Code loops of both parities

Aleš Drápal and Petr Vojtěchovský*

Department of Algebra
Charles University in Prague
and
Department of Mathematics
University of Denver

Apr 6, 2008 / Bloomington

Loops

Translations

$(Q, \cdot)$ a groupoid.
$L_x : Q \to Q$, $y \mapsto xy$ a *left translation*.
$R_x : Q \to Q$, $y \mapsto yx$ a *right translation*.

Quasigroups and loops

Quasigroup $=$ groupoid where all translations are bijections.
Loop $=$ quasigroup with neutral element 1.

Example

	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	3	4	5	1	2
4	4	5	2	3	1
5	5	3	1	2	4

Loops

Translations

$(Q, \cdot)$ a groupoid.
$L_x : Q \to Q$, $y \mapsto xy$ a *left translation*.
$R_x : Q \to Q$, $y \mapsto yx$ a *right translation*.

Quasigroups and loops

Quasigroup $=$ groupoid where all translations are bijections.
Loop $=$ quasigroup with neutral element 1.

Example

	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	3	4	5	1	2
4	4	5	2	3	1
5	5	3	1	2	4

Loops

Translations

$(Q, \cdot)$ a groupoid.
$L_x : Q \to Q$, $y \mapsto xy$ a *left translation*.
$R_x : Q \to Q$, $y \mapsto yx$ a *right translation*.

Quasigroups and loops

Quasigroup $=$ groupoid where all translations are bijections.
Loop $=$ quasigroup with neutral element 1.

Example

	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	3	4	5	1	2
4	4	5	2	3	1
5	5	3	1	2	4

Application of code loops

Constructing the Monster group M (Conway)

$\mathcal{H}$ = Hamming code of length 7

$\downarrow$

$\mathcal{G}$ = extended binary Golay code

$\downarrow$

$\mathcal{P}$ = Parker loop, the code loop of $\mathcal{G}$, is a Moufang loop, satisfies $x(y(xz)) = ((xy)x)z$

$\downarrow$

N = group with triality of $\mathcal{P}$, contains a Sylow 2-subgroup of M

$\downarrow$ "add" the lattice Λ_{24}

M

Even code loops

Theorem (Griess)

For every doubly even binary code U there exists a unique (up to equivalence) $\theta : U \times U \to \mathbb{F}_2$ such that:

- $\theta(u, u) = \frac{|u|}{4} \mod 2$,
- $\theta(u, v) - \theta(v, u) = \frac{|u \cap v|}{2} \mod 2$,
- $\theta(u, v) + \theta(u + v, w) - \theta(v, w) - \theta(u, v + w) = |u \cap v \cap w| \mod 2$.

Definition

$U(\theta) = \mathbb{F}_2 \times U$ with multiplication

$$(a, u)(b, v) = (a + b + \theta(u, v), u + v)$$

is the *even code loop* associated with U.

Even code loops

Theorem (Griess)

For every doubly even binary code U there exists a unique (up to equivalence) $\theta : U \times U \to \mathbb{F}_2$ such that:

- $\theta(u,u) = \frac{|u|}{4} \mod 2$,
- $\theta(u,v) - \theta(v,u) = \frac{|u \cap v|}{2} \mod 2$,
- $\theta(u,v) + \theta(u+v,w) - \theta(v,w) - \theta(u,v+w) = |u \cap v \cap w| \mod 2$.

Definition

$U(\theta) = \mathbb{F}_2 \times U$ with multiplication

$$(a,u)(b,v) = (a+b+\theta(u,v), u+v)$$

is the *even code loop* associated with U.

Even code loops

Theorem (Griess)

For every doubly even binary code U there exists a unique (up to equivalence) $\theta : U \times U \to \mathbb{F}_2$ such that:

- $\theta(u,u) = \frac{|u|}{4} \mod 2,$
- $\theta(u,v) - \theta(v,u) = \frac{|u \cap v|}{2} \mod 2,$
- $\theta(u,v) + \theta(u+v,w) - \theta(v,w) - \theta(u,v+w) = |u \cap v \cap w| \mod 2.$

Definition

$U(\theta) = \mathbb{F}_2 \times U$ with multiplication

$$(a,u)(b,v) = (a+b+\theta(u,v), u+v)$$

is the *even code loop* associated with U.

Even code loops

Theorem (Griess)

For every doubly even binary code U there exists a unique (up to equivalence) $\theta : U \times U \to \mathbb{F}_2$ such that:

- $\theta(u,u) = \frac{|u|}{4} \mod 2$,
- $\theta(u,v) - \theta(v,u) = \frac{|u \cap v|}{2} \mod 2$,
- $\theta(u,v) + \theta(u+v,w) - \theta(v,w) - \theta(u,v+w) = |u \cap v \cap w| \mod 2$.

Definition

$U(\theta) = \mathbb{F}_2 \times U$ with multiplication

$$(a,u)(b,v) = (a+b+\theta(u,v),\ u+v)$$

is the *even code loop* associated with U.

Theorem (Griess)

For every doubly even binary code U there exists a unique (up to equivalence) $\theta : U \times U \to \mathbb{F}_2$ such that:

- $\theta(u,u) = \frac{|u|}{4} \mod 2$,
- $\theta(u,v) - \theta(v,u) = \frac{|u \cap v|}{2} \mod 2$,
- $\theta(u,v) + \theta(u+v,w) - \theta(v,w) - \theta(u,v+w) = |u \cap v \cap w| \mod 2$.

Definition

$U(\theta) = \mathbb{F}_2 \times U$ with multiplication

$$(a,u)(b,v) = (a+b+\theta(u,v),\, u+v)$$

is the *even code loop* associated with U.

Commutators and associators

Definition

Commutator: $xy = (yx)C(x, y)$.
Associator: $(xy)z = (x(yz))A(x, y, z)$.

In $U(\theta)$,

$$(a, u)(a, u) = (a + a + \theta(u, u), u + u) = (\theta(u, u), 0),$$

$$C(x, y) = C((a, u), (b, v)) = (\theta(u, v) - \theta(v, u), 0),$$

$$A(x, y, z) = (\theta(u, v) + \theta(u + v, w) - \theta(v, w) - \theta(u, v + w), 0)$$

Commutators and associators

Definition

Commutator: $xy = (yx)C(x,y)$.
Associator: $(xy)z = (x(yz))A(x,y,z)$.

In $U(\theta)$,

$$(a,u)(a,u) = (a + a + \theta(u,u), u + u) = (\theta(u,u), 0),$$

$$C(x,y) = C((a,u),(b,v)) = (\theta(u,v) - \theta(v,u), 0),$$

$$A(x,y,z) = (\theta(u,v) + \theta(u+v,w) - \theta(v,w) - \theta(u,v+w), 0)$$

Polarization of codewords

Example

Define $P : U \to \mathbb{F}_2$, $u \mapsto |u|/4$. Then

- $P(u+v) - P(u) - P(v) = |u \cap v|/2$.
- $P(u+v+w) - P(u+v) - P(u+w) - P(v+w) + P(u) + P(v) + P(w) = |u \cap v \cap w|$.

Polarization of codewords

Example

Define $P : U \to \mathbb{F}_2$, $u \mapsto |u|/4$. Then

- $P(u+v) - P(u) - P(v) = |u \cap v|/2$.
- $P(u+v+w) - P(u+v) - P(u+w) - P(v+w) + P(u) + P(v) + P(w) = |u \cap v \cap w|$.

Polarization of codewords

Example

Define $P : U \to \mathbb{F}_2$, $u \mapsto |u|/4$. Then

- $P(u+v) - P(u) - P(v) = |u \cap v|/2$.
- $P(u+v+w) - P(u+v) - P(u+w) - P(v+w) + P(u) + P(v) + P(w) = |u \cap v \cap w|$.

Combinatorial polarization

Definition

V vector space over F, $P : V \to F$, $P(0) = 0$. For $n > 0$ define:

$$\Delta_n P(u_1, \dots, u_n) = \sum_{1 \le i_1 < \cdots < i_m \le n} (-1)^{n-m} P(u_{i_1} + \cdots + u_{i_m}).$$

$\Delta_n P(u, v, w, \dots) =$
$\Delta_{n-1} P(u + v, w, \dots) - \Delta_{n-1} P(u, w, \dots) - \Delta_{n-1} P(v, w, \dots).$

Definition

$\mathrm{cdeg}(P) =$ least n such that $\Delta_n P \neq 0$ and $\Delta_{n+1} P = 0$.

Over prime fields, $\mathrm{cdeg}(P) = n$ iff $\Delta_n P$ is symmetric n-linear.

Combinatorial polarization

Definition

V vector space over F, $P : V \to F$, $P(0) = 0$. For $n > 0$ define:

$$\Delta_n P(u_1, \dots, u_n) = \sum_{1 \le i_1 < \cdots < i_m \le n} (-1)^{n-m} P(u_{i_1} + \cdots + u_{i_m}).$$

$$\Delta_n P(u, v, w, \dots) =$$
$$\Delta_{n-1} P(u + v, w, \dots) - \Delta_{n-1} P(u, w, \dots) - \Delta_{n-1} P(v, w, \dots).$$

Definition

$\mathrm{cdeg}(P) =$ least n such that $\Delta_n P \neq 0$ and $\Delta_{n+1} P = 0$.

Over prime fields, $\mathrm{cdeg}(P) = n$ iff $\Delta_n P$ is symmetric n-linear.

Definition

V vector space over F, $P : V \to F$, $P(0) = 0$. For $n > 0$ define:

$$\Delta_n P(u_1, \dots, u_n) = \sum_{1 \le i_1 < \cdots < i_m \le n} (-1)^{n-m} P(u_{i_1} + \cdots + u_{i_m}).$$

$\Delta_n P(u, v, w, \dots) =$
$\Delta_{n-1} P(u + v, w, \dots) - \Delta_{n-1} P(u, w, \dots) - \Delta_{n-1} P(v, w, \dots)$.

Definition

$\mathrm{cdeg}(P) =$ least n such that $\Delta_n P \neq 0$ and $\Delta_{n+1} P = 0$.

Over prime fields, $\mathrm{cdeg}(P) = n$ iff $\Delta_n P$ is symmetric n-linear.

Combinatorial polarization

Definition

V vector space over F, $P : V \to F$, $P(0) = 0$. For $n > 0$ define:

$$\Delta_n P(u_1, \dots, u_n) = \sum_{1 \le i_1 < \cdots < i_m \le n} (-1)^{n-m} P(u_{i_1} + \cdots + u_{i_m}).$$

$$\Delta_n P(u, v, w, \dots) = \Delta_{n-1} P(u + v, w, \dots) - \Delta_{n-1} P(u, w, \dots) - \Delta_{n-1} P(v, w, \dots).$$

Definition

$\mathrm{cdeg}(P) =$ least n such that $\Delta_n P \neq 0$ and $\Delta_{n+1} P = 0$.

Over prime fields, $\mathrm{cdeg}(P) = n$ iff $\Delta_n P$ is symmetric n-linear.

Characterization of code loops by polarization

Theorem (Aschbacher, Chein, Goodaire, Griess, Hsu)

Let U be doubly even, $\theta : U \times U \to \mathbb{F}_2$ a cocycle. Let $U(\theta)$ be as above, with commutator C and associator A. Then TFAE:

- *$U(\theta)$ is an even code loop.*
- *There is $P : U \to \mathbb{F}_2$ such that $C = \Delta_2 P$, $A = \Delta_3 P$ (can take $P(u) = \theta(u, u)$).*
- *$Q = U(\theta)$ is a Moufang loop with Frattini subloop of order dividing 2.*

Theorem (Hsu)

Nonassociative symplectic Moufang p-loops exist only for $p \leq 3$.

Characterization of code loops by polarization

Theorem (Aschbacher, Chein, Goodaire, Griess, Hsu)

Let U be doubly even, $\theta : U \times U \to \mathbb{F}_2$ a cocycle. Let $U(\theta)$ be as above, with commutator C and associator A. Then TFAE:

- *$U(\theta)$ is an even code loop.*
- *There is $P : U \to \mathbb{F}_2$ such that $C = \Delta_2 P$, $A = \Delta_3 P$ (can take $P(u) = \theta(u, u)$).*
- *$Q = U(\theta)$ is a Moufang loop with Frattini subloop of order dividing 2.*

Theorem (Hsu)

Nonassociative symplectic Moufang p-loops exist only for $p \leq 3$.

Characterization of code loops by polarization

Theorem (Aschbacher, Chein, Goodaire, Griess, Hsu)

Let U be doubly even, $\theta : U \times U \to \mathbb{F}_2$ a cocycle. Let $U(\theta)$ be as above, with commutator C and associator A. Then TFAE:

- *$U(\theta)$ is an even code loop.*
- *There is $P : U \to \mathbb{F}_2$ such that $C = \Delta_2 P$, $A = \Delta_3 P$ (can take $P(u) = \theta(u,u)$).*
- *$Q = U(\theta)$ is a Moufang loop with Frattini subloop of order dividing 2.*

Theorem (Hsu)

Nonassociative symplectic Moufang p-loops exist only for $p \leq 3$.

Characterization of code loops by polarization

Theorem (Aschbacher, Chein, Goodaire, Griess, Hsu)

Let U be doubly even, $\theta : U \times U \to \mathbb{F}_2$ a cocycle. Let $U(\theta)$ be as above, with commutator C and associator A. Then TFAE:

- *$U(\theta)$ is an even code loop.*
- *There is $P : U \to \mathbb{F}_2$ such that $C = \Delta_2 P$, $A = \Delta_3 P$ (can take $P(u) = \theta(u, u)$).*
- *$Q = U(\theta)$ is a Moufang loop with Frattini subloop of order dividing 2.*

Theorem (Hsu)

Nonassociative symplectic Moufang p-loops exist only for $p \leq 3$.

Characterization of code loops by polarization

Theorem (Aschbacher, Chein, Goodaire, Griess, Hsu)

Let U be doubly even, $\theta : U \times U \to \mathbb{F}_2$ a cocycle. Let $U(\theta)$ be as above, with commutator C and associator A. Then TFAE:

- *$U(\theta)$ is an even code loop.*
- *There is $P : U \to \mathbb{F}_2$ such that $C = \Delta_2 P$, $A = \Delta_3 P$ (can take $P(u) = \theta(u, u)$).*
- *$Q = U(\theta)$ is a Moufang loop with Frattini subloop of order dividing 2.*

Theorem (Hsu)

Nonassociative symplectic Moufang p-loops exist only for $p \leq 3$.

The coding construction required for $p = 2$

Given U with basis $\{u_1, \ldots, u_n\}$, $P : U \to \mathbb{F}_2$, $\mathrm{cdeg}(P) \le 3$, find V doubly even with basis $\{e_1, \ldots, e_n\}$ such that

- $P(u_i) = |e_i|/4$,
- $\Delta_2 P(u_i, u_j) = |e_i \cap e_j|/2$,
- $\Delta_3 P(u_i, u_j, u_k) = |e_i \cap e_j \cap e_k|$.

Theorem (P.V.)

Can be done for any $\mathrm{cdeg}(P) \le r$ and codes of level $r - 1$.

The coding construction required for $p = 2$

Given U with basis $\{u_1, \dots, u_n\}$, $P : U \to \mathbb{F}_2$, $\mathrm{cdeg}(P) \leq 3$, find V doubly even with basis $\{e_1, \dots, e_n\}$ such that

- $P(u_i) = |e_i|/4$,
- $\Delta_2 P(u_i, u_j) = |e_i \cap e_j|/2$,
- $\Delta_3 P(u_i, u_j, u_k) = |e_i \cap e_j \cap e_k|$.

Theorem (P.V.)

Can be done for any $\mathrm{cdeg}(P) \leq r$ and codes of level $r - 1$.

The coding construction required for $p = 2$

Given U with basis $\{u_1, \ldots, u_n\}$, $P : U \to \mathbb{F}_2$, $\mathrm{cdeg}(P) \leq 3$, find V doubly even with basis $\{e_1, \ldots, e_n\}$ such that

- $P(u_i) = |e_i|/4$,
- $\Delta_2 P(u_i, u_j) = |e_i \cap e_j|/2$,
- $\Delta_3 P(u_i, u_j, u_k) = |e_i \cap e_j \cap e_k|$.

Theorem (P.V.)

Can be done for any $\mathrm{cdeg}(P) \leq r$ and codes of level $r - 1$.

The coding construction required for $p = 2$

Given U with basis $\{u_1, \dots, u_n\}$, $P : U \to \mathbb{F}_2$, $\mathrm{cdeg}(P) \le 3$, find V doubly even with basis $\{e_1, \dots, e_n\}$ such that

- $P(u_i) = |e_i|/4$,
- $\Delta_2 P(u_i, u_j) = |e_i \cap e_j|/2$,
- $\Delta_3 P(u_i, u_j, u_k) = |e_i \cap e_j \cap e_k|$.

Theorem (P.V.)

Can be done for any $\mathrm{cdeg}(P) \le r$ and codes of level $r - 1$.

The coding construction required for $p = 2$

Given U with basis $\{u_1, \ldots, u_n\}$, $P : U \to \mathbb{F}_2$, $\mathrm{cdeg}(P) \le 3$, find V doubly even with basis $\{e_1, \ldots, e_n\}$ such that

- $P(u_i) = |e_i|/4$,
- $\Delta_2 P(u_i, u_j) = |e_i \cap e_j|/2$,
- $\Delta_3 P(u_i, u_j, u_k) = |e_i \cap e_j \cap e_k|$.

Theorem (P.V.)

Can be done for any $\mathrm{cdeg}(P) \le r$ and codes of level $r - 1$.

Odd p: Results of Richardson

In Richardson's thesis:

- constructed large p-subgroups of M for $p = 3, 5, 7$.
- started with self-orthogonal codes over $\mathbb{F}_p$
- noticed connection to polarization
- defined *odd code loops*

Odd p: Results of Richardson

In Richardson's thesis:

- constructed large p-subgroups of M for $p = 3, 5, 7$.
- started with self-orthogonal codes over $\mathbb{F}_p$
- noticed connection to polarization
- defined *odd code loops*

Odd p: Results of Richardson

In Richardson's thesis:

- constructed large p-subgroups of M for $p = 3, 5, 7$.
- started with self-orthogonal codes over $\mathbb{F}_p$
- noticed connection to polarization
- defined *odd code loops*

Odd p: Results of Richardson

In Richardson's thesis:

- constructed large p-subgroups of M for $p = 3, 5, 7$.
- started with self-orthogonal codes over $\mathbb{F}_p$
- noticed connection to polarization
- defined *odd code loops*

Odd p: Results of Richardson

In Richardson's thesis:

- constructed large p-subgroups of M for $p = 3, 5, 7$.
- started with self-orthogonal codes over $\mathbb{F}_p$
- noticed connection to polarization
- defined *odd code loops*

Narrow definition of odd code loops

Definition

- U self-orthogonal code over $\mathbb{F}_p$
- $z \in U$ such that $z_i \neq 0$ for every i and z is invariant under all permutation matrices in $\mathrm{Aut}\, U$
- $\theta(u, v) = \sum_i z_i^{-1} u_i^2 v_i$
- $U(\theta)$ is *odd code loop*

Narrow definition of odd code loops

Definition

- U self-orthogonal code over $\mathbb{F}_p$
- $z \in U$ such that $z_i \neq 0$ for every i and z is invariant under all permutation matrices in $\mathrm{Aut}\, U$
- $\theta(u, v) = \sum_i z_i^{-1} u_i^2 v_i$
- $U(\theta)$ is *odd code loop*

Narrow definition of odd code loops

Definition

- U self-orthogonal code over $\mathbb{F}_p$
- $z \in U$ such that $z_i \neq 0$ for every i and z is invariant under all permutation matrices in $\mathrm{Aut}\, U$
- $\theta(u, v) = \sum_i z_i^{-1} u_i^2 v_i$
- $U(\theta)$ is *odd code loop*

Narrow definition of odd code loops

Definition

- U self-orthogonal code over $\mathbb{F}_p$
- $z \in U$ such that $z_i \neq 0$ for every i and z is invariant under all permutation matrices in $\mathrm{Aut}\, U$
- $\theta(u, v) = \sum_i z_i^{-1} u_i^2 v_i$
- $U(\theta)$ is *odd code loop*

Narrow definition of odd code loops

Definition

- U self-orthogonal code over $\mathbb{F}_p$
- $z \in U$ such that $z_i \neq 0$ for every i and z is invariant under all permutation matrices in $\mathrm{Aut}\, U$
- $\theta(u, v) = \sum_i z_i^{-1} u_i^2 v_i$
- $U(\theta)$ is *odd code loop*

General definition of odd code loops

$f(u,v,w) = \sum_i z_i^{-1} u_i v_i w_i$ is symmetric trilinear,
$f(u,u,v) = \theta(u,v)$.

Definition

- U self-orthogonal code over $\mathbb{F}_p$
- $f : U \times U \times U \to \mathbb{F}_p$ symmetric trilinear form
- $\theta(u,v) = f(u,u,v)$
- $U(\theta)$ is *general odd code loop*

General definition of odd code loops

$f(u,v,w) = \sum_i z_i^{-1} u_i v_i w_i$ is symmetric trilinear,
$f(u,u,v) = \theta(u,v)$.

Definition

- U self-orthogonal code over $\mathbb{F}_p$
- $f : U \times U \times U \to \mathbb{F}_p$ symmetric trilinear form
- $\theta(u,v) = f(u,u,v)$
- $U(\theta)$ is *general odd code loop*

General definition of odd code loops

$f(u,v,w) = \sum_i z_i^{-1} u_i v_i w_i$ is symmetric trilinear,
$f(u,u,v) = \theta(u,v)$.

Definition

- U self-orthogonal code over $\mathbb{F}_p$
- $f : U \times U \times U \to \mathbb{F}_p$ symmetric trilinear form
- $\theta(u,v) = f(u,u,v)$
- $U(\theta)$ is *general odd code loop*

General definition of odd code loops

$f(u,v,w) = \sum_i z_i^{-1} u_i v_i w_i$ is symmetric trilinear,
$f(u,u,v) = \theta(u,v)$.

Definition

- U self-orthogonal code over $\mathbb{F}_p$
- $f : U \times U \times U \to \mathbb{F}_p$ symmetric trilinear form
- $\theta(u,v) = f(u,u,v)$
- $U(\theta)$ is *general odd code loop*

General definition of odd code loops

$f(u,v,w) = \sum_i z_i^{-1} u_i v_i w_i$ is symmetric trilinear,
$f(u,u,v) = \theta(u,v)$.

Definition

- U self-orthogonal code over $\mathbb{F}_p$
- $f : U \times U \times U \to \mathbb{F}_p$ symmetric trilinear form
- $\theta(u,v) = f(u,u,v)$
- $U(\theta)$ is *general odd code loop*

General definition of odd code loops

$f(u,v,w) = \sum_i z_i^{-1} u_i v_i w_i$ is symmetric trilinear,
$f(u,u,v) = \theta(u,v)$.

Definition

- U self-orthogonal code over $\mathbb{F}_p$
- $f : U \times U \times U \to \mathbb{F}_p$ symmetric trilinear form
- $\theta(u,v) = f(u,u,v)$
- $U(\theta)$ is *general odd code loop*

Middle ground: Characteristic forms

Definition (Characteristic forms)

Call a symmetric form $f : V^n \to \mathbb{F}_p$ *characteristic* if

$$f(u_1, \dots, u_n) = 0$$

whenever an argument is repeated at least p times, $p = \mathrm{char}\, F$.

Theorem

Let $P : V \to F$, $f = \Delta_n P : V^n \to F$. Then f is characteristic. Conversely, every characteristic form $g : V^n \to F$ is of the form $\Delta_n R$ for some $R : V \to F$.

Think of quadratic forms and the associated symmetric bilinear forms.

Middle ground: Characteristic forms

Definition (Characteristic forms)

Call a symmetric form $f : V^n \to \mathbb{F}_p$ *characteristic* if

$$f(u_1, \ldots, u_n) = 0$$

whenever an argument is repeated at least p times, $p = \mathrm{char}\, F$.

Theorem

Let $P : V \to F$, $f = \Delta_n P : V^n \to F$. Then f is characteristic. Conversely, every characteristic form $g : V^n \to F$ is of the form $\Delta_n R$ for some $R : V \to F$.

Think of quadratic forms and the associated symmetric bilinear forms.

Middle ground: Characteristic forms

Definition (Characteristic forms)

Call a symmetric form $f : V^n \to \mathbb{F}_p$ *characteristic* if

$$f(u_1, \dots, u_n) = 0$$

whenever an argument is repeated at least p times, $p = \operatorname{char} F$.

Theorem

Let $P : V \to F$, $f = \Delta_n P : V^n \to F$. Then f is characteristic. Conversely, every characteristic form $g : V^n \to F$ is of the form $\Delta_n R$ for some $R : V \to F$.

Think of quadratic forms and the associated symmetric bilinear forms.

Odd code loops

Definition

- U self-orthogonal code over $\mathbb{F}_p$
- $f : U \times U \times U \to \mathbb{F}_p$ **characteristic** trilinear form
- $\theta(u, v) = f(u, u, v)$
- $U(\theta)$ is *odd code loop*

Odd code loops

Definition

- U self-orthogonal code over $\mathbb{F}_p$
- $f : U \times U \times U \to \mathbb{F}_p$ **characteristic** trilinear form
- $\theta(u, v) = f(u, u, v)$
- $U(\theta)$ is *odd code loop*

Odd code loops

Definition

- U self-orthogonal code over $\mathbb{F}_p$
- $f : U \times U \times U \to \mathbb{F}_p$ **characteristic** trilinear form
- $\theta(u, v) = f(u, u, v)$
- $U(\theta)$ is *odd code loop*

Odd code loops

Definition

- U self-orthogonal code over $\mathbb{F}_p$
- $f : U \times U \times U \to \mathbb{F}_p$ **characteristic** trilinear form
- $\theta(u, v) = f(u, u, v)$
- $U(\theta)$ is *odd code loop*

Odd code loops

Definition

- U self-orthogonal code over $\mathbb{F}_p$
- $f : U \times U \times U \to \mathbb{F}_p$ **characteristic** trilinear form
- $\theta(u, v) = f(u, u, v)$
- $U(\theta)$ is *odd code loop*

Characterizations of odd code loops

Theorem

The following concepts are equivalent:

- *odd code loops*
- *loops $U(\theta)$ where $C(u,-v) = \Delta_2 P$, $A(u,v,w) = \Delta_3 P$, $P(\lambda u) = \lambda^3 P(u)$,*
- *conjugacy closed loops ($L_x^{-1} L_y L_x$ is a left translation, $R_x^{-1} R_y R_x$ is a right translation) with certain properties*

When $p > 3$, there is a unique choice for P already to satisfy $\Delta_3 P = A$.

Characterizations of odd code loops

Theorem

The following concepts are equivalent:

- *odd code loops*
- *loops $U(\theta)$ where $C(u,-v) = \Delta_2 P$, $A(u,v,w) = \Delta_3 P$, $P(\lambda u) = \lambda^3 P(u)$,*
- *conjugacy closed loops ($L_x^{-1} L_y L_x$ is a left translation, $R_x^{-1} R_y R_x$ is a right translation) with certain properties*

When $p > 3$, there is a unique choice for P already to satisfy $\Delta_3 P = A$.

Theorem

The following concepts are equivalent:

- *odd code loops*
- *loops $U(\theta)$ where $C(u, -v) = \Delta_2 P$, $A(u, v, w) = \Delta_3 P$, $P(\lambda u) = \lambda^3 P(u)$,*
- *conjugacy closed loops ($L_x^{-1} L_y L_x$ is a left translation, $R_x^{-1} R_y R_x$ is a right translation) with certain properties*

When $p > 3$, there is a unique choice for P already to satisfy $\Delta_3 P = A$.

Characterizations of odd code loops

Theorem

The following concepts are equivalent:

- *odd code loops*
- *loops* $U(\theta)$ *where* $C(u,-v) = \Delta_2 P$, $A(u,v,w) = \Delta_3 P$, $P(\lambda u) = \lambda^3 P(u)$,
- *conjugacy closed loops (*$L_x^{-1} L_y L_x$ *is a left translation,* $R_x^{-1} R_y R_x$ *is a right translation) with certain properties*

When $p > 3$, there is a unique choice for P already to satisfy $\Delta_3 P = A$.

Characterizations of odd code loops

Theorem

The following concepts are equivalent:

- *odd code loops*
- *loops* $U(\theta)$ *where* $C(u,-v) = \Delta_2 P$, $A(u,v,w) = \Delta_3 P$, $P(\lambda u) = \lambda^3 P(u)$,
- *conjugacy closed loops (*$L_x^{-1} L_y L_x$ *is a left translation,* $R_x^{-1} R_y R_x$ *is a right translation) with certain properties*

When $p > 3$, there is a unique choice for P already to satisfy $\Delta_3 P = A$.

The coding construction in the odd case

Let $\{e_1, \ldots, e_n\}$ be a basis of V.
Given a characteristic trilinear form $f : V^3 \to \mathbb{F}_p$, find self-orthogonal U with basis $\{u_1, \ldots, u_n\}$ such that

$$f(e_i, e_j, e_k) = \sum_r u_{i,r} u_{j,r} u_{k,r}.$$

We need to control $\sum u_i v_i w_i$, $\sum u_i^2 v_i$, $\sum u_i^3$ at the same time.

The coding construction in the odd case

Let $\{e_1, \ldots, e_n\}$ be a basis of V.
Given a characteristic trilinear form $f : V^3 \to \mathbb{F}_p$, find self-orthogonal U with basis $\{u_1, \ldots, u_n\}$ such that

$$f(e_i, e_j, e_k) = \sum_r u_{i,r} u_{j,r} u_{k,r}.$$

We need to control $\sum u_i v_i w_i$, $\sum u_i^2 v_i$, $\sum u_i^3$ at the same time.

One variable

Problem

Given $b_1, \ldots, b_{p-1} \in \mathbb{F}_p$, *find* $x \in \mathbb{F}_p^n$ *such that*

$$\sum_i x_i^\lambda = b_\lambda$$

for every $1 \leq \lambda \leq p-1$.

Set $a_j = |\{i;\ x_i = j\}|$.

Then

$$\sum_i x_i^\lambda = b_\lambda$$

becomes

$$a_1 \cdot 1^\lambda + a_2 \cdot 2^\lambda + \cdots + a_{p-1} \cdot (p-1)^\lambda = b_\lambda.$$

One variable continued

Set $a_j = |\{i;\ x_i = j\}|$.

Then

$$\sum_i x_i^\lambda = b_\lambda$$

becomes

$$a_1 \cdot 1^\lambda + a_2 \cdot 2^\lambda + \cdots + a_{p-1} \cdot (p-1)^\lambda = b_\lambda.$$

One variable continued

$$A = \begin{pmatrix} 1^1 & 2^1 & \cdots & (p-1)^1 \\ 1^2 & 2^2 & \cdots & (p-1)^2 \\ \vdots & & \ddots & \\ 1^{p-1} & 2^{p-1} & \cdots & (p-1)^{p-1} \end{pmatrix}$$

(Vandermonde) There is a unique solution subject to the constraints $0 \leq a_i < p$.

One variable continued

$$A = \begin{pmatrix} 1^1 & 2^1 & \cdots & (p-1)^1 \\ 1^2 & 2^2 & \cdots & (p-1)^2 \\ \vdots & & \ddots & \\ 1^{p-1} & 2^{p-1} & \cdots & (p-1)^{p-1} \end{pmatrix}$$

(Vandermonde) There is a unique solution subject to the constraints $0 \leq a_i < p$.

Multiple variables

Problem

Given $b_{\lambda_1,\dots,\lambda_d} \in \mathbb{F}_p$ *for every* $1 \le \lambda_i \le p-1$, *find* $x_1, \dots,$ $x_d \in (\mathbb{F}_p)^n$ *such that*

$$\sum_r {x_{1,r}}^{\lambda_1} \cdots {x_{d,r}}^{\lambda_d} = b_{\lambda_1,\dots,\lambda_d}.$$

Proof boils down to showing that $|A^{\otimes d}| \neq 0$.

Theorem (Determinant of Kronecker product)

Let A *be an* $n \times n$ *and* B *an* $m \times m$ *matrix. Then*

$$|A \otimes B| = |A|^m |B|^n.$$

Multiple variables

Problem

Given $b_{\lambda_1,\ldots,\lambda_d} \in \mathbb{F}_p$ *for every* $1 \le \lambda_i \le p-1$*, find* $x_1, \ldots,$ $x_d \in (\mathbb{F}_p)^n$ *such that*

$$\sum_r x_{1,r}{}^{\lambda_1} \cdots x_{d,r}{}^{\lambda_d} = b_{\lambda_1,\ldots,\lambda_d}.$$

Proof boils down to showing that $|A^{\otimes d}| \neq 0$.

Theorem (Determinant of Kronecker product)

Let A *be an* $n \times n$ *and* B *an* $m \times m$ *matrix. Then*

$$|A \otimes B| = |A|^m |B|^n.$$

Problem

Given $b_{\lambda_1,\dots,\lambda_d} \in \mathbb{F}_p$ for every $1 \le \lambda_i \le p-1$, find $x_1, \dots,$ $x_d \in (\mathbb{F}_p)^n$ such that

$$\sum_r {x_{1,r}}^{\lambda_1} \cdots {x_{d,r}}^{\lambda_d} = b_{\lambda_1,\dots,\lambda_d}.$$

Proof boils down to showing that $|A^{\otimes d}| \neq 0$.

Theorem (Determinant of Kronecker product)

Let A be an $n \times n$ and B an $m \times m$ matrix. Then

$$|A \otimes B| = |A|^m |B|^n.$$

Multiple variables with nonnegative exponents

Problem

Given $b_{\lambda_1,\dots,\lambda_d} \in \mathbb{F}_p$ *for every* $0 \le \lambda_i \le p-1$, *find* $x_1, \dots,$ $x_d \in (\mathbb{F}_p)^n$ *such that*

$$\sum_r {x_{1,r}}^{\lambda_1} \cdots {x_{d,r}}^{\lambda_d} = b_{\lambda_1,\dots,\lambda_d}.$$

Proof by disjunction trick. The code is no more of optimal length.

Multiple variables with nonnegative exponents

Problem

Given $b_{\lambda_1,\dots,\lambda_d} \in \mathbb{F}_p$ *for every* $0 \le \lambda_i \le p-1$, *find* $x_1, \dots,$ $x_d \in (\mathbb{F}_p)^n$ *such that*

$$\sum_r {x_{1,r}}^{\lambda_1} \cdots {x_{d,r}}^{\lambda_d} = b_{\lambda_1,\dots,\lambda_d}.$$

Proof by disjunction trick. The code is no more of optimal length.