H(C) = \min\limits_{\mathbf{c} \neq \mathbf{c}' \in C} d_H(\mathbf{c}, \mathbf{c}')$.

*Minimum Hamming weight*: $w_H(C) = \min\limits_{\mathbf{0} \neq \mathbf{c} \in C} w_H(\mathbf{c})$.

# Construction of Codes: Introduction

$\mathbb{F}_q^n$: vector space over a finite field $\mathbb{F}_q$. *Code*: $C \subseteq \mathbb{F}_q^n$.

$\langle -, - \rangle$: usual Euclidean inner product in $\mathbb{F}_q^n$. That is

$$\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1 + \cdots + x_n y_n \in \mathbb{F}_q, \ \forall\, \mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n.$$

*Dual code*: $C^\perp := \left\{ \mathbf{x} \in \mathbb{F}_q^n \mid \langle \mathbf{c}, \mathbf{x} \rangle = 0, \ \forall\ \mathbf{c} \in C \right\}$.

*Self-orthogonal*: $C \subseteq C^\perp$. *Self-dual*: $C = C^\perp$.

*Minimum Hamming distance*: $d_H(C) = \min\limits_{\mathbf{c} \neq \mathbf{c}' \in C} d_H(\mathbf{c}, \mathbf{c}')$.

*Minimum Hamming weight*: $w_H(C) = \min\limits_{\mathbf{0} \neq \mathbf{c} \in C} w_H(\mathbf{c})$.

$C$ is linear $(C \leq \mathbb{F}_q^n) \Rightarrow d_H(C) = w_H(C)$.

# Construction of Codes: Plotkin's Construction

There are many known methods for constructing longer codes from shorter ones.

# Construction of Codes: Plotkin's Construction

There are many known methods for constructing longer codes from shorter ones.

*Plotkin's* $(\mathbf{u} \mid \mathbf{u}+\mathbf{v})$*-construction*, where $C_i \subseteq \mathbb{F}_q^n, i = 1, 2$ be codes over $\mathbb{F}_q$ and $\mathbf{u} \in C_1, \mathbf{v} \in C_2$, gives a $(2n, |C_1| \cdot |C_2|, \min\{2d_1, d_2\})$ code.

# Construction of Codes: Plotkin's Construction

There are many known methods for constructing longer codes from shorter ones.

*Plotkin's* $(\mathbf{u} \mid \mathbf{u}+\mathbf{v})$*-construction*, where $C_i \subseteq \mathbb{F}_q^n, i = 1, 2$ be codes over $\mathbb{F}_q$ and $\mathbf{u} \in C_1, \mathbf{v} \in C_2$, gives a $(2n, |C_1| \cdot |C_2|, \min\{2d_1, d_2\})$ code.

This construction can be rewritten as the following form:

$$[C_1, C_2] \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \left\{ (\mathbf{u}, \mathbf{v}) \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \;\middle|\; \mathbf{u} \in C_1, \mathbf{v} \in C_2 \right\}.$$

# Construction of Codes: Another Construction

*The* $(\mathbf{u}+\mathbf{v}+\mathbf{w}\,|\,2\mathbf{u}+\mathbf{v}\,|\,\mathbf{u})$*-construction* gives a code with parameters

$$(3n, |C_1|\cdot|C_2|\cdot|C_3|, \min\{3d_1, 2d_2, d_3\}),$$

where $\mathbf{u}\in C_1, \mathbf{v}\in C_2, \mathbf{w}\in C_3$.

# Construction of Codes: Another Construction

*The* $(\mathbf{u}+\mathbf{v}+\mathbf{w}\,|\,2\mathbf{u}+\mathbf{v}\,|\,\mathbf{u})$*-construction* gives a code with parameters

$$(3n, |C_1|\cdot|C_2|\cdot|C_3|, \min\{3d_1, 2d_2, d_3\}),$$

where $\mathbf{u}\in C_1, \mathbf{v}\in C_2, \mathbf{w}\in C_3$.

The $(\mathbf{u}+\mathbf{v}+\mathbf{w}\,|\,2\mathbf{u}+\mathbf{v}\,|\,\mathbf{u})$-construction can be written as follows.

$$[C_1, C_2, C_3]\begin{pmatrix}1 & 2 & 1\\ 1 & 1 & 0\\ 1 & 0 & 0\end{pmatrix} = \left\{(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)\begin{pmatrix}1 & 2 & 1\\ 1 & 1 & 0\\ 1 & 0 & 0\end{pmatrix} \;\middle|\; \mathbf{c}_j \in C_j\right\}.$$

# Construction of Codes: Turyn's Construction

## Turyn's $(\mathbf{a}+\mathbf{x}\,|\,\mathbf{b}+\mathbf{x}\,|\,\mathbf{a}+\mathbf{b}+\mathbf{x})$-construction

$$C=[C_1,C_1,C_2]T=\left\{(\mathbf{a},\mathbf{b},\mathbf{x})\begin{pmatrix}1&0&1\\0&1&1\\1&1&1\end{pmatrix}\;\middle|\;\mathbf{a},\mathbf{b}\in C_1,\mathbf{x}\in C_2\right\}.$$

# Construction of Codes: Turyn's Construction

Turyn's $(\mathbf{a}+\mathbf{x}\,|\,\mathbf{b}+\mathbf{x}\,|\,\mathbf{a}+\mathbf{b}+\mathbf{x})$-construction

$$C=[C_1,C_1,C_2]T=\left\{(\mathbf{a},\mathbf{b},\mathbf{x})\begin{pmatrix}1&0&1\\0&1&1\\1&1&1\end{pmatrix}\;\middle|\;\mathbf{a},\mathbf{b}\in C_1,\mathbf{x}\in C_2\right\}.$$

Forney gave an estimation about Hamming distance bound for this construction:

$$\min\{d_H(C_1\cap C_2),\,2d_H(C_1),3d_H(C_2)\}\geq$$
$$d_H(C)\geq\min\{d_H(C_1\cap C_2),\,2d_H(C_1),3d_H(C_1+C_2)\}.$$

# Construction of Codes: Turyn's Construction

Turyn's $(\mathbf{a}+\mathbf{x}\,|\,\mathbf{b}+\mathbf{x}\,|\,\mathbf{a}+\mathbf{b}+\mathbf{x})$-construction

$$C=[C_1,C_1,C_2]T=\left\{(\mathbf{a},\mathbf{b},\mathbf{x})\begin{pmatrix}1&0&1\\0&1&1\\1&1&1\end{pmatrix}\;\middle|\;\mathbf{a},\mathbf{b}\in C_1,\mathbf{x}\in C_2\right\}.$$

Forney gave an estimation about Hamming distance bound for this construction:

$$\min\{d_H(C_1\cap C_2),\,2d_H(C_1),3d_H(C_2)\}\geq$$
$$d_H(C)\geq\min\{d_H(C_1\cap C_2),\,2d_H(C_1),3d_H(C_1+C_2)\}.$$

---

G. D. Forney, *Coset codes II: binary lattices*, IEEE Trans. Inform. Theory, **34** (1988), 1152–1187.

# Construction of Codes: Matrix Product Codes

Blackmore and Norton (2001) generalized these constructions to a more general setting.

Let $C_j$ be $(n, M_j)$ codes over $\mathbb{F}_q, 1 \le j \le m$,
A be an $m \times l$ matrix over $\mathbb{F}_q$.
A *matrix product code* (MPC) $C = [C_1, \cdots, C_m]A$ over $\mathbb{F}_q$ is the set of all the matrix products (as codewords)

$$(\mathbf{c}_1, \cdots, \mathbf{c}_m)A = \begin{pmatrix} c_{11}a_{11} + \cdots + c_{1m}a_{m1} & \cdots & c_{11}a_{1l} + \cdots + c_{1m}a_{ml} \\ \cdots & \cdots & \cdots \\ c_{n1}a_{11} + \cdots + c_{nm}a_{m1} & \cdots & c_{n1}a_{1l} + \cdots + c_{nm}a_{ml} \end{pmatrix},$$

where $\mathbf{c}_j$'s are written as $n \times 1$ column vectors. That is:

$$C = [C_1, \cdots, C_m]A = \{(\mathbf{c}_1, \cdots, \mathbf{c}_m)A \,|\, \mathbf{c}_j \in C_j\}.$$

# Construction of Codes: Matrix Product Codes

Blackmore and Norton (2001) generalized these constructions to a more general setting.

Let $C_j$ be $(n, M_j)$ codes over $\mathbb{F}_q, 1 \leq j \leq m$,
A be an $m \times l$ matrix over $\mathbb{F}_q$.
A *matrix product code* (MPC) $C = [C_1, \cdots, C_m]A$ over $\mathbb{F}_q$ is the set of all the matrix products (as codewords)

$$(\mathbf{c}_1, \cdots, \mathbf{c}_m)A = \begin{pmatrix} c_{11}a_{11} + \cdots + c_{1m}a_{m1} & \cdots & c_{11}a_{1l} + \cdots + c_{1m}a_{ml} \\ \cdots & \cdots & \cdots \\ c_{n1}a_{11} + \cdots + c_{nm}a_{m1} & \cdots & c_{n1}a_{1l} + \cdots + c_{nm}a_{ml} \end{pmatrix},$$

where $\mathbf{c}_j$'s are written as $n \times 1$ column vectors. That is:

$$C = [C_1, \cdots, C_m]A = \{(\mathbf{c}_1, \cdots, \mathbf{c}_m)A \,|\, \mathbf{c}_j \in C_j\}.$$

How to determine the parameters of the MPCs?

# Construction of Codes: NSC Matrix

Consider the following three matrices:

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

# Construction of Codes: NSC Matrix

Consider the following three matrices:

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Blackmore and Norton introduced the following concepts.

An $m \times l$ matrix is a *non-singular by columns matrix* (NSC) if for any $1 \leq k \leq m$, and any $1 \leq j_1 < \cdots < j_k \leq l$, the determinant of the following submatrix is nonzero in $\mathbb{F}_q$:

$$\det A(j_1, \cdots, j_k) = \det \begin{pmatrix} a_{1j_1} & \cdots & a_{1j_k} \\ \cdots & \cdots & \cdots \\ a_{kj_1} & \cdots & a_{kj_k} \end{pmatrix} \neq 0.$$

A matrix is called triangular if it is a column permutation of an upper-triangular matrix.

# Construction of Codes: Distance Bound

## Theorem 1.1 (Blackmore-Norton)

Let $C_k$ be $(n, M_k, d_H(C_k))$ codes over $\mathbb{F}_q$ for $1 \leq k \leq m$.

(i) If A is an $m \times l$ NSC matrix over $\mathbb{F}_q$. Then $C$ is a $(nl, \prod_{k=1}^{m} M_k, d_H(C))$ code with the minimum distance

$$d_H(C) \geq \min\{(l-k+1)d_H(C_k) \,|\, 1 \leq k \leq m\}.$$

# Construction of Codes: Distance Bound

## Theorem 1.1 (Blackmore-Norton)

Let $C_k$ be $(n, M_k, d_H(C_k))$ codes over $\mathbb{F}_q$ for $1 \leq k \leq m$.

(i) If A is an $m \times l$ NSC matrix over $\mathbb{F}_q$. Then $C$ is a $(nl, \prod_{k=1}^{m} M_k, d_H(C))$ code with the minimum distance

$$d_H(C) \geq \min\{(l-k+1)d_H(C_k) \,|\, 1 \leq k \leq m\}.$$

(ii) If $A$ is an $m \times m\,(l = m)$ NSC square matrix. Then

$$d_H(C^{\perp}) \geq \min\left\{1 \cdot d_H(C_1^{\perp}), 2 \cdot d_H(C_2^{\perp}), \cdots, m \cdot d_H(C_m^{\perp})\right\}.$$

# Construction of Codes: Distance Bound

## Theorem 1.1 (Blackmore-Norton)

Let $C_k$ be $(n, M_k, d_H(C_k))$ codes over $\mathbb{F}_q$ for $1 \leq k \leq m$.

(i) If A is an $m \times l$ NSC matrix over $\mathbb{F}_q$. Then $C$ is a $(nl, \prod_{k=1}^{m} M_k, d_H(C))$ code with the minimum distance

$$d_H(C) \geq \min\{(l-k+1)d_H(C_k) \,|\, 1 \leq k \leq m\}.$$

(ii) If $A$ is an $m \times m\,(l = m)$ NSC square matrix. Then

$$d_H(C^{\perp}) \geq \min\left\{1 \cdot d_H(C_1^{\perp}), 2 \cdot d_H(C_2^{\perp}), \cdots, m \cdot d_H(C_m^{\perp})\right\}.$$

Furthermore, if $A$ is triangular then the two equalities above hold.

# Construction of Codes: Distance Bound

## Theorem 1.1 (Blackmore-Norton)

Let $C_k$ be $(n, M_k, d_H(C_k))$ codes over $\mathbb{F}_q$ for $1 \le k \le m$.

(i) If A is an $m \times l$ NSC matrix over $\mathbb{F}_q$. Then $C$ is a $(nl, \prod_{k=1}^{m} M_k, d_H(C))$ code with the minimum distance

$$d_H(C) \ge \min\{(l-k+1)d_H(C_k) \,|\, 1 \le k \le m\}.$$

(ii) If $A$ is an $m \times m\,(l = m)$ NSC square matrix. Then

$$d_H(C^{\perp}) \ge \min\left\{1 \cdot d_H(C_1^{\perp}), 2 \cdot d_H(C_2^{\perp}), \cdots, m \cdot d_H(C_m^{\perp})\right\}.$$

Furthermore, if $A$ is triangular then the two equalities above hold.

---

T. Blackmore and G. H. Norton, *Matrix-product codes over* $\mathbb{F}_q$, Appl. Algebra Engrg. Comm. Comput., **12** (2001), 477–500.

# Construction of Codes: Distance Bound-Continued

## Theorem 1.2 (van Asch)

Let $R$ be a finite chain ring. Let $C_k$ be $(n, M_k, d_{hom}(C_k))$ codes over $R$ for $1 \leq k \leq m$.

(i) If A is an $m \times l$ NSC matrix over $R$. Then $C$ is a $(nl, \prod_{j=k}^{m} M_k, d_{hom}(C))$ code with the minimum homogeneous distance

$$d_{hom}(C) \geq \min\{(l-k+1)d_{hom}(C_k) \,|\, 1 \leq k \leq m\}.$$

# Construction of Codes: Distance Bound-Continued

## Theorem 1.2 (van Asch)

Let $R$ be a finite chain ring. Let $C_k$ be $(n, M_k, d_{hom}(C_k))$ codes over $R$ for $1 \leq k \leq m$.

(i) If A is an $m \times l$ NSC matrix over $R$. Then $C$ is a $(nl, \prod_{j=k}^{m} M_k, d_{hom}(C))$ code with the minimum homogeneous distance

$$d_{hom}(C) \geq \min\{(l-k+1)d_{hom}(C_k) \,|\, 1 \leq k \leq m\}.$$

(ii) If $A$ is an $m \times m\,(l = m)$ NSC square matrix. Then

$$d_{hom}(C^{\perp}) \geq \min\left\{1 \cdot d_{hom}(C_1^{\perp}), 2 \cdot d_{hom}(C_2^{\perp}), \cdots, m \cdot d_{hom}(C_m^{\perp})\right\}.$$

# Construction of Codes: Distance Bound-Continued

## Theorem 1.2 (van Asch)

Let $R$ be a finite chain ring. Let $C_k$ be $(n, M_k, d_{hom}(C_k))$ codes over $R$ for $1 \leq k \leq m$.

(i) If A is an $m \times l$ NSC matrix over $R$. Then $C$ is a $(nl, \prod_{j=k}^{m} M_k, d_{hom}(C))$ code with the minimum homogeneous distance

$$d_{hom}(C) \geq \min\{(l-k+1)d_{hom}(C_k) \,|\, 1 \leq k \leq m\}.$$

(ii) If $A$ is an $m \times m\,(l = m)$ NSC square matrix. Then

$$d_{hom}(C^{\perp}) \geq \min\left\{1 \cdot d_{hom}(C_1^{\perp}), 2 \cdot d_{hom}(C_2^{\perp}), \cdots, m \cdot d_{hom}(C_m^{\perp})\right\}.$$

Furthermore, if $A$ is triangular then the two equalities above hold.

# Construction of Codes: Distance Bound-Continued

## Theorem 1.2 (van Asch)

Let $R$ be a finite chain ring. Let $C_k$ be $(n, M_k, d_{hom}(C_k))$ codes over $R$ for $1 \leq k \leq m$.

(i) If A is an $m \times l$ NSC matrix over $R$. Then $C$ is a $(nl, \prod_{j=k}^{m} M_k, d_{hom}(C))$ code with the minimum homogeneous distance

$$d_{hom}(C) \geq \min\{(l-k+1)d_{hom}(C_k) \,|\, 1 \leq k \leq m\}.$$

(ii) If $A$ is an $m \times m\,(l = m)$ NSC square matrix. Then

$$d_{hom}(C^{\perp}) \geq \min\left\{1 \cdot d_{hom}(C_1^{\perp}), 2 \cdot d_{hom}(C_2^{\perp}), \cdots, m \cdot d_{hom}(C_m^{\perp})\right\}.$$

Furthermore, if $A$ is triangular then the two equalities above hold.

---

B. van Asch, *Matrix-product codes over finite chain rings*, Appl. Algebra Engrg. Comm. Comput., **19** (2008), 39–49.

# What Are We Going to Do?

# What Are We Going to Do?

- Discuss the properties of matrix product codes over finite commutative Frobenius rings.

- Bound the minimum distance of matrix product codes constructed with several types of matrices in different ways.

- Explicitly describe the dual codes of matrix product codes in terms of matrix product codes again.

# Matrices over Rings: Notations

$R$, a finite commutative ring with identity $1 \neq 0$. Writing the identity element 1 of the ring $R$ as the sum of the primitive idempotents of $R$, we obtain an isomorphism

$$R \xrightarrow[\varphi]{\cong} R_1 \oplus \cdots \oplus R_s, \quad r \longmapsto (r^{(1)}, \cdots, r^{(s)}), \tag{2.1}$$

where $R_1, \cdots, R_s$ are local commutative rings.

With the isomorphism (2.1), in the following we usually identify $R$ with $R_1 \oplus \cdots \oplus R_s$ and just write $r = (r^{(1)}, \cdots, r^{(s)})$.

# Matrices over Rings: Frobenius Rings

R is called Frobenius if $(C^{\perp})^{\perp} = C$ for any submodule $C$ of any free $R$-module $R^n$.

- $R$ is Frobenius $\Rightarrow |C^{\perp}||C| = |R|^n$ for any submodule $C$ of $R^n$.
- The reason that finite Frobenius rings are suitable for coding alphabets is that two fundamental theorems (Macwilliams identity and Macwilliams extension theorem) hold (Jay Wood, 1999).
- With the isomorphism (2.1), $R$ is Frobenius $\Leftrightarrow$ every local component $R_i$ is Frobenius.

# Matrices over Rings: Notations-Continued

A matrix $A = (a_{ij})_{m\times l} \in \mathrm{M}_{m\times l}(R)$ can be written as

$$A = \left(A^{(1)}, \cdots, A^{(s)}\right), \quad A^{(k)} = \left(a_{ij}^{(k)}\right)_{m\times l} \in \mathrm{M}_{m\times l}(R_k),\ 1 \le k \le s, \tag{2.2}$$

where the matrix addition and product are the coordinate-wise addition and product, respectively.

Written any element $\mathbf{a} = (a_1, \cdots, a_n)^T \in R^n$ as a column vector. With the identification in (2.1), we can write

$$R^n = R_1^n \oplus \cdots \oplus R_s^n, \quad \mathbf{a} = \left(\mathbf{a}^{(1)}, \cdots, \mathbf{a}^{(s)}\right),$$

where $\mathbf{a}^{(k)} = (a_1^{(k)}, \cdots, a_n^{(k)})^T$ is a column vector in $R_k^n$.

# Matrices over Rings: Linear Independence

For any integer $t \geq 1$, let $\mathbf{a}_i = (a_{i1}, \cdots, a_{in}) \in R^n, i = 1, \cdots, t$.

The vectors $\mathbf{a}_1, \cdots, \mathbf{a}_t$ are said to be *linearly dependent* if there exists $(b_1, \cdots, b_t)$ in the set difference $R^t \setminus \{\mathbf{0}\}$ such that $b_1\mathbf{a}_1 + \cdots + b_t\mathbf{a}_t = \mathbf{0}$; otherwise, $\mathbf{a}_1, \cdots, \mathbf{a}_t$ are said to be *linearly independent*.

# Matrices over Rings: Linear Independence

For any integer $t \geq 1$, let $\mathbf{a}_i = (a_{i1}, \cdots, a_{in}) \in R^n, i = 1, \cdots, t$.

The vectors $\mathbf{a}_1, \cdots, \mathbf{a}_t$ are said to be *linearly dependent* if there exists $(b_1, \cdots, b_t)$ in the set difference $R^t \setminus \{\mathbf{0}\}$ such that $b_1\mathbf{a}_1 + \cdots + b_t\mathbf{a}_t = \mathbf{0}$; otherwise, $\mathbf{a}_1, \cdots, \mathbf{a}_t$ are said to be *linearly independent*.

The vectors $\mathbf{a}_1, \cdots, \mathbf{a}_t \in R^n$ are linearly independent if and only if, for all $k$ with $1 \leq k \leq s$, the vectors $\mathbf{a}_1^{(k)}, \cdots, \mathbf{a}_t^{(k)} \in R_k^n$ are linearly independent.

# Matrices over Rings: Linear Independence

For any integer $t \geq 1$, let $\mathbf{a}_i = (a_{i1}, \cdots, a_{in}) \in R^n, i = 1, \cdots, t$.

The vectors $\mathbf{a}_1, \cdots, \mathbf{a}_t$ are said to be *linearly dependent* if there exists $(b_1, \cdots, b_t)$ in the set difference $R^t \setminus \{\mathbf{0}\}$ such that $b_1\mathbf{a}_1 + \cdots + b_t\mathbf{a}_t = \mathbf{0}$; otherwise, $\mathbf{a}_1, \cdots, \mathbf{a}_t$ are said to be *linearly independent*.

The vectors $\mathbf{a}_1, \cdots, \mathbf{a}_t \in R^n$ are linearly independent if and only if, for all $k$ with $1 \leq k \leq s$, the vectors $\mathbf{a}_1^{(k)}, \cdots, \mathbf{a}_t^{(k)} \in R_k^n$ are linearly independent.

If an $R$-submodule of $R^n$ is generated by vectors $\mathbf{a}_1, \cdots, \mathbf{a}_t$ which are linearly independent, then it is a free $R$-module of rank $t$ and we say that $\mathbf{a}_1, \cdots, \mathbf{a}_t$ form a *basis* of the free submodule.

# Matrices over Rings: Definitions

Let $A = (a_{ij})_{m \times l}$ be a matrix over $R$.

- If the rows of $A$ are linearly independent, then we say that $A$ is a *full-row-rank (FRR)* matrix.

- If there is an $l \times m$ matrix $B$ over $R$ such that $AB = I$, then we say that $A$ is *right-invertible* and $B$ is a right inverse of $A$.

- If $m = l$ and the determinant $\det A$ is a unit of $R$, then we say that $A$ is *non-singular*.

- If, for every $t$ with $1 \leq t \leq m$, any $t \times t$ submatrix of the first (resp., last) $t$ rows of $A$ is non-singular, then we say that $A$ is *non-singular by columns* (resp., *reversely non-singular by columns*).

# Matrices over Rings: Solutions of LES

## Proposition 2.1

Let $A \in \mathrm{M}_{m\times l}(R)$ be FRR and let $X = (x_1, \cdots, x_l)^T$, where $x_i$'s are variables. Then the set of solutions of the linear equation system (LES) $AX = \mathbf{0}$ is a free submodule in $R^l$ of rank $l - m$ and we have an FRR $(l - m) \times l$ matrix $G$ over $R$ whose rows form a basis of this free submodule.

# Matrices over Rings: Solutions of LES

## Proposition 2.1

Let $A \in \mathrm{M}_{m\times l}(R)$ be FRR and let $X = (x_1, \cdots, x_l)^T$, where $x_i$'s are variables. Then the set of solutions of the linear equation system (LES) $AX = \mathbf{0}$ is a free submodule in $R^l$ of rank $l - m$ and we have an FRR $(l - m) \times l$ matrix $G$ over $R$ whose rows form a basis of this free submodule.

Idea of proof:

- $R$ is local $\Rightarrow$ there exists an invertible $l \times l$ matrix $P$ over $R$ such that $AP = (\, I \mid 0\,)_{m\times l}$. Write $AX = \mathbf{0}$ as $(AP)(P^{-1}X) = \mathbf{0}$.
- From local to general case.

# Matrix Product Codes: Notations

$A = (a_{ij})_{m\times l} \in \mathrm{M}_{m\times l}(R)$. For any index $1 \le k \le m$.

$U_A(k)$: linear code over $R$ of length $l$ generated by the $i$th rows of $A$, for $i = 1, 2, \cdots, k$.

$L_A(k)$: linear code over $R$ of length $l$ generated by the $i$th rows of $A$, for $i = k, k+1, \cdots, m$.

$U_A(m) = L_A(1)$: linear code over $R$ of length $l$ generated by all the rows of $A$. Convention: $U_A(0) = L_A(m+1) = \{0\}$.

Using the notation above, the set of solutions of the linear equation system $AX = \mathbf{0}$ is the dual code $L_A(1)^\perp$ of the code $L_A(1)$.

If $A$ is FRR then $L_A(1)^\perp = L_G(1)$, where $G$ is defined in Prop 2.1.

# Matrix Product Codes: Distance Bound

$C_j$: $(n, M_j)$ codes over $R (j = 1, \cdots, m)$ . $A = (a_{ij})_{m \times l}$: FRR matrix over $R$. Matrix product code

$$[C_1, \cdots, C_m]A = \{(\mathbf{c}_1, \cdots, \mathbf{c}_m)A \mid \mathbf{c}_1 \in C_1, \cdots, \mathbf{c}_m \in C_m\}. \quad (3.1)$$

# Matrix Product Codes: Distance Bound

$C_j$: $(n, M_j)$ codes over $R (j = 1, \cdots, m)$ . $A = (a_{ij})_{m \times l}$: FRR matrix over $R$. Matrix product code

$$[C_1, \cdots, C_m]A = \{(\mathbf{c}_1, \cdots, \mathbf{c}_m)A \mid \mathbf{c}_1 \in C_1, \cdots, \mathbf{c}_m \in C_m\}. \quad (3.1)$$

## Theorem 3.1

Assume the notations given above. Let $w$ be a weight on $R$. Then $C = [C_1, \cdots, C_m]A$ is an $\left(nl, \prod_{j=1}^{m} M_j\right)$ code over $R$ with minimum distance $d_w(C)$ satisfying

$$d_w(C) \geq \min\left\{d_H(C_k) d_w\left(U_A(k)\right) \mid k = 1, \cdots, m\right\}, \quad (3.2U)$$

$$d_w(C) \geq \min\left\{d_H(C_k) d_w\left(L_A(k)\right) \mid k = 1, \cdots, m\right\}. \quad (3.2L)$$

# Matrix Product Codes: Distance Bound-Continued

Idea of proof:

# Matrix Product Codes: Distance Bound-Continued

Idea of proof:

(i) $\boxed{A \text{ is FRR}} + \boxed{\text{Equation 3.1}} \Rightarrow C$ is an $\left(nl, \prod_{j=1}^{m} M_j\right)$ code.

# Matrix Product Codes: Distance Bound-Continued

Idea of proof:

(i) $\boxed{A \text{ is FRR}} + \boxed{\text{Equation 3.1}} \Rightarrow C$ is an $\left(nl, \prod_{j=1}^{m} M_j\right)$ code.

(ii) For any $\mathbf{c} \neq \mathbf{c}' \in C$. Write $\mathbf{c}_j - \mathbf{c}'_j = \mathbf{b}_j$. There is an index $k$ such that $\mathbf{b}_j = \mathbf{0}$ for all $j < k$ but $\mathbf{b}_k \neq \mathbf{0}$.

# Matrix Product Codes: Distance Bound-Continued

Idea of proof:

(i) $\boxed{A \text{ is FRR}} + \boxed{\text{Equation 3.1}} \Rightarrow C$ is an $\left(nl, \prod_{j=1}^{m} M_j\right)$ code.

(ii) For any $\mathbf{c} \neq \mathbf{c}' \in C$. Write $\mathbf{c}_j - \mathbf{c}'_j = \mathbf{b}_j$. There is an index $k$ such that $\mathbf{b}_j = \mathbf{0}$ for all $j < k$ but $\mathbf{b}_k \neq \mathbf{0}$.

$$\mathbf{c} - \mathbf{c}' = (\mathbf{0}, \cdots, \mathbf{0}, \mathbf{b}_k, \cdots, \mathbf{b}_m)A = (\mathbf{b}_k, \cdots, \mathbf{b}_m) \begin{pmatrix} A_k \\ \vdots \\ A_m \end{pmatrix}.$$

# Matrix Product Codes: Distance Bound-Continued

Idea of proof:

(i) $\boxed{A \text{ is FRR}} + \boxed{\text{Equation 3.1}} \Rightarrow C$ is an $\left(nl, \prod_{j=1}^{m} M_j\right)$ code.

(ii) For any $\mathbf{c} \neq \mathbf{c}' \in C$. Write $\mathbf{c}_j - \mathbf{c}'_j = \mathbf{b}_j$. There is an index $k$ such that $\mathbf{b}_j = \mathbf{0}$ for all $j < k$ but $\mathbf{b}_k \neq \mathbf{0}$.

$$\mathbf{c} - \mathbf{c}' = (\mathbf{0}, \cdots, \mathbf{0}, \mathbf{b}_k, \cdots, \mathbf{b}_m)A = (\mathbf{b}_k, \cdots, \mathbf{b}_m) \begin{pmatrix} A_k \\ \vdots \\ A_m \end{pmatrix}.$$

For each nonzero $b_{ik}$, the weight of the $i$th row of $\mathbf{c} - \mathbf{c}'$ is:

$$w(b_{ik}A_k + b_{i,k+1}A_{k+1} + \cdots + b_{im}A_m) \geq d_w(L_A(k)).$$

# Matrix Product Codes: Distance Bound-Continued

Idea of proof:

(i) $\boxed{A \text{ is FRR}} + \boxed{\text{Equation 3.1}} \Rightarrow C$ is an $\left(nl, \prod_{j=1}^{m} M_j\right)$ code.

(ii) For any $\mathbf{c} \neq \mathbf{c}' \in C$. Write $\mathbf{c}_j - \mathbf{c}'_j = \mathbf{b}_j$. There is an index $k$ such that $\mathbf{b}_j = \mathbf{0}$ for all $j < k$ but $\mathbf{b}_k \neq \mathbf{0}$.

$$\mathbf{c} - \mathbf{c}' = (\mathbf{0}, \cdots, \mathbf{0}, \mathbf{b}_k, \cdots, \mathbf{b}_m)A = (\mathbf{b}_k, \cdots, \mathbf{b}_m) \begin{pmatrix} A_k \\ \vdots \\ A_m \end{pmatrix}.$$

For each nonzero $b_{ik}$, the weight of the $i$th row of $\mathbf{c} - \mathbf{c}'$ is:

$$w(b_{ik}A_k + b_{i,k+1}A_{k+1} + \cdots + b_{im}A_m) \geq d_w(L_A(k)).$$

(iii) The proof of the second inequality is similar.

# Matrix Product Codes: Duals of MPCs

The following result describes the dual of a matrix product code constructed with an FRR matrix.

## Theorem 3.2

Let $C_1, \cdots, C_m$ be codes over a Frobenius ring $R$ of length $n$, and let $A \in \mathrm{M}_{m\times l}(R)$ be FRR. Assume that $B \in \mathrm{M}_{l\times m}(R)$ is a right inverse of $A$ and $G \in \mathrm{M}_{(l-m)\times l}(R)$ is a generator matrix of the dual code $L_A(1)^\perp$ of $L_A(1)$. Set $\tilde{B} = \left(B \mid G^T\right)$. Then the dual code of $C = [C_1, \cdots, C_m]A$ is

$$\begin{aligned} C^\perp &= [\, C_1^\perp, \cdots, C_m^\perp, \underbrace{R^n, \cdots, R^n}_{l-m}]\tilde{B}^T \\ &= [C_1^\perp, \cdots, C_m^\perp]B^T + \mathrm{M}_{n\times(l-m)}(R)G. \end{aligned}$$

# Matrix Product Codes: Duals of MPCs

The following result describes the dual of a matrix product code constructed with an FRR matrix.

## Theorem 3.2

Let $C_1, \cdots, C_m$ be codes over a Frobenius ring $R$ of length $n$, and let $A \in \mathrm{M}_{m\times l}(R)$ be FRR. Assume that $B \in \mathrm{M}_{l\times m}(R)$ is a right inverse of $A$ and $G \in \mathrm{M}_{(l-m)\times l}(R)$ is a generator matrix of the dual code $L_A(1)^\perp$ of $L_A(1)$. Set $\tilde{B} = \left(B \mid G^T\right)$. Then the dual code of $C = [C_1, \cdots, C_m]A$ is

$$\begin{aligned} C^\perp &= [\, C_1^\perp, \cdots, C_m^\perp, \underbrace{R^n, \cdots, R^n}_{l-m}]\tilde{B}^T \\ &= [C_1^\perp, \cdots, C_m^\perp]B^T + \mathrm{M}_{n\times(l-m)}(R)G. \end{aligned}$$

Note that here we don't need $A$ to be square.

# Matrix Product Codes: Duals-Continued

Idea of proof:

# Matrix Product Codes: Duals-Continued

Idea of proof:

We can prove that $\tilde{B} = \left(B \mid G^T\right)$ is invertible such that $A$ is the $m \times l$ submatrix of $\tilde{A} = \tilde{B}^{-1} = \left(\frac{A}{A'}\right)$. Then

$$C = [C_1, \cdots, C_m]A = [C_1, \cdots, C_m, \underbrace{0, \cdots, 0}_{l-m}]\tilde{A}.$$

# Matrix Product Codes: Duals-Continued

Idea of proof:

We can prove that $\tilde{B} = \left(B \mid G^T\right)$ is invertible such that $A$ is the $m \times l$ submatrix of $\tilde{A} = \tilde{B}^{-1} = \left(\frac{A}{A'}\right)$. Then

$$C = [C_1, \cdots, C_m]A = [C_1, \cdots, C_m, \underbrace{0, \cdots, 0}_{l-m}]\tilde{A}.$$

Show that

$$[C_1^{\perp}, \cdots, C_m^{\perp}, \underbrace{R^n, \cdots, R^n}_{l-m}]\tilde{B}^T \subseteq C^{\perp}.$$

# Matrix Product Codes: Duals-Continued

Idea of proof:

We can prove that $\tilde{B} = \left(B \,|\, G^T\right)$ is invertible such that $A$ is the $m \times l$ submatrix of $\tilde{A} = \tilde{B}^{-1} = \left(\frac{A}{A'}\right)$. Then

$$C = [C_1, \cdots, C_m]A = [C_1, \cdots, C_m, \underbrace{0, \cdots, 0}_{l-m}]\tilde{A}.$$

Show that

$$[C_1^{\perp}, \cdots, C_m^{\perp}, \underbrace{R^n, \cdots, R^n}_{l-m}]\tilde{B}^T \subseteq C^{\perp}.$$

$R$ is Frobenius $\Rightarrow |[C_1^{\perp}, \cdots, C_m^{\perp}, \underbrace{R^n, \cdots, R^n}_{l-m}]\tilde{B}^T| = |C^{\perp}|$.

# SFRR Matrices: Singleton Bound

Let $C$ be a nonzero code of length $n$ over a finite commutative ring $R$. The following is the *Singleton bound* for codes over $R$:

$$d_H(C) \leq n - \log_{|R|} |C| + 1. \tag{4.1}$$

If $C$ is a free code over $R$ of length $l$, then the equation above becomes

$$d_H(C) \leq l - \mathrm{rank}(C) + 1.$$

If the equality holds in (4.1), then we say that $C$ is a *maximum distance separable* (MDS) code over $R$.

A free code of length $l$ and rank $m$, which we shall call an $[l, m]$ code (over $R$), has FRR generator matrices of size $m \times l$.

# SFRR Matrices: Definitions

Let $A$ be an FRR $m \times l$ matrix over $R$.

(i) If $U_A(m) = L_A(1)$ is an $[l, m]$ MDS code, then we say that $A$ is a *strongly full-row-rank (SFRR) matrix*.

(ii) For $t \geq 2$, if there is a sequence of indices $0 = i_0 < i_1 < \cdots < i_t = m$ such that $U_A(i_h)$, for $h = 0, 1, \cdots, t$, are MDS codes, then we say that $A$ is an *$(i_1, \cdots, i_{t-1})$-SFRR matrix*. (When $t = 1$, $A$ is just an SFRR matrix.)

(iii) For $t \geq 2$, if there is a sequence of indices $1 = i_0 < i_1 < \cdots < i_{t-1} < i_t = m + 1$ such that $L_A(i_h)$, for $h = 0, 1, \cdots, t$, are MDS codes, then we say that $A$ is a *reversely $(i_1, \cdots, i_{t-1})$-SFRR matrix*. (When $t = 1$, $A$ is just an SFRR matrix.)

# SFRR Matrices: Some Properties

Suppose $A \in \mathrm{M}_{m\times l}(R)$ is FRR. We have the following proposition.

## Proposition 4.2

Let $0 = i_0 < i_1 < \cdots < i_t = m$. Assume that $\tilde{A} \in \mathrm{M}_{l\times l}(R)$ is an invertible matrix with $A$ as the submatrix consisting of its first $m$ rows. Then the following are equivalent.

(i) $A$ is an $(i_1, \cdots, i_{t-1})$-SFRR matrix.

(ii) $(\tilde{A}^{-1})^T$ is a reversely $(i_1+1, \cdots, i_{t-1}+1, m+1)$-SFRR matrix (or, if $m = l$, a reversely $(i_1+1, \cdots, i_{t-1}+1)$-SFRR matrix).

# SFRR Matrices: Some Properties–Continued

## Corollary 4.1

Let $A \in \mathrm{M}_{m\times l}(R)$ be FRR. Assume that $\tilde{A} \in \mathrm{M}_{l\times l}(R)$ is an invertible matrix that has $A$ as the submatrix of its first $m$ rows. Then the following statements are equivalent:

(i) $A$ is non-singular by columns.

(ii) $A$ is a $(1, 2, \cdots, m-1)$-SFRR matrix.

(iii) $(\tilde{A}^{-1})^T$ is a reversely $(2, \cdots, m, m+1)$-SFRR matrix. (When $m = l$, $(\tilde{A}^{-1})^T$ is a reversely $(2, \cdots, m)$-SFRR matrix.)

In particular, when $m = l$, the square matrix $A$ is non-singular by columns if and only if $(A^{-1})^T$ is reversely non-singular by columns.

# SFRR Matrices: An Example

## Example 4.1

$T = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$, for the $(a+x|b+x|a+b+x)$-construction.

- $T$ is a (2)-SFRR matrix.
- $T$ is not NSC, since $U_T(1)$ is not MDS.
- $T$ is also a reversely (3)-SFRR matrix.
- $(T^{-1})^T = \begin{pmatrix} 0 & -1 & 1 \\ -1 & 0 & 1 \\ 1 & 1 & -1 \end{pmatrix}$ is a reversely (3)-SFRR matrix.

# SFRR Matrices: Hamming Distance Lower Bound

## Theorem 4.1

Let $A \in \mathrm{M}_{m\times l}(R)$ be an $(i_1, \cdots, i_{t-1})$-SFRR matrix, where $0 = i_0 < i_1 < \cdots < i_t = m$. Let $C_1, \cdots, C_m$ be codes over $R$ of length $n$ and let $C = [C_1, \cdots, C_m]A$. Then

$$d_H(C) \geq \min\left\{(l - i_h + 1)d_H(C_{k_h}) \mid h = 1, \cdots, t,\ i_{h-1} < k_h \leq i_h\right\}. \tag{4.1U}$$

Furthermore, if the following three conditions are satisfied:

(E1) $C_1, \cdots, C_m$ are linear,

(E2) $C_1 = \cdots = C_{i_1}$, $C_{i_1+1} = \cdots = C_{i_2}$, $\cdots$, $C_{i_{t-1}+1} = \cdots = C_{i_t} (= C_m)$,

(E3) $C_{i_1} \supseteq C_{i_2} \supseteq \cdots \supseteq C_{i_t}$,

then

$$d_H(C) = \min\left\{(l - i_h + 1)d_H(C_{i_h}) \mid h = 1, \cdots, t\right\}. \tag{4.2U}$$

# SFRR Matrices: Sketch Proof of Theorem 4.1

**Idea of proof** (I) By Theorem 3.1 (3.2U), we have

$$d_H(C) \geq \min\left\{d_H(U_A(k))d_H(C_k) \mid 1 \leq k \leq m\right\}.$$

$$\boxed{i_{h-1} < k \leq i_h \Rightarrow U_A(k) \subseteq U_A(i_h)} + \boxed{d_H(U_A(i_h)) = l - i_h + 1}$$

$$d_H(U_A(k))d_H(C_k) \geq (l - i_h + 1)d_H(C_k), \qquad i_{h-1} < k \leq i_h.$$

(II) Set $m_h = i_h - i_{h-1}$, for $h = 1, \cdots, t$. We can show that there is a block lower triangular matrix $Q$ such that $QA$ is a block upper triangular matrix

$$QA = \begin{pmatrix} Q_1 & & & \\ * & Q_2 & & \\ \vdots & \ddots & \ddots & \\ * & \cdots & * & Q_t \end{pmatrix} A = \begin{pmatrix} I_{m_1} & * & \cdots & * & \cdots & * \\ & I_{m_2} & \cdots & * & \cdots & * \\ & & \ddots & \vdots & \vdots & \vdots \\ & & & I_{m_t} & \cdots & * \end{pmatrix}.$$

# SFRR Matrices: Sketch Proof-Continued

The matrix $Q_h$ is an invertible $m_h \times m_h$ matrix for each $h = 1, \cdots, t$, and the $i_h$th row of $QA$ takes the form

$$\big(\underbrace{0, \cdots, 0}_{i_h - 1}, 1, u_{i_h, i_h+1}, \cdots, u_{i_h, l}\big)$$

with $u_{i_h,j}$ being a unit of $R$ for every $j = i_h + 1, \cdots, l$.

Using (E1),(E2) and (E3), one can get

$$C = [C_1, \cdots, C_m]A = ([C_1, \cdots, C_m]Q^{-1})QA = [C_1, \cdots, C_m]QA.$$

Inequality (4.1U) in Theorem 4.1 + Condition (E2) implies

$$d_H(C) \geq \min\big\{(l - i_h + 1)d_H(C_{i_h}) \mid h = 1, \cdots, t\big\}.$$

# SFRR Matrices: Sketch Proof-Continued

Now it is enough to show, for each $h$ with $1 \leq h \leq t$, there is some $\mathbf{c} \in C$ such that $w_H(\mathbf{c}) = (l - i_h + 1)d_H(C_{i_h})$.

Take $\mathbf{c}_{i_h} = (c_1, \cdots, c_n)^T \in C_{i_h}$ such that $w_H(\mathbf{c}_{i_h}) = d_H(C_{i_h})$, and take a codeword $\mathbf{c} \in C$:

$$\mathbf{c} = (\mathbf{0}, \cdots, \mathbf{0}, \mathbf{c}_{i_h}, \mathbf{0}, \cdots, \mathbf{0})(QA) = \big(\underbrace{\mathbf{0}, \cdots, \mathbf{0}}_{i_h - 1}, \mathbf{c}_{i_h}, u_{i_h, i_h+1}\mathbf{c}_{i_h}, \cdots, u_{i_h, l}\mathbf{c}_{i_h}\big).$$

Then

$$w_H(\mathbf{c}) = w_H(\mathbf{c}_{i_h}) + w_H(u_{i_h, i_h+1}\mathbf{c}_{i_h}) + \cdots + w_H(u_{i_h, l}\mathbf{c}_{i_h}) = (l - i_h + 1)d_H(C_{i_h}).$$

# SFRR Matrices: A Dual Version of Theorem 4.1

## Theorem 4.2

Let $A$ be a reversely $(i_1, \cdots, i_{t-1})$-SFRR $m \times l$ matrix over $R$, where $1 = i_0 < i_1 < \cdots < i_{t-1} < i_t = m + 1$. Then

$$d_H(C) \geq \min\left\{(l - m + i_h) d_H(C_{k_h}) \mid h = 0, 1, \cdots, t-1,\ i_h \leq k_h < i_{h+1}\right\}. \tag{4.2L}$$

With further conditions (E1$^*$)=(E1) and

(E2$^*$) $(C_1 =) C_{i_0} = \cdots = C_{i_1 - 1},\ C_{i_1} = \cdots = C_{i_2 - 1},\ \cdots,\ C_{i_{t-1}} = \cdots = C_m$,

(E3$^*$) $C_{i_0} \subseteq C_{i_1} \subseteq \cdots \subseteq C_{i_{t-1}}$,

then

$$d_H(C) = \min\left\{(l - m + i_h) d_H(C_{i_h}) \mid h = 0, 1, \cdots, t-1\right\}. \tag{4.3L}$$

# SFRR Matrices: A Dual Version of Theorem 4.1

## Theorem 4.2

Let $A$ be a reversely $(i_1, \cdots, i_{t-1})$-SFRR $m \times l$ matrix over $R$, where $1 = i_0 < i_1 < \cdots < i_{t-1} < i_t = m + 1$. Then

$$d_H(C) \geq \min\left\{(l - m + i_h) d_H(C_{k_h}) \mid h = 0, 1, \cdots, t-1,\ i_h \leq k_h < i_{h+1}\right\}. \tag{4.2L}$$

With further conditions (E1*)=(E1) and

(E2*) $(C_1 =) C_{i_0} = \cdots = C_{i_1 - 1},\ C_{i_1} = \cdots = C_{i_2 - 1}, \cdots, C_{i_{t-1}} = \cdots = C_m,$

(E3*) $C_{i_0} \subseteq C_{i_1} \subseteq \cdots \subseteq C_{i_{t-1}},$

then

$$d_H(C) = \min\left\{(l - m + i_h) d_H(C_{i_h}) \mid h = 0, 1, \cdots, t-1\right\}. \tag{4.3L}$$

The proof for the dual version is the same as that for Theorem 4.1.

# SFRR Matrices: Duals

Let $A \in \mathrm{M}_{m\times l}(R)$ be an $(i_1, \cdots, i_{t-1})$-SFRR matrix, where $R$ is a finite Frobenius ring and $0 = i_0 < i_1 < \cdots < i_t = m$.

In the following, we estimate the minimum Hamming distance of $C^{\perp}$, where $C = [C_1, \cdots, C_m]A$, $C_1, \cdots, C_m$ are codes of length $n$.

- Dual code of $C$:

$$C^{\perp} = [C_1^{\perp}, \cdots, C_m^{\perp}, \underbrace{R^n, \cdots, R^n}_{l-m}](\tilde{A}^{-1})^T, \tag{4.4}$$

where $\tilde{A} \in \mathrm{M}_{l\times l}(R)$ is an invertible matrix with $A$ as the submatrix consisting of its first $m$ rows.

- If $m < l$, we have $C_{m+1}^{\perp} = \cdots = C_l^{\perp} = R^n$ and set $i_{t+1} = l$ for convenience.

# SFRR Matrices: Duals-Continued

## Theorem 4.3

Let the notations be as above. Then

$$d_H(C^{\perp}) \geq \min\left\{(i_h+1)d_H(C_{k_h}^{\perp}) \mid h = 0, 1, \cdots, t,\ i_h+1 \leq k_h < i_{h+1}+1\right\}. \tag{4.5}$$

Furthermore, if the following three conditions are satisfied:

(E1) $C_1, \cdots, C_m$ are linear,

(E2) $C_1 = \cdots = C_{i_1},\ C_{i_1+1} = \cdots = C_{i_2},\ \cdots,\ C_{i_{t-1}+1} = \cdots = C_{i_t}$,

(E3) $C_{i_1} \supseteq C_{i_2} \supseteq \cdots \supseteq C_{i_t}$,

then the equality holds in (4.5), i.e.,

$$d_H(C^{\perp}) = \min\left\{(i_h+1)d_H(C_{i_h+1}^{\perp}) \mid h = 0, 1, \cdots, t\right\}. \tag{4.6}$$

# SFRR Matrices: Duals-Continued

## Theorem 4.3

Let the notations be as above. Then

$$d_H(C^{\perp}) \geq \min\left\{(i_h+1)d_H(C_{k_h}^{\perp}) \mid h=0,1,\cdots,t,\ i_h+1 \leq k_h < i_{h+1}+1\right\}. \tag{4.5}$$

Furthermore, if the following three conditions are satisfied:

(E1) $C_1,\cdots,C_m$ are linear,

(E2) $C_1=\cdots=C_{i_1}$, $C_{i_1+1}=\cdots=C_{i_2}$, $\cdots$, $C_{i_{t-1}+1}=\cdots=C_{i_t}$,

(E3) $C_{i_1}\supseteq C_{i_2}\supseteq\cdots\supseteq C_{i_t}$,

then the equality holds in (4.5), i.e.,

$$d_H(C^{\perp}) = \min\left\{(i_h+1)d_H(C_{i_h+1}^{\perp}) \mid h=0,1,\cdots,t\right\}. \tag{4.6}$$

If $m<l$, the terms in (4.5) for $h=t$ are: $(i_t+1)d_H(C_{k_t}^{\perp})=m+1$.

# SFRR Matrices: Sketch Proof of Theorem 4.3

$A$ is $(i_1, \cdots, i_{t-1})$-SFRR, $0 = i_0 < i_1 < \cdots < i_t = m$, $\tilde{B} = \tilde{A}^{-1}$.

$\boxed{U_{\tilde{A}}(i_h) = U_A(i_h), \text{ MDS codes}} \Leftrightarrow \boxed{L_{\tilde{B}^T}(i_h + 1), \text{ MDS codes}}$.

$\boxed{\mathrm{rank}\big(L_{\tilde{B}^T}(i_h + 1)\big) = l - i_h} \Rightarrow \boxed{d_H\big(L_{\tilde{B}^T}(i_h + 1)\big) = i_h + 1}$, where $h = 0, 1, \cdots, t$. By Theorem 4.2 (see (4.2L)), we have that

$$d_H(C^{\perp}) \geq \min\Big\{ (i_h+1) d_H(C_{k_h}^{\perp}) \mid h = 0, 1, \cdots, t,\ i_h+1 \leq k_h < i_{h+1}+1 \Big\}.$$

If $i_t = m < l$, for any $k$ with $m < k \leq l, C_k^{\perp} = R^n$, then

$$(i_t+1) d_H(C_{k_t}^{\perp}) = m+1, \qquad i_t+1 = m+1 \leq k_t < l+1 = i_{t+1}+1.$$

$\boxed{\text{Conditions (E1)-(E3) hold}} \Rightarrow \boxed{\text{Conditions (E1}^*\text{)-(E3}^*\text{) hold}}$ for dual codes. By Theorem 4.2 (see (4.3L)), the equality (4.6) holds.

# SFRR Matrices: Special Case

## Corollary 4.2

Let $A \in \mathrm{M}_{m\times l}(R)$ be a $(1, 2, \cdots, m-1)$-SFRR matrix, let $C_1, \cdots, C_m$ be codes of length $n$, and $C = [C_1, \cdots, C_m]A$. Then

$$d_H(C) \geq \min\left\{ l \cdot d_H(C_1), (l-1)d_H(C_2), \cdots, (l-m+1)d_H(C_m) \right\}$$

and

$$d_H(C^\perp) \geq \begin{cases} \min\left\{ 1 \cdot d_H(C_1^\perp), \cdots, m \cdot d_H(C_m^\perp), m+1 \right\} & \text{if } m < l, \\ \min\left\{ 1 \cdot d_H(C_1^\perp), \cdots, m \cdot d_H(C_m^\perp) \right\} & \text{if } m = l. \end{cases}$$

Further, if $C_1, \cdots, C_m$ are linear and $C_1 \supseteq \cdots \supseteq C_m$, then equalities are attained in all these inequalities.

# SFRR Matrices: Special Case

## Corollary 4.2

Let $A \in \mathrm{M}_{m\times l}(R)$ be a $(1, 2, \cdots, m-1)$-SFRR matrix, let $C_1, \cdots, C_m$ be codes of length $n$, and $C = [C_1, \cdots, C_m]A$. Then

$$d_H(C) \geq \min\left\{ l \cdot d_H(C_1), (l-1)d_H(C_2), \cdots, (l-m+1)d_H(C_m) \right\}$$

and

$$d_H(C^\perp) \geq \begin{cases} \min\left\{ 1 \cdot d_H(C_1^\perp), \cdots, m \cdot d_H(C_m^\perp), m+1 \right\} & \text{if } m < l, \\ \min\left\{ 1 \cdot d_H(C_1^\perp), \cdots, m \cdot d_H(C_m^\perp) \right\} & \text{if } m = l. \end{cases}$$

Further, if $C_1, \cdots, C_m$ are linear and $C_1 \supseteq \cdots \supseteq C_m$, then equalities are attained in all these inequalities.

Corollary 4.2 generalizes the results of Blakemore-Norton (2001) and Van-Asch (2008) from two directions:

(I) fields (chain rings) $\Rightarrow$ commutative rings;

(II) square $\Rightarrow$ non-square.

# Two-way (m') Matrices: Turyn's Construction-Revisited

Turyn's $(\mathbf{a}+\mathbf{x}\,|\,\mathbf{b}+\mathbf{x}\,|\,\mathbf{a}+\mathbf{b}+\mathbf{x})$-construction gives a MPC

$$C=[C_1,C_1,C_2]T=\left\{(\mathbf{a},\mathbf{b},\mathbf{x})\begin{pmatrix}1&0&1\\0&1&1\\1&1&1\end{pmatrix}\;\middle|\;\mathbf{a},\mathbf{b}\in C_1,\mathbf{x}\in C_2\right\}.$$

# Two-way (m') Matrices: Turyn's Construction-Revisited

Turyn's $(\mathbf{a}+\mathbf{x}\,|\,\mathbf{b}+\mathbf{x}\,|\,\mathbf{a}+\mathbf{b}+\mathbf{x})$-construction gives a MPC

$$C=[C_1,C_1,C_2]T=\left\{(\mathbf{a},\mathbf{b},\mathbf{x})\begin{pmatrix}1&0&1\\0&1&1\\1&1&1\end{pmatrix}\;\middle|\;\mathbf{a},\mathbf{b}\in C_1,\mathbf{x}\in C_2\right\}.$$

The matrix $T$ is (2)-SFRR and reversely (3)-SFRR, by Theorem 4.1 and Theorem 4.2, we obtain a lower bound for code $C$:

$$d_H(C)\geq \max\left\{\min\{2d_H(C_1),d_H(C_2)\},\ \min\{d_H(C_1),3d_H(C_2)\}\right\}.$$

# Two-way (m') Matrices: Turyn's Construction-Revisited

Turyn's $(\mathbf{a}+\mathbf{x}\,|\,\mathbf{b}+\mathbf{x}\,|\,\mathbf{a}+\mathbf{b}+\mathbf{x})$-construction gives a MPC

$$C=[C_1,C_1,C_2]T=\left\{(\mathbf{a},\mathbf{b},\mathbf{x})\begin{pmatrix}1&0&1\\0&1&1\\1&1&1\end{pmatrix}\;\middle|\;\mathbf{a},\mathbf{b}\in C_1,\mathbf{x}\in C_2\right\}.$$

The matrix $T$ is (2)-SFRR and reversely (3)-SFRR, by Theorem 4.1 and Theorem 4.2, we obtain a lower bound for code $C$:

$$d_H(C)\geq\max\left\{\min\{2d_H(C_1),d_H(C_2)\},\ \min\{d_H(C_1),3d_H(C_2)\}\right\}.$$

Forney's (1988) result for the Hamming distance bound:

$$\min\{d_H(C_1\cap C_2),\,2d_H(C_1),3d_H(C_2)\}\geq d_H(C)\geq\min\{d_H(C_1\cap C_2),\,2d_H(C_1),3d_H(C_1+C_2)\}.$$

Note that the two lower bounds cannot be compared directly, in many cases, the latter is better then the former.

# Two-way (m') Matrices: Definition

We will generalize Forney's result to a more general case.

Let $A \in \mathrm{M}_{m\times l}(R)$ be FRR. $A$ is called a *two-way $(m')$-SFRR* matrix if there is an index $m'$ with $1 \leq m' < m$ such that $A$ is both an $(m')$-SFRR matrix and a reversely $(m'+1)$-SFRR matrix.

# Two-way (m') Matrices: Definition

We will generalize Forney's result to a more general case.

Let $A \in \mathrm{M}_{m\times l}(R)$ be FRR. $A$ is called a *two-way $(m')$-SFRR* matrix if there is an index $m'$ with $1 \leq m' < m$ such that $A$ is both an $(m')$-SFRR matrix and a reversely $(m'+1)$-SFRR matrix.

Set $m' + m'' = m$, any $m \times l$ matrix $A$ can be written as $A = \left(\frac{A'}{A''}\right)$, where $A'$ is an $m' \times l$ matrix consisting of the first $m'$ rows of $A$ while $A''$ is an $m'' \times l$ matrix consisting of the last $m''$ rows of $A$.
With this partitioned form, $A$ is a two-way $(m')$-SFRR matrix if and only if $A'$, $A''$ and $A$ are all SFRR matrices.

# Two-way (m') Matrices: Bounds for Codes

Let $A \in \mathrm{M}_{m\times l}(R)$, let $m' + m'' = m$ with $m' \geq m'' \geq 1$, and let $C'$ and $C''$ be linear codes over $R$ of length $n$. Consider the matrix product code

$$C = [\underbrace{C', \cdots, C'}_{m'}, \underbrace{C'', \cdots, C''}_{m''}]A. \tag{5.1}$$

If $A$ is a two-way $(m')$-SFRR matrix, then from (4.1U) and (4.2L) of Theorem 4.1 and Theorem 4.2, we have a lower bound for $d_H(C)$ as follows:

$$d_H(C) \geq \max\left\{ \begin{array}{l} \min\{(l-m'+1)d_H(C'),\ (l-m+1)d_H(C'')\}, \\ \min\{(l-m+1)d_H(C'),\ (l-m''+1)d_H(C'')\} \end{array} \right\}. \tag{5.2}$$

# Two-way (m') Matrices: Bounds for Codes

Let $C_\cap = C' \cap C''$, we have more bounds for $d_H(C)$ as follows.

## Theorem 5.1

Let the notations be as in (5.1). If $A$ is a two-way $(m')$-SFRR matrix, then

$$d_H(C) \geq \min\left\{(l-m'+1)d_H(C'), (l-m''+1)d_H(C'+C''), (l-m+1)d_H(C_\cap)\right\} \tag{5.3}$$

and

$$d_H(C) \leq \min\left\{(l-m'+1)d_H(C'), (l-m''+1)d_H(C''), (l-m+1)d_H(C_\cap)\right\}. \tag{5.4}$$

Note that the two lower bounds in (5.2) and in (5.3) cannot be compared directly in general, since $d_H(C'')$ in (5.2) and $(l-m''+1)d_H(C'+C'')$ in (5.3) are not comparable in general.

# Two-way (m') Matrices: Idea of Proof

**Idea of proof:** We first consider the upper bound (5.4).

$$\boxed{C = [C', \cdots, C', C'', \cdots, C'']A \supseteq [C', \cdots, C', C_\cap, \cdots, C_\cap]A} \Rightarrow$$

$$d_H(C) \leq \min\left\{(l - m' + 1)d_H(C'), (l - m + 1)d_H(C_\cap)\right\}. \quad (5.5)$$

$$\boxed{C = [C', \cdots, C', C'', \cdots, C'']A \supseteq [C_\cap, \cdots, C_\cap, C'', \cdots, C'']A} \Rightarrow$$

$$d_H(C) \leq \min\left\{(l - m'' + 1)d_H(C''), (l - m + 1)d_H(C_\cap)\right\}. \quad (5.6)$$

For the lower bound (5.3). We partition $A$ as $A = \left(\frac{A'}{A''}\right)$, where $A'$ ($A''$) is the $m' \times l$ ($m'' \times l$) matrix consisting of the first $m'$ (the last $m''$) rows of $A$. By computing the Hamming weight of nonzero codeword $\mathbf{c} = (\mathbf{c}'_1, \cdots, \mathbf{c}'_{m'})A' + (\mathbf{c}''_1, \cdots, \mathbf{c}''_{m''})A''$ of $C$, we can obtain (5.3).

# Two-way (m') Matrices: Turyn's Construction-Revisted

Take $R$ to be the binary field and $T = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$. Then $T$ is a two-way (2)-SFRR matrix. The bounds in (5.3) and (5.4) of Theorem 5.1 give the estimation on the minimum distance of $C$:

$$\begin{aligned} & \min\{d_H(C' \cap C''), 2d_H(C'), 3d_H(C'')\} \geq \\ d_H(C) \quad & \geq \min\{d_H(C' \cap C''), 2d_H(C'), 3d_H(C' + C'')\}. \end{aligned}$$

Another lower bound is given by (5.2):

$$d_H(C) \geq \max\left\{ \min\{2d_H(C'), d_H(C'')\}, \ \min\{d_H(C'), 3d_H(C'')\}\right\}.$$

# Two-way Matrices: An Example, where $R$ is a binary field

Table 5.1

| Code | generator matrix | Code | generator matrix |
|---|---|---|---|
| $C_1$: [4,1,4] | (1,1,1,1) | $C_2 \cap C_1$: [4,0,0] | |
| $C_2$: [4,2,2] | $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$ | $C_2 + C_1$: [4,3,1] | $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ |
| $C_3$: [4,2,2] | $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ | $C_3 \cap C_3'$: [4,1,4] | (1,1,1,1) |
| $C_3'$: [4,2,2] | $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ | $C_3 + C_3'$: [4,3,2] | $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ |

# Two-way Matrices: An Example, where $R$ is a binary field

Table 5.1

| Code | generator matrix | Code | generator matrix |
|---|---|---|---|
| $C_1$: [4,1,4] | (1,1,1,1) | $C_2 \cap C_1$: [4,0,0] | |
| $C_2$: [4,2,2] | $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$ | $C_2 + C_1$: [4,3,1] | $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ |
| $C_3$: [4,2,2] | $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ | $C_3 \cap C_3'$: [4,1,4] | (1,1,1,1) |
| $C_3'$: [4,2,2] | $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ | $C_3 + C_3'$: [4,3,2] | $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ |

Table 5.2

| Code $C$ | parameters | argument for $d_H(C)$ |
|---|---|---|
| $[C_2, C_2, C_1]T$ | $[12, 5, 4]$ | $d_H(C) \geq 4$ (by (5.2)), $d_H(C) \geq 3$ (by (5.3)) |
| $[C_3, C_3, C_3']T$ | $[12, 6, 4]$ | $d_H(C) \geq 4$ (by (5.3)), $d_H(C) \geq 2$ (by (5.2)) |
| $[C_3, C_3, C_1]T$ | $[12, 5, 4]$ | by (4.2U),(note that $C_3 \supseteq C_1$) |

# Acknowledgements


- I thank Professor Jon-Lark Kim, for the invitation and for his hospitality.
- I thank KIAS for their support.

# Thank You