Code loops in dimension up to 8

E.A. O'Brien and Petr Vojtěchovský

Arbeitstagung Allgemeine Algebra
Czech University of Life Sciences
May 29, 2016

Outline

Outline

Outline

The construction of the Monster simple group is based on the binary Golay code, the Leech lattice, and a remarkable nonassociative loop discovered by R.A. Parker.

-- J.H. Conway in “The Monster Group and its 196884-dimensional space”

Some history

Some history

1984 The Monster group is discovered by Griess

Some history

1984 The Monster group is discovered by Griess
1985 Conway publishes a simplified construction

Some history

1984 The Monster group is discovered by Griess
1985 Conway publishes a simplified construction
1986 Griess generalizes Parker's construction, coins the name **code loop**

Some history

1984 The Monster group is discovered by Griess

1985 Conway publishes a simplified construction

1986 Griess generalizes Parker's construction, coins the name **code loop**

1990 Chein and Goodaire describe Moufang loops with a unique nonidentity square

Some history

1984 The Monster group is discovered by Griess

1985 Conway publishes a simplified construction

1986 Griess generalizes Parker's construction, coins the name **code loop**

1990 Chein and Goodaire describe Moufang loops with a unique nonidentity square

1994 Aschbacher classifies symplectic Moufang 2-loops in terms of the squaring map and obtains local 2-subgroups of certain sporadic groups

Some history

1984 The Monster group is discovered by Griess

1985 Conway publishes a simplified construction

1986 Griess generalizes Parker's construction, coins the name **code loop**

1990 Chein and Goodaire describe Moufang loops with a unique nonidentity square

1994 Aschbacher classifies symplectic Moufang 2-loops in terms of the squaring map and obtains local 2-subgroups of certain sporadic groups

1995 Richardson constructs local p-subgroups in certain sporadic groups using odd code loops

Some history

1984 The Monster group is discovered by Griess
1985 Conway publishes a simplified construction
1986 Griess generalizes Parker's construction, coins the name **code loop**
1990 Chein and Goodaire describe Moufang loops with a unique nonidentity square
1994 Aschbacher classifies symplectic Moufang 2-loops in terms of the squaring map and obtains local 2-subgroups of certain sporadic groups
1995 Richardson constructs local p-subgroups in certain sporadic groups using odd code loops
2000 Hsu realizes that code loops, symplectic Moufang 2-loops and small Frattini Moufang 2-loops are the same thing

Some history

1984 The Monster group is discovered by Griess

1985 Conway publishes a simplified construction

1986 Griess generalizes Parker's construction, coins the name **code loop**

1990 Chein and Goodaire describe Moufang loops with a unique nonidentity square

1994 Aschbacher classifies symplectic Moufang 2-loops in terms of the squaring map and obtains local 2-subgroups of certain sporadic groups

1995 Richardson constructs local p-subgroups in certain sporadic groups using odd code loops

2000 Hsu realizes that code loops, symplectic Moufang 2-loops and small Frattini Moufang 2-loops are the same thing

2007 Nagy and V enumerate code loops of order 64

Some history

1984 The Monster group is discovered by Griess

1985 Conway publishes a simplified construction

1986 Griess generalizes Parker's construction, coins the name **code loop**

1990 Chein and Goodaire describe Moufang loops with a unique nonidentity square

1994 Aschbacher classifies symplectic Moufang 2-loops in terms of the squaring map and obtains local 2-subgroups of certain sporadic groups

1995 Richardson constructs local p-subgroups in certain sporadic groups using odd code loops

2000 Hsu realizes that code loops, symplectic Moufang 2-loops and small Frattini Moufang 2-loops are the same thing

2007 Nagy and V enumerate code loops of order 64

2008 Nagy shows how to construct code loops directly from squaring maps

Some history

1984 The Monster group is discovered by Griess
1985 Conway publishes a simplified construction
1986 Griess generalizes Parker's construction, coins the name **code loop**
1990 Chein and Goodaire describe Moufang loops with a unique nonidentity square
1994 Aschbacher classifies symplectic Moufang 2-loops in terms of the squaring map and obtains local 2-subgroups of certain sporadic groups
1995 Richardson constructs local p-subgroups in certain sporadic groups using odd code loops
2000 Hsu realizes that code loops, symplectic Moufang 2-loops and small Frattini Moufang 2-loops are the same thing
2007 Nagy and V enumerate code loops of order 64
2008 Nagy shows how to construct code loops directly from squaring maps
2010 Drápal and V describe code loops in both parities combinatorially

Some history

1984 The Monster group is discovered by Griess

1985 Conway publishes a simplified construction

1986 Griess generalizes Parker's construction, coins the name **code loop**

1990 Chein and Goodaire describe Moufang loops with a unique nonidentity square

1994 Aschbacher classifies symplectic Moufang 2-loops in terms of the squaring map and obtains local 2-subgroups of certain sporadic groups

1995 Richardson constructs local p-subgroups in certain sporadic groups using odd code loops

2000 Hsu realizes that code loops, symplectic Moufang 2-loops and small Frattini Moufang 2-loops are the same thing

2007 Nagy and V enumerate code loops of order 64

2008 Nagy shows how to construct code loops directly from squaring maps

2010 Drápal and V describe code loops in both parities combinatorially

2015 Hora and Pudlák classify trilinear alternating forms over $\mathbb{F}_2$ in dimension 8

Doubly even codes

For a vector v in $\mathbb{F}_2^n$ let $|v|$ be the **Hamming weight** of v, the number of nonzero coordinates of v.

Let $u \cap v$ be the vector such that $(u \cap v)_i = \min\{u_i, v_i\}$.

Definition

A binary code V is **doubly even** if $|v|$ is a multiple of 4 for every $v \in V$.

If V is doubly even then $|u \cap v|/2$ is an integer for every u, $v \in V$.

Loops and Moufang loops

Definition

A **loop** is a groupoid $(Q, \cdot)$ with identity element 1 such that the translations $L_x : y \mapsto xy$, $R_x : y \mapsto yx$ are bijections of Q.

Definition

A loop is **Moufang** if it satisfies the identity $x(y(xz)) = ((xy)x)z$.

Factor sets for doubly even codes

Let V be a doubly even code. A mapping $\theta : V \times V \to \mathbb{F}_2$ is a **factor set** if

- $\theta(u, u) \equiv |u|/4$,
- $\theta(u, v) + \theta(v, u) \equiv |u \cap v|/2$,
- $\theta(u, v) + \theta(u + v, w) + \theta(v, w) + \theta(u, v + w) \equiv |u \cap v \cap w|$.

Theorem (Griess)

Every doubly even code V admits a factor set, uniquely determined up to a coboundary.

Griess' code loops

Definition

Let V be a doubly even code and $\theta : V \times V \to \mathbb{F}_2$ its factor set. Define $\mathcal{Q}(V,\theta)$ on $\mathbb{F}_2 \times V$ by

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

Theorem (Griess)

The loop $\mathcal{Q}(V,\theta)$ is always Moufang and its isomorphism type does not depend on the choice of the factor set θ. It is the **code loop** *of V.*

Combinatorial polarization

Let $f : V \to F$ be mapping such that $f(0) = 0$. The m**-th derived form** $f_m : V^m \to F$ is defined by

$$f_m(u_1, \dots, u_m) = \sum_{I \subseteq \{1,\dots,m\}} (-1)^{m-|I|} f(\sum_{i \in I} u_i).$$

Notes:

- $f_2(u_1, u_2) = f(u_1 + u_2) - f(u_1) - f(u_2)$
- every f_m is symmetric
- $f_{m+1} = 0$ if and only if f_m is m-additive.
- over $\mathbb{F}_2$, every f_m is alternating (vanishes when argument is repeated)

Symplectic 2-loops and the squaring map

Definition

A 2-loop Q is *symplectic* if it contains a central subloop F of order 2 such that $Q/F = V$ is an elementary abelian 2-group.

In a symplectic 2-loop $\mathcal{Q}(V, \theta)$, the **squaring map** $P : x \mapsto x^2$ can be viewed as a map $V \to F$ since $(a, u)(a, u) = (\theta(u, u), 0)$.

Symplectic Moufang 2-loops

Theorem (Aschbacher)

Let V be a vector space over $\mathbb{F}_2$. Then:

- *A symplectic 2-loop over V is Moufang if and only if P_2 is the commutator map, P_3 is the associator map and $P_4 = 0$.*
- *Given a map $f : V \to F$ such that $f_4 = 0$, there is a symplectic Moufang 2-loop with $P = f$.*
- *Two 2-symplectic Moufang loops over V are isomorphic if and only if their squaring maps are conjugate in $GL(V)$.*

Results of Hsu

A Moufang p-loop Q is **small Frattini** if it possesses a normal subloop F of order dividing p such that Q/F is an elementary abelian p-group.

Theorem (Hsu)

- *In a small Frattini Moufang loop the subloop F is central.*
- *Nonassociative small Frattini Moufang loops exist iff $p \leq 3$.*
- *Small Frattini Moufang 2-loops $=$ code loops $=$ symplectic Moufang 2-loops.*

Outline

1. Introduction
   - History
   - Code loops
   - Combinatorial polarization
   - Symplectic Moufang 2-loops
   - Results of Hsu
2. Enumeration
   - Trilinear alternating forms
   - Stratified action of $GL(V)$
   - Code loops

Trilinear alternating forms

Two trilinear alternating forms $f, g : V^3 \to F$ are **equivalent** if there is $\varphi \in GL(V)$ such that $f(\varphi(u), \varphi(v), \varphi(w)) = g(u, v, w)$.

Theorem (Cohen and Helminck 1988)

Classified trilinear alternating forms over $\mathbb{F}_2$ in dimension ≤ 7.

Theorem (Hora and Pudlák 2015)

There are 32 trilinear alternating forms over $\mathbb{F}_2$ in dimension $d = 8$.

- $d = 9$, $F = \mathbb{F}_2$ has just been done by Hora and Pudlák
- for $d = 9$, $F = \mathbb{C}$, there are infinitely many pairwise nonequivalent trilinear alternating forms

Main idea of the classification of forms

- find powerful invariants (radicals, radical polynomials, graphs based on radical polynomials), hopefully obtaining a complete set $\mathcal{F}$ of representatives
- for each representative f calculate the stabilizer G_f in $G = GL(V)$. How?
- either by clever analysis, or
- by brute force, using randomized stabilizer (birthday paradox) to obtain a subgroup H_f of G_f for every f, then check $\sum_{f\in\mathcal{F}}[G : H_f] = |\text{space}|$ to guarantee $H_f = G_f$

Examples: Two forms in dimension 8

The following two trilinear alternating forms have the largest (resp. smallest) stabilizer:

Examples: Two forms in dimension 8

The following two trilinear alternating forms have the largest (resp. smallest) stabilizer:

- $f = f_0 = 0$, $|G_f| = 5348063769211699200$

Examples: Two forms in dimension 8

The following two trilinear alternating forms have the largest (resp. smallest) stabilizer:

- $f = f_0 = 0$, $|G_f| = 5348063769211699200$
- $f = f_{21} = 123 + 145 + 168 + 347 + 258 + 267$, $|G_f| = 192$

Examples: Two forms in dimension 8

The following two trilinear alternating forms have the largest (resp. smallest) stabilizer:

- $f = f_0 = 0$, $|G_f| = 5348063769211699200$
- $f = f_{21} = 123 + 145 + 168 + 347 + 258 + 267$, $|G_f| = 192$

Small stabilizers are very hard to find.

Parameters for combinatorial polarization

Recall that code loops over V are in one-to-one correspondence with (squaring) maps $P : V \to \mathbb{F}_2$ such that P_3 is a trilinear alternating form.

Let $(e_1, \dots, e_d)$ be an ordered basis of V.

- Since $P_3 = 0$, the map $P : V \to \mathbb{F}_2$ is determined by the values

  $$P(e_i) = \omega_i, \quad P_2(e_i, e_j) = \omega_{ij}, \quad P_3(e_i, e_j, e_k) = \omega_{ijk}$$

  for $1 \leq i < j < k \leq d$.
- Conversely, given any parameters ω_i, ω_{ij}, $\omega_{ijk} \in \mathbb{F}_2$, there is a unique $P : V \to \mathbb{F}_2$ with $P_3 = 0$ and those parameters.

The parameter space

Let $F=\mathbb{F}_2$, $V=F^d$ and $\Omega_d=F^{\binom{d}{1}+\binom{d}{2}+\binom{d}{3}}$.

- The group $GL(V)$ acts on maps $V\to F$ by $P^\varphi(u)=P(\varphi(u))$.
- $GL(V)$ also acts on maps $P:V\to F$ with $P_3=0$.
- Thus $GL(V)$ acts on the **parameter space** Ω_d.

The action of $GL(V)$ on the parameter space

Lemma

Let V be a vector space over $F=\mathbb{F}_2$ with ordered basis $(e_1,\dots,e_d)$. Let $B=(b_{ij})\in GL(V)$ and $\omega\in\Omega_d$. The coordinates of ω^B are obtained as follows:

$$\omega^B_{uvw}=\sum_{i<j<k}(b_{iu}b_{jv}b_{kw}+b_{iu}b_{kv}b_{jw}+b_{ju}b_{iv}b_{kw}+b_{ju}b_{kv}b_{iw}+b_{ku}b_{iv}b_{jw}+b_{ku}b_{jv}b_{iw})\omega_{ijk}$$

$$\begin{aligned}\omega^B_{uv}=&\sum_{i<j}(b_{iu}b_{jv}+b_{ju}b_{iv})\omega_{ij}\\&+\sum_{i<j<k}(b_{iu}b_{ju}b_{kv}+b_{iu}b_{ku}b_{jv}+b_{ju}b_{ku}b_{iv}+b_{iu}b_{jv}b_{kv}+b_{ju}b_{iv}b_{kv}+b_{ku}b_{iv}b_{jv})\omega_{ijk}\end{aligned}$$

$$\omega^B_u=\sum_i b_{iu}\omega_i+\sum_{i<j}b_{iu}b_{ju}\omega_{ij}+\sum_{i<j<k}b_{iu}b_{ju}b_{ku}\omega_{ijk}.$$

Stratified group action I

The action of $GL(V)$ on Ω_d is stratified in the following sense.

Definition

Let $X = X_1 \times \cdots \times X_m$ be a set and suppose that a group G acts on X. The action of G on X is **stratified** (with respect to the decomposition $X_1 \times \cdots \times X_m$) if:

(i) for every $1 \leq i \leq m$ the action of G on X induces an action on $X_i \times \cdots \times X_m$, and

(ii) for every $1 \leq i \leq m$ and every $(x_i, \ldots, x_m) \in X_i \times \cdots \times X_m$ the stabilizer $G_{(x_i,\ldots,x_m)}$ induces an action on $X_1 \times \cdots \times X_{i-1} \times (x_i, \ldots, x_m)$.

Stratified group action II

Theorem

If the action of a group G on $X = X_1 \times \cdots \times X_m$ is stratified, then X/G consists of all tuples $(x_1, \ldots, x_m)$, where

$$
\begin{aligned}
&x_m \in X_m/G,\\
&x_{m-1} \in (X_{m-1} \times x_m)/G_{x_m},\\
&\ldots\\
&x_1 \in (X_1 \times (x_2, \ldots, x_m))/G_{(x_2,\ldots,x_m)}.
\end{aligned}
$$

Outline of the algorithm

- for $d \leq 6$ it takes a few seconds
- for $d = 7$ and, mainly $d = 8$, we can use existing classifications of trilinear alternating forms (which we independently verified in a matter of days)
- there are many code loops in $d = 8$ because some of the stabilizers G_A are very small
- we use permutation representation for the affine action on $\mathbb{F}_2^{\binom{d}{2}} \times A$; each generator takes a few hours to process with $d = 8$, $\binom{d}{2} = 28$.
- the action on $\mathbb{F}_2^{\binom{d}{1}} \times C \times A$ has to be run for many pairs $C \times A$.

Enumeration of code loops

g_n = groups of order n
m_n = Moufang loops of order n
ℓ_n = code loops of order n

d	0	1	2	3	4	5	6	7	8
n	2	4	8	16	32	64	128	256	512
g_n	1	2	5	14	51	267	2328	56092	10494213

Enumeration of code loops

g_n = groups of order n
m_n = Moufang loops of order n
ℓ_n = code loops of order n

d	0	1	2	3	4	5	6	7	8
n	2	4	8	16	32	64	128	256	512
g_n	1	2	5	14	51	267	2328	56092	10494213
m_n	1	2	5	19	122	4529	?	?	?

Enumeration of code loops

g_n = groups of order n
m_n = Moufang loops of order n
ℓ_n = code loops of order n

d	0	1	2	3	4	5	6	7	8
n	2	4	8	16	32	64	128	256	512
g_n	1	2	5	14	51	267	2328	56092	10494213
m_n	1	2	5	19	122	4529	?	?	?
ℓ_n	1	2	4	10	23	88			

Enumeration of code loops

g_n = groups of order n
m_n = Moufang loops of order n
ℓ_n = code loops of order n

d	0	1	2	3	4	5	6	7	8
n	2	4	8	16	32	64	128	256	512
g_n	1	2	5	14	51	267	2328	56092	10494213
m_n	1	2	5	19	122	4529	?	?	?
ℓ_n	1	2	4	10	23	88	767	80826	937791557