Coboundaries and a new invariant for cryptographic functions

K. J. Horadam

Mathematics, RMIT
Melbourne, Australia

Discrete Mathematics Seminar
Monash University, April 24 2012
Cocycles and their equivalences

Equivalence for functions

Putting the two together
Outline

1. Cocycles and their equivalences
   - Cocycles and the Five-fold Constellation
   - Cocycles and their equivalence classes

2. Equivalence for functions
   - Equivalence of functions between groups
   - Cryptographic functions: CCZ and EA Equivalence

3. Putting the two together
   - A new nonlinearity measure from coboundaries
   - An invariant of EA class
Our raw materials

\[ G, N \text{ finite groups with } N \text{ abelian} \]

- Cocycle \( \psi : G \times G \to N \),
  \[ \psi(g, h) + \psi(gh, k) = \psi(g, hk) + \psi(h, k), \quad g, h, k, \in G \]
  \[ \psi(1, 1) = 0 \]

- Represent as Cocyclic matrix \( M_\psi = [\psi(g, h)]_{g,h \in G} \)

For concreteness (main case for applications):
\( G = N = \mathbb{Z}_2^n = \) binary strings of length \( n \) under XOR;
under a suitable definition of string multiplication,
this is the finite field \( \mathbb{F}_{2^n} \)
Our raw materials

**Cocycles and their equivalences**

*Equivalence for functions*

*Putting the two together*

**Cocycles and the Five-fold Constellation**

**Cocycles and their equivalence classes**

---

Our raw materials

**G, N finite groups with N abelian**

- **Cocycle** $\psi : G \times G \to N$,
  
  $\psi(g, h) + \psi(gh, k) = \psi(g, hk) + \psi(h, k)$, $g, h, k, \in G$

  $\psi(1, 1) = 0$

- Represent as **Cocyclic matrix** $M_\psi = [\psi(g, h)]_{g,h \in G}$

For concreteness (main case for applications):

- $G = N = \mathbb{Z}_2^n = $ binary strings of length $n$ under XOR;
- under a suitable definition of string multiplication,
- this is the finite field $\mathbb{F}_{2^n}$
Our raw materials

\[ G, \, N \text{ finite groups with } N \text{ abelian} \]

- **Cocycle** \( \psi : G \times G \rightarrow N \),
  \[ \psi(g, h) + \psi(gh, k) = \psi(g, hk) + \psi(h, k), \quad g, h, k, \in G \]
  \[ \psi(1, 1) = 0 \]

- Represent as **Cocyclic matrix** \( M_\psi = [\psi(g, h)]_{g, h \in G} \)

For concreteness (main case for applications):

\( G = N = \mathbb{Z}_2^n = \) binary strings of length \( n \) under XOR;
under a suitable definition of string multiplication, this is the finite field \( \mathbb{F}_{2^n} \)
Our raw materials

\( G, N \) finite groups with \( N \) abelian

- **Cocycle** \( \psi : G \times G \to N \),
  \[\psi(g, h) + \psi(gh, k) = \psi(g, hk) + \psi(h, k), \quad g, h, k, \in G\]
  \[\psi(1, 1) = 0\]

- Represent as **Cocyclic matrix** \( M_\psi = [\psi(g, h)]_{g,h \in G} \)

  For concreteness (main case for applications):
  \( G = N = \mathbb{Z}_2^n = \text{binary strings of length } n \text{ under XOR}; \)
  under a suitable definition of string multiplication,
  this is the **finite field** \( \mathbb{F}_{2^n} \)
A small binary example

\[ G = N = \mathbb{Z}_2^2 = (\mathbb{F}_4, +) \]

1. Orthogonal cocycle \( \psi : \mathbb{Z}_2^2 \times \mathbb{Z}_2^2 \to \mathbb{Z}_2^2, \psi(b, d) = bd \)

2. Cocyclic generalised Hadamard matrix:

\[
[\psi(b, d)] = \begin{bmatrix}
00 & 00 & 00 & 00 \\
00 & 10 & 01 & 11 \\
00 & 01 & 11 & 10 \\
00 & 11 & 10 & 01
\end{bmatrix}
\]
If $|N|$ divides $|G|$ in optimal *orthogonal* case, objects from five areas are equivalent (Hadamard Matrices, Group Extensions, Relative Difference Sets, Combinatorial Designs, Correlated Sequences)
The basic **cohomology** class of cocycles: the coboundaries

- A cocycle is a **coboundary** if it is of the form $\psi = \partial f$ for some $f : G \rightarrow N$ with $f(1) = 0$,

  $$\partial f(g, h) = -f(g) - f(h) + f(gh), \quad g, h \in G$$

- Note: relationship between $f$ and $\partial f$ like that (for vector spaces) between quadratic form and its polar bilinear form
- Often can move "back and forth" between 1D and 2D functions from $G$ to $N$. 

Horadam
The basic **cohomology** class of cocycles: the coboundaries

- A cocycle is a **coboundary** if it is of the form $\psi = \partial f$ for some $f: G \to N$ with $f(1) = 0$,

$$
\partial f(g, h) = -f(g) - f(h) + f(gh), \ g, h \in G
$$

- Note: relationship between $f$ and $\partial f$ like that (for vector spaces) between quadratic form and its polar bilinear form

- Often can move "back and forth" between 1D and 2D functions from $G$ to $N$. 

Horadam
A cocycle is a coboundary if it is of the form $\psi = \partial f$ for some $f : G \rightarrow N$ with $f(1) = 0$,

$$\partial f(g, h) = -f(g) - f(h) + f(gh), \ g, h \in G$$

Note: relationship between $f$ and $\partial f$ like that (for vector spaces) between quadratic form and its polar bilinear form

Often can move "back and forth" between 1D and 2D functions from $G$ to $N$. 
Outline

1. Cocycles and their equivalences
   - Cocycles and the Five-fold Constellation
   - Cocycles and their equivalence classes

2. Equivalence for functions
   - Equivalence of functions between groups
   - Cryptographic functions: CCZ and EA Equivalence

3. Putting the two together
   - A new nonlinearity measure from coboundaries
   - An invariant of EA class
We push equivalence of relative difference sets around the constellation to get equivalence of cocycles,

- Call this equivalence class of cocycle $\psi$ its Bundle.
  (NOT the same as cohomology class (natural equivalence) of $\psi$).
Bundles (Equivalence Classes) of Coboundaries

- A Bundle of \((2D)\) coboundaries contains \textbf{only} coboundaries.

\[
\partial f \sim \partial f' \iff f' = [\gamma \circ (f \cdot r) \circ \theta] + \chi
\]

where \(f \cdot r(g) = f(rg) - f(g)\) is the \textbf{shift} of \(f\) by \(r\), \(\gamma \in \text{Aut}(N), \theta \in \text{Aut}(G), r \in G\) and \(\chi\) is a homomorphism.

- Call this equivalence class of \((1D)\) functions the \textbf{bundle} \(b(f)\) of \(f\).
Outline

1. Cocycles and their equivalences
   - Cocycles and the Five-fold Constellation
   - Cocycles and their equivalence classes

2. Equivalence for functions
   - Equivalence of functions between groups
   - Cryptographic functions: CCZ and EA Equivalence

3. Putting the two together
   - A new nonlinearity measure from coboundaries
   - An invariant of EA class
Nonlinearity for functions between groups

Many measures of "high nonlinearity" in cryptography, signal design, combinatorics, projective geometry.

- bent/almost bent
- maximally nonlinear
- perfect nonlinear/almost PN
- directional derivative near-uniform distn
- well-correlated/uncorrelated
- planar/semiplanar

These measures can be classified very broadly by the measuring instrument used:

- Fourier Transform/DFT/WHT/Characters
- Difference distribution
Equivalence of functions

- Competing notions of equivalence of functions depend on differing measures of "nonlinearity" for differing applications.
- For cryptographic purposes, want to collect functions into equivalence classes which preserve measures of both types: differential uniformity (combinatorial/geometric condition) and nonlinearity (discrete Fourier spectrum condition).
- Two types of equivalence have crystallised as important for functions $f(x)$ over $\mathbb{F}_p^n$: CCZ equivalence and EA equivalence.
Outline

1. Cocycles and their equivalences
   - Cocycles and the Five-fold Constellation
   - Cocycles and their equivalence classes

2. Equivalence for functions
   - Equivalence of functions between groups
   - Cryptographic functions: CCZ and EA Equivalence

3. Putting the two together
   - A new nonlinearity measure from coboundaries
   - An invariant of EA class
CCZ Equivalence

- Carlet-Charpin-Zinoviev (CCZ) Equivalence (CCZ 1998)
  \( \varphi \sim \phi \) iff their graphs are equivalent, ie there exists (additive) affine permutation \( \alpha \) of \( (\mathbb{F}_{2^n})^2 \):

  \[
  \alpha(\mathcal{G}(\varphi)) = \mathcal{G}(\phi)
  \]

  where the graph \( \mathcal{G}(\phi) \) of \( \phi \) is \( \{(x, \phi(x)), \ x \in \mathbb{F}_{2^n}\} \).

- CCZ equivalence preserves differential uniformity, the nonlinearity and the resistance to algebraic cryptanalysis.

- CCZ equivalence does not preserve algebraic degree.
EA Equivalence

- **Extended Affine (EA) Equivalence** (Budaghyan, Carlet, Pott 2006) \( \phi \sim \varphi \) iff there exist affine functions \( \gamma, \theta, \chi \) with \( \gamma, \theta \) permutations: \( \phi = \gamma \circ \varphi \circ \theta + \chi \).

- EA equivalence preserves differential uniformity, the nonlinearity, resistance to algebraic cryptanalysis and algebraic degree.

- Definitions extend immediately to \( \mathbb{F}_p^n \) and functions \( f : G \to N \) between arbitrary finite groups.

- When \( G = N = (\mathbb{F}_p^n, +) \), the EA class of \( f \) is exactly its bundle \( b(f) \) (can ignore the shift).
EA Equivalence

- **Extended Affine (EA) Equivalence** (Budaghyan, Carlet, Pott 2006) $\phi \sim \varphi$ iff there exist affine functions $\gamma, \theta, \chi$ with $\gamma, \theta$ permutations: $\phi = \gamma \circ \varphi \circ \theta + \chi$.

- EA equivalence preserves differential uniformity, the nonlinearity, resistance to algebraic cryptanalysis and algebraic degree.

- Definitions extend immediately to $\mathbb{F}_{p^n}$ and functions $f : G \rightarrow N$ between arbitrary finite groups.

- When $G = N = (\mathbb{F}_p^n, +)$, the EA class of $f$ is exactly its bundle $b(f)$ (can ignore the shift).
Functions With Low Differential Uniformity

(Nyberg 1994) Functions $f(x)$ over $G = (\mathbb{F}_{p^n}, +)$ resist differential cryptanalysis if

$$\Delta_f = \max_{x \neq 0 \in G} \{|\{y : f(x + y) - f(y) = a\}| : a \in G\}$$

is small

- $p$ odd, $\Delta_f = 1$ is possible (PN functions)
- Example $p = 7$, $f(x) = x^2$, $x \in \mathbb{F}_7$,
  $$f(x + a) - f(x) = 2ax + a^2 \pmod{7}$$

<table>
<thead>
<tr>
<th>$x$</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>$a = 1$</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>$a = 2$</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>6</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Functions With Low Differential Uniformity: \( p = 2 \)

- \( f(x + a) + f(x) = f(x + a) + f(x + a + a) \) gives paired solutions \( X \) and \( X + a \) when \( p = 2 \)
- \( \Delta_f \) is even, \( \Delta_f = 2 \) is best possible (APN functions)
- \( p = 2, n = 8 \), inverse function \( x^{-1} \) with \( \Delta = 4 \) used in AES
- Power functions \( f(x) = x^d \) the main focus of search until \( \sim 2005 \).
EA Equivalence and Non-power Functions

BUT.....

- There are APN functions \textbf{EA-inequivalent} to power functions: Edel, Kyureghyan, Pott (2006); Budaghyan, Carlet, Felke, Leander (2006); Budaghyan, Carlet, Pott (2006); Budaghyan, Carlet, Leander (2007) ...

- \( p \) odd. There are PN functions \textbf{EA-inequivalent} to power functions: Ding, Yuan (2006), Zha, Kyureghyan, Wang (2008), Zhou, Li (2008)

- An enormous outpouring of APN, PN examples found since then!! \textbf{WE HAVE A PROBLEM}....
BUT.....

- There are APN functions \textit{EA-inequivalent} to power functions: Edel, Kyureghyan, Pott (2006); Budaghyan, Carlet, Felke, Leander (2006); Budaghyan, Carlet, Pott (2006); Budaghyan, Carlet, Leander (2007) ...

- \( p \) odd. There are PN functions \textit{EA-inequivalent} to power functions: Ding, Yuan (2006), Zha, Kyureghyan, Wang (2008), Zhou, Li (2008)

- An enormous outpouring of APN, PN examples found since then!! \textit{WE HAVE A PROBLEM}....
EA Equivalence and CCZ Equivalence over $\mathbb{F}_{p^n}$

- EA equivalence $\Rightarrow$ CCZ equivalence
- BUT..... THE PROBLEM IS
  It is very hard to know when CCZ equivalent functions are EA-inequivalent.

eg. The function $f : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_{2^m}$, $m$ divisible by 6, $f(x) =$

$$[x + tr_{m/3}(x^{2(2i+1)} + x^{4(2i+1)}) + tr(x)tr_{m/3}(x^{2i+1} + x^{2^2i(2i+1)})]^{2^i+1},$$

with $\gcd(m, i) = 1$, is APN. Budaghyan, Carlet, Pott (2005).

- IS IT NEW? IS IT DIFFERENT? HOW CAN WE TELL?
1. Cocycles and their equivalences
   - Cocycles and the Five-fold Constellation
   - Cocycles and their equivalence classes

2. Equivalence for functions
   - Equivalence of functions between groups
   - Cryptographic functions: CCZ and EA Equivalence

3. Putting the two together
   - A new nonlinearity measure from coboundaries
   - An invariant of EA class
We need as many invariants for EA and CCZ classes as possible.
Preferably they will be easy to compute.
We can apply the 1D ↔ 2D link at ★ ★ to determine a new nonlinearity measure from coboundaries.
The subgroup generated by $\text{im}(\partial f)$

We focus on the subset $\text{im}(\partial f)$, subgroup $\langle \text{im}(\partial f) \rangle$ and the corresponding $p$-ary codes.

**Definition**

Let $G = N = \mathbb{Z}_p^n$ and $f : \mathbb{Z}_p^n \to \mathbb{Z}_p^n$ with $f(0) = 0$. Define $n(f) := \dim_p \langle \text{im}(\partial f) \rangle$.

**Basic properties** of $n(f)$, $0 \leq n(f) \leq n$.

**Lemma**

- $n(f) = 0 \iff f$ is linear
- $n(f) \geq n - \lfloor \log_p \Delta(f) \rfloor$, $\Delta(f) =$ differential uniformity of $f$
The subgroup generated by $\text{im}(\partial f)$

We focus on the subset $\text{im}(\partial f)$, subgroup $\langle \text{im}(\partial f) \rangle$ and the corresponding $p$-ary codes.

**Definition**

Let $G = N = \mathbb{Z}_p^n$ and $f : \mathbb{Z}_p^n \to \mathbb{Z}_p^n$ with $f(0) = 0$. Define $n(f) := \dim_p \langle \text{im}(\partial f) \rangle$.

**Basic properties of** $n(f)$, $0 \leq n(f) \leq n$.

**Lemma**

- $n(f) = 0 \iff f$ is linear
- $n(f) \geq n - \lfloor \log_p \Delta(f) \rfloor$, $\Delta(f) = \text{differential uniformity of } f$
We focus on the subset $\text{im}(\partial f)$, subgroup $\langle \text{im}(\partial f) \rangle$ and the corresponding $p$-ary codes.

**Definition**

Let $G = N = \mathbb{Z}_p^n$ and $f : \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p^n$ with $f(0) = 0$. Define $n(f) := \dim_p \langle \text{im}(\partial f) \rangle$.

**Lemma**

- $n(f) = 0 \iff f$ is linear
- $n(f) \geq n - \lfloor \log_p \Delta(f) \rfloor$, $\Delta(f) =$ differential uniformity of $f$
Outline

1. Cocycles and their equivalences
   - Cocycles and the Five-fold Constellation
   - Cocycles and their equivalence classes

2. Equivalence for functions
   - Equivalence of functions between groups
   - Cryptographic functions: CCZ and EA Equivalence

3. Putting the two together
   - A new nonlinearity measure from coboundaries
   - An invariant of EA class
Invariants associated with $\text{im}(\partial f)$

$n(f)$ is an invariant of the class $b(f)$. (Can ignore shift action.)

Lemma

If $f \simeq_b f'$ then $n(f) = n(f')$ and so $\langle \text{im}(\partial f) \rangle \cong \langle \text{im}(\partial f') \rangle$.

In case $p = 2$, as well as dimension of $\text{im}(\partial f)$, can use kernel of code $\text{im}(\partial f)$ to distinguish.

Kernel of a binary code $C$

$K(C) = \{ x \in \mathbb{F}_{2^n} \mid x + C = C \}$.

$\ker(C) = \dim_2 K(C)$. (Phelps, Rifa, Villanueva 2005)
Invariants associated with $\text{im}(\partial f)$

$n(f)$ is an invariant of the class $\mathbf{b}(f)$. (Can ignore shift action.)

**Lemma**

If $f \simeq_b f'$ then $n(f) = n(f')$ and so $\langle \text{im}(\partial f) \rangle \cong \langle \text{im}(\partial f') \rangle$.

In case $p = 2$, as well as dimension of $\text{im}(\partial f)$, can use kernel of code $\text{im}(\partial f)$ to distinguish.

Kernel of a binary code $C$

$$K(C) = \{ x \in \mathbb{F}_{2^n} \mid x + C = C \}.$$ 

$\ker(C) = \dim_2 K(C)$. (Phelps, Rifa, Villanueva 2005)
Invariants associated with \( \text{im}(\partial f) \)

\( n(f) \) is an invariant of the class \( b(f) \). (Can ignore shift action.)

**Lemma**

If \( f \simeq_b f' \) then \( n(f) = n(f') \) and so \( \langle \text{im}(\partial f) \rangle \cong \langle \text{im}(\partial f') \rangle \).

In case \( p = 2 \), as well as dimension of \( \text{im}(\partial f) \), can use kernel of code \( \text{im}(\partial f) \) to distinguish.

**Kernel** of a binary code \( C \)

\[
K(C) = \{ x \in \mathbb{F}_2^n \mid x + C = C \}.
\]

\( \ker(C) = \dim_2 K(C) \). (Phelps, Rifa, Villanueva 2005)
At least 5 permutation representatives of EA classes over $\mathbb{F}_{16}$ with $\Delta(f) = 4$ and algebraic degree 3 (East 2008).

Work in progress (Mercè Villanueva, KJH, Asha Rao):
There are a total of 10 of these (found by exhaustive search 2012).
At least 5 permutation representatives of EA classes over $\mathbb{F}_16$ with $\Delta(f) = 4$ and algebraic degree 3 (East 2008).

Work in progress (Mercè Villanueva, KJH, Asha Rao): There are a total of 10 of these (found by exhaustive search 2012).
We compute \( \dim, \ker \) of codes given by graph \( \mathcal{G}(f) \) (CCZ class invariants) and by \( \text{im}(\partial f) \). \( \text{im}(\partial f) \) measures something new!

<table>
<thead>
<tr>
<th>( j )</th>
<th>( \Delta(f) )</th>
<th>( \text{alg}^\circ )</th>
<th>( (\dim, \ker)(\mathcal{G}(f)) )</th>
<th>( (\dim, \ker)(\text{im}(\partial f)) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( f_3 )</td>
<td>4</td>
<td>3</td>
<td>(8, 0)</td>
<td>(4, 4)</td>
</tr>
<tr>
<td>( f_4 )</td>
<td>4</td>
<td>3</td>
<td>(8, 0)</td>
<td>(4, 1)</td>
</tr>
<tr>
<td>( f_5 )</td>
<td>4</td>
<td>3</td>
<td>(8, 0)</td>
<td>(4, 4)</td>
</tr>
<tr>
<td>( f_6 )</td>
<td>4</td>
<td>3</td>
<td>(8, 0)</td>
<td>(4, 4)</td>
</tr>
<tr>
<td>( f_7 )</td>
<td>4</td>
<td>3</td>
<td>(8, 0)</td>
<td>(4, 0)</td>
</tr>
</tbody>
</table>