Circulant graphs, nonlinear loop transversal codes and nonassociative loops

Jonathan D.H. Smith

Joint work with Giora Slutzki and Pranava K. Jha

Department of Mathematics,
Iowa State University,
Ames, IA 50011-2064, U.S.A.

e-mail: jdhsmith@iastate.edu

http://orion.math.iastate.edu/jdhsmith/homepage.html
Abstract codes
Abstract codes

Channel: Abelian group \((A, +, 0)\),
Abstract codes

Channel: Abelian group \((A, +, 0)\), elements are (received) words.
Abstract codes

**Channel:** Abelian group \((A, +, 0)\), elements are (received) words.

**Code:** Subset \(K\) of \(A\),
Abstract codes

**Channel:** Abelian group \((A, +, 0)\), elements are *(received)* words.

**Code:** Subset \(K\) of \(A\), elements are *codewords*. 
Abstract codes

**Channel:** Abelian group \((A, +, 0)\), elements are (received) **words**.

**Code:** Subset \(K\) of \(A\), elements are **codewords**.

**Ball** or **error set:** Subset \(B\) of \(A\),
Abstract codes

Channel: Abelian group \((A, +, 0)\), elements are (received) words.

Code: Subset \(K\) of \(A\), elements are codewords.

Ball or error set: Subset \(B\) of \(A\), elements are errors.
Abstract codes

Channel: Abelian group \((A, +, 0)\), elements are (received) words.

Code: Subset \(K\) of \(A\), elements are codewords.

Ball or error set: Subset \(B\) of \(A\), elements are errors.

Restricted addition \(\nabla : K \times B \rightarrow A; (k, b) \mapsto k + b\) is an isomorphism of sets,
Abstract codes

Channel: Abelian group \((A, +, 0)\), elements are (received) words.

Code: Subset \(K\) of \(A\), elements are codewords.

Ball or error set: Subset \(B\) of \(A\), elements are errors.

Restricted addition \(\nabla : K \times B \to A; (k, b) \mapsto k + b\) is an isomorphism of sets, with decoding inverse \(\Delta : A \to K \times B; x \mapsto (x^\delta, x^\varepsilon)\).
Abstract codes

**Channel:** Abelian group \((A, +, 0)\), elements are (received) words.

**Code:** Subset \(K\) of \(A\), elements are codewords.

**Ball** or **error set:** Subset \(B\) of \(A\), elements are errors.

Restricted addition \(\nabla : K \times B \to A; (k, b) \mapsto k + b\) is an isomorphism of sets, with **decoding** inverse \(\Delta : A \to K \times B; x \mapsto (x^\delta, x^\epsilon)\).

**Coding scheme** or “code” \((A, \Delta)\).
Abstract codes

**Channel:** Abelian group \((A, +, 0)\), elements are **received** words.

**Code:** Subset \(K\) of \(A\), elements are **codewords**.

**Ball or error set:** Subset \(B\) of \(A\), elements are **errors**.

Restricted addition \(\nabla: K \times B \rightarrow A; (k, b) \mapsto k + b\) is an isomorphism of sets, with **decoding** inverse \(\Delta: A \rightarrow K \times B; x \mapsto (x^\delta, x^\varepsilon)\).

**Coding scheme** or “code” \((A, \Delta)\).

Then \((k, b) \xrightarrow{\nabla} k + b \xrightarrow{\Delta} ((k + b)^\delta, (k + b)^\varepsilon) = (k, b)\)
Abstract codes

**Channel**: Abelian group \((A, +, 0)\), elements are *(received)* words.

**Code**: Subset \(K\) of \(A\), elements are **codewords**.

**Ball** or **error set**: Subset \(B\) of \(A\), elements are **errors**.

Restricted addition \(\nabla : K \times B \to A; (k, b) \mapsto k + b\) is an isomorphism of sets, with **decoding** inverse \(\Delta : A \to K \times B; x \mapsto (x^\delta, x^\varepsilon)\).

**Coding scheme** or *“code”* \((A, \Delta)\).

Then \((k, b) \overset{\nabla}{\mapsto} k + b \overset{\Delta}{\mapsto} ((k + b)^\delta, (k + b)^\varepsilon) = (k, b)\)
gives \((k + b)^\delta = k\) and \((k + b)^\varepsilon = b\) for codewords \(k\) and errors \(b\),
Abstract codes

**Channel:** Abelian group \((A, +, 0)\), elements are (received) words.

**Code:** Subset \(K\) of \(A\), elements are **codewords**.

**Ball** or **error set:** Subset \(B\) of \(A\), elements are **errors**.

Restricted addition \(\nabla : K \times B \rightarrow A; (k, b) \mapsto k + b\) is an isomorphism of sets, with **decoding** inverse \(\Delta : A \rightarrow K \times B; x \mapsto (x^\delta, x^\varepsilon)\).

**Coding scheme** or “code” \((A, \Delta)\).

Then \((k, b) \xrightarrow{\nabla} k + b \xrightarrow{\Delta} ((k + b)^\delta, (k + b)^\varepsilon) = (k, b)\)
gives \((k + b)^\delta = k\) and \((k + b)^\varepsilon = b\) for codewords \(k\) and errors \(b\),
while \(x \xrightarrow{\Delta} (x^\delta, x^\varepsilon) \xrightarrow{\nabla} x^\delta + x^\varepsilon = x\)
Abstract codes

Channel: Abelian group \((A, +, 0)\), elements are \((\text{received})\) words.

Code: Subset \(K\) of \(A\), elements are \text{codewords}.

Ball or error set: Subset \(B\) of \(A\), elements are \text{errors}.

Restricted addition \(\nabla: K \times B \rightarrow A; (k, b) \mapsto k + b\) is an isomorphism of sets, with \text{decoding} inverse \(\Delta: A \rightarrow K \times B; x \mapsto (x^\delta, x^\varepsilon)\).

Coding scheme or “code” \((A, \Delta)\).

Then \((k, b) \xrightarrow{\nabla} k + b \xrightarrow{\Delta} ((k + b)^\delta, (k + b)^\varepsilon) = (k, b)\)
gives \((k + b)^\delta = k\) and \((k + b)^\varepsilon = b\) for codewords \(k\) and errors \(b\),

while \(x \xrightarrow{\Delta} (x^\delta, x^\varepsilon) \xrightarrow{\nabla} x^\delta + x^\varepsilon = x\)
gives \(x = x^\delta + x^\varepsilon\) for received words \(x\).
Some terminology
Some terminology

Coding scheme \((A, \Delta)\) (or code \(K\)) is:
Some terminology

Coding scheme \((A, \Delta)\) (or code \(K\)) is:

- coherent
Some terminology

Coding scheme \((A, \Delta)\) (or code \(K\)) is:

- **coherent** if \(\forall k \in K, k^\delta = k\)
Some terminology

Coding scheme $(A, \Delta)$ (or code $K$) is:

- **coherent** if $\forall k \in K$, $k^\delta = k$ and $|\delta(B)| = 1$;
Some terminology

Coding scheme \((A, \Delta)\) (or code \(K\)) is:

- **coherent** if \(\forall k \in K\), \(k^\delta = k\) and \(|\delta(B)| = 1\);
- **linear**
Some terminology

Coding scheme \((A, \Delta)\) (or code \(K\)) is:

- **coherent** if \(\forall k \in K, k^\delta = k\) and \(|\delta(B)| = 1\);
- **linear** if \(K\) is a subgroup of \(A\).
Some terminology

Coding scheme \((A, \Delta)\) (or code \(K\)) is:

- **coherent** if \(\forall k \in K\), \(k^\delta = k\) and \(|\delta(B)| = 1\);
- **linear** if \(K\) is a subgroup of \(A\).

The ball \(B\) is **symmetric** if \(B = -B\).
Some terminology

Coding scheme \((A, \Delta)\) (or code \(K\)) is:

- **coherent** if \(\forall k \in K, k^\delta = k\) and \(|\delta(B)| = 1\);
- **linear** if \(K\) is a subgroup of \(A\).

The ball \(B\) is **symmetric** if \(B = -B\).

**Lemma:** Suppose \((A, \Delta)\) is coherent and \(B\) is symmetric.
Some terminology

Coding scheme \((A, \Delta)\) (or code \(K\)) is:

- **coherent** if \(\forall k \in K, k^\delta = k\) and \(|\delta(B)| = 1\);
- **linear** if \(K\) is a subgroup of \(A\).

The ball \(B\) is **symmetric** if \(B = -B\).

**Lemma:** Suppose \((A, \Delta)\) is coherent and \(B\) is symmetric. Then:
Some terminology

Coding scheme \((A, \Delta)\) (or code \(K\)) is:

- **coherent** if \(\forall k \in K, \ k^\Delta = k\) and \(|\delta(B)| = 1\);
- **linear** if \(K\) is a subgroup of \(A\).

The ball \(B\) is **symmetric** if \(B = -B\).

**Lemma:** Suppose \((A, \Delta)\) is coherent and \(B\) is symmetric. Then:

**(a):** The ball contains 0;
Some terminology

Coding scheme \((A, \Delta)\) (or code \(K\)) is:

- **coherent** if \(\forall k \in K, \ k^\Delta \equiv k\) and \(|\delta(B)| = 1\);
- **linear** if \(K\) is a subgroup of \(A\).

The ball \(B\) is **symmetric** if \(B = -B\).

**Lemma:** Suppose \((A, \Delta)\) is coherent and \(B\) is symmetric. Then:

(a): The ball contains \(0\);

(b): \(K \cap B = \{0\}\);
Some terminology

Coding scheme \((A, \Delta)\) (or code \(K\)) is:

- **coherent** if \(\forall k \in K\), \(k\delta = k\) and \(|\delta(B)| = 1\);
- **linear** if \(K\) is a subgroup of \(A\).

The ball \(B\) is **symmetric** if \(B = -B\).

**Lemma:** Suppose \((A, \Delta)\) is coherent and \(B\) is symmetric. Then:

(a): The ball contains 0;
(b): \(K \cap B = \{0\}\);
(c): The error map gives a bijection \(\varepsilon: B \to B; b^\varepsilon = b - 0^\delta\).
Algebra of the ball
For $m \in \mathbb{N}$, define an $m$-ary operation $\mu^m$ on $B$ by

$$b_1 \ldots b_m \mu^m = (b_1 + \ldots + b_m)^\varepsilon$$

for $b_1, \ldots, b_m \in B$. 

Algebra of the ball
Algebra of the ball

For \( m \in \mathbb{N} \), define an \( m \)-ary operation \( \mu^m \) on \( B \) by

\[
b_1 \ldots b_m \mu^m = (b_1 + \ldots + b_m)^c \quad \text{for } b_1, \ldots, b_m \in B.
\]

For \( m = 2 \), write \( b_1 b_2 \mu^2 = b_1 * b_2 \).
Algebra of the ball

For \( m \in \mathbb{N} \), define an \( m \)-ary operation \( \mu^m \) on \( B \) by

\[
b_1 \ldots b_m \mu^m = (b_1 + \ldots + b_m)^\varepsilon \quad \text{for} \quad b_1, \ldots, b_m \in B.
\]

For \( m = 2 \), write \( b_1 b_2 \mu^2 = b_1 \ast b_2 \), commutative binary \textbf{multiplication} on the ball.
Algebra of the ball

For $m \in \mathbb{N}$, define an $m$-ary operation $\mu^m$ on $B$ by

$$b_1 \ldots b_m \mu^m = (b_1 + \ldots + b_m)^\varepsilon \quad \text{for } b_1, \ldots, b_m \in B.$$ 

For $m = 2$, write $b_1 b_2 \mu^2 = b_1 * b_2$, commutative binary multiplication on the ball.

Note that $\mu^m$ only involves $\bigcup_{j=1}^m jB$, 

Algebra of the ball

For $m \in \mathbb{N}$, define an $m$-ary operation $\mu^m$ on $B$ by

$$b_1 \ldots b_m \mu^m = (b_1 + \ldots + b_m)^e$$

for $b_1, \ldots, b_m \in B$.

For $m = 2$, write $b_1 b_2 \mu^2 = b_1 \ast b_2$, commutative binary multiplication on the ball.

Note that $\mu^m$ only involves $\bigcup_{j=1}^{m} jB$, so $(B, \mu^m)$ is a local structure within $A$. 
Algebra of the ball

For $m \in \mathbb{N}$, define an $m$-ary operation $\mu^m$ on $B$ by

$$b_1 \ldots b_m \mu^m = (b_1 + \ldots + b_m)^e$$

for $b_1, \ldots, b_m \in B$.

For $m = 2$, write $b_1 b_2 \mu^2 = b_1 \ast b_2$, commutative binary multiplication on the ball.

Note that $\mu^m$ only involves $\bigcup_{j=1}^{m} jB$, so $(B, \mu^m)$ is a local structure within $A$.

For $m$ in a magma $(M, \circ)$,
Algebra of the ball

For $m \in \mathbb{N}$, define an $m$-ary operation $\mu^m$ on $B$ by
\[ b_1 \ldots b_m \mu^m = (b_1 + \ldots + b_m)^c \quad \text{for } b_1, \ldots, b_m \in B. \]

For $m = 2$, write $b_1 b_2 \mu^2 = b_1 \ast b_2$, commutative binary multiplication on the ball.

Note that $\mu^m$ only involves $\bigcup_{j=1}^{m} jB$, so $(B, \mu^m)$ is a local structure within $A$.

For $m$ in a magma $(M, \circ)$, define left and right multiplications by
\[ L_\circ(m) : M \to M ; x \mapsto m \circ x \quad \text{and} \quad R_\circ(m) : M \to M ; x \mapsto x \circ m. \]
Algebra of the ball

For $m \in \mathbb{N}$, define an $m$-ary operation $\mu^m$ on $B$ by
\[ b_1 \ldots b_m \mu^m = (b_1 + \ldots + b_m)^c \quad \text{for } b_1, \ldots, b_m \in B. \]

For $m = 2$, write $b_1 b_2 \mu^2 = b_1 \ast b_2$, commutative binary multiplication on the ball.

Note that $\mu^m$ only involves $\bigcup_{j=1}^{m} jB$, so $(B, \mu^m)$ is a local structure within $A$.

For $m$ in a magma $(M, \circ)$, define left and right multiplications by
\[ L_{\circ}(m) : M \to M; x \mapsto m \circ x \quad \text{and} \quad R_{\circ}(m) : M \to M; x \mapsto x \circ m. \]

**Lemma:** The left multiplication $L_{\ast}(b) : B \to B$ is injective for each error $b$. 

The Division Algorithm
The Division Algorithm

Channel $\mathcal{A} = \mathbb{Z}$,
The Division Algorithm

Channel $A = \mathbb{Z}$,

linear code $K = d\mathbb{Z}$ for divisor $1 < d \in \mathbb{Z}$,
The Division Algorithm

Channel $A = \mathbb{Z}$,

linear code $K = d\mathbb{Z}$ for divisor $1 < d \in \mathbb{Z}$,

asymmetric ball $B = \mathbb{Z}/d = \{0, 1, \ldots, d - 1\}$. 
The Division Algorithm

Channel $A = \mathbb{Z}$,

linear code $K = d\mathbb{Z}$ for divisor $1 < d \in \mathbb{Z}$,

asymmetric ball $B = \mathbb{Z}/d = \{0, 1, \ldots, d - 1\}$.

Division Algorithm $x = dq + r$

for dividend $x \in \mathbb{Z}$, remainder $r \in \mathbb{Z}/d$, and quotient $q$. 
The Division Algorithm

Channel $A = \mathbb{Z}$,

linear code $K = d\mathbb{Z}$ for divisor $1 < d \in \mathbb{Z}$,

asymmetric ball $B = \mathbb{Z}/d = \{0, 1, \ldots, d - 1\}$.

Division Algorithm $x = dq + r$

for dividend $x \in \mathbb{Z}$, remainder $r \in \mathbb{Z}/d$, and quotient $q$

yields a coherent decoding $\Delta: x \mapsto (dq, r)$. 
The Division Algorithm

Channel $A = \mathbb{Z}$,

linear code $K = d\mathbb{Z}$ for divisor $1 < d \in \mathbb{Z}$,

asymmetric ball $B = \mathbb{Z}/d = \{0, 1, \ldots, d - 1\}$.

Division Algorithm $x = dq + r$

for dividend $x \in \mathbb{Z}$, remainder $r \in \mathbb{Z}/d$, and quotient $q$

yields a coherent decoding $\Delta: x \mapsto (dq, r)$.

Then the multiplication $(B, \ast)$ on the ball

gives the group $(\mathbb{Z}/d, +)$ of residues modulo $d$ under addition.
The Division Algorithm

Channel $A = \mathbb{Z}$,
linear code $K = d\mathbb{Z}$ for divisor $1 < d \in \mathbb{Z}$,
asymmetric ball $B = \mathbb{Z}/d = \{0, 1, \ldots, d - 1\}$.

Division Algorithm $x = dq + r$
for dividend $x \in \mathbb{Z}$, remainder $r \in \mathbb{Z}/d$, and quotient $q$
yields a coherent decoding $\Delta : x \mapsto (dq, r)$.

Then the multiplication $(B, \ast)$ on the ball
gives the group $(\mathbb{Z}/d, +)$ of residues modulo $d$ under addition.

Have extensions to Gaussian integers, Eisenstein integers, Hurwitz integers, etc.
Hamming codes
Hamming codes

Hypercube $A = (\mathbb{Z}/2)^3$, 
Hamming codes

Hypercube $A = (\mathbb{Z}/2)^3$, code $K = \{000, 111\}$. 
Hamming codes

Hypercube \( A = (\mathbb{Z}/2)^3 \), code \( K = \{000, 111\} \), ball \( B = \{000, 001, 010, 100\} \).
Hamming codes

Hypercube $A = (\mathbb{Z}/2)^3$, code $K = \{000, 111\}$, ball $B = \{000, 001, 010, 100\}$. 
Hamming codes

Hypercube $A = (\mathbb{Z}/2)^3$, code $K = \{000, 111\}$, ball $B = \{\textbf{000}, 001, 010, 100\}$.

$(B, \ast) \cong (\mathbb{Z}/2)^2$
Hamming codes

Hypercube $A = (\mathbb{Z}/2)^3$, code $K = \{000, 111\}$, ball $B = \{000, 001, 010, 100\}$.

$\star \cong (\mathbb{Z}/2)^2$ via $001 \leftrightarrow 01$, $010 \leftrightarrow 10$, $100 \leftrightarrow 11$, 
Hamming codes

Hypercube $A = (\mathbb{Z}/2)^3$, code $K = \{\text{000}, \text{111}\}$, ball $B = \{\text{000}, \text{001}, \text{010}, \text{100}\}$.

$(B, \ast) \cong (\mathbb{Z}/2)^2$ via $001 \mapsto 01, 010 \mapsto 10, 100 \mapsto 11$, i.e., $2^r \mapsto 1 + r$. 
Local duality of linear codes
Local duality of linear codes

For $b_1, b_2, \cdots \in B$, 
Local duality of linear codes

For $b_1, b_2, \cdots \in B$, define $\prod_{i=1}^{m} b_i$ recursively

by $\prod_{i=1}^{1} b_i = b_1$ and $\prod_{i=1}^{m+1} b_i = b_{m+1} \ast \prod_{i=1}^{m} b_i$. 
Local duality of linear codes

For $b_1, b_2, \cdots \in B$, define $\prod_{i=1}^{m} b_i$ recursively by $\prod_{i=1}^{1} b_i = b_1$ and $\prod_{i=1}^{m+1} b_i = b_{m+1} \ast \prod_{i=1}^{m} b_i$.

Principle of Local Duality:
Local duality of linear codes

For \( b_1, b_2, \cdots \in B \), define \( \prod_{i=1}^{m} b_i \) recursively
by \( \prod_{i=1}^{1} b_i = b_1 \) and \( \prod_{i=1}^{m+1} b_i = b_{m+1} \ast \prod_{i=1}^{m} b_i \).

Principle of Local Duality:

If \( K \) is coherent, linear, and symmetric \( B \) spans \( A \),
Local duality of linear codes

For $b_1, b_2, \cdots \in B$, define $\prod_{i=1}^{m} b_i$ recursively by

$$\prod_{i=1}^{1} b_i = b_1 \quad \text{and} \quad \prod_{i=1}^{m+1} b_i = b_{m+1} \ast \prod_{i=1}^{m} b_i.$$ 

**Principle of Local Duality:**

If $\mathcal{K}$ is coherent, linear, and symmetric $B$ spans $A$, then $(B, \ast)$ is an abelian group.
Local duality of linear codes

For $b_1, b_2, \cdots \in B$, define $\prod_{i=1}^{m} b_i$ recursively by

$$\prod_{i=1}^{1} b_i = b_1 \quad \text{and} \quad \prod_{i=1}^{m+1} b_i = b_{m+1} \ast \prod_{i=1}^{m} b_i.$$ 

Principle of Local Duality:

If $K$ is coherent, linear, and symmetric $B$ spans $A$, then $(B, \ast)$ is an abelian group and

$$K = \{ \sum_{i=1}^{m} b_i - \prod_{i=1}^{m} b_i \mid 0 < m \in \mathbb{N}, b_i \in B \}.$$
Local duality of linear codes

For \( b_1, b_2, \cdots \in B \), define \( \prod_{i=1}^{m} b_i \) recursively

\[
\prod_{i=1}^{1} b_i = b_1 \quad \text{and} \quad \prod_{i=1}^{m+1} b_i = b_{m+1} \star \prod_{i=1}^{m} b_i.
\]

Principle of Local Duality:

If \( K \) is coherent, linear, and symmetric \( B \) spans \( A \),

then \( (B, \star) \) is an abelian group

and \( K = \{ \sum_{i=1}^{m} b_i - \prod_{i=1}^{m} b_i \mid 0 < m \in \mathbb{N}, b_i \in B \} \).

Example: In the Hamming code \((\mathbb{Z}/2)^3\),

\[
111 = 001 + 010 + 100 = 001 + 010 - 001 \star 010.
\]
Local duality of linear codes

For \( b_1, b_2, \ldots \in B \), define \( \prod_{i=1}^{m} b_i \) recursively by

\[
\prod_{i=1}^{1} b_i = b_1 \quad \text{and} \quad \prod_{i=1}^{m+1} b_i = b_{m+1} \ast \prod_{i=1}^{m} b_i.
\]

**Principle of Local Duality:**

If \( K \) is coherent, linear, and symmetric \( B \) spans \( A \),

then \( (B, \ast) \) is an abelian group

and \( K = \{ \sum_{i=1}^{m} b_i - \prod_{i=1}^{m} b_i \mid 0 < m \in \mathbb{N}, b_i \in B \} \).

**Example:** In the Hamming code \((\mathbb{Z}/2)^3\),

\[
111 = 001 + 010 + 100 = 001 + 010 - 001 \ast 010.
\]

Coding scheme specified entirely by the **syndrome function** \( 2^r \mapsto 1 + r \).
Greedy syndrome functions
Greedy syndrome functions

Single-error-correcting:
Greedy syndrome functions

**Single-error-correcting:** logarithm function $2^r \leftrightarrow 1 + r$. 
Greedy syndrome functions

**Single-error-correcting:** logarithm function \(2^r \mapsto 1 + r\).

**Double-error-correcting:**
Greedy syndrome functions

Single-error-correcting: logarithm function $2^r \mapsto 1 + r$.

Double-error-correcting:
Quasigroups and loops
Quasigroups and loops

A magma is a **quasigroup** if the left and right multiplications biject.
Quasigroups and loops

A magma is a **quasigroup** if the left and right multiplications biject.

**Examples:** Groups, Latin squares, integers under subtraction, nonzero octonions, …
Quasigroups and loops

A magma is a **quasigroup** if the left and right multiplications biject.

**Examples:** Groups, Latin squares, integers under subtraction, nonzero octonions, ... 

A **loop** is a quasigroup with an identity element.
Quasigroups and loops

A magma is a **quasigroup** if the left and right multiplications biject.

**Examples:** Groups, Latin squares, integers under subtraction, nonzero octonions, . . .

A **loop** is a quasigroup with an identity element.

Coding scheme \((A, \Delta)\) (or code \(K\)) is **quasilinear** if \((B, \ast)\) is a quasigroup.
Quasigroups and loops

A magma is a **quasigroup** if the left and right multiplications biject.

**Examples:** Groups, Latin squares, integers under subtraction, nonzero octonions, . . .

A **loop** is a quasigroup with an identity element.

Coding scheme \((A, \Delta)\) (or code \(K\)) is **quasilinear** if \((B, \ast)\) is a quasigroup.

**Proposition:** Consider a coding scheme \(\Delta : A \rightarrow K \times B\).
Quasigroups and loops

A magma is a **quasigroup** if the left and right multiplications biject.

**Examples:** Groups, Latin squares, integers under subtraction, nonzero octonions, . . .

A **loop** is a quasigroup with an identity element.

Coding scheme \((A, \Delta)\) (or code \(K\)) is **quasilinear** if \((B, \ast)\) is a quasigroup.

**Proposition:** Consider a coding scheme \(\Delta : A \to K \times B\).

*(a):* If \(B\) is finite, then \(K\) is quasilinear.
Quasigroups and loops

A magma is a quasigroup if the left and right multiplications biject.

Examples: Groups, Latin squares, integers under subtraction, nonzero octonions, …

A loop is a quasigroup with an identity element.

Coding scheme \((A, \Delta)\) (or code \(K\)) is quasilinear if \((B, \ast)\) is a quasigroup.

Proposition: Consider a coding scheme \(\Delta: A \to K \times B\).

(a): If \(B\) is finite, then \(K\) is quasilinear.

(b): If \(B\) is symmetric, then \(K\) is quasilinear.
Quasigroups and loops

A magma is a **quasigroup** if the left and right multiplications biject.

**Examples:** Groups, Latin squares, integers under subtraction, nonzero octonions, …

A **loop** is a quasigroup with an identity element.

Coding scheme \( (A, \Delta) \) (or code \( K \)) is **quasilinear** if \( (B, \ast) \) is a quasigroup.

**Proposition:** Consider a coding scheme \( \Delta : A \rightarrow K \times B \).

- (a): If \( B \) is finite, then \( K \) is quasilinear.
- (b): If \( B \) is symmetric, then \( K \) is quasilinear.

Furthermore, if \( \Delta \) is coherent, then \( (B, \ast, 0^\delta) \) is a commutative loop.
Nonlinear perfect codes in circulants
Nonlinear perfect codes in circulants

Cycle $C_6$ or circulant $C_6(1)$
Nonlinear perfect codes in circulants

Cycle $C_6$ or circulant $C_6(1)$
Nonlinear perfect codes in circulants

Wreath product $C_6 \wr K_2$ or circulant $C_{12}(1, 5, 6)$
A nonassociative loop on the ball
A nonassociative loop on the ball

<table>
<thead>
<tr>
<th>$x \in A$</th>
<th>$-5$</th>
<th>$-4$</th>
<th>$-3$</th>
<th>$-2$</th>
<th>$-1$</th>
<th>$0$</th>
<th>$1$</th>
<th>$2$</th>
<th>$3$</th>
<th>$4$</th>
<th>$5$</th>
<th>$6$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x^\varepsilon \in B$</td>
<td>$1$</td>
<td>$5$</td>
<td>$6$</td>
<td>$-5$</td>
<td>$5$</td>
<td>$6$</td>
<td>$-5$</td>
<td>$-1$</td>
<td>$0$</td>
<td>$1$</td>
<td>$-1$</td>
<td>$0$</td>
</tr>
</tbody>
</table>
A nonassociative loop on the ball

<table>
<thead>
<tr>
<th>$x \in A$</th>
<th>$-5$</th>
<th>$-4$</th>
<th>$-3$</th>
<th>$-2$</th>
<th>$-1$</th>
<th>$0$</th>
<th>$1$</th>
<th>$2$</th>
<th>$3$</th>
<th>$4$</th>
<th>$5$</th>
<th>$6$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x^\varepsilon \in B$</td>
<td>$1$</td>
<td>$5$</td>
<td>$6$</td>
<td>$-5$</td>
<td>$5$</td>
<td>$6$</td>
<td>$-5$</td>
<td>$-1$</td>
<td>$0$</td>
<td>$1$</td>
<td>$-1$</td>
<td>$0$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$*$</th>
<th>$6$</th>
<th>$-5$</th>
<th>$-1$</th>
<th>$0$</th>
<th>$1$</th>
<th>$5$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$6$</td>
<td>$6$</td>
<td>$-5$</td>
<td>$-1$</td>
<td>$0$</td>
<td>$1$</td>
<td>$5$</td>
</tr>
<tr>
<td>$-5$</td>
<td>$-5$</td>
<td>$-1$</td>
<td>$0$</td>
<td>$1$</td>
<td>$5$</td>
<td>$6$</td>
</tr>
<tr>
<td>$-1$</td>
<td>$-1$</td>
<td>$0$</td>
<td>$-5$</td>
<td>$5$</td>
<td>$6$</td>
<td>$1$</td>
</tr>
<tr>
<td>$0$</td>
<td>$0$</td>
<td>$1$</td>
<td>$5$</td>
<td>$6$</td>
<td>$-5$</td>
<td>$-1$</td>
</tr>
<tr>
<td>$1$</td>
<td>$1$</td>
<td>$5$</td>
<td>$6$</td>
<td>$-5$</td>
<td>$-1$</td>
<td>$0$</td>
</tr>
<tr>
<td>$5$</td>
<td>$5$</td>
<td>$6$</td>
<td>$1$</td>
<td>$-1$</td>
<td>$0$</td>
<td>$-5$</td>
</tr>
</tbody>
</table>
A nonassociative loop on the ball

\[
\begin{array}{c|cccccccccccc}
  x \in A & -5 & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
  x^\epsilon \in B & 1 & 5 & 6 & -5 & 5 & 6 & -5 & -1 & 0 & 1 & -1 & 0 \\
\end{array}
\]

\[
\begin{array}{c|cccccccc}
  * & 6 & -5 & -1 & 0 & 1 & 5 \\
  6 & 6 & -5 & -1 & 0 & 1 & 5 \\
  -5 & -5 & -1 & 0 & 1 & 5 & 6 \\
  -1 & -1 & 0 & -5 & 5 & 6 & 1 \\
  0 & 0 & 1 & 5 & 6 & -5 & -1 \\
  1 & 1 & 5 & 6 & -5 & -1 & 0 \\
  5 & 5 & 6 & 1 & -1 & 0 & -5 \\
\end{array}
\]

\[(1 \ast 1) \ast 1 = (1 \ast 1) \ast (1 \ast 1)\]
A nonassociative loop on the ball

\[
\begin{array}{|c|cccccccccccc|}
\hline
x \in A & -5 & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
x^\xi \in B & 1 & 5 & 6 & -5 & 5 & 6 & -5 & -1 & 0 & 1 & -1 & 0 \\
\hline
\end{array}
\]

\[
\begin{array}{|c|cccccccccccc|}
\hline
* & 6 & -5 & -1 & 0 & 1 & 5 \\
\hline
6 & 6 & -5 & -1 & 0 & 1 & 5 \\
\hline
-5 & -5 & -1 & 0 & 1 & 5 & 6 \\
-1 & -1 & 0 & -5 & 5 & 6 & 1 \\
\hline
0 & 0 & 1 & 5 & 6 & -5 & -1 \\
\hline
1 & 1 & 5 & 6 & -5 & -1 & 0 \\
5 & 5 & 6 & 1 & -1 & 0 & -5 \\
\hline
\end{array}
\]

\[
(1 * 1) * 1 = (-1 * 1) * 1 \\
= (1 * 1) * (1 * 1)
\]
A nonassociative loop on the ball

\[
x \in A \quad -5 \quad -4 \quad -3 \quad -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6
\]

\[
x^\varepsilon \in B \quad 1 \quad 5 \quad 6 \quad -5 \quad 5 \quad 6 \quad -5 \quad -1 \quad 0 \quad 1 \quad -1 \quad 0
\]

\[
\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|}
\hline
* & 6 & -5 & -1 & 0 & 1 & 5 \\
\hline
6 & 6 & -5 & -1 & 0 & 1 & 5 \\
\hline
-5 & -5 & -1 & 0 & 1 & 5 & 6 \\
-1 & -1 & 0 & -5 & 5 & 6 & 1 \\
\hline
0 & 0 & 1 & 5 & 6 & -5 & -1 \\
\hline
1 & 1 & 5 & 6 & -5 & -1 & 0 \\
5 & 5 & 6 & 1 & -1 & 0 & -5 \\
\hline
\end{array}
\]

\[
((1 \ast 1) \ast 1) \ast 1 = (-1 \ast 1) \ast 1 = 6 \ast 1 = (-1) \ast (-1) = (1 \ast 1) \ast (1 \ast 1)
\]
A nonassociative loop on the ball

\[
\begin{array}{c|cccccccccccc}
    x \in A & -5 & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
    x^\varepsilon \in B & 1 & 5 & 6 & -5 & 5 & 6 & -5 & -1 & 0 & 1 & -1 & 0 \\
\end{array}
\]

\[
\begin{array}{|c|cccc}
    \ast & 6 & -5 & -1 & 0 & 1 & 5 \\
\hline
    6 & 6 & -5 & -1 & 0 & 1 & 5 \\
    -5 & -5 & -1 & 0 & 1 & 5 & 6 \\
    -1 & -1 & 0 & -5 & 5 & 6 & 1 \\
    0 & 0 & 1 & 5 & 6 & -5 & -1 \\
    1 & 1 & 5 & 6 & -5 & -1 & 0 \\
    5 & 5 & 6 & 1 & -1 & 0 & -5 \\
\end{array}
\]

\[
((1 \ast 1) \ast 1) \ast 1 = (-1 \ast 1) \ast 1 = 6 \ast 1 = 1 \neq -5 = (-1) \ast (-1) = (1 \ast 1) \ast (1 \ast 1)
\]
Thank you for your attention!