Wireless network coding over finite rings

Emanuele Viterbo†

joint work with:
Joseph Boutros‡, Yi Hong†

(†) ECSE, Monash University, Clayton, Victoria
(‡) TAMUQ, Doha, Qatar

Algebraic Structure in Network Information Theory
Banff, Canada, August 18th, 2011
Motivation

- Mathematicians love prime numbers $p$ and engineers love $2^m$

- Bit labeling is a problem with $p$ (loss of rate and additional complexity)

- Linear codes $(n, k)$ over $\mathbb{F}_p$ can be mapped by Construction A to a lattice $\Lambda$ and by working $\text{mod } p$ to a subset of $(p\text{-PAM})^n$ finite constellation

- In lattice network coding $+\text{ and } \times \mod p$ operations provide the natural operations for $p\text{-PAM} \mod p$ constellations and we use the fact that the ring $\mathbb{Z}_p$ is equivalent to the field $\mathbb{F}_p$.

- Feng, Silva, and Kschischang, (2010-2011) have shown how to construct lattice network codes by concatenating linear codes over $\mathbb{F}_p$ with a finite 2D constellation with $p$ points.

- Narayanan (2011) has shown how to improve the shaping of the $p$ and $p^2$ point 2D constellations.
The infinite rings $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$

- **Basis:** $\{1, \theta\}$ where $\theta = i = \sqrt{-1}$ or $\theta = \omega = e^{i2\pi/3}$
- **Elements:** $\{a + b\theta : a, b \in \mathbb{Z}\}$
- **Units:** $\{\pm 1, \pm i\} \{\pm 1, \pm \omega, \pm \omega^*\}$
Motivation Cont’d

- To have almost always invertible network equations we need large \( p \)

- An invertible matrix \( A \) over a ring \( R \) must have

  \[
  \frac{1}{\det(A)} \in R
  \]

- Often rings have few invertible elements (units of \( R \)) hence we have a very limited choice for the network equations.

- We need more freedom so we need to put in more units.

- This can be effectively achieved by working in finite rings where the integers are taken mod \( 2^m \)

  \[
  R = \mathbb{Z}_{2^m}[\theta] = \{a + \theta b|a, b \in \mathbb{Z}_{2^m}\}
  \]
The Gaussian integers \( \mod 2^m \)

**Problem:** Build a large set of invertible matrices over the finite ring

\[
R = \mathbb{Z}_2m[i] = \{a + ib | a, b \in \mathbb{Z}_2m\}
\]

- **Units of** \( R \): \( R^* = \mathbb{Z}_2m[i] = \{a + ib | a, b \in \mathbb{Z}_2m, a + b = 1 \mod 2^m\} = D_2 + (1, 0) \cap B \)
- **Non units** \( \bar{R} = \mathbb{Z}_2m[i] = \{a + ib | a, b \in \mathbb{Z}_2m, a + b = 0 \mod 2^m\} = D_2 \cap B \)
- **Properties:**
  - \( \bar{R} + \bar{R} = \bar{R} \)
  - \( R^* + R^* = \bar{R} \)
  - \( R^* + \bar{R} = \bar{R} \)
  - \( \bar{R} \bar{R} = \bar{R} \)
  - \( R^* R^* = R^* \)
  - \( R^* \bar{R} = \bar{R} \)

- **A possible solution:** the matrix \( A = (a_{ij}) \) is invertible if \( a_{ii} \in R^* \) and \( a_{ij} \in \bar{R} \).

What is this? can it be improved/generalized to Eisenstein integers or even quaternions?
The finite rings

- Red diamonds are the units $R^*$
- Blue circles are non-invertible elements $\overline{R}$
Commutative rings

A commutative ring $R$ is a set closed under two binary operations, addition and multiplication such that

1. $R$ is an Abelian group under addition
2. $ab = ba$ for all $a, b \in R$ (commutativity)
3. $a(bc) = (ab)c$ for all $a, b, c \in R$ (associativity)
4. there exists a element $1 \in R$ such that $1a = a$ for all $a \in R$ (identity element)
5. $a(b + c) = ab + ac$ for all $a, b, c \in R$ (distributivity)

- Examples of rings: $\mathbb{Z}, \mathbb{Z}[i]$
- These are not rings: $2\mathbb{Z} + 1, \mathbb{Z}^+$
Ideals

An ideal in a commutative ring $R$ is a subset $I$ such that for all $a, b \in R$

1. $0 \in I$;
2. if $a, b \in I$, then $a + b \in I$;
3. if $a \in I$ and $r \in R$, then $ra \in I$.

Examples of ideals: $2\mathbb{Z}$, $(1 + i)\mathbb{Z}[i]$

Examples of ideals: $2\mathbb{Z} + 1$, $\mathbb{Z}^+$

Examples of ideals: $2\mathbb{Z}$, $(1 + i)\mathbb{Z}[i]$

Examples of ideals: $2\mathbb{Z} + 1$, $\mathbb{Z}^+$

Examples of ideals: $2\mathbb{Z}$, $(1 + i)\mathbb{Z}[i]$

Examples of ideals: $2\mathbb{Z} + 1$, $\mathbb{Z}^+$
Invertible elements in $\mathbb{Z}_{2^m}$

The group of units of $\mathbb{Z}_{2^m}$ is

$$\{1, 3, 5, \ldots, 2^m - 1\}$$

**Proof**

- Let $a \in \mathbb{Z}_{2^m}$. It is enough consider the modular equation to find the inverse element $x$

  $$ax = 1 \mod 2^m$$

- This has a solution, if and only if we can solve

  $$ax - 2^m q = 1$$

  for some integers $x$ and $q$.

- It is well known that the above equation can be solved using the extended Euclidean algorithm if and only if $\text{GCD}(a, 2^m) = 1$ which is the case for all odd $a = 2k + 1$.

- Note that an even $a = 2k$ will have $\text{GCD}(a, 2^m) \geq 2$. 
**Group of units of \( R \)**

The group of units of \( R \) is given by

\[
R^* = \{a + ib | a, b \in \mathbb{Z}_{2^m}, a + b = 1 \mod 2 \}
\]

and the non units form the maximal ideal

\[
\bar{R} = \{a + ib | a, b \in \mathbb{Z}_{2^m}, a + b = 0 \mod 2 \}
\]

*Proof*

- Let \( a + ib \in R \). It is enough to consider the inverse element

\[
x = \frac{a - ib}{a^2 + b^2}
\]

This is in \( R \) iff \( a^2 + b^2 \) is invertible in \( \mathbb{Z}_{2^m} \).

- This is true iff \( a^2 + b^2 = 1 \mod 2 \), which is equivalent to \( a + b = 1 \mod 2 \).

- To prove that \( \bar{R} \) is an ideal we consider 3) property of ideals.

- Let \( a + ib \in \bar{R} \) and \( x + iy \in R \) then by adding real and imaginary part of the product we get

\[
(ax - by) + (bx + ay) = (a + b)x + (a - b)y = 0 \mod 2
\]

since \( a - b = 0 \mod 2 \).

- Finally, since \( R = R^* \cup \bar{R} \), \( \bar{R} \) is a maximal ideal of \( R \), i.e. is not contained in any larger non trivial ideal of \( R \).
More definitions

- Given the two rings $R$ and $S$, a \textit{ring homomorphism} is a mapping $\varphi : R \rightarrow S$ such that for all $a, b \in R$
  1. $\varphi(a + b) = \varphi(a) + \varphi(b)$
  2. $\varphi(ab) = \varphi(a)\varphi(b)$
  3. $\varphi(1) = 1$

- Given the two sided ideal $I$ we define the \textit{quotient ring} $R/I$ where addition $\oplus$ and multiplication $\otimes$ are defined as
  \[(a + I) \oplus (b + I) = ((a + b) + I)\]
  \[(a + I) \otimes (b + I) = (ab + I)\]

  where $a, b \in R$ and '+' and $\cdot$ are the operations in the ring $R$

- We define the \textit{natural map} $\phi : R \rightarrow R/I$ as the ring homomorphism defined by $a \mapsto a + I$. 

Wireless network coding over finite rings • BIRS
**Mapping to $\mathbb{F}_2$**

The quotient ring $R/\bar{R}$ is isomorphic to the field $\mathbb{F}_2$.

*Proof* – The image of the natural map $\phi : R \to R/\bar{R}$ is composed of two elements $\bar{R}$ and $R^*$. By mapping

\[
\begin{align*}
\bar{R} & \mapsto 0 \\
R^* & \mapsto 1
\end{align*}
\]

the above properties provide the explicit addition and multiplication tables of $\mathbb{F}_2 = \{0, 1\}$.

Alternatively, the proof is a direct application on the quotient of a commutative ring by a maximal ideal.
The invertible matrices

The matrices $A = (a_{ij})$ with $a_{ii} \in \mathbb{R}^*$ and $a_{ij} \in \bar{\mathbb{R}} \ i \neq j$ are invertible in the ring of matrices $\mathcal{M}_n(R)$ with coefficients in $R$.

Proof – It is enough to show that $\det(A) \in R^*$, i.e., it has an inverse in $R$.

Extending the natural map $\phi$ we define the the matrix ring homomorphism

$$\Phi : \mathcal{M}_n(R) \to \mathcal{M}_n(\mathbb{F}_2).$$

All the matrices $A$ are mapped to the identity matrix $I$ in $\mathcal{M}_n(\mathbb{F}_2)$, which is invertible in $\mathbb{F}_2$. Using the properties of ring homomorphisms in the Leibniz formula for the determinant

$$\det(A) = \sum_{\pi \in S_n} sgn(\pi) \prod_{i=1}^{n} a_{i,\pi(i)}$$

we have

$$\phi(\det(A)) = \det(\Phi(A)) = \det(I) = 1$$

which implies that that $\det(A) \in R^*$. 
More invertible matrices

More invertible matrices can be obtained by applying the inverse map $\Phi^{-1}$ to any binary invertible matrix.

\[
\begin{pmatrix}
R^* & \bar{R} & \bar{R} \\
\bar{R} & R^* & \bar{R} \\
\bar{R} & \bar{R} & R^*
\end{pmatrix}
\begin{pmatrix}
\bar{R} & \bar{R} & R^* \\
R^* & \bar{R} & \bar{R} \\
\bar{R} & R^* & \bar{R}
\end{pmatrix}
\begin{pmatrix}
R^* & \bar{R} & \bar{R} \\
\bar{R} & \bar{R} & R^* \\
\bar{R} & R^* & \bar{R}
\end{pmatrix}
\ldots
\]
"Disquisitiones"

- We have made the engineers happy with $2^m$.
- We can still generate many invertible network equations, which quantize the channel well.
- We do not rely on large field and randomness.
- In physical layer network coding we need a ring structure because of the multiplicative effect of the channel.
- The field structure is often used because we know a lot about codes over fields ...
- ... but the code over the field is not usually easy to match to a finite constellation: Hamming distance or Lee distance is not matched to Euclidean distance.
- Using the ring structure we do not need to go through a linear code over a field and we are allowed to take any lattice that we like, as for BCM and set-partitioning.
- With ring codes we can work with channels that are ring homomorphisms transformations of the input ring.