Coboundaries and a new invariant for cryptographic functions

K. J. Horadam

Mathematics, RMIT
Melbourne, Australia

Discrete Mathematics Seminar
Monash University, April 24 2012

Outline

Outline

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 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 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 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 $\mathbb{F}_{2^n}$

A small binary example

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

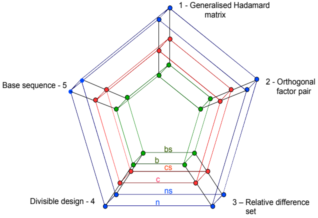
1. Orthogonal cocycle $\psi : \mathbb{Z}_2^2 \times \mathbb{Z}_2^2 \to \mathbb{Z}_2^2$, $\psi(b, d) = bd$
2. Cocyclic generalised Hadamard matrix:

$$[\psi(b,d)] = \begin{bmatrix} 00 & 00 & 00 & 00 \\ 00 & 10 & 01 & 11 \\ 00 & 01 & 11 & 10 \\ 00 & 11 & 10 & 01 \end{bmatrix}$$

Optimal Case: The Five-fold Constellation

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 $f : G \to N$ with $f(1) = 0$,

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

- Note: relationship between f and ∂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.

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 $f(1) = 0$,

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

- Note: relationship between f and ∂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.

The basic cohomology class of cocycles: the coboundaries

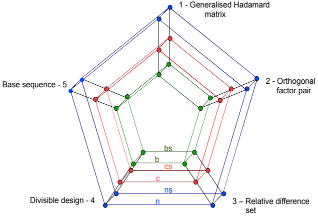
- A cocycle is a coboundary if it is of the form $\psi = \partial f$ for some $f : G \to N$ with $f(1) = 0$,

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

- Note: relationship between f and ∂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

Bundles (Equivalence Classes) of Cocycles



We push equivalence of relative difference sets around the constellation to get equivalence of cocycles,

- Call this equivalence class of cocycle ψ its Bundle. (NOT the same as cohomology class (natural equivalence) of ψ).

Bundles (Equivalence Classes) of Coboundaries

- A Bundle of (2D) coboundaries contains only coboundaries.
- ★

$$\partial f \sim \partial f' \Leftrightarrow$$

$$f' = [\gamma \circ (f \cdot r) \circ \theta] + \chi$$

★

where $f \cdot r(g) = f(rg) - f(g)$ is the shift of f by r, $\gamma \in \mathrm{Aut}(N), \theta \in \mathrm{Aut}(G), r \in G$ and χ is a homomorphism.
- Call this equivalence class of (1D) functions the bundle $\mathbf{b}(f)$ of f.

Outline

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

CCZ Equivalence

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

$$\alpha(\mathcal{G}(\varphi)) = \mathcal{G}(\phi)$$

  where the graph $\mathcal{G}(\phi)$ of ϕ 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 γ, θ, χ with γ, θ 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 γ, θ, χ with γ, θ 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 $p = 7, \quad f(x) = x^2, \ x \in \mathbb{F}_7,$ $f(x+a) - f(x) = 2ax + a^2 \pmod 7$

x	0	1	2	3	4	5	6
$a = 1$	1	3	5	0	2	4	6
$a = 2$	4	1	5	2	6	3	0
$\vdots$							

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 $p = 2$
  Δ_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 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 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!! WE HAVE A PROBLEM....

EA Equivalence and Non-power Functions

BUT.....

- There are APN functions 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 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!! 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 $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, m divisible by 6, $f(x) =$

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

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

- IS IT NEW? IS IT DIFFERENT? HOW CAN WE TELL?

Outline

We need as many invariants for EA and CCZ classes as possible.
Preferably they will be easy to compute.
We can apply the 1D $\leftrightarrow$ 2D link at $\bigstar$ $\bigstar$ to determine a new nonlinearity measure from coboundaries.

The subgroup generated by $\mathrm{im}(\partial f)$

We focus on the subset $\mathrm{im}(\partial f)$, subgroup $\langle \mathrm{im}(\partial f) \rangle$ 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 $n(f) := \dim_p \langle \mathrm{im}(\partial f) \rangle$.

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

Lemma

- $n(f) = 0 \Leftrightarrow f$ *is linear*
- $n(f) \ge n - \lfloor \log_p \Delta(f) \rfloor$, $\Delta(f)$ = *differential uniformity of f*

The subgroup generated by $\mathrm{im}(\partial f)$

We focus on the subset $\mathrm{im}(\partial f)$, subgroup $\langle \mathrm{im}(\partial f) \rangle$ 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 $n(f) := \dim_p \langle \mathrm{im}(\partial f) \rangle$.

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

Lemma

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

The subgroup generated by $\mathrm{im}(\partial f)$

We focus on the subset $\mathrm{im}(\partial f)$, subgroup $\langle \mathrm{im}(\partial f) \rangle$ 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 $n(f) := \dim_p \langle \mathrm{im}(\partial f) \rangle$.

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

Lemma

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

Outline

Invariants associated with $\mathrm{im}(\partial f)$

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

Lemma

If $f \simeq_{\mathbf{b}} f'$ then $n(f) = n(f')$ and so $\langle \mathrm{im}(\partial f) \rangle \cong \langle \mathrm{im}(\partial f') \rangle$.

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

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

Lemma

If $f \simeq_{\mathbf{b}} f'$ then $n(f) = n(f')$ and so $\langle \mathrm{im}(\partial f)\rangle \cong \langle \mathrm{im}(\partial f')\rangle$.

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

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

Lemma

If $f \simeq_{\mathbf{b}} f'$ then $n(f) = n(f')$ and so $\langle \mathrm{im}(\partial f)\rangle \cong \langle \mathrm{im}(\partial f')\rangle$.

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

Preliminary Results

At least 5 permutation representatives of EA classes over $\mho_{16}$ 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).

Preliminary Results

At least 5 permutation representatives of EA classes over $\mho_{16}$ 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 $\mathrm{im}(\partial f)$. $\mathrm{im}(\partial f)$ measures something new!

j	$\Delta(f)$	alg°	$(\dim, \ker)(\mathcal{G}(f))$	$(\dim, \ker)(\mathrm{im}(\partial f))$
f_3	4	3	$(8, 0)$	$(4, 4)$
f_4	4	3	$(8, 0)$	$(4, 1)$
f_5	4	3	$(8, 0)$	$(4, 4)$
f_6	4	3	$(8, 0)$	$(4, 4)$
f_7	4	3	$(8, 0)$	$(4, 0)$